

УДК 621.316.925(075.8)

Преднамеренные электромагнитные деструктивные воздействия — угроза национальной безопасности страны

ISSN 1812-5220
© Проблемы анализа риска, 2016

В. И. Гуревич,
Центральная лаборатория
Электрической компании
Израиля

Аннотация

Проблема преднамеренных электромагнитных деструктивных воздействий (ПЭДВ) на электроэнергетические системы становится в последнее время все более актуальной в связи с двумя современными тенденциями: расширяющимся применением микроэлектроники и микропроцессорной техники в электроэнергетике, с одной стороны, и интенсивными разработками средств дистанционного поражения электронной аппаратуры — с другой. Наиболее мощным и разрушительным средством поражения электронной аппаратуры является электромагнитный импульс высотного ядерного взрыва (ЭМИ ЯВ). История экспериментальных высотных ядерных взрывов насчитывает уже полвека. За это время были опубликованы на английском языке многие десятки научных работ, детально описывающих это явление и меры защиты от него. Однако все эти материалы остались неизвестными российским специалистам-энергетикам, и поэтому редкие публикации на эту тему вызывают лишь шквал отрицательных эмоций и негодования. Такое отношение к проблеме и ее полное игнорирование угрожают национальной безопасности страны и должны быть в корне изменены.

Ключевые слова: преднамеренные электромагнитные деструктивные воздействия, ПЭДВ, высотный ядерный взрыв, электромагнитный импульс, ЭМИ ЯВ.

Содержание

Введение

1. Как решается проблема ПЭДВ в США
2. Положение дел в России

Заключение

Литература

От редакции

Проблеме преднамеренных электромагнитных деструктивных воздействий (ПЭДВ) на электронную аппаратуру уже 20—30 лет уделяется большое внимание как в отечественной, так и зарубежной литературе. Так, еще в 2006 г. В.Е. Фортов — президент РАН — опубликовал интервью на эту тему. Такой многолетний интерес вызван тем, что есть и техногенная проблема, и техногенные риски. Внимание к этой проблематике в последние годы усиливается вследствие возможных преднамеренных террористических актов. Наш журнал тоже уделяет этой проблеме достойное внимание как одной из разновидностей многослойной системы оценки и анализа различных рисков. Хотя эта статья и публикуется в разделе «Дискуссионный клуб», что в определенной степени обусловлено полемическим характером ее заключительной части, это не умаляет заслуженного, во многом пионерского, вклада ее автора — к.т.н. В.И. Гуревича в разработку, развитие и популяризацию ПЭДВ. Редакция также надеется на дальнейшие публикации по оценке этого вида рисков.

Введение

...Наша уязвимость увеличивается ежедневно вместе с расширением нашего использования электроники и ростом нашей зависимости от нее в наших гражданских и в военных секторах.

Д-р Вильям Грэхем,
Председатель Комиссии Конгресса
США по ЭМИ ЯВ

Проблема преднамеренных электромагнитных деструктивных воздействий (ПЭДВ) на электронную аппаратуру стала актуальной уже через несколько лет после проведения США в 1946 г. на атолле Бикини (Маршалловы острова) испытательных ядерных взрывов под шифром «Операция Кроссоудс». В ходе этих испытательных взрывов было обнаружено новое физическое явление — возникновение мощного импульса электромагнитного излучения, охватывающего обширную зону, к которому сразу же был проявлен повышенный интерес со стороны военных. С целью изучения этого явления в период с 1958 по 1962 г. последовала целая серия высотных (40—450 км) ядерных взрывов различной мощности, произведенных США и Советским Союзом. Было установлено поражающее действие

электромагнитного импульса высотного ядерного взрыва (ЭМИ ЯВ) на электронную аппаратуру, системы связи, радиостанции и радары, энергосистемы на расстоянии в тысячи километров от эпицентра взрыва (рис. 1).

Примерно с 80-х годов прошлого века в ряде стран начали усиленно работать над созданием так называемого супер-ЭМИ — ядерного заряда, в котором эффект ЭМИ многократно усилен по сравнению с обычным ядерным зарядом. Параллельно во многих странах велись работы по созданию сверхмощных направленных источников ЭМИ неядерного типа, а также электромагнитных бомб, боеголовок ракет, гранат и других боеприпасов, являющихся неядерными источниками ЭМИ, предназначенными для поражения электронных устройств важнейших систем инфраструктуры, в первую очередь систем связи, водо- и электроснабжения. В последнее время на рынке в свободной продаже появились мощные компактные источники ЭМИ, представляющие опасность уже не как средства ведения боевых действий противоборствующими сторонами, а как инструменты криминальных и террористических структур.

Применение специального оружия, способного разрушить систему электроснабжения и другие

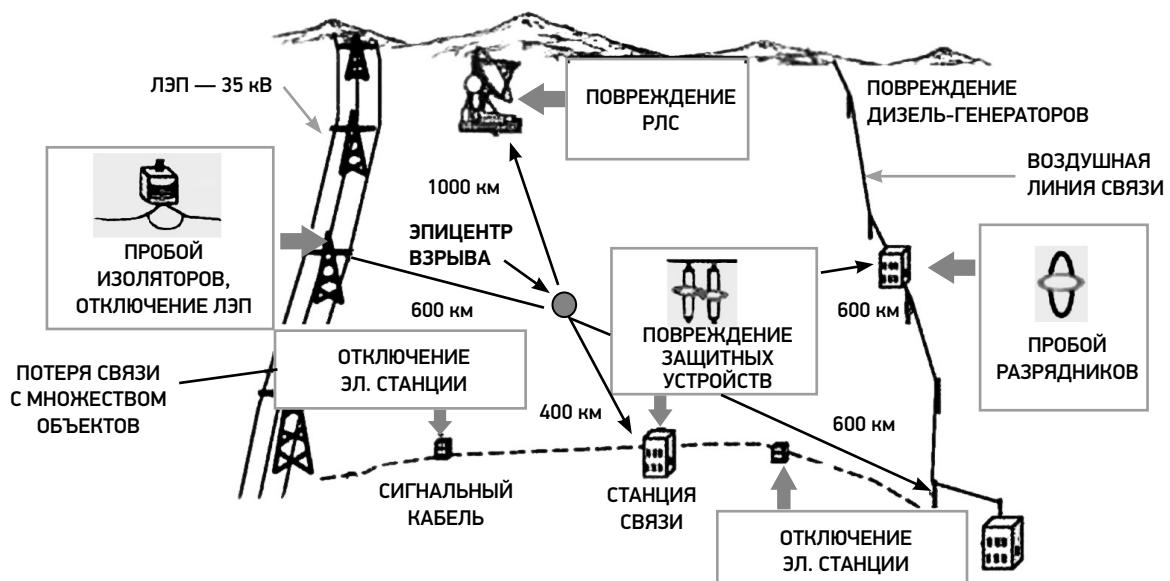


Рис. 1. Повреждения оборудования, подвергшегося воздействию высотного ЭМИ ЯВ над Казахстаном в 1962 г. Впервые рисунок был представлен на английском языке начальником ЦНИИ-12, генерал-майором, д.т.н., профессором В.М. Лоборевым на международной конференции EUROEM во Франции в 1994 г. [1]

важнейшие элементы национальной инфраструктуры, не воздействуя напрямую на человека, является весьма заманчивым, поскольку может привести к коллапсу целой страны, при том что лица, ответственных за принятие решения о применении такого оружия, никто не сможет осудить за массовое убийство гражданского населения, поскольку это оружие не имеет прямого воздействия на людей.

Проблема преднамеренных электромагнитных деструктивных воздействий (ПЭДВ) на электроэнергетические системы становится в последнее время все более актуальной в связи с тремя современными тенденциями:

- расширяющимся применением микроэлектроники и микропроцессорной техники в электроэнергетике;



Рис. 2. Источник направленного сверхвысокочастотного излучения, смонтированный в пикапе на базе легковушки с пластмассовым кунгом



Рис. 3. Походный разрушитель электроники под названием 2100 Series Suitcase на основе генератора Маркса, производимый компанией Applied Physical Electronics

- возрастанием уязвимости самой микропроцессорной техники к внешним электромагнитным воздействиям вследствие постоянного увеличения плотности микроэлементов в объеме кристалла, уменьшения изоляционных слоев в кристалле, снижения рабочих напряжений (со стандартных 5 до 1,5 В в некоторых новых микросхемах), увеличения производительности и рабочей частоты микропроцессоров, расширения применения внутренней памяти в микросхемах различного назначения, перехода от магнитных накопителей информации к флэш-памяти и т.д.;

- интенсивными разработками средств дистанционного поражения электронной аппаратуры, ведущимися во многих странах, и прогрессом, достигнутым в этой области.

Последние разработки в области неядерных средств ПЭДВ — это американская система СНАМР, разработанная компанией Raytheon и установленная в боеголовке крылатой ракеты Boeing. Эта система представляет собой сверхмощный источник направленного микроволнового излучения, дистанционно поражающего электронные системы, расположенные по траектории полета крылатой ракеты. А также российская ракета «Алабуга» с электромагнитной боевой частью, способной произвести одиночный электромагнитный импульс, поражающий электронные системы в радиусе до 3 км.

Особое место занимают компактные системы ПЭДВ, которые могут быть расположены в автомобилях (рис. 2) и даже в небольших чемоданчиках (рис. 3). Такие компактные системы ПЭДВ являются весьма привлекательными средствами поражения местных систем электроснабжения террористическими организациями, и их практическое использование — лишь вопрос времени.

Проблема ПЭДВ касается не только такой сугубо гражданской отрасли, как электроэнергетика, но и военных, поскольку военные базы и полигоны получают электроэнергию и воду от гражданских систем и серьезные сбои в функционировании этих систем неминуемо скажутся на боеготовности армии со всеми ее системами вооружения, защищенными от ПЭДВ. На восстановление электроснабжения обширных регионов страны с разрушенными ЭМИ яв компьютеризированными системами управления, контроля, связи, релейной защиты (не говоря уже

о повреждениях силовых трансформаторов [2]) могут потребоваться месяцы. Современные системы резервного электроснабжения на основе дизель-генераторов — не решение проблемы, поскольку они предназначены для поддержания электроснабжения лишь отдельных относительно небольших объектов в течение нескольких часов и к тому же они имеют такие же незащищенные микропроцессорные системы управления режимом работы, как и все другие системы в электроэнергетике.

1. Как решается проблема ПЭДВ в США

Проблема не в технологиях. Мы знаем, как защититься от этого.

Проблема не в деньгах, это стоит не так уж дорого.

Проблема в политике.

Как всегда, появляется политика, которая мешает делу.

Д-р Питер Винсент Прай,
Task Force on National
and Homeland Security

Проблема ПЭДВ известна уже более 50 лет, в связи с чем возникает естественный вопрос о том, почему же до настоящего времени она не решена. Может быть эта проблема вообще не имеет решения?

Рассмотрим, как обстоят дела в мире с защитой от ПЭДВ (и в первую очередь от ЭМИ ЯВ) на примере двух ведущих мировых держав: США и России.

В США различными аспектами проблемы ПЭДВ занимаются десятки организаций, не считая университетов:

- Metatech Corp.
- Department of Homeland Security (DHS)
- EMP Commission of Congress
- North American Electric Reliability Corp. (NERC)
 - Department of Energy
 - Department of Defense (DoD)
 - Critical Infrastructure Partnership Advisory Council (CIPAC)
 - Electric Infrastructure Security Council (EIS)
 - Defense Science Board (DSB)
 - US Strategic Command (USSTRATCOM)
 - Defense Threat Reduction Agency (DTRA)
 - Defense Logistics Agency (DLA)
 - Air Force Weapons Laboratory

- FBI
- Sandia National Laboratories
- Lawrence Livermore National Laboratory (LINL)
- Oak Ridge National Laboratory
- Idaho National Laboratories
- Los Alamos National Laboratories
- Martin Marietta Energy Systems, Inc.
- National Security Telecommunications Advisory Committee
 - Federal Emergency Management Agency (FEMA)
 - National Academy of Science
 - Task Force on National and Homeland Security
 - EMPrimus
 - EMAG Associates
 - Neighborhood of Alternative Homes (NOAH)
 - EMPact America
 - Federal Energy Regulatory Commission (FERC)
 - Electric Power Research Institute (EPRI)
 - NASA
 - US Northern Command (NORTHCOM)
 - SHIELD Act
 - EMP Grid
 - EMP Technology Holding
 - Strategic National Risk Assessment (SNRA)
 - Walpole Fire Department

Большая часть отчетов этих организаций по этой теме является открытой или была рассекречена в последнее время и выложена в свободном доступе в Интернете. Особый интерес представляют собой очень подробные многостраничные отчеты об исследованиях проблемы, выполненные в Metatech Corp., Oak Ridge National Laboratory и др.

Международная электротехническая комиссия (МЭК), являющаяся законодателем мод в области электротехники и электроники, выпустила свыше 20 стандартов, посвященных различным аспектам проблемы ПЭДВ, и в частности ЭМИ ЯВ:

1. IEC TR 61000-1-3 Electromagnetic compatibility (EMC) — Part 1-3: General—The effects of high-altitude EMP (HEMP) on civil equipment and systems.
2. IEC 61000-1-5 High power electromagnetic (HPEM) effects on civil systems.
3. IEC 61000-2-9 Electromagnetic compatibility (EMC)—Part 2: Environment—Section 9: Description of HEMP environment—Radiated disturbance. Basic EMC publication.

4. IEC 61000-2-10 Electromagnetic compatibility (EMC)—Part 2-10: Environment—Description of HEMP environment—Conducted disturbance.

5. IEC 61000-2-11 Electromagnetic compatibility (EMC)—Part 2-11: Environment—Classification of HEMP environments.

6. IEC 61000-2-13 Electromagnetic compatibility (EMC)—Part 2-13: Environment—High-power electromagnetic (HPEM) environments—Radiated and conducted.

7. IEC 61000-4-23 Electromagnetic compatibility (EMC) — Part 4-23: Testing and measurement techniques — Test methods for protective devices for HEMP and other radiated disturbances.

8. IEC 61000-4-24 Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques — Section 24: Test methods for protective devices for HEMP conducted disturbance — Basic EMC Publication.

9. IEC 61000-4-25 Electromagnetic compatibility (EMC) — Part 4-25: Testing and measurement techniques — HEMP immunity test methods for equipment and systems.

10. IEC 61000-4-32 Electromagnetic compatibility (EMC) — Part 4-32: Testing and measurement techniques — High-altitude electromagnetic pulse (HEMP) simulator compendium.

11. IEC 61000-4-33 Electromagnetic compatibility (EMC) — Part 4-33: Testing and measurement techniques — Measurement methods for high-power transient parameters.

12. IEC 61000-4-35 Electromagnetic compatibility (EMC) — Part 4-35: Testing and measurement techniques — HPEM simulator compendium.

13. IEC 61000-4-36 Electromagnetic compatibility (EMC) — Testing and measurement techniques — IEMI Immunity Test Methods for Equipment and Systems.

14. IEC/TR 61000-5-3 Electromagnetic compatibility (EMC)—Part 5-3: Installation and mitigation guidelines—HEMP protection concepts.

15. IEC/TS 61000-5-4 Electromagnetic compatibility (EMC)—Part 5: Installation and mitigation guidelines—Section 4: Immunity to HEMP—Specifications for protective devices against HEMP radiated disturbance. Basic EMC Publication.

16. IEC 61000-5-5 Electromagnetic compatibility (EMC)—Part 5: Installation and mitigation guide-

lines—Section 5: Specification of protective devices for HEMP conducted disturbance. Basic EMC Publication.

17. IEC 61000-5-6 Electromagnetic compatibility (EMC) — Part 5-6: Installation and mitigation guidelines — Mitigation of external EM influences.

18. IEC 61000-5-7 Electromagnetic compatibility (EMC) — Part 5-7: Installation and mitigation guidelines — Degrees of protection provided by enclosures against electromagnetic disturbances (EM code).

19. IEC 61000-5-8 Electromagnetic compatibility (EMC) — Part 5-8: Installation and mitigation guidelines — HEMP protection methods for the distributed infrastructure.

20. IEC 61000-5-9 Electromagnetic compatibility (EMC) — Part 5-9: Installation and mitigation guidelines — System-level susceptibility assessments for HEMP and HPEM.

21. IEC 61000-4-36 Electromagnetic compatibility (EMC) — Testing and measurement techniques — IEMI Immunity Test Methods for Equipment and Systems.

Некоторые из стандартов еще находятся в стадии разработки.

Свой стандарт предлагает и американская ассоциация инженеров-электриков IEEE — IEEE P1642 Recommended Practice for Protecting Public Accessible Computer Systems from Intentional EMI.

Аналогичный документ разработала и Европейская Комиссия — Topic SEC-2011.2.2-2 Protection of Critical Infrastructure (structures, platforms and networks) against Electromagnetic (High Power Microwave (HPM)) Attacks.

В СИГРЭ создана отдельная рабочая группа по этой теме — CIGRE WG C4.206 Protection of the High Voltage Power Network Control Electronics against IEMI.

Много стандартов выпущено Министерством обороны США и НАТО:

1. MIL-STD-2169B High — Altitude Electromagnetic Pulse (HEMP) Environmental, 2012.

2. MIL-STD-188-125-1 High — Altitude Electromagnetic Pulse (HEMP) Protection for Ground Based C41 Facilities Performing Critical. Time-Urgent Mission. Part 1 Fixed Facilities, 2005.

3. MIL-STD-188-125-2 High — Altitude Electromagnetic Pulse (HEMP) Protection for Ground Based C41 Facilities Performing Critical. Time-Urgent Mission. Part 2 Transportable Systems, 1999.

4. MIL-STD-461F Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, 2007.

5. MIL-STD-464C Electromagnetic Environmental Effects. Requirements for Systems, 2010. — Test Operations Procedure Report No. 01-2-620 High-Altitude Electromagnetic Pulse (HEMP) Testing.

6. MIL-STD-1377 Effectiveness of Cable, Connector, and Weapon Enclosure Shielding and Filters in Precluding Hazards of Electromagnetic Radiation to Ordnance (HERO), 1971.

7. MIL-HDBK-240 Hazards of Electromagnetic Radiation to Ordnance (HERO) Test Guide, 2002.

8. NATO AECTP-500 Ed. 4. Electromagnetic Environmental Effects Test and Verification, 2011.

9. NATO AECTP-250 Ed. 2 — Electrical and Electromagnetic Environmental Conditions, 2011.

Следует признать, что, несмотря на обилие организаций, занимающихся вопросами ПЭДВ в США, и наличие огромного объема технической документации, реальные успехи в области защиты объектов электроэнергетики в США весьма незначительны (речь идет о нескольких подстанциях, снабженных средствами защиты от ПЭДВ). На вопрос автора Генеральному директору Electric Infrastructure Security Council (EIS) господину Avi Schnurr на одной из конференций по этой тематике о причинах такого положения дел его ответ был таков, что гражданский персонал энергосистем еще не в полной мере осознал актуальность темы и необходимость инвестиций в защиту энергообъектов от ПЭДВ. На самом деле проблема имеет, конечно, более глубокие корни, рассмотренные автором в [3]. Тем не менее, несмотря на отсутствие заметного прогресса в деле реальной защиты энергообъектов, следует признать несомненные успехи США в области информированности гражданских специалистов-энергетиков о проблеме и путях ее решения, доступность информационных ресурсов, огромный объем работ в области стандартизации и исследований. Кроме того, на Западе, и в США в частности, уже существует обширный рынок средств защиты энергообъектов от ПЭДВ, производимых десятками компаний.

Вся эта предварительная работа заняла десятки лет, но именно она позволила создать необходимые предпосылки для начала практических работ по защите энергообъектов от ПЭДВ.

2. Положение дел в России

Вы можете дурачить всех людей некоторое время; можете даже все время дурачить некоторых людей; но вам никогда не удастся дурачить всех людей все время.

Абраам Линкольн

В России опубликовано в открытом доступе лишь несколько официальных документов в этой области:

- ГОСТ Р 53111-2008. Устойчивость функционирования сети связи общего пользования;
- РД 45.083-99. Рекомендации по обеспечению стойкости аппаратурных комплексов объектов проводной электросвязи к воздействию дестабилизирующих факторов;
- ГОСТ Р 52863-2007. Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования.

Первые два документа относятся лишь к узкой области техники — системам связи — и основаны на требованиях обычных, а не специальных стандартов по электромагнитной совместимости (ЭМС). Последний документ предназначен для более широкого применения, но также основан на требованиях общих стандартов по ЭМС. Все специальные требования (а это как раз требования по ПЭДВ) обозначены в этом стандарте значком «Х» без указания технических параметров, что представляется несколько странным, учитывая название стандарта.

Имеются, естественно, и непубликуемые в открытом доступе материалы, например: «Нормы по стойкости аппаратуры, приборов, устройств и оборудования ЕСС РФ к воздействию ИИ и ЭМИ ЯВ» — Решение ГКЭС при Минсвязи России № 143 от 31.01.1996, а также и закрытые (в отличие от западных) военные стандарты. Правда, и этот материал имеет весьма узкую область применения, но само по себе его наличие указывает на определенную озабоченность специалистов проблемой ПЭДВ. Хотя, как можно видеть из приведенного выше перечня стандартов, нормы стойкости и методы испытания аппаратуры к воздействию ЭМИ ЯВ уже давно не являются секретными и публикуются на Западе в открытом доступе, причем как

стандарты МЭК общего пользования, так и военные (за очень редким исключением, например MIL-STD-2169B). Вряд ли можно признать логичной и оправданной политику России в области чисто технической проблемы, в результате которой большинство российских специалистов во многих областях гражданской техники (например, в области электроэнергетики), так или иначе связанных с проблемами ПЭДВ, не имеют о них ни малейшего представления.

Имеются в России и специализированные испытательные центры, которые снабжены всем необходимым для проверки устойчивости оборудования к воздействию ЭМИ ЯВ:

- комплекс «Аллюр» ФГУП ВЭИ им. Ленина в г. Истре Московской обл.;
- испытательный центр ФГУ «12 ЦНИИ МО РФ» в Сергиевом Посаде;
- испытательный комплекс «26 Центрально-го научно-исследовательского института» МО РФ в Санкт-Петербурге.

Но кто из гражданских специалистов в области электроэнергетики России знает о существовании этих центров? Опять все та же проблема — полное отсутствие информации по этой актуальной теме для гражданских специалистов.

Фактически единственным автором, пишущим о проблемах ПЭДВ в электроэнергетике России, был и остается до сих пор автор данной статьи (конечно, если не принимать во внимание многочисленных плагиаторов). Первая его статья на эту тему была опубликована 11 лет тому назад на русском и на английском языках [4, 5], но осталась незамеченной в России (в отличие от статьи, опубликованной на английском языке). Но зато другая статья автора, в которой была затронута проблема уязвимости микропроцессорных реле защиты к ПЭДВ, опубликованная в шестом номере журнала «Новости электротехники» за 2005 г. [6], вызвала шквал эмоций у специалистов-энергетиков, поскольку посягнула на коммерческие интересы производителей микропроцессорных реле защиты в России. Вот лишь несколько цитат из отзывов ведущих российских специалистов, опубликованных в следующем номере того же журнала:

- «Утверждение о возможности преднамеренных дистанционных воздействий на микропро-

цессорную релейную защиту с целью нарушения ее нормальной работы кажется надуманным», — Э. Палей, помощник Генерального директора ОАО «ПО ЭЛТЕХНИКА», А. Лисицын, директор департамента противоаварийной автоматики, систем управления и релейной защиты НТЦ ЕЭС;

• «Применение устройств с микропроцессорными технологиями не изменяет доступность оборудования терроризму, в том числе и “электронному”», — Н. Дони, Первый заместитель Генерального директора ООО НПП «ЭКРА»;

• «Воздвигать барьеры на пути внедрения микропроцессорной техники в энергетику и пытаться затормозить технический прогресс в России — занятие вредное и абсолютно бесперспективное», — Г. Нудельман, Председатель Совета директоров ОАО «ВНИИР».

После обвинения автора в «попытке затормозить технический прогресс в России» уже не остается ничего другого, как объявить его иностранным шпионом и врагом народа.

Естественно, что при таком подходе к проблеме ведущих специалистов-энергетиков России о каком информировании технической общественности России можно говорить? «Держать и не пуштать» — вот их главная цель! Именно такой подход и был использован этими деятелями в дальнейшем по отношению к последующим статьям автора. Например, по настоянию одного из них дважды снимались с публикации в последний момент уже сверстанные и вычитанные статьи по этой теме в журнале «Электроэнергия. Передача и распределение». А в отзыве того же деятеля на статью автора: «Пришло время трезво оценить ситуацию», опубликованную в 3 номере за 2014 г. газеты «Энергетика и промышленность России», он назвал призывы автора обратить внимание специалистов на проблемы ПЭДВ в электроэнергетике страшилками, а сам отзыв опубликовал под названием: «Надежней всего жить в пещере у костра», весьма красноречиво отражающим позицию российских специалистов, не знающих о проблеме и не желающих о ней ничего знать!

Единственными, кто по достоинству оценил публикации автора на эту тему, были многочисленные плагиаторы, которые, не стесняясь, заимствовали идеи, изложенные в публикациях автора, а часто

и просто полностью копировали целые разделы из разных статей автора, компоновали их в виде отдельной статьи и публиковали под своим именем.

Заключение

Используя название упомянутой выше статьи «Пришло время трезво оценить ситуацию» в качестве призыва, автор обращается к руководителям отрасли с предложением отбросить наконец личные амбиции и начать серьезно работать над решением проблемы. В США процесс осмысления и выработки теоретических основ решения проблемы занял несколько десятилетий. Но России нет смысла в точности повторять пройденный США путь, поскольку на сегодняшний день теоретические основы решений проблемы уже заложены. Необходимо лишь взять то, что уже наработано, серьезно проанализировать, доработать, если необходимо, и начать готовить электроэнергетику к реально существующим рискам. Первыми помощниками в этом деле для российских специалистов могут стать книги автора: «Уязвимости микропроцессорных реле защиты: проблемы и решения» [7] и «Защита оборудования подстанций от электромагнитного импульса» [8].

Литература

1. Loborev V.M. Up to date state of the NEMP problems and topical research directions, in Euro Electromagnetic Conf. (EUROEM), Bordeaux, France. June 1994. P. 15—21.
2. Гуревич В.И. Проблема защиты силового электрооборудования энергосистем от магнитогидродинамического эффекта электромагнитного импульса // Энергоэксперт. 2015. № 6. С. 40—45.
3. Гуревич В.И. Электромагнитный Армагеддон? // Альтернативная энергетика и экология. 2015. № 13—14. С. 113—121.
4. Gurevich V. The Hazards of Electromagnetic Terrorism. // Public Utilities Fortnightly. June 2005. P. 84—86.
5. Гуревич В.И. Электромагнитный терроризм — новая реальность 21 века // Мир техники и технологий. 2005. № 12. С. 14—15.
6. Гуревич В.И. Микропроцессорные реле защиты: новые перспективы или новые проблемы? // Новости электротехники. 2005. № 6 (36). С. 57—60.
7. Гуревич В.И. Уязвимости микропроцессорных реле защиты: проблемы и решения. М.: Инфра-Инженерия, 2014. 256 с.
8. Гуревич В.И. Защита оборудования подстанций от электромагнитного импульса. М.: Инфра-Инженерия, 2016. 302 с.

Сведения об авторе

Гуревич Владимир Игоревич: кандидат технических наук, почетный профессор, ведущий специалист Центральной лаборатории Электрической компании Израиля
Количество публикаций: 13 книг, свыше 200 статей, свыше 120 авторских свидетельств и патентов

Область научных интересов: преднамеренные электромагнитные деструктивные воздействия (ПЭДВ) на электроэнергетические системы, средства и методы защиты от них, электрические реле и релейная защита, проблемы микропроцессорных устройств релейной защиты
Контактная информация:

Адрес: Central Electric Laboratory, Israel Electric Corp.,
POB 10, Haifa 31000, Israel
Тел.: +7 076-863-72-93
E-mail: gurevich@iec.co.il