ПОВЫШЕНИЕ УСТОЙЧИВОСТИ ЭНЕРГОСИСТЕМ К ПРЕДНАМЕРЕННЫМ ЭЛЕКТРОМАГНИТНЫМ ДЕСТРУКТИВНЫМ ВОЗДЕЙСТВИЯМ – АКТУАЛЬНАЯ ЗАДАЧА СОВРЕМЕННОСТИ

ГУРЕВИЧ В.И., К.Т.Н.

Проблема преднамеренных электромагнитных деструктивных воздействий (ПЭДВ) на электронную аппаратуру военного назначения стала актуальной уже через несколько лет после проведения США в 1946 г. на атолле Бикини (Маршалловы острова) испытательных ядерных взрывов под шифром «Операция Кроссроудс». Тенденции и темпы развития современных технических средств дистанционного поражения электронной аппаратуры обуславливают необходимость незамедлительного начала конкретных работ по защите энергосистем от ПЭДВ.

В ходе испытательных ядерных взрывов на атолле Бикини 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 гг. последовала целая серия высотных (40–450 км) ядерных взрывов различной мощности, произведенных США и Советским Союзом. Было установлено поражающее действие электромагнитного импульса ядерного взрыва (ЭМИ ЯВ) на электронную аппаратуру, системы связи, радиостанции и радары, энергосистемы на расстоянии в тысячи километров от эпицентра взрыва. В то время вся информация об этом явлении была строго засекречена. В последствие стало известно, что 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.

По мере расширения работ в этой области, информация о них начала проникать в открытую печать и стала достоянием общественности [1–4]. В странах СНГ первыми публикациями по теме ПЭДВ в электроэнергетике, в частности, в релейной защите, были статьи автора [5–7]. Первая в России книга, обобщающая информацию в этой области, также принадлежит перу автора [8].

Сегодня серьезность проблемы ПЭДВ в электроэнергетике признана на официальном уровне во всем мире, кроме стран на постсоветском пространстве, включая Россию. В США, например, создана специальная комиссия при Конгрессе, несколько крупнейших государственных организаций занимаются решением этой проблемы, множество частных компаний предлагают консультационные услуги в этой области, занимаются тестированием оборудования и производством средств защиты.

ПУТИ РЕШЕНИЯ ПРОБЛЕМЫ

Может ли быть решена эта проблема? Безусловно, да! За примером решения проблемы ходить далеко не надо: вся ответственная военная электронная аппаратура защищена от воздействия ПЭДВ. Но, к сожалению, гражданская инфраструктура не может строиться на принципах военного строительства по всем понятным экономическим причинам. Так что же делать? Анализ ситуации показывает, что проблема защиты энергосистемы страны – комплексная и не может быть решена лишь силами энергетиков. По нашему мнению, в стране должна быть создана Национальная программа, направленная на повышение живучести энергосистемы, включающая множество участников: кроме самих энергетиков в ней должны принять участие разработчики и производители электронной аппаратуры для электроэнергетики, испытательные и сертификационные центры, проектировщики,

организации, занимающие стандартизацией. С чего же начать, и что должна включать в себя эта Программа?

В ОБЛАСТИ ЭЛЕКТРОЭНЕРГЕТИКИ

Работа должна начинаться с выбора наиболее важных объектов энергосистемы, требующих защиты в первую очередь: узловых подстанций, наиболее важных электростанций.

На выбранных объектах должны быть определены критические виды оборудования, которые, с одной стороны, наиболее подвержены воздействию ПЭДВ, а с другой, без которых невозможно функционирование данного объекта электроэнергетики. Например, на подстанциях к таким критическим видам оборудования можно отнести микропроцессорные устройства релейной защиты (МУРЗ), зарядно-подзарядные агрегаты систем оперативного постоянного тока (СОПТ), частично системы АСУ ТП (в той их части, которая связана с осуществлением дистанционного управления положением выключателей).

Непосредственно на выбранных объектах для критических видов оборудования должны быть обеспечены резервные комплекты этого оборудования с изъятыми из них электронными модулями и печатными платами, содержащими чувствительные электронные компоненты. Эти модули и печатные платы должны храниться в специальных закрытых стальных контейнерах, обеспечивающих защиту таких высокочувствительных компонентов, как элементы памяти и микропроцессоры от повреждения высокочастотными электромагнитными полями высокой напряженности. Ограничиваться хранением лишь комплекта запасных электронных модулей не достаточно, так как в работающем под напряжением электрооборудовании (например, в зарядно-подзарядном агрегате, рис. 1) при воздействии ПЭДВ с большой вероятностью будут повреждены не только высокочувствительные электронные компоненты, но и такие узлы, как силовой трансформатор, конденсаторы фильтров, внутренние жгуты проводов и кабелей, автоматические выключатели и т.п. В то время как, в отключенном зарядно-подзарядном агрегате с изъятыми из него электронными модулями и платами, вышеперечисленные элементы останутся неповрежденными.

Программируемые модули МУРЗ, хранящиеся отдельно, должны быть заранее запрограммированы, конфигурированы, помечены и подготовлены для установки в конкретные МУРЗ.

Критические виды электронного оборудования (например, такие как МУРЗ) должны быть установлены в металлических шкафах, защищенных от проникновения высокочастотного электромагнитного излучения. Должна быть проведена ревизия конструкции таких шкафов. Если окажется, что они содержат стеклянные окна или двери, рис. 2, открытые жалюзи, вырезы, то такие шкафы потребуют модернизации, например, нанесения специального отражающего покрытия на стеклянные окна и двери, заполнение вентиляционных жалюзей специальной металлической вставкой, напоминающей мочалку из стальных нитей.

Если критические виды электронного оборудования установлены на открытых панелях, то они требуют защиты стальным коробом со стороны монтажа. Лицевая поверхность таких панелей может быть защищена шторами из специальной металлизированной ткани.

Окна в помещениях с установленными критическими видами электронного оборудования должны быть закрыты и покрыты специальным прозрачным отражающим покрытием. Двери должны быть металлическими. Само помещение должно быть железобетонным. В крайнем случае, его стены, потолки и пол должны быть окрашены специальной полупроводящей краской, отражающей высокочастотное электромагнитное излучение. Такие краски выпускаются промышленностью. Возможно применение специальных защитных штор и ковров с металлическими нитями, также имеющихся на рынке.

Во внешних электрических цепях, к которым подключены критические объекты (включая цепи питания, входные и выходные цепи), должны быть установлены в достаточно большом количестве мощные промышленные варисторы, выпускаемые в одно- и трехфазном исполнении в корпусах, предназначенных для установки на стандартную DIN-рейку, и снабженные предохранителями и индикаторами состояния этих предохранителей, рис. 3. Чем большее количество цепей будет защищено варисторами,

Рис. 1. Устройство зарядно-подзарядного агрегата типа SCR45A60V

Рис. 2. Микропроцессорные устройства релейной защиты, смонтированные в шкафах со стеклянными дверями

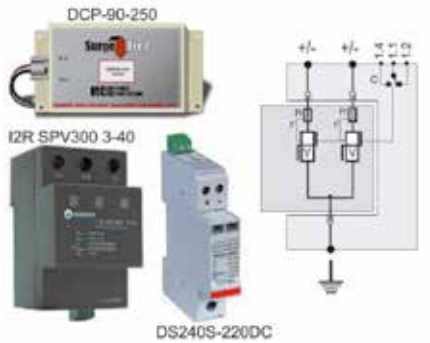

Рис. 3. Различные типы мощных промышленных варисторов, предназначенных для защиты электрических сетей оперативного питания переменного и постоянного тока

тем меньше вероятность повреждения этих цепей и электронного оборудования, включенного в эти цепи.

Контрольные кабели в цепях критических видов аппаратуры, не имеющие экранов, должны быть заменены на экранированные. При этом следует учитывать, что существует множество типов кабельных экранов и далеко не все они подходят для защиты от ПЭДВ. Экраны кабелей должны быть обязательно заземлены с двух сторон. Если имеет место индуцированная наводка переменного тока промышленной частоты в экране от протекающего по кабелю переменного тока, заземление одного из концов экрана осуществляют через конденсатор.

Контрольные кабели, подключенные к критическим видам оборудования, должны быть снабжены фильтрами, подавляющими наведенный в кабеле высокочастотный сигнал. Такие фильтры, специально предназначенные для защиты от ПЭДВ, широко представлены сегодня на рынке. Простейшим вариантом высокочастотного фильтра являются ферритовые кольца (цилиндры), укрепленные непосредственно на контрольных кабелях (но не на экранах, разумеется!). Это дешевые и доступные элементы, которые должны широко использоваться вне зависимости от использования других средств защиты.

Более подробно перечисленные выше средства защиты от ПЭДВ описаны в [8].

Совершенно очевидно, что все описанные выше мероприятия в полном объеме могут быть реализованы лишь на вновь строящихся объектах электроэнергетики. Однако среди этих мероприятий имеется достаточно простых и не очень дорогих технических решений, которые с успехом могут быть реализованы и на существующих объектах электроэнергетики.

В ОБЛАСТИ СТАНДАРТИЗАЦИИ

Отсутствие стандартизации в области микропроцессорной релейной защиты (как в области конструкций МУРЗ, так и в области программного обеспечения) – серьезная проблема, существенно затрудняющая организацию мероприятий по защите объектов электроэнергетики от ПЭДВ [9]. Полная несовместимость модулей МУРЗ различных производителей, и даже различных моделей одного и того же производителя, требуют значительных затрат на приобретение и хранение комплектов запасных модулей отдельно для каждого типа МУРЗ. Несовместимость программного обеспечения существенно затруднит и замедлит время проверки исправности модулей и восстановления функционирования релейной защиты.

Рис. 4. Компактные стенды для испытания электронной аппаратуры на устойчивость к воздействию ЭМИ ЯВ, производимые различными компаниями

Учитывая, что отсутствие стандартов в области МУРЗ обуславливает значительный ущерб также и в нормальных режимах эксплуатации релейной защиты [9], задача скорейшего проведения работ по стандартизации в этой области становится особенно актуальной и требует безотлагательного решения. Конкретные решения проблем стандартизации в области современной релейной защиты предложены в [9].

К проблемам стандартизации в области релейной защиты тесно прилегает и проблема тестирования исправности МУРЗ после зафиксированного применения ПЭДВ, поскольку стандартизация сегодня отсутствует не только в области самих МУРЗ, но и в области тестовых систем и применяемых ими алгоритмов. Но и эта проблема имеет свое решение [9].

В ОБЛАСТИ ПРОИЗВОДСТВА УСТРОЙСТВ РЗА

Снижение уязвимости самих МУРЗ к электромагнитным воздействиям – важнейшее направление в деле повышения устойчивости энергосистем к ПЭДВ. Одним из новых эффективных направлений снижения уязвимости релейной защиты является создание гибридных реле защиты, содержащих электромеханический пусковой орган, совмещенный с микропроцессорным терминалом [10–12]. Такое гибридное устройство релейной защиты позволит совместить высокую устойчивость к ПЭДВ электромеханики с широчайшими функциональными возможностями микропроцессорной техники и существенно снизить вероятность неправильного функционирования РЗ при воздействии на нее ПЭДВ.

Снижения уязвимости МУРЗ можно достичь также и совершенствованием конструкции входных трансформаторов тока и напряжения, применением на входах специальных фильтров, подавляющих высокочастотные сигналы и высоковольтные импульсы, дополнительных ограничителей уровня напряжений на всех входах и выходах, усилением изоляции и уровня гальванической развязки элементов входных и выходных цепей [12]. Должно быть директивно принято решение о том, что все новые типы МУРЗ должны быть снабжены специальными средствами защиты от ПЭДВ. Для реализации этого условия должны быть подготовлены типовые технические требования к МУРЗ, включающие набор стандартных требований по электромагнитной совместимости [9] и дополнительных требования по защите от ПЭДВ [13].

В ОБЛАСТИ СЕРТИФИКАЦИИ И ИСПЫТАНИЙ

Наличие специальных технических требований по устойчивости МУРЗ и элементов АСУ ТП к ПЭДВ обуславливает необходимость создания специальных сертификационных и испытательных центров, обеспечивающих проверку этой устойчивости. Имеющиеся сегодня во многих странах испытательные центры военного назначения не очень удобно использовать для тестирования аппаратуры гражданского назначения. Более правильным решением проблемы нам представляется использование уже имеющихся испытательных центров, занимающихся вопросами электромагнитной совместимости.

Естественно, потребуется закупка для этих центров специальной аппаратуры. Такая аппаратура, рис. 4, представлена сегодня на рынке несколькими специализированными компаниями [13] и может быть свободно приобретена. Стоимость полного комплекта оборудования, необходимого для проведения таких испытаний составляет около 500 тыс. долларов США. Помимо самой аппаратуры, потребуется также разработка методики таких испытаний, с учетом уже имеющегося опыта [13–14].

ВЫВОДЫ

1. Проблема ПЭДВ должна быть признана в России и странах постсоветского пространства как серьезная опасность, угрожающая инфраструктуре страны, в частности энергосистеме.

2. Предшествующими работами созданы все необходимые предпосылки и накоплен базовый опыт, достаточный для информационного обеспечения работ по повышению устойчивости энергосистем к ПЭДВ, а имеющееся на рынке оборудование для защиты и для испытаний чувствительной аппаратуры позволяет реально приступить к выполнению конкретных работ.

3. Для успешной реализации всего комплекса работ потребуется участие различных организаций при координирующей роли специального государственного органа.

4. Тенденции и темпы развития современных технических средств дистанционного поражения электронной аппаратуры обуславливают необходимость незамедлительного начала конкретных работ по защите энергосистем от ПЭДВ.

ЛИТЕРАТУРА

1. *Wik M. W.* Electromagnetic Terrorism – What are the Risks? What can be Done? – International Product Compliance Magazine, 1997.

2. *Kappenman J., Radasky W., Gilbert J.* Electric Power Grid Vulnerability to Natural and Intentional Geomagnetic Disturbances. – EMC Zurich Symposium (14–18 February 2005 in Zurich, Switzerland).

3. *Radasky W.* The Emerging Threat of Electromagnetic Transients on the Critical Infrastructure. – U.S. Department of Homeland Security Conferences (26–27 April 2005 in Boston, USA).

4. *Gurevich V.* The Hazards of Electromagnetic Terrorism. – Public Utilities Fortnightly, 2005, June, pp. 84–86.

5. *Гуревич В.И.* Электромагнитный терроризм: угроза рукотворной молнии. – PRO Электричество, 2005, № 11, с. 32–35.

6. *Гуревич В.И.* Микропроцессорные реле защиты: новые перспективы или новые проблемы? – Новости электротехники, 2005, № 6 (36), с. 57–60.

7. *Гуревич В.И.* Электромагнитный терроризм – новая реальность XXI века. – Мир техники и технологий, 2005, № 12, с. 14–15.

8. *Гуревич В.И.* Уязвимости микропроцессорных реле защиты. Проблемы и решения – Инфра-Инженерия, Москва, 2014, 256 с.

9. *Гуревич В.И.* Проблемы стандартизации в релейной защите – ДЕАН, Санкт-Петербург, 2014, 152 с.

10. *Гуревич В.И.* Снижение уязвимости микропроцессорных устройств релейной защиты к преднамеренным дистанционным деструктивным воздействиям. – Релейная защита и автоматизация, 2013, № 4, с. 48–50.

11. *Гуревич В.И.* Снижение уязвимости микропроцессорных устройств релейной защиты к преднамеренным дистанционным деструктивным воздействиям: ответы на вопросы специалистов. – Релейная защита и автоматизация , 2014, № 2, с. 20–25.

12. *Гуревич В.И.* Снижение уязвимости микропроцессорных реле защиты к преднамеренным дистанционным деструктивным воздействиям. Продолжение темы. – Релейная защита и автоматизация, 2014, № 4, с. 32–35.

13. *Гуревич В.И.* Проблемы тестирования микропроцессорных реле защиты на устойчивость к преднамеренным электромагнитным деструктивным воздействиям. – Компоненты и технологии, 2014, № 12, с. 161–168.

14. *Гуревич В.И.* Проблемы тестирования микропроцессорных реле защиты на устойчивость к преднамеренным электромагнитным деструктивным воздействиям (продолжение). – Компоненты и технологии, 2015, № 3, с. 158–161.