Интеллектуальные сети: новые перспективы или новые проблемы?

Вашему вниманию предлагается статья кандидата технических наук, эксперта комитета ТС-94 Международной электротехнической комиссии (МЭК) В. И. Гуревича. Автор 5 книг и более 140 научных статей рассуждает о том, что же такое интеллектуальные сети — термин, ставший сегодня, таким популярным. Часть I опубликована в предыдущем номере (№6 (33) ноябрь-декабрь 2010 г.) и на сайте журнала www.market.elec.ru.

Часть II

Smart Grid: панацея или путь к катастрофе?

Как можно было понять из предыдущей части статьи, **Smart Grid** — это концепция глобальной реконструкции всей системы электроснабжения. Очевидно, что такая глобальная программа требует колоссальных инвестиций для своей реализации. При этом возникает вполне правомерный вопрос: а что, собственно говоря, мы получим взамен? Какова будет экономическая отдача от этих инвестиций? К сожалению, ни в одной из многочисленных публикации, описывающей преимущества Smart Grid, нам не удалось найти никаких экономических обоснований целесообразности реализации концепции Smart Grid.

Разве существующая структура электрических сетей не обеспечивает надежного электроснабжения потребителей? Разве микропроцессорные счетчики электроэнергии не находят широкого применения вне рамок концепции Smart Grid? Разве развитию современных микропроцессорных систем автоматической диагностики энергетического оборудования мешает отсутствие Smart Grid? Разве современные МУРЗ не решают всех существующих сегодня задач релейной защиты? Да, с полным изменением конфигурации сетей и появлением огромного количества генерирующих источников в сети, функции и алгоритмы релейной защиты могут существенно измениться. Но, во-первых, как можно практически, а не теоретически, так кардинально изменить сложившуюся за десятилетия структуру электрических сетей в рамках национальных энергосистем? Да и зачем? Что касается огромного количества мелких генерирующих источников (ветрогенераторов, солнечных батарей),

которые по теории апологетов Smart Grid в будущем якобы будут включены в общую электрическую сеть, то такое развитие событий вызывает у нас сильное сомнение. Из собственных впечатлений от путешествий по странам Европы (Италия, Голландия, Германия, Испания и др.) можем сделать вывод, что ни ветрогенераторы, ни солнечные батареи нигде не используются (как объекты электроэнергетических систем) в виде одиночных сетевых энергетических установок (за исключением, конечно, индивидуальных устройств, обеспечивающих энергией отдельные здания). Везде они собраны в крупные энергетические узлы, занимающие огромные площади (см. фото), и уже эти узлы включены в сеть. Например, мощность ветроэлектростанции Thanet, расположенной на юго-восточном побережье графства Кент в Великобритании, состоящей из 100 ветротурбин (по плану их будет 340), составляет 300 МВт. При этом, существующие сегодня микропроцессорные системы автоматического регулирования режимов работы таких энергоузлов и их синхронизации с сетью вполне успешно справляются со своими задачами и без концепции Smart Grid. К тому же, по некоторым данным, ветроэнергетика оказывается и не такая уж прибыльная вещь. По данным экспертов британского Energy Research Centre, производство энергии на прибрежных ветроэлектростанциях оказывается примерно на 90% дороже энергии, производимой из обычных источников топлива и на 50% дороже энергии, полученной из ядерного топлива.

С другой стороны, если допустить все же реализацию концепции Smart Grid в части кардинальной реконструкции электрических сетей, то есть существенного усложнения их структуры и режимов работы, то возникает вопрос о том, насколько вообще предсказуемы будут эти режимы и можно ли будет их заранее рассчитать, кто и как будет рассчитывать уставки для реле защиты в такой сложной сети, насколько эти уставки будут отражать реальные аварийные режимы в сети. В случае возникновения сбоев в работе такой сложной сети с огромным количеством активных компонентов, влияющих друг на друга, выяснить причину этих сбоев, даже с учетом самодиагностики аппаратуры, будет, по нашему мнению очень непросто. Для этого потребуется моделирование режимов работы сети и достаточно длительные исследования. Мы предполагаем, что эксплуатировать такие сети будет намного сложнее, чем существующие и для их обслуживания потребуется персонал значительно более квалифицированный, чем сегодня. А что касается «компьютеризации» всего и вся подряд (что предусмотрено концепцией Smart Grid), то эта тенденция уже идет в промышленности и в энергетике полным ходом. Совершенно ничем не оправданное стремление к подключению всех видов энергетического оборудования к компьютерной сети и повсеместный переход от старой надежной аналоговой электроники к цифровой микропроцессорной, очень часто приводит, как показано в [24], к весьма плачевным результатам.

Отдельная проблема — релейная защита. Согласно концепции Smart Grid она должна развиваться в направлениях:

- еще большей концентрации функций в единичных микропроцессорных модулях;
- комбинации релейной защиты с функциями мониторинга и диагностики оборудования энергосистем;
- использования алгоритмов нечеткой логики, упреждающих функций, искусственного интеллекта, нейронных сетей и т.д.

Как показано в [25–28] надежность МУРЗ уже сегодня ниже надежности ЭМ. Из этого не следует, конечно, что нужно затормозить переход от ЭМ к МУРЗ. Однако, из этого следует, что имеется достаточно серьезная проблема, требующая своего решения. Некоторые пути решения этой проблемы уже предложены автором [29–32].

Вкратце их можно сформулировать следующим образом:

- запрет на использования в МУРЗ функций, не свойственных релейной защите, например, таких, как мониторинг электрооборудования;
- существенное ограничение количества функций в одном микропроцессорном терминале; оптимизация количества таких функций по критерию не только стоимости РЗ, но и ее надежности;
- отказ от использования алгоритмов с недетерминированной логикой, допускающих непредсказуемые действия релейной защиты;
- максимальное упрощение программного интерфейса на основе некоей универсальной для всех МУРЗ программной платформы;
- выпуск ведущими производителями компьютеризированного испытательного оборудования МУРЗ набора программ, полностью совместимых с универсальной программной платформой МУРЗ и позволяющих полностью автоматизировать процесс испытания МУРЗ, существенно снизив влияние «человеческого фактора»;


Солнечные (фотоэлектрические) станции

- новые принципы конструирования МУРЗ, базирующиеся на универсальных взаимозаменяемых функциональных модулях, по типу персональных компьютеров;
- создание рынка универсальных функциональных модулей МУРЗ;
- проведение специальных исследований и разработок, обеспечивающих функционирование релейной защиты в условиях преднамеренных деструктивных электромагнитных воздействий, например, за счет повышения устойчивости МУРЗ к таким воздействиям, а также за счет введения резервного комплекта РЗ при чрезвычайных ситуациях, на роль которого подходят лишь электромеханические реле.

Как можно видеть, сформулированные выше принципы противоположны тенденциям, предусмотренным концепцией Smart Grid. О чем это свидетельствует? О том, что реализация этой концепции приведет к резкому снижению надежности релейной защиты.

Что касается повсеместной замены всех конвенциональных трансформаторов тока и напряжения на опто-электронные с цифровым выходом (в соответствии с концепцией Smart Grid) то целесообразность такой замены, как было показано нами ранее в [33], также весьма сомнительна и с экономической и с технической точек зрения.

Одним словом, польза от комплексной реализации концепции Smart Grid не такая уж и очевидная, как это пытаются представить ее апологеты. Во всяком случае еще никто не доказал ее экономическую целесообразность. С другой стороны, отдельные проекты, экономическая целесообразность которых доказана, активно внедряются и без какой бы то ни было привязки к глобальной концепции Smart Grid.

Сомнения усилятся еще больше, если обратить внимание на некоторые не очень приятные факты, о которых активные сторонники Smart Grid обычно никогда не упоминают.

Речь идет о резком увеличении уязвимости Smart Grid хакерским атакам. Действительно, если все элементы Smart Grid будут управляться по командам, передаваемым по сети по протоколам TCP/IP, то возникает огромная потенциальная опасность внешнего вмешательства в работу энергетической системы. На это обращают внимание многие эксперты [34–55]. Этой теме посвящаются даже международные конференции [56]. Одни лишь апологеты Smart Grid «не замечают» этих проблем. Что же мы слышим в ответ от апологетов Smart Grid? Обычные отговорки о необходимости изоляции внутренней сети Smart Grid от внешней сети Интернет, об использовании паролей доступа и т.п. тривиальных мер по обеспечению безопасности. Все мы хорошо понимаем, что все эти меры защиты могут ограничить доступ к Smart Grid рядовых обывателей, но отнюдь не опытных хакеров, проникающих даже в очень хорошо защищенные сети министерств обороны и банков.

Да что там хакеры, если в армиях многих стран мира появились специальные подразделения, состоящие из высококлассных профессионалов, предназначенные для ведения кибернетических войн, то есть для проникновения в защищенные компьютерные сети противника и выведения их из строя.

Можно с уверенностью утверждать, что компьютерная сеть Smart Grid будет целью номер один для таких подразделений. «Добро пожаловать на войну XXI века, — говорит Ричард Кларк, в недавнем прошлом советник бывшего президента США Джорджа Буша по вопросам кибербезопасности. — Вообразите себе вспыхивающие электрогенераторы, сходящие с рельсов поезда, падающие самолеты, взрывающиеся газопроводы, системы вооружения, вдруг перестающие работать, и войска, которые не знают, куда им двигаться». Перед вами не пересказ эпизода из очередного голливудского блокбастера — это краткое описание высококлассного американского эксперта тех последствий, к которым может привести война нового формата — кибервойна [57]. Нынешний глава Киберкомандования Пентагона (Cyber Command) и начальник Агенства по Национальной Безопасности (АНБ) генерал Александер даже заявил на слушаниях Комитета по делам ВС США палаты представителей конгресса, что кибероружие имеет эффект, сравнимый с эффектом применения оружия массового уничтожения. А один из бывших сотрудников АНБ — Чарльз Миллер даже подсчитал, что на организацию киберструктуры, способной успешно атаковать Америку и полностью парализовать деятельность США, потребуется всего лишь 98 млн долларов [57]. «Для нас это одно из основных перспективных направлений, — подчеркнул на брифинге с журналистами вице-президент подразделения по разработке разведывательных и информационных систем компании Raytheon Стивен Хокинс. — Мы прогнозируем рост объемов рынка на два порядка, его стоимость составит миллиарды долларов». Бороться есть за что — кибербюджет в текущем году достиг 8 млрд долларов, а к 2014-му вырастет до 12 млрд. При этом если ежегодное увеличение расходов по другим направлениям в среднем в ближнесрочной перспективе будет на 3–4%, то в отношении кибербезопасности — не менее 8% ежегодно. Ведущая роль в войне нового типа, естественно, отведена военным, им же достанется и львиная доля кибербюджета: более 50% из 8 млрд долларов 2010 года получит Пентагон. «Кибероружие развивается с большой скоростью. Многие страны — включая США, Россию, Китай, Израиль, Великобританию, Пакистан, Индию, Северную и Южную Корею — развили сложное кибероружие, которое может неоднократно проникать в компьютерные сети и способно разрушать их, утверждают специалисты по кибербезопасности», — пишут авторы статьи Шивон Горман и Стивен Фидлер [58].

Некоторые представители американской разведки и аналитики опасаются, что кибероружие может попасть в руки террористов. «Вопрос стоит так: когда это попадет к «Аль-Каиде»?» — говорит Джеймс Льюис, специалист по кибербезопасности Центра стратегических и международных исследований [58].

Одним из направлений войны нового типа является создание специальных боевых вирусов, способных завладеть компьютерной сетью, наподобие вируса Win32/ Stuxnet, поразившего в сентябре 2010 г. защищенные компьютерные сети ядерной энергетической программы Ирана. Win32/ Stuxnet представляет угрозу для промышленных предприятий. При запуске этой вредоносной программы используется ранее неизвестная уязвимость в обработке файлов с расширением LNK, содержащихся на USB-накопителе. Выполнение вредоносного кода происходит благодаря наличию уязвимости в Windows Shell, связанной с отображением специально подготовленных LNK-файлов. Новый способ распространения может повлечь появление других злонамеренных программ, использующих такую технологию заражения, поскольку на данный момент уязвимость остается открытой [59]. Win32/Stuxnet также может обходить технологию HIPS (Host Intrusion Prevention System), которая защищает от попыток внешнего воздействия на систему. Это стало возможным благодаря наличию во вредоносной программе файлов, имеющих легальные цифровые подписи. Сейчас в сутки этот вирус совершает несколько тысяч атак на компьютеры, имеющие программы Siemens [60]. Атакам подвержены сложные системы, в том числе автоматические, управляющие целыми заводами, а также объектами городской инфраструктуры, включая водопровод, отмечают специалисты. Издание [60] приводит мнение аналитиков, которые считают, что оборудование Siemens стало жертвой первой широкой попытки «промышленного саботажа». На основе проведенного комплексного анализа, эксперты компании Symantec заключили, что Stuxnet — необычайно опасная и сложная угроза безопасности компьютерных систем, основной задачей которой было заражение систем контроля промышленным оборудованием, которые, в частности, используются на электростанциях. Путем изменения кода логических контроллеров (programmable logic controllers — PLC) вирус пытался перепрограммировать системы контроля промышленных систем (industrial control systems — ICS), чтобы, незаметно от операторов систем, захватить над ними контроль. Сложность же вируса, его чрезвычайно высокая избирательность свидетельствуют о том, что данную вредоносную программу создавал не хакер-самоучка, а группа высококвалифицированных специалистов, имевших без преувеличения гигантский бюджет и возможности по интеграции ресурсов [57]. Проанализировав код червя, эксперты «Лаборатории Касперского» сделали вывод, что главная задача Stuxnet — «не шпионаж за зараженными системами, а подрывная деятельность». Stuxnet не крадет деньги, не шлет спам и не ворует конфиденциальную информацию, — утверждает Евгений Касперский. — Этот зловред создан, чтобы контролировать производственные процессы, в буквальном смысле управлять огромными производственными мощностями. В недалеком прошлом мы боролись с киберпреступниками и интернет-хулиганами, теперь, боюсь, наступает время кибертерроризма, кибероружия и кибервойн» [57].

Не меньшую угрозу для Smart Grid представляют собой последние технические достижения в области преднамеренных деструктивных электромагнитных воздействий на электронную аппаратуру, описанных нами ранее в [61].

Немного истории. Электромагнитный импульс, как поражающий фактор ядерного взрыва, был предсказан чисто теоретически еще в 1928 году физиком Артуром Комптоном (США) в 1923 г. Об эффекте Комптона пришлось вспомнить, когда после испытательного взрыва в 1958 году над Тихим океаном первой водородной бомбы возникли неожиданные осложнения на расстоянии сотен миль от места взрыва: погасли уличные фонари на Гавайях, были полностью нарушены системы радионавигации в Австралии, была нарушена радиосвязь во многих других регионах. Вот тут-то и вспомнили о Комптоне. Вспомнили и схватились за голову: оказывается, мощный поток электронов создает в электрических и электронных приборах даже на большом расстоянии такой электромагнитный импульс который выводит из строя эти приборы и может быть использован как самостоятельный вид оружия! Очевидно, с этого момента и начинается история электромагнитного оружия [62].

Первые теоретические идеи о возможности создания неядерных ударно-волновых излучателей сверхмощных электромагнитных импульсов (УВИ) были высказаны в начале 50-х годов прошлого столетия академиком Андреем Сахаровым во время его исследований реакций ядерного синтеза [63]. Уже в 60-е годы не только ученым в СССР, но и политикам стало понятно, что такого рода источники сверхмощных электромагнитных импульсов могут стать основой для создания нового вида оружия. Свидетельством этому стали выступления Н. С. Хрущева в 60-х годах с его упоминаниями некоего «фантастического оружия». Конечно, для создания нового оружия на основе чисто теоретических разработок потребовалось время. Об УВИ, как о самостоятельном устройстве для создания сверхмощных электромагнитных импульсов, в качестве оружия, впервые было официально заявлено советским ученым А. Б. Прищепенко после успешных испытаний 2 марта 1984 г. на полигоне Красноармейского научно-исследовательского института «Геодезия», Моск. обл. (ныне ФКП НИИ «Геодезия»). Позднее, тем же А. Б. Прищепенко были сформулированы общие принципы боевого применения электромагнитных боеприпасов. По опубликованным данным, продолжительность этого импульса составляет десятки или сотни микросекунд, а амплитудные значения возникающего тока достигают десятков миллионов ампер. Для сравнения: при грозовом разряде сила тока в молнии обычно не превышает 20–30 тысяч Ампер и лишь в очень редких случаях может достигать 100 тысяч Ампер.

По свидетельству [64] в 80-х годах Советский Союз неоднократно проводил эксперименты с электромагнитным оружием в космосе, в результате которых неоднократно случались аварии в энергосистемах различных штатов США. Лет двадцать тому назад и автору этих строк довелось лично присутствовать на предзащите докторской диссертации посвященной теоретическим аспектам проблемы передачи энергии мощного сверхвысокочастотного источника из космоса на землю.

В те же годы, в СССР параллельно проводились эксперименты и с генерацией супермощных электрических разрядов (являющихся мощным источников электромагнитного излучения). В многочисленных американских газетах и журналах того времени сообщалось о необычайно мощных электрических разрядах, никогда не встречавшихся ранее, при полном отсутствии грозовой деятельности, зафиксированных над территорией СССР. Еще лет 25 тому назад автор данной статьи лично видел фотографию сверхдлинного разряда между двумя вышками, проходящего горизонтально земле над домами какого-то поселка.

В годы перестройки, очевидно, в ознаменование эпохи новых отношений со странами Запада, российские ученые А. Прищипенко, В. Кисилев и С. Кадимов в своем докладе «Радиочастотное оружие на будущем поле боя» на международной конференции во Франции [65] сообщили мировому сообществу о новом виде оружия, разработанного в СССР. Этот доклад произвел в то время настоящий фурор и привел к тому, что в последствие эти вопросы стали обсуждаться в открытой печати. В дальнейшем в открытой печати появились и другие сообщения о достижениях российских ученых в этой области [66–68]. Сегодня вопросы электромагнитной войны и электромагнитного терроризма уже открыто обсуждаются в прессе, на зарубежных и российских научных конференциях [69, 70]. Не забыты и первые опыты с ядерными взрывами в атмосфере.

Последними исследованиями показано, что ядерный взрыв, произведенный в ближнем космосе (на высоте 200–300 км), практически не будет заметен населением страны, над которой он был произведен, за исключением, правда, того обстоятельства, что все системы жизнеобеспечения (энергоснабжение, водоснабжение, телекоммуникация, связь и т.д.) во мгновение ока одновременно будут выведены из строя. В связи с этим существуют даже стандарты МЭК (см., например, [71]), в которых подробно описана методика проведения испытаний на устойчивость оборудования электрических сетей к воздействию высотного электромагнитного импульса (high-altitude electromagnetic pulse — HEMP). Специально для проведения таких испытаний разработаны мобильные симуляторы, генерирующие импульсы, аналогичные тем, которые наводятся в проводах ЛЭП во время HEMP.

По данным, приведенным в этом документе, при воздействии HEMP на обесточенные ЛЭП перенапряжения достигают такой величины, что происходит пробой даже линейных изоляторов класса 35 кВ и, естественно, всех изоляторов более низкого класса. А при воздействии такого импульса на ЛЭП, находящуюся под напряжением, пробиваются уже и изоляторы класса 110 кВ. При этом уже не приходится говорить обо всем остальном оборудовании, имеющем прямые, индуктивные или емкостные связи с проводами ЛЭП.

Сегодня работы в области электромагнитного оружия сконцентрированы в России, в основном, в трех крупнейших научно-исследовательских центрах: Объединенном институте высоких температур (ОИВТРАН, г. Москва) под руководством академика Фортова В. Е., в Институте сильноточной электроники (ИСЭ СО РАН, г. Томск) под руководством академика Месяца Г. А. и в Троицком институте инновационных и термоядерных исследований (ТРИНИТИ) под руководством проф. Черковца В. Е.

В Московском ОИВТРАН ведутся работы по созданию взрывомагнитных генераторов сверхмощных электромагнитных импульсов [72]. А в Томском ИСЭ СО РАН разрабатываются сверхмощные ультраширокополостные генераторы направленного электромагнитного излучения не взрывного действия, рис. 5 [73].

Не нужно обладать особой фантазией, чтобы представить, как можно разместить компактные генераторы, весом в 300–400 кг, рис. 5, в легком грузовике или в микроавтобусе с пластмассовым кузовом и дистанционно воздействовать на электронное оборудование подстанций и электростанций, вычислительных центров, центров управления полетами и т.п. При такой излучаемой мощности, достаточно нескольких импульсов, чтобы выжечь начинку всех электронных приборов, включая МУРЗ, разумеется. Таково же, очевидно, и назначение последней разработки ОИВТРАН, о которой с гордостью сообщил недавно корреспонденту ИТАР-ТАСС директор этого института академик В. Фортов. Речь идет о взрывном электромагнитном генераторе с импульсной мощностью в тот же миллиард Ватт, упакованном в небольшой чемоданчик, способном при взрыве выжечь всю электронику в радиусе многих сотен метров. Причем, по некоторым сведениями, выходит из

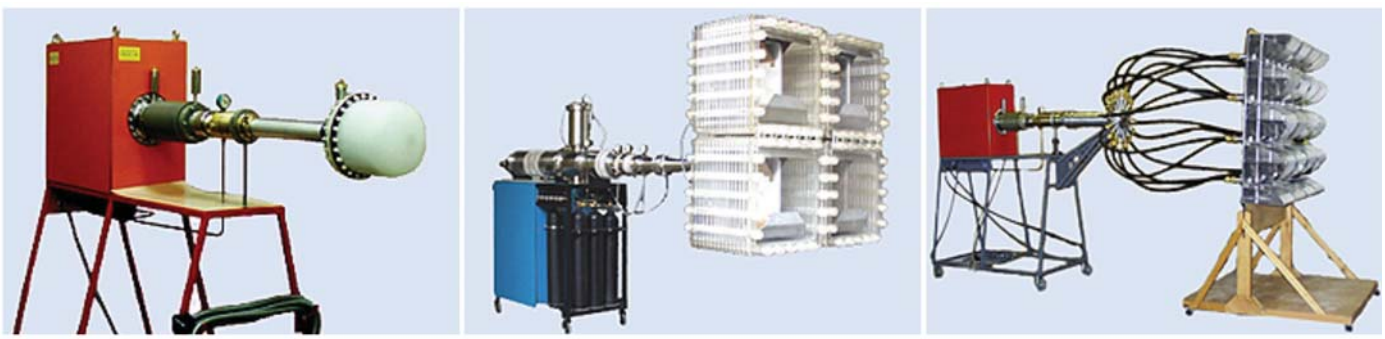

Рисунок 5. Сверхмощные ультраширокополостные импульсные генераторы направленного сверхвысокочастотного электромагнитного излучения ИСЭ СО РАН с выходной мощностью, доходящей до 1 миллиарда Ватт, что сопоставимо с мощностью энергоблока АЭС

строя даже выключенная в момент воздействия электронная аппаратура.

Естественно, что работы в тех же направлениях ведутся и во многих других странах, включая Китай, Индию и Иран. В США, например, интенсивные исследования в этой области ведутся такими крупными корпорациями, как TWR, Raytheon, Lockheed Martin, Los Alamos National Laboratory, Air Force Research Laboratory (Kirtland Air Force Base, New Mexico), а также многими гражданскими организациями и университетами. В Германии работы в этой области уже много лет возглавляет Rheinmetall Weapons and Munitions. В частности, американцами разработаны генераторы мощных электромагнитных импульсов на различных принципах, рис. 6.

Совсем недавно американские компании Boeing и Raytheon получили контракт на разработку ракет с новым высокомощными микроволновыми излучателями вместо классических боеголовок со взрывчатым веществом. Каждая из компаний получила на разработки около миллиона долларов. Это оружие предназначено для уничтожения защищенной электронной аппаратуры противника. Между тем, Boeing уже ведет собственный проект разработки ракеты с высокомощным микроволновым излучателем (CHAMP). Стоимость проекта оценивается в 38 миллионов долларов и финансируется за счет средств ВВС США. Как ожидается, первый прототип ракеты будет готов к испытаниям в течение 2012 года [74].

Основными каналами силового деструктивного воздействия на электронную аппаратуру являются: сети электропитания всех классов напряжения, контрольные кабели и проводные линии связи, компьютерные сети, эфир. Поскольку микропроцессорная аппаратура Smart Grid связана и с внешней сетью электропитания, и с разветвленной сетью контрольных кабелей, и с проводами-антеннами ЛЭП (через ТН и ТТ), и с компьютерной сетью, то оказываемое на них деструктивное воздействие может быть очень сильным и, одновременно, скрытным. Существенно повышает скрытность электромагнитного нападения то обстоятельство, что анализ повреждений в уничтоженном оборудовании не позволяет однозначно идентифицировать причину возникновения повреждения, так как причиной одних и тех же повреждений может быть как преднамеренное (нападение), так и непреднамеренное (например, индукция от молнии) силовое деструктивное воздействие. Это обстоятельство позволяет злоумышленнику успешно использовать эту технологию неоднократно.

Микроволновые источники излучения высокой мощности, работающее в сантиметровом и миллиметровом диапазонах, имеют дополнительный механизм проникновения энергии в оборудование, так сказать, «через заднюю дверь», то есть даже через небольшие отверстия, вырезы, окна и щели в металлических корпусах, через плохо экранированные интерфейсы. Любое отверстие, ведущее внутрь оборудования, ведет себя как щель в микроволновой полости, позволяя микроволновой радиации формировать пространственную стоячую волну внутри оборудования. Компоненты, расположенные в противоположных узлах стоячей волны будут подвергаться воздействию сильного электромагнитного поля и перенапряжений. Особо чувствительны к воздействиям такого рода элементы памяти и современные микропроцессоры с очень высокой степенью интеграции внутренних компонентов.

Отсюда становится понятным, что защититься от всех этих «напастей» не так-то просто. И даже такие известные помехоустойчивые технологии, как оптоволоконные, оказываются подверженными, как это не покажется странным, воздействию мощных электромагнитных импульсов. Во-первых, оптоволоконные линии имеют концевые устройства, выполненные на микроэлектронных компонентах и даже на микропроцессорах, которые предназначены для преобразования электрического сигнала в световой и обратно.

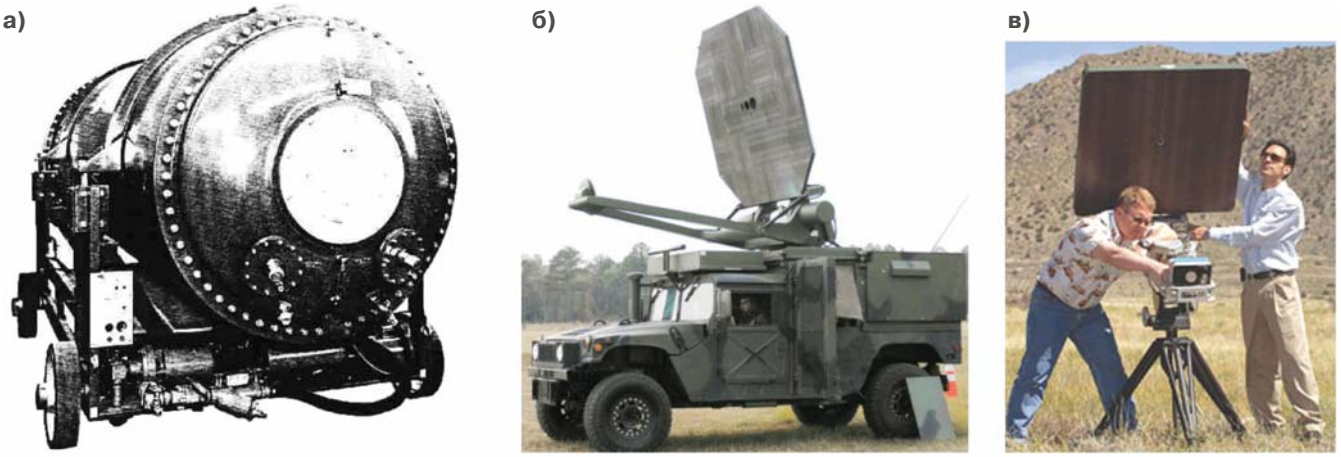

Рисунок 6. а) Сверхмощный передвижной генератор высоковольтных импульсов FEBETRON-2020 (выходное напряжение 2,3 МВ, выходной ток 6000 Ампер); б) мощный СВЧ-генератор направленного действия, смонтированный на автомобиле; в) мощный СВЧ-генератор направленного действия переносного типа

Рисунок 7. Некоторые книги, изданные в России на тему о преднамеренных деструктивных электромагнитных воздействиях

Во-вторых, известно, что вектор поляризации света в оптическом волокне может изменяться под действием внешнего магнитного поля (собственно говоря, именно на этом принципе и построены магнито-оптические трансформаторы тока, широко представленные сегодня на рынке). Это приводит к тому, что сигналы систем релейной защиты и связи, передаваемые по оптическому волокну, встроенному в провода высоковольтной линии электропередач (весьма распространенная сегодня технология) будут подвергаться искажениям при протекании по этим проводам больших импульсных токов, создающих импульсные магнитные поля.

Следует отметить, что еще несколько лет назад средства массовой информации очень неохотно публиковали статьи на эту тему, опасаясь привлечь внимание террористов и криминальных элементов. Однако, после последней крупнейшей аварии в энергосистеме США террористы сами обратили внимание на зависимость современной Западной цивилизации от электроэнергетики в ряде своих высказываний и угроз. После этого последовал шквал статей в «Нью-Йорк Таймс» и других публичных изданиях посвященных вопросу незащищенности важнейших систем жизнеобеспечения общества от электромагнитного терроризма. В [75], например, прямо указывается, что электроэнергетические системы являются сегодня важнейшей целью террористических атак. В этой связи просто поражает беспечность руководства и персонала энергосистем в течение многих лет закрывающих глаза на эту проблему. Как иначе, чем преступной беспечностью, можно назвать полное пренебрежение огромным количеством публикаций на эту тему и в специальных технических изданиях, и в прессе, и в Интернете, и в книгах, наконец, рис. 7, [76–80].

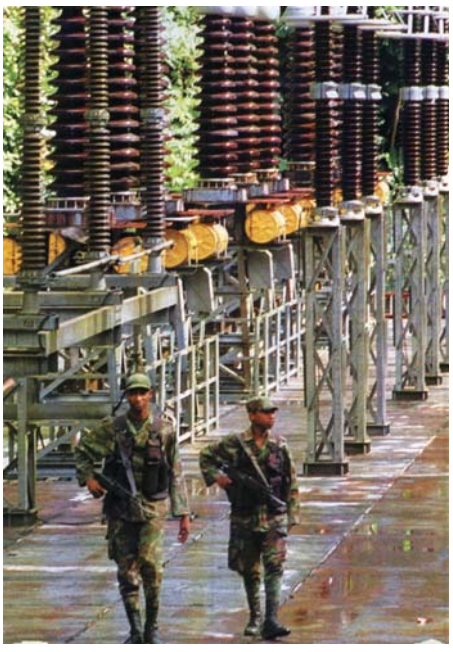

Рисунок 8. Smart Grid – наше будущее?

Автор был просто шокирован полным отсутствием даже минимальных знаний этой проблемы не только у рядовых энергетиков, но и у руководящих работников. Более того, попытки автора поднять эту тему в статьях, на форумах по релейной защите приводили лишь к насмешкам и пренебрежительному фырканью в его адрес.

Концепция Smart Grid, предусматривающая самое широкое применение микропроцессорных устройств во всех элементах энергосистем с одной стороны, и тенденция увеличения плотности элементов в микрочипах (сопровождающаяся снижением их устойчивости к внешним электромагнитным воздействиям) — с другой, на фоне прогресса в области создания средств дистанционного деструктивного воздействия образуют весьма опасный вектор. А страусиная политика нежелания знать и осознавать грядущие опасности еще никогда не приводила к добру…

И все это реалии сегодняшнего дня, когда до полной практической реализации концепции Smart Grid еще очень далеко. Что же будет, если эта концепция действительно получит развитие? Об этом можно судить уже сегодня и с достаточно большой долей достоверности. По нашему мнению, полная реализация концепции Smart Grid приведет к резкому повышению уязвимости энергосистем и к снижению их надежности. Если ранее речь шла о проблемах лишь микропроцессорных устройств релейной защиты [81], то после внедрения концепции Smart Grid те же проблемы перекочуют на гораздо более высокий уровень и станут намного более опасными и глобальными, рис. 8.

Так что же такое Smart Grid?

По нашему мнению, Smart Grid — это грандиозная рекламная компания, в которой заинтересованы сотни фирм-производителей, научно-исследовательские центры и университеты. Целью этой компании является рекламирование огромного количества изделий, технологий и исследований, искусственно привязываемых к модному термину «Smart Grid», а также «выбивание» сотнями интересантов миллиардных инвестиций из государственных бюджетов [82] на разработку и производство изделий и систем, подпадающих под расширенное до невероятных пределов толкование термина «Smart Grid». При этом, чисто экономические интересы апологетов Smart Grid превалируют над естественными сомнениями и опасениями по поводу тех опасностей которым будет подвергнуто общество в случае полномасштабной реализации этой концепции. Игнорирование этих опасностей может привести к глобальным общенациональным катастрофам.

Что касается естественного хода технического прогресса, то он никоим образом не замедлится в случае отказа от этой концепции, а будет лишь более обоснованным, более разумным и осторожным.

В. И. ГУРЕВИЧ,
канд. техн. наук

ЛИТЕРАТУРА

24. Гуревич В. И. Цена прогресса. – «Компоненты и технологии», 2009, № 8, с. 112–118.

25. Гуревич В. Надежность микропроцессорных устройств релейной защиты: мифы и реальность: – Проблемы энергетики, 2008, № 5–6, с. 47–62.

26. Гуревич В. И. Еще раз о надежности микропроцессорных устройств релейной защиты. – «Электротехнический рынок», 2009, № 3(29), с. 40–45.

27. Гуревич В. И. О некоторых оценках эффективности и надежности микропроцессорных устройств релейной защиты. – «Вести в электроэнергетике», 2009, № 5, с. 29–32.

28. Гуревич В. И. Проблемы микропроцессорных реле защиты: кто виноват и что делать? – Энерго-инфо, 2009, № 10, с. 64–69.

29. Гуревич В. И. Прогресс в области конструирования микропроцессорных устройств релейной защиты. – «Электроника-инфо», 2010, № 3, с. 44–47.

30. Гуревич В. И. Сенсационные «открытия» в области релейной защиты. – «Энергетика и промышленность России», 2009, № 23–24.

31. Гуревич В. И. Новая концепция построения микропроцессорных устройств релейной защиты. – «Компоненты и технологии», 2010, № 6, с. 12–15.

32. Гуревич В. И. Как нам обустроить микропроцессорные устройства релейной защиты? – «Энергетика и промышленность России», 2010, № 12(152).

33. Гуревич В. И. Оптоэлектронные трансформаторы: панацея или частное решение частных проблем. – «Вести в электроэнергетике», 2010, № 2, с. 24–28.

34. Robertson J. Security experts offer caution on Smart Grid. – Associated Press, July 31, 2009.

35. Krebs B. «Smart Grid» raises security concerns. – The Washington Post, July 28, 2009.

36. Slocum Z. Report: Smart-grid hackers could cause blackouts. – Cnet.News, March 21, 2009 (http://news.cnet.com/8301-1009_3-10201651-83.html).

37. Baldor L. C. New threat: Hackers look to take over power plants. – Associated Press, April 8, 2010.

38. Nakashima E. Defense official discloses cyberattack. – The Washington Post, August 25, 2010.

39. Gorman S. U.S. Plans Cyber Shield for Utilities, Companies. – The Wall Street Journal, July 8, 2010.

40. Lemos R. Hacking the Smart Grid. – Technology Review, April 05, 2010.

41. Mills E. Experts warn of catastrophe from cyberattacks. – InSecurity Complex, February 23, 2010.

42. Aitoro J. R. Energy set to form new group to protect electric grid from cyberattacks. – NextGov, May 01, 2010.

43. Barret L. U.S. Reviewing Cyber Threat to Power Grid. – Internet News, September 15, 2009 (www.internetnews.com/security/article.php/3839241).

44. Hamilton T. Smart grid saves power, but can it thwart hackers? – TheStar.com, August 03, 2009 (http://www.thestar.com/printArticle/675453).

45. Gross G. Lawmakers: Electric utilities ignore cyber warnings. – Computerworld, July 21, 2009.

46. (http://www.computerworld.com/s/article/print/9135753/Lawmakers_Electric_utilities_ignore_cyber_warnings).

47. Gorman S. Electricity Industry to Scan Grid for Spies. – Wall street Journal, June 18, 2009.

48. Miller S. C. Our infrastructure in their crosshairs. – The News & Observer, May 12, 2009.

49. Smart Grid offers savings, vulnerabilities. – HS Daily Wire, 30 April 2009.

50. Critics: Cybersecurity standards for grid do not go far enough HS Daily Wire, May 01, 2009.

51. Sarwate A. Hot or Not: SCADA security is hot. – SC Magazine US, April 23, 2009.

52. Mills E. Just how vulnerable is the electrical grid? – CNET. News, April 10, 2009.

53. Meserve J. «Smart Grid» may be vulnerable to hackers. – CNN. Com (http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/index.html).

54. Madrigal A. Report: A Smart Grid Is a Hackable Grid. – TheAtlantic.com, October 7, 2010 (http://www.theatlantic.com/ technology/archive/2010/10/report-a-smart-grid-is-a-hackable-grid/64231/).

55. Half of critical infrastructure providers have experienced perceived politically motivated cyber attack. – Transmission & Distribution World, October 6, 2010.

56. Preventing Catastrophic Impacts from Adverse Cyber-Physical Events. – CISW-SG 2010 Smart Grid Survivability Workshop, Arlington, Virginia USA, October 13–14, 2010.

57. Щербаков В. Пространство виртуальное, борьба реальная. – Военно-промышленный курьер, № 40(356), 13.10.2010.

58. Gorman S., Fidler S. Cyber Attacks Test Pentagon, Allies and Foes. – Wall Street Journal, September 25, 2010.

59. Кряквина Ю. ESET предупреждает об атаке червя Win32/ Stuxnet. 19. 07. 2010 – (http://www.ixbt.com/news/soft/index.shtml?13/ 54/55).

60. Компьютерные системы Siemens стали объектом первой глобальной попытки промышленного саботажа. Лондон, 22 июля, ПРАЙМ-ТАСС (http://www.prime-tass.ru/news/0/%7BA89148AF-A72E-49C4-86BC-5D6D8598E340%7D.uif).

61. Гуревич В. И. Проблема электромагнитных воздействий на микропроцессорные устройства релейной защиты. – «Компоненты и технологии», 2010, № 2, с. 60–64; № 3, с. 91–96; № 4, с. 46–51.

62. Гуревич В. И. Электромагнитный терроризм – новая реальность 21 века. – Мир техники и технологий, 2005, № 12, с. 14–15.

63. Сахаров А. Д. Взрывомагнитные генераторы // Успехи физических наук. 1966. Вып. 4. Т. 83, 84.

64. The shocking history of Soviet Russia's Electromagnetic (EM) war attacks on the United States. – Интернет сайт: (http://www.bayside.org/news8/sovietelectromagneticattacksonunitedstates.htm).

65. A. B. Prishchepenko, V. V. Kiseljov, and I. S. Kudimov, «Radio frequency weapon at the future battlefield», Electromagnetic environment and consequences, Proceedings of the EUROEM94, Bordeaux, France, May 30–June 3, 1994, part 1, p. 266–271.

66. Кадуков А. Е., Разумов А. В. Основы технического и оперативно-тактического применения электромагнитного оружия. Петербургский журнал электроники, вып. 2, 2000.

67. Россия выставляет на рынок оружие будущего. Газета «Независимое военное обозрение» № 39(261), 19–25 октября 2001.

68. Прищипенко А. Новый вызов террористов – электромагнитный. Газета «Независимое военное обозрение», 05.11.2004.

69. Богданов В. Н., Жуковский М. И., Сафронов Н. Б. Электромагнитный терроризм – состояние проблемы. Доклад представлен Научно-техническим центром «Атлас» ФСБ России. Материалы конференции «Информационная безопасность регионов России – 2005», С. Петербург, 14–16 июня 2005 г.

70. Daamen D. Avant-garde Terrorism: Intentional Electro Magnetic Interference. On Methods and Their Possible Impact. – Report. Spring 2002.

71. IEC/TR 61000-1-3 Electromagnetic compatibility (EMC) – Part 1–3: General – The effects of high-altitude EPM (HEMP) on civil equipment and systems.

72. Взрывные генераторы мощных импульсов электрического тока / Под ред. В. Е. Фортова. – М.: Наука, 2002.

73. Месяц Г. А. Генерирование мощных наносекундных импульсов. – М.: Сов. радио, 1973.

74. Trimble S. Boeing, Raytheon win work on high power microwave missile. – Flight International, 24.09.2010.

75. Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. (http://www.empcommission.org/docs/empc_exec_rpt.pdf).

76. А. Б. Прищепенко. Взрывы и волны. Взрывные источники электромагнитного излучения радиочастотного диапазона. Учебное пособие по специальности 170103 «Средства поражения и боеприпасы» М. БИНОМ. Лаборатория знаний. 2008 г. ISBN 978-5-94774-726-3.

77. Прищепенко А. Б. Оружие уникальных возможностей // Независимое военное обозрение. 1998. 17–23 июля. № 26.

78. Ганнота А. Объект поражения – электроника // Независимое военное обозрение. 2001. № 13.

79. Электромагнитный терроризм на рубеже тысячелетий /Под ред. Т. Р. Газизова. – Томск: Томский гос. ун-т. 2002.

80. В. Д. Добрыкин, А. И. Куприянов, В. Г. Пономарев, Л. Н. Шустов. Радиоэлектронная борьба: силовое поражение радиоэлектронных систем. – М.: Вузовская книга, 2007.

81. Проблемы микропроцессорных устройств релейной защиты (http://digital-relay-problems.tripod.com/).

82. Sonenklar C. Obama admin tabs $3 billion for Smart Grid. – (http://www.heatingoil.com/blog/obama-admin-tabs-3-billion-for-smart-grid-1028/).