во многой мудрости много печали;
и кто умножает познания, умножает скорбь
Книга Екклесиаста

«ИНТЕЛЛЕКТУАЛИЗАЦИЯ» РЕЛЕЙНОЙ ЗАЩИТЫ: БЛАГИЕ НАМЕРЕНИЯ ИЛИ ДОРОГА В АД?

Владимир Гуревич, *канд. техн. наук*
Электротехническая компания Израиля

В одном старом научно-фантастическом романе был представлен занятный сюжет, развитие которого началось с довольно невинной вещи: необычного ночного звонка на все телефоны всем жителям планеты Земля. Этим звонком всем людям Земли возвестил о своем рождении Глобальный Разум. Оказалось, что на каком-то этапе развития количественный рост компьютеров перерос в новое качество: миллионы компьютеров, объединенных в общую сеть и управляющих всем и вся на планете Земля, вдруг осознали себя как единое целое, способное к самовоспроизводству посредством автоматизированных заводов и роботов, включенных в ту же сеть, а также к защите с помощью компьютеризированных систем вооружения, рассчитанных на уничтожение человека. С точки зрения Глобального Разума человечество было ничем иным, как рудиментом, балластом, пожирающим ресурсы планеты. О дальнейшем развитии сюжета читатели могут предугадать сами.

Компьютерами с сетевым подключением уже сегодня управляются практически все виды современных промышленных производств, системы управления водоснабжением и электроснабжением, системы телекоммуникации и связи. В технической, а не в фантастической литературе появились термины: «разумная электрическая сеть» (Smart Grid), релейная защита с «искусственным интеллектом» (Artificial Intelligence). В технической, а не в фантастической литературе рассматриваются сегодня вопросы создания «умного жилища» (Smart House), в котором даже холодильник будет сам оценивать запасы хранящихся в нем продуктов, и на основе анализа их потребления будет составлять заказ и отсылать его по сети в ближайший супермаркет. Сегодня микропроцессоры можно найти уже где угодно, даже в крышке унитаза [1].

Человечество семимильными шагами движется к созданию непредсказуемого Глобального Разума, предугаданного в старом фантастическом романе...

Но, вернемся в реальность. А она такова, что основными причинами крупнейших аварий в энергосистемах, происшедших на разных континентах (США: 1965, 1977, 2003 гг.; Франция: 1978 г.; Канада: 1982, 2003 гг.; Италия: 2003 г.; Лондон: 2003 г.; Швеция: 1983, 2003 гг.), были неправильные, а вернее непредсказуемые, действия релейной защиты в сложных аварийных режимах, отключивших не те участки сети, которые нужно было отключить в данной конкретной ситуации. Если бы действия релейной защиты в тех конкретных условиях были бы иными, системных аварий удалось бы избежать. Речь идет об энергосистемах США и Западной Европы, уже в значительной степени оборудованных компьютерами и микропроцессорными защитами. Для сравнения отметим, что в одной из крупнейших в мире энергосистем с ничтожно малым процентом компьютеризированных релейных защит и старым изношенным оборудованием, таких аварий не было. Речь идет об энергосистеме России. Ответ на вопрос о том, почему так происходит, можно найти в книге крупнейшего специалиста в области современной релейной защиты доктора технических наук Э. Д. Шнеерсона [2]:

«Само по себе повышение технического уровня устройств релейной защиты (УРЗ) не обязательно ведет к эквивалент-

ному повышению эффективности в части реагирования на возникающие повреждения. Так, например, устаревшие к настоящему времени электромеханические и отчасти электронные статические УРЗ при правильном выборе защитных функций и уставок безусловно обеспечат более эффективную защиту сети, чем микропроцессорные УРЗ без достаточно обоснованного выбора указанных параметров».

Действительно, ведь поведение в аварийных ситуациях электромеханических и электронных статических УРЗ было жестко детерминировано принципом их действия и заложенными в них уставками. Современные же тенденции [2–7] в развитии микропроцессорных устройств релейной защиты (МУРЗ) связаны с увеличением степени их «самостоятельности» (т. е., фактически, непредсказуемости) в выборе решений. Речь идет об использовании в релейной защите возможности самообучения, характерной для адаптивных нейронных сетей, использованию технологий искусственного интеллекта с нечеткой логикой и т.д.

Еще одной тенденцией, четко просматривающейся в развитии современных МУРЗ, является их чрезмерное усложнение за счет придания им посторонних функций, совершенно не характерных для релейной защиты. Вот, например, как выглядит перечень функций, выполняемых так называемым «разумным контроллером» (Intelligent Protection and Automation Controller iPAC фирмы Dynatrol Systems Inc.):

Измеряемые величины:

- действующие значения токов и напряжений;
- действующее значение тока в нейтрали;
- коэффициент мощности;
- полная мощность;
- активная мощность;
- реактивная мощность;
- измерение гармоник в токе и напряжении на основе разложения в ряд Фурье;
- вычисление коэффициента гармоник (THD – Total Harmonic Distortion);
- измерение частоты.

Защитные функции (в скобках указаны их стандартные номера):

- синхронизация с сетью (25);
- пониженное напряжение (27);
- направление мощности (32);
- ассиметрия фазных напряжений (46);
- токовая отсечка (50);
- зависимая токовая защита (51);
- повышенное напряжение (59);
- баланс напряжений (60);
- токовая направленная защита (67);
- автоматическое повторное включение с функциями контроля режима (79);
- понижение и повышение частоты (81);
- управление отключающей катушкой выключателя (86);
- дифференциальная защита трансформатора (97).

Добавьте к этому мониторинг внешних цепей тока и напряжения, регистрацию событий, функции цифрового осциллографа аварийных режимов и другие, ставшие уже обычными, функции МУРЗ.

Не говоря уже об опасности чрезмерной концентрации защитных функций в единичном терминале (например, в микропроцессорном реле типа SYMAP производства компании Stucke Elektronik GmbH заложено 39 отдельных защитных функций), придание релейной защите дополнительных, не свойственных собственно защите, функций приводит не только к физическому усложнению устройства и, как следствие, к снижению ее надежности, но и к усложнению его программного обеспечения и пользовательского интерфейса. Это, в свою очередь, приводит к резкому возрастанию ошибок при работе с программным обеспечением (так называемый «человеческий фактор»). При наличии такого большого количества функций, использующих одни и те же внутренние ресурсы МУРЗ при возможности конкуренции между встроенными логическими функциями во время сложного аварийного режима, сопровождающегося переходом одного вида повреждения в другое, уже далеко не всегда становится возможным предугадать поведение защиты. А повреждение одного из общих для всех функций внутренних элементов МУРЗ (источника питания, ватчдога, памяти, микропроцессора или вспомогательных узлов, обслуживающих его и т.п.) приведет к мгновенной потере сразу всех защитных функций одновременно.

Несмотря на уже существующие сегодня очевидные проблемы с чрезмерной концентрации защитных функций в единичном терминале, ведущие специалисты Российского ВНИИ Релестроения в своих философствованиях о будущем релейной защиты не только ратуют за дополнительное «навешивание» посторонних функций на релейную защиту, но и идут еще дальше. Они выдвигают фантастические идеи так называемой «многомерной релейной защиты» [6] и «релейной защиты с упреждающими функциями» [8], действующей на основе ее собственного накопленного ранее опыта, ее соб-

Рис. 1

ственного анализа текущего состояния защищаемого объекта и прогнозирования его будущего состояния. По существу, речь идет уже о возможности совершенно непредсказуемых действий релейной защиты, как самостоятельного Разума, принимающего самостоятельные (заранее не детерминированные) решения и способного самостоятельно производить изменения режимов работы энергосистемы (посредством выключателей) еще до наступления аварийных режимов [9].

Необходимо подчеркнуть, что в развитии технологий диагностики и прогнозирования состояния электрооборудования с использованием компьютерных технологий нет ничего плохого и его можно было бы только приветствовать, если бы его не пытались «скрестить» с релейной защитой.

Помимо опасности потери контроля над действиями релейной защиты, современные тенденции ее развития резко повышают опасность хакерских атак на энергосистемы, поскольку через компьютеризированные системы релейной защиты имеется возможность изменять состояние и воздействовать на режимы работы энергосистемы. Несмотря на серьезную озабоченность специалистов этой проблемой [10], тенденция все большей и большей подверженности энергосистем хакерским атакам лишь увеличивается.

Еще одной серьезной угрозой устойчивости энергосистем, основывающейся на современных тенденциях ее развития, является развитие технологий искусственного преднамеренного деструктивного воздействия на электронную и компьютерную аппаратуру, рис. 1, [11–17]. Развитию этих технологий во всем мире способствуют, с одной стороны, все большее распространение микропроцессорных технологий и элементов памяти, обладающих высокой чувствительностью к внешним электромагнитным излучениям и тенденция постоянного увеличения плотности элементов микроэлектроники за счет снижения толщины рабочих и изоляционных слоев в кристаллах, с другой стороны. Эти две направленные навстречу друг другу тенденции образуют весьма опасный вектор развития современной технологии. Более того, сегодня для создания устройства, способного уничтожить всю электронную аппаратуру у Вашего соседа, не нужно особых знаний и особой аппаратуры. В Интернете можно найти множество описаний таких устройств, выполненных на основе самых обычных бытовых микроволновых печей, рис. 2 [17].

Что же касается специальных «боевых»

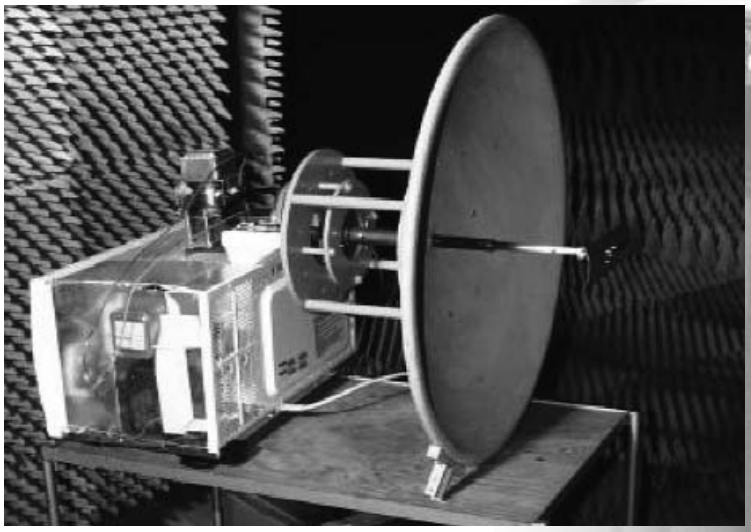

Рис. 2

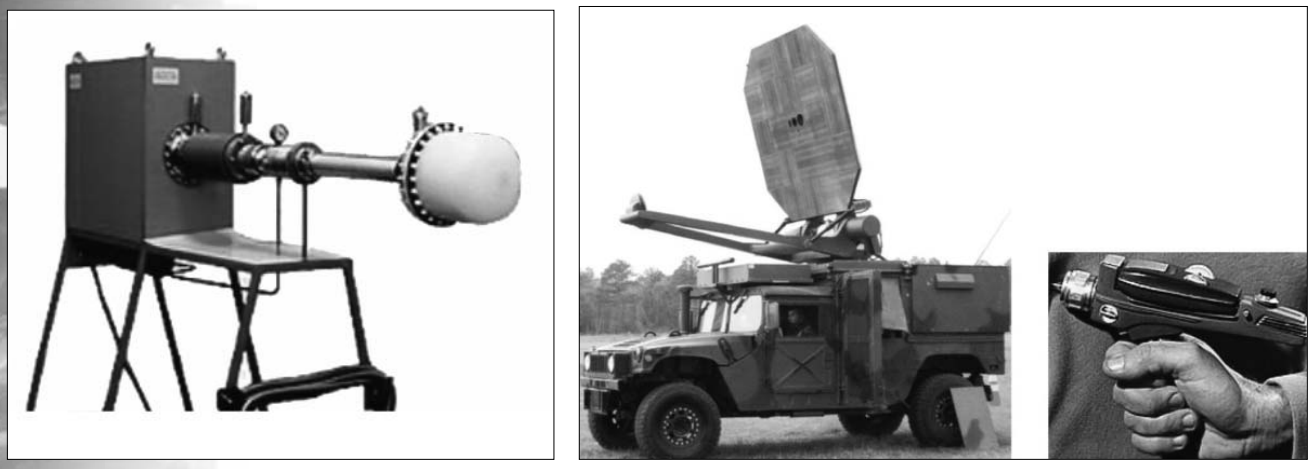

Рис. 2

устройств, то в этой области достигнуты весьма впечатляющие успехи, рис. 3. Компактные перевозимые импульсные генераторы ультраширокополостного излучения мощностью в миллиард Ватт, переносные излучатели в виде пистолета и ружья, взрывные устройства в виде портфеля-дипломата, уничтожающего при взрыве всю электронику вокруг себя в радиусе многих сотен метров, специальные боеприпасы и еще многое другое, направленное исключительно на дистанционное поражение электронной аппаратуры.

Так куда же мы движемся и к чему придем? Почему существующие тенденции остаются незамеченными специалистами? Очевидно, в сохранении такой тенденции имеется слишком много интересантов. Однако, более важным, на наш взгляд, является не вопрос о том, кто виноват, а вопрос о том, что делать.

В отличие от изолированных компьютерных систем измерения и мониторинга, релейная защита непосредственно связана с возможностью воздействия на режимы работы энергосистемы. В этом заключается главное и основополагающее отличие релейной защиты, от всех других компьютеризированных устройств и систем, используемых в электроэнергетике, которое обуславливает и необходимость иного подхода к релейной защите.

В приведенном выше тезисе и заключается, по нашему мнению, ответ на поставленный вопрос. А иной подход – это максимальное повышение надежности РЗ за счет отказа от использования в ней функций, не свойственных релейной защите, ограничение количества функций в одном МП терминале, отказ от использования алгоритмов с недетерминированной логикой, допускающих непредсказуемые действия релейной защиты, максимальное упрощение программного интерфейса, проведение специальных исследований и разработок, обеспечивающих функционирование релейной защиты в условиях преднамеренных деструктивных электромагнитных воздействий, например, за счет введения резервного комплекта РЗ при чрезвычайных ситуациях. На роль такого резервного комплекта РЗ, устойчивого к воздействию преднамеренных электромагнитных воздействий, не требующего оперативного питания и всегда готового к работе подходят лишь электромеханические реле. Поэтому, по нашему мнению, электромеханические реле еще рано списывать со счетов. Наоборот, их необходимо совершенствовать за счет использования новых технологий и материалов и обновлять их номенклатуру.

Поскольку алгоритмы собственно релейной защиты не такие уж и сложные (если все они могли быть с большой надежностью реализованы на электромеханике, составляющей сегодня свыше 90% всех реле защиты в России), то это означает, что современные защиты могут быть максимально простыми. Никаких новых функций в релейной защите с началом использования МУРЗ не появилось, а были лишь улучшены некоторые характеристики РЗ, в частности у дистанционных защит появилась полигональная характеристика вместо круговой характеристики старых электромеханических реле. Поэтому никаких объективных причин для существенного усложнения функций релейной защиты, наблюдаемого сегодня, в действительности не существует.

С другой стороны, в последнее время появляются все более сложные и совершенные системы мониторинга режимов работы электрооборудования на основе постоянного

контроля электрических характеристик (тангенса угла диэлектрических потерь, частичных разрядов в изоляции, тока утечки разрядников, количества и качественного состава газов, растворенных в трансформаторном масле и т.п.) и прогнозирования развития процессов во времени. Все более сложными становятся системы АСУТП, системы измерения в реальном времени векторных значений токов, напряжений и мощностей, системы регистрации и осциллографирования аварийных режимов и т.д. В отличие от релейной защиты все эти системы не могут непосредственно воздействовать на режим работы энергосистем и поэтому никаких ограничений в тенденциях их развития не существует.

Назначением релейной защиты может быть, по нашему мнению, только непосредственно релейная защита (то есть выявление аварийного режима и выдача команды на электрические аппараты, производящие изменения режима работы защищаемого объекта с целью ликвидации аварийного режима) и не более того. Все остальные проблемы должны решаться другими, независимыми от релейной защиты системами. Поэтому дальнейшее развитие микропроцессорной релейной защиты и других микропроцессорных и компьютерных систем в электроэнергетике должно происходить независимыми параллельными курсами, не связанными между собой.

Для того, чтобы пресечь произвол производителей, навязывающих энергетикам все более «навороченные» и все менее надежные МУРЗ [18,19], необходимо, по нашему мнению, сформулировать основные требования к принципам конструирования МУРЗ (не к техническим параметрам, а именно к принципам конструирования) в соответствующем стандарте. В эти же принципы могли бы войти и высказанные ранее предложения [20] по конструктивному исполнению МУРЗ в виде набора отдельных универсальных по функциям, размерам и контактным присоединениям заменяемых модулей (печатных плат) по аналогии с персональными компьютерами.

Литература

1. *Гуревич В. И.* Цена прогресса // Компоненты и технологии. – 2009. – № 8.

2. *Шнеерсон Э. М.* Цифровая релейная защита. – М.: Энергоатомиздат, 2007.

3. *Bittencourt A., M. R. de Carvalho, Rolim J. G.* Adaptive Strategies in Power Systems Protection using Artificial Intelligence Techniques. – The 15th International Conference on Intelligent System Applications to Power Systems, Curitiba, Brazil November 8–12, 2009.

4. *Laughton M. A.* Artificial Intelligence Techniques in Power Systems, In book "Artificial intelligence techniques in power systems", The Institution of Engineering and Technology, 1997, p. 1–18.

5. *Khosla R., Dillion T.* Neuro-Expert System Applications in Power Systems. – In book "Artificial intelligence techniques in power systems", The Institution of Engineering and Technology, 1997, 238 – 258.

6. *Лямец Ю.Я., Кержаев Д.В., Нудельман Г.С., Романов Ю.В.* Многомерная релейная защита: Тезисы докладов Второй Междунар. науч.-техн. конф. «Современные направления развития систем релейной защиты и автоматики энергосистем», Москва 7–10 сентября 2009 г.

7. *Камель Т.С., Хассан М.А., Эль-Моршеди А.* (Cairo University, Египет) Применение систем искусственного интеллекта в дистанционной защите линии электропередачи: Тезисы докладов Второй Междунар. науч.-техн. конф. «Современные направления развития систем релейной защиты и автоматики энергосистем», Москва 7–10 сентября 2009 г.

8. *Булычев А., Нудельман Г.* Релейная защита. Совершенствование за счет упреждающих функций // Новости электротехники». – 2009. – № 4(58).

9. *Гуревич В. И.* Сенсационные «открытия» в области релейной защиты // Энергетика и промышленность России. – 2009. – № 23-24 (139-140).

10. *ЦРУ:* Хакинг электрических сетей возможен. CNews.ru: Лента новостей. 24.01.2008, (http://www.cnews.ru/news/line/index.shtml?2008/01/24/285018).

11. *Гуревич В.И.* Электромагнитный терроризм – новая реальность 21 века // Мир техники и технологий. – 2005. – № 12. – С.14 –15.

12. *Daamen D.* Avant-garde Terrorism: Intentional Electro Magnetic Interference, 2002. – 23 p.

13. 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).

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

15. *Лоборев В., Парфенов Ю., Фортов В.* Коллапс бесшумного взрыва // Литературная Газета, № 5 (5865), 6–12 февраля 2002 г.

16. *Покровский В.* Электромагнитный фактор // Независимая Газета, 08. 10. 2003.

17. Backstrom M. Is Intentional EMI a Threat Against the Civilian Society?, SAAB Communication, 2006.

18. *Гуревич В.* Надежность микропроцессорных устройств релейной защиты: мифы и реальность // Проблемы энергетики. – 2008. – № 5–6. – С. 47–62.

19. *Гуревич В. И.* Еще раз о надежности микропроцессорных устройств релейной защиты // Электротехнический рынок. – 2009. –№ 3 (29). – С. 40–45.

20. *Гуревич В. И.* Микропроцессорные реле защиты: в поисках оптимальности // Энергетика и промышленность России. – № 21 (137) ноябрь 2009 г.