

В последние 15–20 лет во всем мире наблюдается повсеместное вытеснение электромеханических реле защиты микропроцессорными устройствами релейной защиты (МУРЗ). МУРЗ и многочисленные программируемые логические контроллеры, управляющие режимами работы электроэнергетического оборудования, прочно вошли в нашу жизнь, и во многих случаях без них уже невозможно обеспечить нормальное функционирование электроэнергетического комплекса.

Но так ли безоблачна ситуация с точки зрения безопасности энергосистем? Об этом рассуждает Владимир Игоревич Гуревич.

ТЕХНИЧЕСКИЙ ПРОГРЕСС В РЕЛЕЙНОЙ ЗАЩИТЕ

Опасные тенденции развития РЗА

Дешевизна и доступность микропроцессоров (МП), промышленных контроллеров и современных электронных компонентов высокой степени интеграции, чрезвычайно высокая производительность оборудования, предназначенного для автоматической установки и распайки элементов поверхностного монтажа на печатную плату, автоматические системы тестирования готовых печатных плат – все это снимает имевшиеся ранее ограничения на сложность электронных систем и область их применения.

Применение электронных узлов на основе МП во всех областях техники при непрекращающемся их усложнении является сегодня определяющей тенденцией развития, которую принято называть «прогрессом в развитии техники и технологии».

Конечно, есть такие области жизнедеятельности человечества, в которых без вычислительных операций и без МП просто не обойтись. Однако далеко не во всех случаях применение микропроцессорной техники реально обосновано техническими требованиями к изделию.

Тенденция снижения надежности релейной защиты, связанная с переходом на МУРЗ, замеченная в самом начале этого процесса, прослеживается и до сих пор, несмотря на то, что современные поколения МУРЗ имеют мало общего с самими первыми образцами.

Занимаясь эксплуатацией и ремонтом сложных электротехнических устройств промышленного назначения, таких как релейная защита, мощные зарядные устройства, инверторы и конверторы, источники бесперебойного питания и т.п., я начал сомневаться в том, что упомянутая выше тенденция и есть «технический прогресс».

Наблюдаемый сегодня бум усложнения аппаратуры и расширения применения микропроцессоров во всех областях техники, на мой взгляд, связан не столько с реальными потребностями, сколько со стремлением производителей превзойти конкурентов любой ценой, получить сверхприбыль.

Само по себе желание создать какой-либо новый продукт или снизить затраты на производство можно было бы только приветствовать, если бы тенденция замены хорошо зарекомендовавших себя безупречной работой в течение десятков лет аналоговых систем на дискретных электронных компонентах микропроцессорными устройствами не приводила к существенному усложнению электротехнического оборудования, его неремонтопригодности, снижению надежности, резкому повышению затрат на эксплуатацию.

При заказе оборудования все эти проблемы остаются в тени, и сталкиваются с ними лишь с началом эксплуатации оборудования. Это и есть та цена, которую потребителям приходится платить за так называемый «технический прогресс», то есть бездумное и безответственное усложнение электротехнического оборудования, осуществляемое часто без всяких на то оснований и лишь в угоду технической моде и погоней производителей за прибылью. Более подробно эта проблема освещена в [1].



Владимир Гуревич,
к.т.н., начальник сектора
Центральной электрической
лаборатории Электрической
компании Израэля,
г. Хайфа

SMART GRID

Не осталось уже, наверное, ни одного средства массовой информации, не написавшего восторженных од в честь так называемых «интеллектуальных сетей» (Smart Grid), выдаваемых за последний писк технической моды, сулящий невиданные ранее блага. Оказывается, что не только микропроцессорные счетчики электроэнергии, но даже электропечные трансформаторы, устройства компенсации реактивной мощности, сверхпроводящие силовые кабели и т.д. и т.п. – всё это элементы «умной сети», под развитие производства которых нужны деньги. И вот уже образуются государственные целевые инвестиционные программы, выделяются миллиардные инвестиции и начинает крутиться огромный механизм по «отсасыванию» и распылению средств из государственных бюджетов под направление, которому никто толком даже не может дать четкого и понятного определения.

Известно, однако, что «умная сеть» предполагает установку МП на все без исключения элементы системы производства, распределения и учета электроэнергии и организацию между ними информационных каналов на основе компьютерных сетей, преимущественно беспроводных (Wi-Fi). По идее аполетов Smart Grid энергосистема будущего должна выглядеть как современная сетевая компьютерная игра с тысячами участников, в роли которых выступают компоненты электрических сетей. А если добавить сюда еще миллионы квартирных счетчиков электроэнергии, объединенных в общую сеть? Тогда станет понятной как грандиозность, так и опасность этой затеи, ведь резко возрастет уязвимость электроэнергетической системы к хакерским атакам, компьютерным вирусам и преднамеренным деструктивным дистанционным электромагнитным воздействиям (ПДДВ).

Увы, эти опасности мало заботят ученых и инженеров, получающих зарплаты из фондов развития «умных сетей». От них часто приходится слышать заявления такого рода: наша задача развивать технический прогресс, а заботиться о защите безопасности национальной электроэнергетики – это прерогатива других органов. Ущербность и недалекость такой идеологии очевидна.

ПРОБЛЕМЫ РАЗВИТИЯ МУРЗ

В многочисленных моих публикациях (полные версии материалов выложены на сайте <http://www.gurevich-publications.com>) неоднократно обращалось внимание на опасность некоторых тенденций в развитии релейной защиты, усиленно пропагандируемых разработчиками и производителями МУРЗ. Речь идет о следующем:

1. Снижение надежности релейной защиты по мере расширения применения МУРЗ.
2. Непрерывное усложнение МУРЗ и увеличение концентрации защитных функций в одном терминале.
3. Навешивание на МУРЗ несвойственных релейной защите функций, например, мониторинг электрооборудования.

4. Использование в МУРЗ недетерминированной логики, обуславливающей опасность потери контроля над действиями релейной защиты.
5. Расширение использования в МУРЗ свободнопрограммируемой логики, сопровождающееся значительным увеличением процента ошибок персонала и неправильных действий защит [2].
6. Усложнение проверок исправности и вообще эксплуатации релейной защиты по мере накопления в одной энергосистеме множества типов МУРЗ разных производителей, закупаемых по тендерам и отличающихся между собой как конструкцией, так и программным обеспечением. Отсутствие стандартов, оговаривающих единые универсальные требования к конструкции и к программному обеспечению МУРЗ, увеличивает интеллектуальную нагрузку на персонал и приводит к значительным экономическим потерям.
7. Существенное ослабление электромагнитной защищенности релейной защиты и в целом энергосистемы по мере расширения использования МУРЗ.
8. Повышение уязвимости энергосистем к хакерским атакам по мере расширения применения микропроцессорной техники и при использовании более дешевых сетей Ethernet и Wi-Fi вместо относительно защищенных оптоэлектронных кабелей в системах релейной защиты.

МНЕНИЯ СПЕЦИАЛИСТОВ

После периода весьма бурной критической реакции на публикации автора и полного отрицания негативных последствий перечисленных выше тенденций в развитии релейной защиты, в последние годы появляется понимание сформулированных ранее мною проблем многими специалистами.

Так, например, В. Morris, R. Moxley, С. Kusch (Schweitzer Engineering Laboratories, США) на Второй Международной конференции «Современные направления развития систем релейной защиты и автоматики энергосистем» (Москва, 7–10 сентября 2009 г.) [3] поставили под сомнение необходимость всё большего усложнения защит, аргументируя это сравнительными оценками надежности защит на основе простых электромеханических реле и многофункциональных микропроцессорных систем защиты. Они заявили о выявленной ими тенденции снижения надежности систем релейной защиты, построенных на основе всё более усложняющихся микропроцессорных устройств.

О недостаточной надежности МУРЗ говорил также В.И. Пуляев (ФСК ЕЭС, Россия) на Третьей Международной конференции «Современные направления развития систем релейной защиты и автоматики энергосистем» (Санкт-Петербург, 30 мая – 3 июня 2011 г.) [4]. Он отметил, в частности, что значительная доля сбоев релейной защиты приходится на микропроцессорные устройства (примерно 23% из всех случаев), которые составляют всего около 10% от общего количества устройств защиты. Это, безусловно, один из важнейших факторов, определяющих необходимость принятия специальных мер по повышению надежности МУРЗ.

Ныне покойный А.И. Шалин (д.т.н., профессор кафедры электрических станций Новосибирского государственного технического университета) писал в [5] о том, что процент неправильных действий современных панелей и шкафов РЗ часто оказывается существенно выше, чем старых защит, выполненных на электромеханических реле, а статистические данные подтверждают факт существенного снижения эффективности и надежности при переходе от защит, выполненных на электромеханических реле, к микропроцессорным терминалам.

J. Stokoe и J. Gray в своем докладе на 7-й Международной конференции «Developments in Power Systems Protection» (Амстердам, 9–12 апреля 2001 г.) говорили, что старые электромеханические реле были прочными и долговечными устройствами со сроком службы 25 лет, тогда как срок службы современных микропроцессорных защит составляет 15 лет и менее. Им вторили J. Polimas и А. Rahim (PB Power, United Kingdom), утверждавшие, что при переходе от электромеханических реле к микропроцессорным срок службы защит уменьшился с 40 лет (для электромеханики) до 15–20, а иногда и вообще до нескольких лет после введения в эксплуатацию (для МУРЗ) [6].

Руководитель компьютерного отделения Инженерно-технологического колледжа (University of Poona, Maharashtra, India) Ashok Kumar Tiwari В. Е. отмечал, что объединение в одном микропроцессорном терминале множества функций резко снижает надежность релейной защиты, поскольку при отказе этого терминала будет утеряно сразу слишком много функций по сравнению со случаем, когда эти функции распределены среди нескольких терминалов [6].

О необходимости ограничения количества функций, реализуемых в одном терминале МУРЗ, говорили также в своем докладе на упомянутой выше Третьей Международной конференции «Современные направления развития систем релейной защиты и автоматики энергосистем» В.А. Ефремов и С.В. Иванов (ИЦ «Бреслер»), Д. В. Шабанов (ФСК ЕЭС России).

А. Федосов и Е. Пусенков (филиал ОАО «СО ЕЭС» ОДУ Сибири) в [7] отмечали отсутствие универсальных жестких требований к аппаратной части МУРЗ и к программному обеспечению и вследствие этого слишком большое многообразие программ и алгоритмов, заложенных в МУРЗ, используемых в одной энергосистеме, что приводит к проблемам при эксплуатации и к увеличению вероятности ложной работы данных устройств.

О резком повышении уровня сложности работ персонала, обслуживающего релейную защиту с переходом от электромеханики к МУРЗ, как о причине тяжелых аварий в энергосистемах писали также D. Rayworth и М. А. Rahim (PB Power, UK) [6].

Сложность программного интерфейса и необходимость введения чрезмерного количества уставок при программировании МУРЗ отмечали А. Беляев, В. Широков и А. Емельянец (Специализированное управление «Леноргэнергогаз», г. Санкт-Петербург) в [8].

О неудовлетворительном состоянии электромагнитной обстановки на большинстве старых подстанций, которые проектировались и строились под электромеханическую релейную защиту, а не под микропроцессорную, и о возникающих из-за этого многочисленных сбоях в работе МУРЗ, на различных конференциях говорили А.М. Бордачев (ОАО «Институт Энергосетьпроект»), М. Матвеев и М. Кузнецов (ООО «ЭЗОП»), Р. Борисов (НПФ «ЭЛНАП») и другие специалисты. Они отмечали, что чувствительность к электромагнитным помехам устройств релейной защиты на микропроцессорной элементной базе на несколько порядков выше, чем у их традиционных электромеханических аналогов, и поэтому для обеспечения электромагнитной совместимости (ЭМС) вторичных цепей необходимо резко повысить уровень их электромагнитной защиты. Без проведения комплекса работ по обеспечению ЭМС невозможно достигнуть приемлемых характеристик надежности МУРЗ.

КИБЕРПРОБЛЕМА

С проблемой низкой устойчивости МУРЗ к электромагнитным помехам тесно связана еще более сложная и тяжелая проблема преднамеренных дистанционных деструктивных воздействий на МУРЗ, на которую мы впервые обратили внимание специалистов в [9].

Сегодня во многих странах мира уже разработана аппаратура, способная дистанционно вывести из строя любые микропроцессорные системы промышленного назначения (включая и МУРЗ, естественно), поэтому этой проблеме посвящены не только многочисленные публикации в технических журналах таких известных специалистов, как Manuel W. Wik (Defence Materiel Administration, Sweden) и William A. Radasky (Metatech Corporation, USA), но также и отчеты специальных комиссий при Конгрессе США [10].

Парализация систем управления, масштабные отключения целых энергосистем, хаос в системах контроля, отключение интернета и сотовой связи – так, по мнению американских ученых, выглядит сценарий последствий кибернетической атаки. Причем, учитывая стратегическую важность такого объекта, как энергосистемы, заниматься атаками будут уже не хакеры-одиночки, а специальные военные кибернетические подразделения, уже созданные во многих странах мира.

В прошлом году при Агентстве национальной безопасности США – одной из самых могущественных и засекреченных спецслужб мира, возглавляемой генералом К. Александером, – было создано отдельное Киберкомандование, объединившее все существовавшие ранее подразделения киберзащиты Пентагона. ▶

► Еще год назад в системе Киберкомандования работало около тысячи человек, но после объявления о начале масштабной программы рекрутирования специалистов соответствующего профиля численность этой структуры АНБ должна увеличиться до 10 тысяч человек. Часть из них будут обеспечивать безопасность не только военной и государственной инфраструктуры, но и наиболее важных коммерческих объектов страны.

Нынешний глава Киберкомандования заявил на слушаниях Комитета по делам Вооруженных сил США палаты представителей конгресса, что кибероружие имеет эффект, сравнимый с эффектом применения оружия массового уничтожения.

Многие страны, включая США, Россию, Китай, Израиль, Великобританию, Пакистан, Индию, Северную и Южную Корею, уже создали сложное кибероружие, которое может неоднократно проникать в компьютерные сети и способно разрушать их, утверждают специалисты по кибербезопасности.

В 2010 г. кибербюджет США составил 8 млрд долларов, и в последующем он будет только возрастать. В 2011 г. США планируют принять новую доктрину кибербезопасности. О ее направленности можно судить по опубликованной в сентябре программной статье заместителя главы Пентагона Уильяма Линна III с символическим названием «Защищая новое пространство». Ее главная мысль такова, что отныне США будут считать киберпространство таким же потенциальным полем боя, как сушу, море и воздух.

Параллельно над созданием концепции коллективной киберобороны начали работать и в НАТО. На ноябрьском 2010 г. саммите альянса было решено разработать «План действий в области киберобороны». Важное место в нем отведено созданию центра НАТО по реагированию на киберинциденты.

Об эффективности кибероружия можно судить по широко известной кибератаке на Иранский центр по обогащению урана в Натанзе с помощью компьютерного червя Win32/Stuxnet.

Еще одна масштабная атака на японскую корпорацию Mitsubishi Heavy Industries, занимающуюся разработкой и производством различных типов военной техники, произошла в сентябре 2011 г. Компьютерное оборудование корпорации (45 закрытых серверов и около 50 ПК) оказалось заражено целым набором вирусов, которые полностью взяли его под контроль. Они позволяли управлять компьютерами со стороны, перемещать имеющуюся на них информацию, давали возможность активизировать встроенные в компьютеры микрофоны и камеры, что позволяло злоумышленникам на расстоянии следить за происходящим в рабочих и исследовательских помещениях. Информация со взятых под контроль компьютеров перекачивалась на 14 сайтов на территории Китая, Гонконга, США, Индии.

Современные технологии позволяют запускать в компьютерную систему вирусы дистанционно в виде кодированного радиоизлучения с помощью беспилотных летательных аппаратов-ретрансляторов. Особенно уязвимы к таким проникновениям извне беспроводные системы Wi-Fi, на основе которых и планируется создание систем Smart Grid.

В прошлом уже были зарегистрированы и попытки компьютерного проникновения в энергосистему Израиля, предпринятые Ираном. Старший аналитик ЦРУ США Том Donahue заявил на встрече правительственных чиновников и сотрудников американских компаний, владеющих системами электро-, водо-, нефте- и газоснабжения, об известных ЦРУ многочисленных попытках проникновения в энергосистемы США.

Очевидно, можно констатировать, что кибернетические войны уже начались и их интенсивность со временем будет лишь нарастать, в то время как уязвимость энергосистем при существующих ныне тенденциях будет увеличиваться.

ЧТО ДЕЛАТЬ?

Таким образом, сегодня уже нельзя продолжать закрывать глаза на существование целого клубка проблем, связанных с распространением МУРЗ.

Пора положить конец процессу бесконтрольного развития непроверенных и опасных тенденций в релейной защите и системах автоматизации, включая Smart Grid.

Для этого необходимо создание специального Координационного совета по релейной защите и интеллектуальным сетям, который должен заниматься анализом существующих тенденций, выработкой национальной стратегии и координацией

стандартизации в этих областях. В состав Совета должны войти независимые эксперты и специалисты в области релейной защиты, микроэлектроники, защиты информации, электромагнитной совместимости, не имеющие экономических связей с предприятиями – разработчиками и производителями МУРЗ или элементов Smart Grid.

Следует иметь в виду, что меркантильные финансовые интересы отдельных специалистов и даже целых научных и производственных коллективов, заинтересованных в финансировании любых новых цифровых технологий в области электроэнергетики, и в частности в области релейной защиты, независимо от отдаленных последствий использования этих технологий, не ограниченных какими бы то ни было рамками, могут привести в недалеком будущем к национальным катастрофам.

Новые технологии в области релейной защиты, автоматизации, систем связи и передачи данных не должны внедряться в эксплуатацию до тех пор, пока:

- не будут всесторонне рассмотрены возможные отрицательные последствия их широкого распространения с учетом уже накопленного опыта;
- не будут разработаны эффективные меры защиты от ПДДВ, будь то хакерские атаки или преднамеренные электромагнитные воздействия.

Разработке мер защиты чувствительной электронной аппаратуры, применяемой в электроэнергетике, от ПДДВ должно уделяться не меньшее внимание и должны выделяться не меньшие средства, чем на разработку новых технологий, таких как Smart Grid.

Никакая новая технология, основанная на использовании цифровой микроэлектроники, не может считаться совершенной и готовой к применению в электроэнергетике без разработки мер ее защиты от ПДДВ. В новые стандарты по микропроцессорной релейной защите обязательно должны войти требования по защите от ПДДВ, поскольку имеющиеся сегодня нормативно-технические документы в области ЭМС отражают требования по устойчивости аппаратуры лишь к естественным, а не к преднамеренным разрушающим электромагнитным воздействиям. Необходимо тщательно изучить пути повышения надежности функционирования МУРЗ за счет резервирования ее современными гибридными реле [11].

По моему мнению, только в таком направлении должен дальше развиваться технический прогресс в важнейшей области – электроэнергетике, основе национальной инфраструктуры любой страны.

ЛИТЕРАТУРА

1. Гуревич В. И. Цена прогресса // Компоненты и технологии. 2009. № 8.
2. Гуревич В. И. Логика в свободном полете // PRO Электричество. 2011. № 2.
3. Булычев А.В. Конференция по развитию РЗА энергосистем. Интеллектуальные возможности релейной защиты // Новости ЭлектроТехники. 2009. № 4(58).
4. Булычев А.В. Системы релейной защиты и автоматизации. Направления развития обсуждали в городе на Неве // Новости ЭлектроТехники. 2011. № 3(69).
5. Шалин А.И. Микропроцессорные реле защиты: необходим анализ эффективности и надежности // Новости ЭлектроТехники. 2006. № 2(38).
6. Проблемы микропроцессорных устройств релейной защиты – <http://digital-relay-problems.tripod.com>.
7. Федосов А., Пусенков Е. Проблемы, возникающие при внедрении микропроцессорной техники в системах противоаварийной автоматизации // Электрические станции. 2009. № 12.
8. Беляев А., Широков В., Емельянец А. Цифровые терминалы РЗА. Опыт адаптации к российским условиям // Новости ЭлектроТехники. 2009. № 5(59).
9. Гуревич В. И. Актуальные проблемы релейной защиты: альтернативный взгляд // Вести в электроэнергетике. 2010. № 3.
10. Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack. 2008.
11. Гуревич В. И. Перспективы применения гибридной технологии в релейной защите и автоматике // Компоненты и технологии. 2011. № 10.