Владимир Гуревич
к.т.н., Электрическая компания Израиля

Уязвимость современной релейной защиты: поможет ли защита от кибератак?

Современные тенденции развития релейной защиты (РЗ), связанные с заменой электромеханических реле (ЭМРЗ) микропроцессорными устройствами (МУРЗ), обусловили появление совершенно новой проблемы, не известной ранее в этой области. Такой проблемой является возможность преднамеренного дистанционного деструктивного воздействия (ПДДВ) на релейную защиту с целью выведения ее из строя или принудительного выполнения операций, не связанных с текущим режимом работы защищаемого электрооборудования. В структуре современной энергосистемы МУРЗ являются самым критичным звеном [1], которое, с одной стороны, наиболее уязвимо к ПДДВ, а с другой — непосредственно связано с силовыми коммутационными аппаратами, влияющими на состояние энергосистемы. Поэтому именно на МУРЗ и направлены в первую очередь ПДДВ в виде кибератак [2] и преднамеренных электромагнитных деструктивных воздействий (ПЭДВ) [3, 4].

Как известно, у реле защиты имеется два вида отказов: так называемые несрабатывания и излишние срабатывания (которые в данном контексте равноценны ложным срабатываниям). Как показано в [1, 2], излишние (ложные) срабатывания РЗ могут привести к значительно более тяжелым авариям, чем несрабатывания. Это, в частности, объясняется тем, что несрабатывания защиты какого-то определенного типа дублируется защитами других типов или более удаленными защитами, защитами других ступеней, в то время как излишние срабатывания РЗ предотвратить существующими сегодня средствами практически невозможно. Этот тезис не является чем-то неожиданным и встречался ранее у других авторов [4]. При этом, как показано в [1], возникает совершенно новая ситуация, при которой неисправное реле защиты в результате излишнего срабатывания может выдать ложную команду на отключение выключателя и тем самым искусственно прервать нормальное функционирование системы электроснабжения. При этом не только остаются без электроэнергии тысячи потребителей, что сопряжено с большим ущербом, сопоставимым по своим последствиям с аварийным режимом в системе электроснабжения, но и возникает опасность крупной системной аварии, вызванной внезапными перетоками мощностей при таком отключении в сложной и разветвленной энергосистеме. Как показано в [5], в 25—28% случаев причиной крупнейших системных аварий в мире были отказы РЗ. А если добавить к этому, что в 50—70% случаев перехода обычного аварийного режима в тяжелую системную аварию повинна также РЗ [5], то получается, что именно РЗ ответственна практически за все системные сбои. Интересные количественные данные в подтверждение сказанного были недавно приведены в докладе представителей фирмы ОРГРЭС из Москвы [6]: *«В 2012 г. было зафиксировано 53 214 случаев срабатывания устройств РЗА на объектах ЕНЭС. Из*

них правильных срабатываний было 52763 (99,15%), неправильных — 451, включая 213 излишних, 160 ложных срабатываний и 76 отказов в срабатывании… В 2012 г. основной показатель правильной работы МП РЗА составил 98,97%, что ниже основного обобщенного показателя правильной работы электромеханических устройств РЗА (99,31%)».

Из этих данных следует, во-первых, что количество ложных и излишних срабатываний (373) в обычных условиях эксплуатации (т.е. без преднамеренных дистанционных деструктивных воздействий) намного превышает число отказов в срабатывании (76), а во-вторых — современные МУРЗ менее надежны, чем старые и изношенные ЭМРЗ.

Специальные исследования, проведенные комитетом *B5* СИГРЭ и представленные в его отчете, подтвердили актуальность проблемы и вывод о том, что с широким применением самого современного стандарта *IEC 61850* с его *GOOSE*-сообщениями и современных сетевых технологий *Ethernet* в РЗ ее уязвимость к кибератакам возрастает [7]. Осознание необходимости кибербезопасности МУРЗ в последние годы привело к интенсификации многочисленных исследовательских работ в этой области во всем мире. Например, в США под руководством главы АНБ генерала А. Кейта эти вопросы курирует огромное подразделение, состоящее из нескольких тысяч человек [8], в России — специальное подразделение ФСБ. Существуют и Указы Президента РФ «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ» и «Основы государственной политики РФ в области международной информационной безопасности на период до 2020 г.», которые прокомментированы специалистами как ответ на принятую в 2011 г. США Международную стратегию по действиям в киберпространстве [9]. В ней США впервые приравняли акты компьютерных диверсий к традиционным военным действиям, оставив за собой право реагировать на них всеми средствами вплоть до применения ядерного оружия. По сообщениям из печати известно, что в Израиле проблемы кибербезопасности энергосистемы страны совместно со специалистами самой энергокомпании решает особое подразделение в Службе общей безопасности — *Israel Security Agency* (ШАБАК). Не так давно в головном российском институте — ВНИИ релестроения был также создан отдел, занимающийся специфическими проблемами кибербезопасности РЗ. По данным *Gartner,* в 2013 г. объем мирового рынка кибербезопасности увеличится до 67,2 млрд долл. против 61,8 млрд долл. в 2012 г. К 2016 г. оборот достигнет 86 млрд долл.

Так что же такое кибербезопасность? Анализ многочисленных публикаций на эту тему показывает, что под этим термином обычно понимается информационная безопасность. Следует учитывать, что словосочетание «информационная безопасность» в разных контекстах может иметь более узкий или широкий смысл. В широком смысле это подразумевает весь комплекс организационных и технических мер обеспечения безопасности. Виды информационной безопасности условно подразделяются на пассивные и активные. Под пассивным риском подразумевается опасность внеправового использования информационных ресурсов без нарушения работы информационной системы. К пассивному риску можно отнести, например, доступ к базе данных или прослушивание каналов передачи информации. Под активным риском подразумевается опасность сбоя в действующей информационной системы путем целенаправленной атаки на ее компоненты. Активными видами угрозы компьютерной безопасности являются, например, физический вывод из строя компьютера или нарушение его работоспособности, а также умышленное вмешательство в нормальный алгоритм функционирования оборудования, управляемого компьютером. Типичный пример — небезызвестный вирус *Stuxnet* [8]. Мы будем подразумевать под информационной безопасностью технику защиты информации от преднамеренного или случайного несанкционированного доступа и нанесения тем самым вреда нормальному процессу обмена данными в системе, а также хищения, модификации и уничтожение информации.

Основные проблемы, на которые приходится обращать внимание в сфере инженерно-технической защиты информации:

- перехват электронных излучений и электрических сигналов;
- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей;
- применение подслушивающих устройств;
- дистанционное фотографирование;
- перехват акустических излучений и восстановление текста, отправленного на принтер;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- маскировка под запросы системы;
- использование программных ловушек;
- использование недостатков языков программирования и операционных систем;
- незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- злоумышленный вывод из строя механизмов защиты;
- расшифровка специальными программами закодированной информации;
- информационные инфекции (вирусы различного типа, в том числе «логические бомбы», «троянские кони», «черви», «перехватчики паролей» и т.п.).

В качестве мер информационной безопасности применяются обычно следующие средства.

1. Сетевой экран (нем. *brandmauer* или англ. *firewall*) — комплекс аппаратных или программных средств, осуществляющих контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. При этом обеспечивается:
   - фильтрация доступа к заведомо незащищенным службам;
   - препятствие получению закрытой информации из защищенной подсети, а также внедрению в защищенную подсеть ложных данных с помощью уязвимых служб;
   - контроль доступа к узлам сети;
   - регистрация всех попыток доступа как из внешней, так и из внутренней сети;
   - регламентирование порядка доступа к сети;
   - уведомление о подозрительной деятельности, попытках зондирования или атаки на узлы сети или сам экран.
2. Антивирусные программы, предназначенные для обнаружения компьютерных вирусов, а также вредоносных программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом. Обнаружение вирусов основано обычно на сравнении кодов просматриваемых антивирусной программой с известными кодами (сигнатурой) вредоносных программ, имеющихся в библиотеке антивирусной программы. В последнее время активно развиваются и так называемые проактивные технологии антивирусной защиты, главной целью которых в отличие от реактивных (сигнатурных) технологий является предотвращение заражения системы пользователя, а не поиск уже известного вредоносного программного обеспечения в системе.
3. Криптографические методы защиты информации, т.е., по сути, кодирование и шифрование информации, ключи доступа, специальные протоколы аутентификации сети и пользователя.

Эти общеизвестные технические меры можно дополнить некоторыми специфическими мерами, принятыми в микропроцессорной РЗ. Одна из них — отказ от использования общих информационных шин (шин процессов), поскольку атака на такую шину является наиболее простым и действенным средством, способным нарушить работу целой подстанции. Вместо таких шин применяют также множественные соединения типа «точка — точка», что позволяет вводить более устойчивые к атакам коммуникационные протоколы (включая одностороннюю передачу данных). Эти и многие другие специфические меры защиты РЗ, касающиеся в основном защиты протоколов передачи данных, повышения криптостойкости паролей и т.п., подробно рассмотрены в [10].

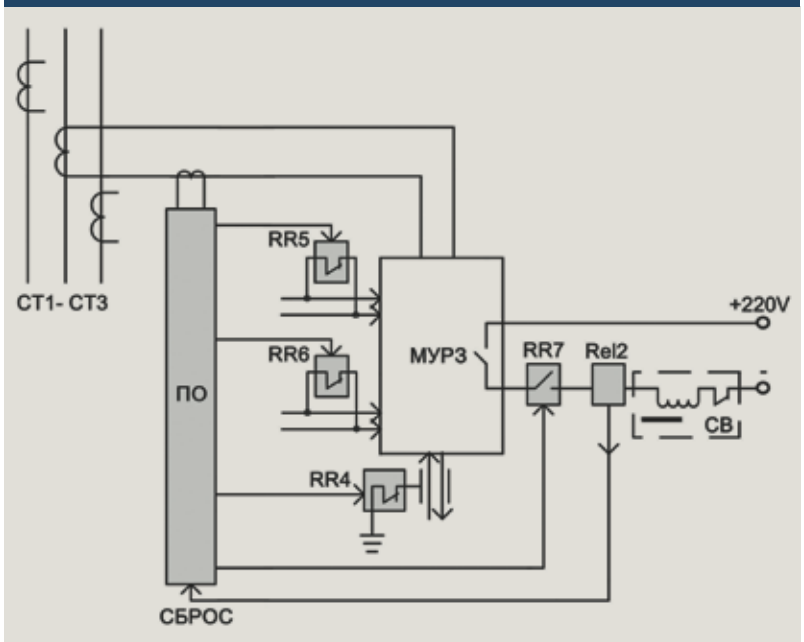
А сейчас главный вопрос: являются ли все эти общепринятые меры информационной безопасности достаточными для обеспечения надежности микропроцессорной РЗ? Наш ответ — нет: традиционными и хорошо известными методами обеспечения информационной безопасности невозможно полностью исключить несанкционированные действия РЗ. Причем речь идет не о том, что какие-то способы защиты пока еще недостаточно эффективны (что на самом деле имеет место), а о принципиальной невозможности такой защиты. Из приведенного выше анализа следует, что все известные технические меры защиты информации направлены на защиту информационных каналов связи от несанкционированного доступа и самой информации от кражи или порчи. Такие информационные каналы связи широко используются в микропроцессорной РЗ, и они, безусловно, должны быть надежно защищены. Но вот только ли через такие каналы можно заставить МУРЗ отключить выключатели и развалить сеть? Ведь, помимо информационных каналов связи, МУРЗ содержит большое количество так называемых дискретных входов (ДВ), чувствительных к присутствию или отсутствию напряжения. Это напряжение подается на ДВ с помощью контактов внешних электромеханических реле. Факт наличия или отсутствия напряжения на ДВ зашифровать или закодировать невозможно, да и конструкция ДВ в МУРЗ не предназначена для приема закодированной информации. Достаточно заранее модифицировать свободно-программируемую логику МУРЗ таким образом, чтобы при дистанционной подаче напряжения посредством какого-то внешнего реле на какой-то один заранее выбранный ДВ происходило срабатывание выходных реле МУРЗ, воздействующих на выключатели, и его можно будет использовать в определенный момент в качестве средства диверсии в энергосистеме. И никакие из рассмотренных выше мер защиты от кибератак здесь не помогут, потому что никакой кибератаки при таком воздействии на МУРЗ не было. С учетом того что, помимо указанных воздействий, весьма пагубное влияние на МУРЗ могут оказать также мощные направленные ультрашироколосные радиоизлучения и электромагнитный импульс [3], следует перейти от использования в РЗ термина «кибератака» к использованию термина «преднамеренные дистанционные деструктивные воздействия», включающему все виды преднамеренных деструктивных воздействий на РЗ. Такой переход представляется тем более обоснованным, поскольку разработанные нами технические решения направлены на высокоэффективную защиту МУРЗ от всех видов таких воздействий одновременно.

Что же предлагается для снижения уязвимости МУРЗ к ПДДВ?

Как уже было неоднократно показано ранее, задачу повышения на-

дежности РЗ невозможно решить при совмещении функций МУРЗ с функциями, не имеющими отношения к РЗ, например таких популярных, как мониторинг исправности электрооборудования, дистанционное управление выключателями и т.п. МУРЗ должны использоваться исключительно для целей РЗ. Тем более что для решения других задач, например мониторинга электрооборудования, сегодня на рынке имеется огромное количество специализированных устройств — от простейших реле, контролирующих целостность цепи отключающей катушки выключателя, до сложнейших комплексов, контролирующих в режиме реального времени состав газов, растворенных в масле трансформаторов, или уровень частичных разрядов в изоляции. Дистанционное управление выключателями должно быть отделено от РЗ и осуществляться отдельными аппаратными средствами, а не посредством МУРЗ. Только в этом случае можно повысить надежность РЗ и хорошо защитить ее от ПДДВ. При таком разделении функций появляется возможность не только обеспечить высокоэффективную защиту МУРЗ (см. рисунок), но и реализовать защищенную дистанционную систему управления выключателями [11].

Структурная схема устройства защиты МУРЗ от ПДДВ



Общая идея, лежащая в основе предлагаемого аппаратного метода защиты МУРЗ от ПДДВ, заключается в использовании совместно с МУРЗ электромеханического пускового органа на герконах (ПО), функционально включенного последовательно с МУРЗ, и быстродействующих электромеханических исполнительных элементов *(RR1—RR7)*, производящих блокировку чувствительных входов МУРЗ и отключение его выходной цепи. Возврат сработавшего ПО в исходное состояние осуществляется по факту срабатывания выключателя и дублируется командой «СБРОС» по истечении заранее заданного небольшого промежутка времени.

Без активации током и/или напряжением такого пускового органа МУРЗ не сможет «управлять» режимом функционирования энергосистемы, даже будучи подвергнутым ПДДВ или просто мощной электромагнитной помехе. Если же пусковой орган был активирован и МУРЗ деблокировано, то ничто не мешает использованию особых характеристик и широких функциональных возможностей МУРЗ. При этом излишние срабатывания самого пускового органа никак не влияют на работу РЗ, и поэтому никаких особых требований к точности срабатывания пускового органа не предъявляется. Важно лишь, чтобы он срабатывал всегда до МУРЗ, т.е. имел несколько меньшие уставки срабатывания по контролируемому параметру. Если срабатывание пускового органа оказалось излишним и срабатывания МУРЗ не произошло, устройство автоматически возвращается в исходное состояние. Основными техническими требованиями к такому устройству являются его исключительная надежность, нечувствительность к коротким импульсным (микро- и наносекундного диапазона) и высокочастотным помехам, стойкость к значительным перенапряжениям, высокий уровень гальванической развязки от внешних цепей, быстродействие на срабатывание (несколько миллисекунд).

Работает устройство следующим образом. В исходном состоянии при нормальном режиме функционирования защищаемого объекта все входные герконовые реле (датчики тока, напряжения и т.д.) пускового органа находятся в отпущенном состоянии, катушки исполнительных герконовых реле *RR4—RR7* обесточены. Нормально замкнутые контакты *RR5* и *RR6* закорачивают дискретные входы МУРЗ, контакты *RR4* — канал связи, а контакты *RR7* разрывают выходную цепь МУРЗ. Таким образом, в этом состоянии МУРЗ оказывается полностью заблокировано и по входу, и по выходу, и никакие ПДДВ не могут привести к его ложному срабатыванию и несанкционированному замыканию цепи отключающей катушки выключателя СВ. Шунтирование дискретных входов МУРЗ и канала связи улучшает также его живучесть при воздействии мощного электромагнитного импульса.

При возникновении аварийного режима защищаемого объекта хо-

тя бы один из контролируемых параметров (ток, напряжение, мощность) резко изменяется, что приводит к срабатыванию хотя бы одного из герконовых реле пускового органа ПО за время не более 1 мс и к последующему срабатыванию реле *RR4—RR6* (размыкание герконов), что происходит не более чем за 2—4 мс, а замыкание мощных контактов герконового реле *RR7* на герконе типа *Bestact R15U* — не более чем за 5 мс. Таким образом, суммарное время реакции всего устройства на аварийный режим не превышает 6 мс, что при собственном минимальном времени срабатывания МУРЗ 30—40 мс вполне приемлемо. В таком режиме устройство защиты МУРЗ будет полностью разблокировано и возвращено в нормальный режим функционирования с сохранением всех его уставок и характеристик.

Выбор герконов в качестве базовых элементов устройства обусловлен совокупностью их важнейших качеств, таких как герметичность, длительный срок службы, высокое быстродействие, специальная газовая среда или вакуум, в которых находятся контакт-детали, отсутствие необходимости в регулировке и зачистке контактов, высокий уровень гальванической развязки между входом (катушка управления) и выходом (герконом), четкий и стабильный порог срабатывания. Датчики тока и напряжения с регулируемым порогом срабатывания на герконах уже давно предложены автором и широко применяются в специальной аппаратуре и в военной технике. В [12] приведено описание некоторых из них, подходящих для использования в описанном устройстве. Все элементы данного устройства могут быть смонтированы в отдельном модуле, поставляемом производителями МУРЗ и располагаемом рядом с МУРЗ в релейном шкафу.

Выводы

1. Кибератаки не являются единственной угрозой современной микропроцессорной релейной защиты, поэтому для повышения надежности РЗ недостаточно использовать лишь известные методы обеспечения информационной безопасности.
2. Термин «кибератаки» предлагается заменить термином «преднамеренные деструктивные дистанционные воздействия», включающие любые виды преднамеренных дистанционных воздействий на РЗ, направленных на несанкционированное вмешательство в ее работу, нарушение нормального алгоритма или выведение из строя.
3. Существующие способы обеспечения информационной безопасности не в состоянии защитить МУРЗ от ПДДВ, в связи с чем необходимо создать принципиально новые средства защиты МУРЗ, дополняющие уже известные методы.
4. В качестве универсального средства защиты МУРЗ от ПДДВ предлагается использовать отдельный модуль, содержащий пусковой орган с быстродействующими электромеханическими датчиками тока и напряжения на герконах и выходными исполнительными реле на герконах, деблокирующих дискретные входы МУРЗ, его выходные цепи и канал связи лишь в момент возникновения в контролируемом объекте аварийного или близкого к аварийному режима.
5. Для реализации полноценной защиты МУРЗ от ПДДВ необходимо прекратить порочную практику выполнения ими вспомогательных функций, не имеющих отношения к РЗ, резко ограничить масштабы использования свободно-программируемой логики, а также разграничить функции дистанционного управления выключателями (ДУВ) и релейной защиты, предусмотрев для ДУВ независимую защищенную систему. эр

Литература

1. *Гуревич В.И.* Вопросы философии в релейной защите // Мир техники и технологий. — 2013. — № 1.
2. *Гуревич В.И.* Нужна ли защита релейной защите? // Электроэнергия. Передача и распределение. — 2013. — № 2.
3. *Гуревич В.И.* Проблема электромагнитных воздействий на микропроцессорные устройства релейной защиты. Ч. 1. // Компоненты и технологии. — 2010. — № 2—4.
4. *Шалин А.И., Трофимов А.С.* Эффективность и надежность релейной защиты энергосистем // Relay Protection and Substation Automation of Modern Power Systems, CIGRE-2007 (Cheboksary, September 9—13, 2007).
5. *Саратова Н.Е.* Анализ подходов к исследованию процессов протекания системных аварий: Системные исследования в энергетике // Материалы конф. молодых ученых. — Иркутск: ИСЭМ, 2007.
6. *Кузьмичев В.А., Сахаров С.Н.* Анализ работы устройств РЗА ЕНЭС в 2012 году: Тезисы докладов // РЕЛАВЭКСПО-2013, Чебоксары.
7. The Impact of Implementing Cyber Security Requirements using IEC 61850 // CIGRE Working Group the B5.38, August 2010.
8. *Гуревич В.И.* Кибероружие против энергетики // PRO Электричество. — 2011. — № 1.
9. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, sealed by the President of the United States, May 2011, 25.
10. *Ward S., O'Brien J., Beresh B., Benmouyal G. at al.* Cyber Security Issues for Protective Relays C1 Working Group Members of Power System Relaying Committee // Power Engineering Society General Meeting, 2007. IEEE, 24—28 June 2007.
11. *Гуревич В.И.* Повышение защищенности дистанционного управления выключателями // Электроэнергия. Передача и распределение. — 2013. — № 5.
12. *Гуревич В.И.* Герконовые реле с регулируемым порогом срабатывания // Компоненты и технологии. — 2013. — № 11.