Повышение защищённости дистанционного управления выключателями

Владимир ГУРЕВИЧ, к.т.н., Израиль

В [1, 2] говорится о необходимости защиты микропроцессорных устройств релейной защиты (МУРЗ) от кибератак и преднамеренных электромагнитных деструктивных воздействий (ПЭДВ) и предлагается устройство защиты, работающее на принципе шунтирования чувствительных входов МУРЗ с одновременным разрывом цепи их выходных контактов посредством быстродействующих электромеханических реле на герконах.

Однако из-за негативной тенденции навешивания на МУРЗ всевозможных дополнительных функций, не имеющих отношения к релейной защите [3, 4], реализация предложенных мер защиты МУРЗ в некоторых случаях будет затруднена. Речь идёт о распространённом использовании МУРЗ для дистанционного управления выключателями (ДУВ). Совершенно очевидно, что такое использование МУРЗ не имеет ничего общего с функциями релейной защиты, а дистанционное подключение к МУРЗ по каналам связи с целью изменения положения выключателей очень трудно отличить аппаратными средствами от кибератаки.

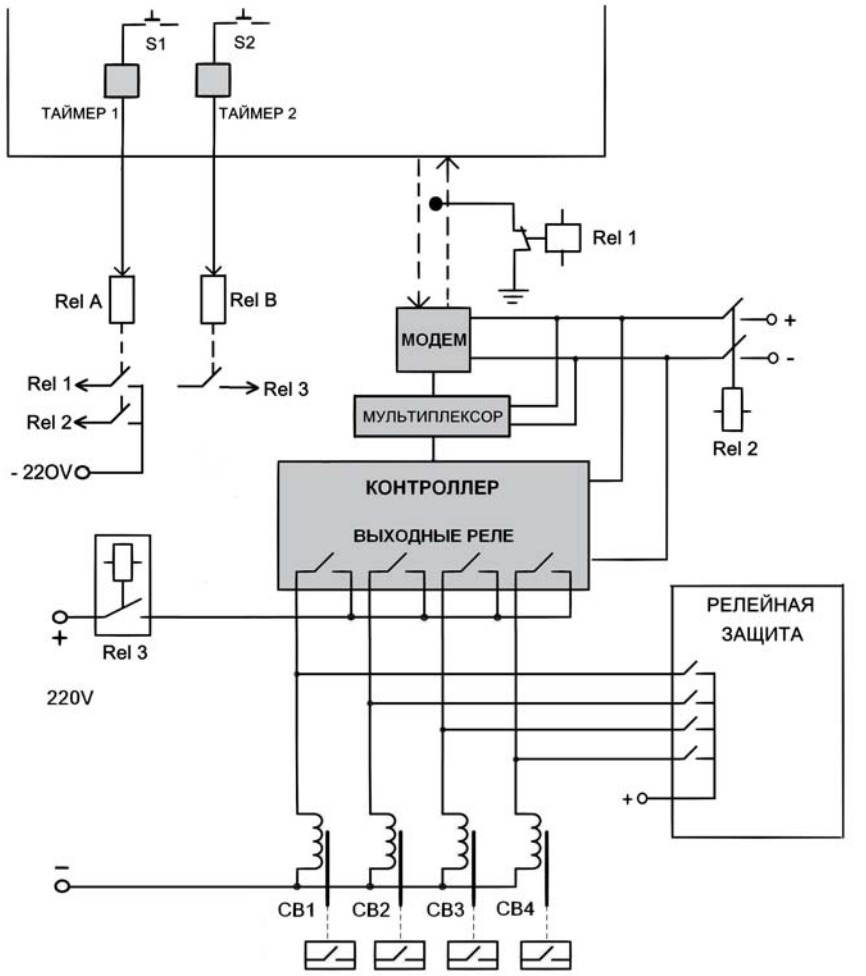
Задачу повышения надёжности релейной защиты невозможно решить при совмещении функций МУРЗ с функциями, не имеющими отношения к РЗ, например таких популярных, как мониторинг исправности электрооборудования, дистанционное управление выключателями и т.п. МУРЗ должны использоваться исключительно для решения задач релейной защиты. Тем более что для решения других задач, например для 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, растворённых в масле трансформаторов, или уровень частичных разрядов в изоляции. По нашему мнению, и ДУВ должно быть отделено от релейной защиты и осуществляться отдельными аппаратными средствами. Только в этом случае можно повысить надёжность РЗ и осуществить её эффективную защиту от преднамеренных дистанционных деструктивных воздействий. При таком разделении функций появляется возможность не только обеспечить высокоэффективную защиту МУРЗ, но и реализовать защищённую дис-

танционную систему управления выключателями (ЗДУВ).

Предлагаемая система ЗДУВ (рис. 1) является гибридной и совмещает в себе как микропроцессорный контроллер с сетевым каналом передачи данных, так и кабельный канал с электромеханическими реле. Основной задачей предлагаемой системы является предотвращение несанкционированных изменений положения выключателей при кибератаке или при повреждениях электронных устройств, входящих в эту систему. Вспомогательной задачей системы является повышение её живучести и сохранение работоспособности после воздействия ПЭДВ. Общая идея такой системы заключается в том, что любая команда на изменение положения выключателя, передаваемая по сетевому каналу, должна быть подтверждена кратковременным дистанционным включением электромеханического реле на подстанции путём подачи напряжения на его катушку по обычному контрольному кабелю. Почему потребовалось использование электромеханического реле и почему нельзя использовать подтверждающий канал на основе волоконно-оптической линии связи (ВОЛС)?

Проблема заключается в том, что ВОЛС не решает задачи защиты от ПЭДВ, поскольку с двух сторон эти ВОЛС снабжены сложными микропроцессорными мультиплексорами, обеспечивающими преобразование электрических сигналов в световые на одном конце ВОЛС и восстановление электрических сигналов из оптических — на другом конце. Как показали проведённые нами исследования некоторых типов мультиплексоров [5], они не выдерживают даже стандартных импульсных перенапряжений в соответствии с требованиями по электромагнитной совместимости (ЭМС). При повреждении внутренних электронных компонентов мультиплексоров под воздействием ПЭДВ состояние их выходных цепей окажется непредсказуемым. Если такой повреждённый мультиплексор будет не способен передать дистанционную команду на изменение положения выключателя, никакой катастрофы не произойдёт, ну а если его выходные цепи окажутся в активированном состоянии, то неприятностей не избежать. То же самое относится и ко всем другим компонентам предлагаемой системы ЗДУВ (модему, контроллеру).

Рис. 1. Предлагаемая структура защищённой системы дистанционного управления выключателями (ЗДУВ). Цепи питания показаны условно для упрощения схемы



Кроме того, поскольку прокладка выделенных ВОЛС и установка аппаратуры сопряжения достаточно дороги, то уже сегодня существует тенденция отказа от использования выделенных ВОЛС и существующих компьютерных сетей на основе дешёвых кабелей с витой парой. Более того, с целью ещё большего удешевления систем управления, релейной защиты и автоматики всерьёз рассматривается возможность перехода на беспроводные технологии WiFi. Во всяком случае, многие мировые лидеры в производстве МУРЗ уже сегодня выпускают их со встроенными модемами WiFi. Собственно говоря, идея перевода всего энергетического оборудования на связи по стандартным компьютерным сетям, включая беспроводные, — это центральная идея концепции «умных сетей» (Smart Grid). В этой связи возрастает актуальность разработки специальных аппаратных средств защиты систем релейной защиты и дистанционного управления коммутационными аппаратами от преднамеренных дистанционных деструктивных воздействий, включающих в себя электромагнитные воздействия [6] и кибератаки [7], не связанных с компьютерными сетями и обладающих повышенной устойчивостью к ПЭДВ. Именно поэтому в качестве элементов такой защиты нами выбраны электромеханические реле, управляемые оперативным напряжением по контрольным кабелям. С целью защиты этого дополнительного канала связи от злонамеренного внешнего подключения и несанкционированной активации

электромеханических реле используются токоведущие жилы, принадлежащие разным контрольным кабелям, а вместо одного реле используются два реле — RelA и RelB (см. рис. 1). Естественно, катушки этих реле и токоведущие жилы кабелей, по которым осуществляется их питание, должны быть защищены (например, с помощью варисторов) от импульсных перенапряжений, которые могут быть наведены в этих жилах под воздействием мощного электромагнитного импульса ПЭДВ. Кроме того, желательно осуществлять питание этих реле переменным током промышленной частоты с конденсатором, включённым в разрыв цепи питания, а на стороне подстанции использовать разделительный трансформатор. Эти меры позволят предотвратить срабатывание реле RelA и RelB от токов сверхнизкой частоты, наводимых в подземных кабелях под воздействием компонента E3 электромагнитного импульса [7].

В предлагаемом устройстве любая команда на изменение положения выключателей, передаваемая по сетевому каналу любого типа, должна сопровождаться кратковременным дистанционным включением двух реле RelA и RelB по контрольному кабелю. Контакты этих реле включают местные электромеханические промежуточные реле: Rel1 (деблокирует сетевой канал связи), Rel2 (подаёт питание на электронные устройства системы) и Rel3 (включает цепь питания катушек выключателей). Все эти местные реле могут быть разными по своим характеристикам. Например, Rel1 — высокочастотное реле, Rel3 — реле с мощными контактами, предназначенными для коммутации индуктивной нагрузки на постоянном токе. Наличие двух управляющих реле RelA и RelB с отдельными каналами управления повышает защищённость системы от несанкционированного доступа.

Первым включается RelA, а после передачи на контроллер необходимой информации об изменении положения того или иного выключателя и замыкании контактов соответствующего выходного реле контроллера включается реле RelB и своим контактом включает реле Rel3. Время включённого состояния реле RelA и RelB автоматически ограничивается таймерами, с тем чтобы предотвратить постоянное включение этих реле при ошибке персонала. Реально это короткий промежуток времени, в течение которого осуществить эффективную кибератаку практически невозможно. А блокирование канала связи и отключение питания контроллера вне этого короткого промежутка времени исключает опасность предварительной активации выходных реле контроллера в результате кибератаки с последующим несанкционированным изменением положения выключателей в момент включения электромагнитного реле RelB. Эти же меры резко снижают и вероятность повреждения чувствительной электронной аппаратуры (модем, мультиплексор, контроллер) от повреждения при воздействии ПЭДВ.

После зарегистрированной кибератаки или электромагнитного импульса дистанционное управление выключателями должно быть запрещено до специальной проверки, поскольку состояние контроллера после таких воздействий на него не известно.

Выходные реле контроллера могут быть маломощными стандартными, которыми комплектуются обычные контроллеры. А вот реле Rel3 должно иметь контакты, способные включать достаточно мощную нагрузку индуктивного характера (катушки управления выключателями) на постоянном токе и при напряжении 220 В.

Анализ спецификаций распространённых типов электромагнитных реле показывает, что большинство из них не предназначены для коммутации (и даже для включения) индуктивных нагрузок на постоянном токе с напряжением 220 В [8]. Для этой цели служат реле специальной конструкции: обеспечивающие многократные последовательные разрывы в коммутируемой цепи (рис. 2) или содержащие постоянный магнит вблизи контактов, предназначенный для выталкивания электрической дуги из межконтактного зазора (рис. 3). Имеются также и реле с тремя разрывами на контакт (рис. 4), позволяющие управлять отключающими катушками высоковольтных выключателей старого типа с большими потребляемыми токами.

В тех случаях, когда использование контрольного кабеля для управления реле RelA и RelB не представляется возможным из-за значительной удалённости диспетчерского пункта от подстанции, возможно применение ВОЛС в качестве разрешающего канала связи. При этом следует иметь ввиду снижение защищённости системы к ПЭДВ. Для предотвращения самопроизвольной выдачи команд на изменение положения выключателей вследствие повреждения электронных устройств системы, они должны быть снабжены самодиагностикой.

Рис. 2. Реле типа C4-X20 фирмы RELECO (с частично удалённым чехлом) с двумя контактами с двойным разрывом и его коммутационная способность на постоянном токе

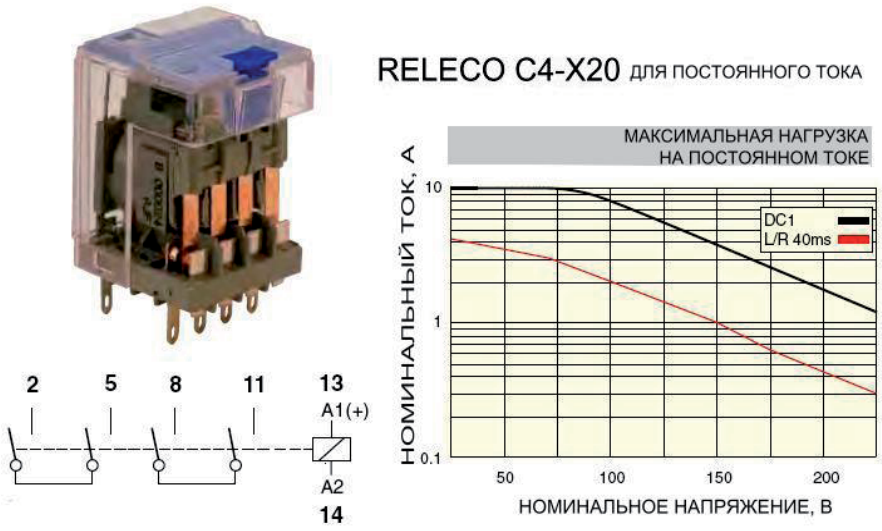
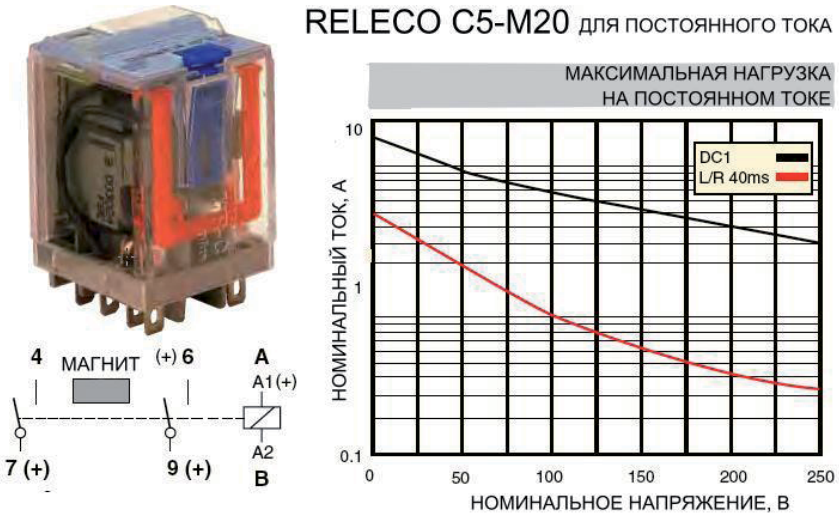


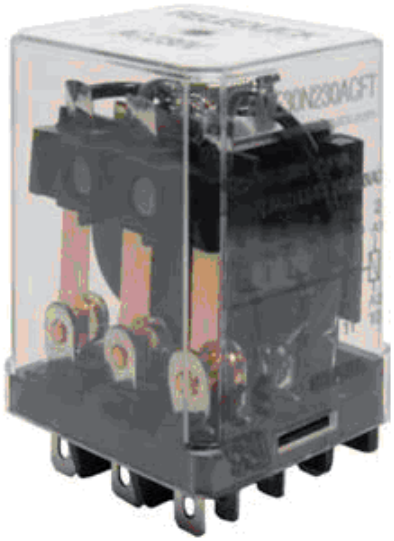
Рис. 3. Реле типа C5-M20 фирмы RELECO с двумя замыкающими контактами и дугогасящим магнитом и коммутационная способность его контактов для индуктивной нагрузки



Канал ВОЛС — постоянным мониторингом собственной исправности, а также положением реле RelA и RelB, а контроллер — внутренней системой самодиагностики, автоматически запускаемой сразу же при активации реле Rel1 Rel2 и включающей в себя опрос состояния выходных реле (они должны быть выключены) и исправность канала связи. При обнаружении неисправности система самодиагностики должна блокировать дальнейшую работу контроллера. Только при поступлении на диспетчерский пункт информации об исправности всех элементов системы может быть разрешено использование её для дистанционного управления выключателями.

Как можно видеть, в обоих случаях, то есть и для защиты МУРЗ [1, 2], и для защиты системы ДУВ, используются электромеханические реле, однако применение этих реле различно, что связано с различным алгоритмом работы МУРЗ и ДУВ. Если в первом случае выдача команды на выключатели производится автоматически при изменении контролируемого режима работы электрической сети или энергетического оборудования, то во втором случае выдача команды на выключатели производится вручную диспетчерским персоналом. С этим связаны и различные принципы реализации защиты. Так, в первом случае важно защитить постоянно работающий в автоматическом режиме МУРЗ от несанкционированного изменения его уставок или внутренней логики, вызывающих срабатывание выходных реле, и нет возможности перед активацией выходных реле проверить правильность команд. Кроме того, нет никакой возможности подать на МУРЗ какой-то внешний разрешающий сигнал при возникновении аварийного режима в контролируемой сети и этот разрешающий сигнал должен формироваться на месте, по факту возникновения аварийного режима. Тогда как во втором случае, когда защищаемый объект (ДУВ) не работает в автоматическом режиме, задача значительно упрощается и становится возможным использование внешнего разрешающего сигнала. Кроме того, в критических случаях ДУВ может быть вообще отменено. Эти естественные различия в принципах организации защиты от преднамеренных деструктивных воздействий ещё раз подтверждают целесообразность разделения задач релейной защиты и дистанционного управления выключателями.

Рис. 4. Реле типа RMEA-FT-1 с одним замыкающим контактом с тройным разрывом, способным коммутировать постоянный ток до 3 А в индуктивной нагрузке при напряжении 220 В (производитель: RELEQUICK S. A.)



Автор выражает искреннюю благодарность гл. спец. ОЭС ЗАО «Самарский Электропроект» Тюрину Дмитрию Юрьевичу за участие в предварительном обсуждении статьи и ценные замечания, учтённые при написании статьи.

ЛИТЕРАТУРА

1. *Гуревич В.И. Нужна ли защита релейной защите? — «ЭЛЕКТРОЭНЕРГИЯ. Передача и распределение», 2013, № 2, с. 94—97.*
2. *Гуревич В.И. Устройство защиты релейной защиты. — «Control Engineering Россия», 2013, № 3, с. 25—29.*
3. *Гуревич В.И. Технический прогресс в релейной защите. Опасные тенденции развития РЗА. — «Новости электротехники», 2011, № 5, с. 38—40.*
4. *Гуревич В.И. Про многофункциональную релейную защиту. — «PRO Электричество», 2012, № 42—43, с. 45—48.*
5. *Гуревич В.И. Актуальные проблемы релейной защиты: альтернативный взгляд. — «Вести в электроэнергетике», 2010, № 3, с. 30—43.*
6. *Гуревич В.И. Микропроцессорные реле защиты. Устройство, проблемы, перспективы. — М.: Инфра-Инженерия, 2011. — 336 с.*
7. *Гуревич В.И. Кибероружие против энергетики. — «PRO Электричество», 2011, № 1, с. 26—29.*
8. *Гуревич В.И. Особенности реле, предназначенных для включения отключающих катушек высоковольтных выключателей. — «Электричество», 2008, № 11, с. 22—29.*