ПРЕДИСЛОВИЕ АВТОРА

Релейная защита занимает особое место в системе производства, передачи и распределения электроэнергии. Она сама по-себе не участвует ни в производстве, ни в передаче, ни в распределении электроэнергии и в нормальных режимах работы энергосистемы себя вообще никак не проявляет. Если ее отключить, то ничего не изменится: генераторы на электростанциях будут по-прежнему вырабатывать электроэнергию, а линии электропередач и распределительные сети будут по-прежнему доставлять произведенную электроэнергию потребителю. Но идиллия эта обманчива: малейшая техническая неисправность в электрооборудовании может привести к коллапсу энергосистемы всей страны, если в дело своевременно не вмешается релейная защита. Все это вещи хорошо известные специалистам и не требующие разъяснений. Но, оказывается, не все так просто. Современные реле защиты – сложнейшие электронные комплексы также подверженные отказам в работе, как и любой другой вид современного электронного оборудования. Что же произойдет при отказе реле защиты во время аварийного режима в энергосистеме? Да, в общем-то, ничего особенного, поскольку реле защиты работает не одно, а в совокупности с множеством других реле защиты. Не сработало вовремя одно реле защиты – сработает какое-то другое. Во всяком случае, все критичные энергетические объекты имеют такую резервную защиту. Но отказ в срабатывании – это не единственный вид неправильных действий реле защиты. Оно может ложно сработать и в нормальном режиме работы. И вот тут-то возникают проблемы намного более серьезные. Дело в том, что излишние срабатывания реле не могут быть «подстрахованы» резервными реле защиты. А что такое излишнее срабатывание реле защиты? Это отключение посредством выключателей тысяч потребителей, линий электропередач, трансформаторов, генераторов и т.п. Далеко не всегда ситуацию может исправить система АПВ или АВР. Возникающие при внезапных отключениях больших мощностей переходные режимы в электрических сетях и в целом в энергосистеме могут привести к последовательному отключению линий и генераторов, то есть к развалу энергосистемы и ее коллапсу. Большинство из известных крупнейших аварий в энергосистемах мира развивались именно по такому сценарию. Получается, что реле защиты само по себе может спровоцировать коллапс в нормально функционирующей энергосистеме.
В последние годы это стали хорошо понимать и те, кто планирует стратегию возможных будущих военных операций.

Современные сценарии силового противодействия между странами все меньше основываются на использовании традиционных средств поражения живой силы и техники противника и все больше на средствах, способных поразить инфраструктуру противника и исключить человеческие жертвы. Разрушение инфраструктуры современного постиндустри-

ального общества оказывается намного более эффективным средством противодействия, чем ведение обычных боевых действий. Электронизация и зависимость инфраструктуры любого высокоразвитого государства от компьютеров существенно облегчает задачу разрушения инфраструктуры, поскольку такое разрушение может быть не физическое, а виртуальное. Некий парадокс заключается в том, что чем более развита инфраструктура страны, тем больше она пострадает при таком виртуальном воздействии.

Какое место в инфраструктуре государства занимает релейная защита энергосистем? Совершенно особое, поскольку именно через реле защиты, управляющих положением выключателей, можно получить доступ к дистанционному изменению конфигурации электрических сетей и нормально функционирующую энергосистему искусственно ввести в состояние коллапса. Сегодня это уже стало хорошо понятно организациям, занимающимся планированием стратегии возможных противостояний. Выполнением заказов этих организаций, направленных на создание специальных видов техники, поражающих высокочувствительную электронную аппаратуру современной электроэнергетики заняты десятки крупнейших корпораций во всех развитых странах мира. Микропроцессорные реле защиты, ввиду их особого положения, являются далеко не последней целью для первоочередного поражения. Сегодня известны два вида дистанционного деструктивного воздействия на микропроцессорные системы: кибернетические атаки и преднамеренные деструктивные электромагнитные воздействия.

Современные тенденции развития релейной защиты, такие как повсеместный переход на микропроцессорные реле; постоянное усложнение аппаратной и программной части этих реле; увеличение количества выполняемых ими функций (в том числе таких, которые не имеют прямого отношения к релейной защите); переход с оптоволоконных на менее защищенные каналы связи (Ethernet, Wi-Fi); продолжающаяся миниатюризация в области электроники; расширяющееся применение элементов флэш-памяти, основанных на изменении и регистрации очень слабого электрического заряда в изолированной области транзистора; рост количества транзисторов в микропроцессорах и снижение их рабочих напряжений – все это и многое другое существенно облегчает задачу дистанционного деструктивного воздействия. С одной стороны, происходит постоянный рост уязвимости релейной защиты, а с другой – постоянное совершенствование методов дистанционного деструктивного воздействия. В результате, эти два опаснейших вектора развития стремительно движутся навстречу друг другу. Как тут не вспомнить знаменитое изречение велико-

ПРЕДИСЛОВИЕ АВТОРА

го Уинстона Черчилля: *«Каменный век может вернуться на сияющих крыльях науки».*

Ситуация усугубляется еще и тем, что доступ к современным средствам поражения компьютерных и микропроцессорных систем имеют и террористические и криминальные структуры. А это делает вероятность встречи этих двух векторов неминуемой. Именно поэтому необходимо хорошо понимать существующие опасности и заранее предпринимать меры защиты от них.

В данной книге автор поставил перед собой цель убедить читателя в реальности существующих опасностей и показать пути решения проблемы.

Автор выражает искреннюю благодарность Гл. спец. ОЭС ЗАО «Самарский Электропроект» Тюрину Дмитрию Юрьевичу за участие в плодотворных дискуссиях по теме и ценные замечания, учтенные при написании книги, а также всем другим специалистам, принимавшим участие в обсуждении вопросов, освещенных в книге.

Отзывы на книгу просьба направлять автору по адресу: vladimir.gurevich@gmail.com

Автор