УДК 621.3

Кибербезопасность как обязательный элемент обеспечения функциональной надёжности в электроэнергетике

Плешко Д. Ю.
Научный руководитель – САПОЖНИКОВА А. Г.

Энергетика является сама по себе критической инфраструктурой с одной стороны, а с другой стороны любая другая инфраструктура имеющая статус критической в той или иной мере, сегодня, зависит от нее напрямую. Например, электротранспортная, социальная инфраструктура, водо, газо, теплоснабжение и многое другое. Уровень надежности работы всех перечисленных инфраструктур напрямую зависит от уровня надежности работы электроэнергетической компании.

Понятие «надежности» в электроэнергетике всегда было на первом месте. Это отражалось во всех документах, проектах и технических решениях. Каждый новый шаг на пути технического прогресса переосмыслялся с точки зрения сохранения (повышения) уровня надежности и только после этого находил применение в отраслевых стандартах и типовых проектных решениях. Она же послужила причиной появления первых интеллектуальных устройств и автоматизированных систем управления на объектах энергетики. Но затем количество таких устройств и систем начало резко расти, постепенно заменяя собой все вторичное оборудование.

Автоматизированные системы диспетчерского и технологического управления, цифровые терминалы защит, противоаварийная автоматика стали неотъемлемой частью любого современного предприятия. Корпорации, используя возможности современного оборудования, стремятся вынести управляющий контур на уровень центров диспетчеризации, контролирующие организации собирать информацию, в реальном времени, с возможно большего количества технологических объектов напрямую. В результате возникает сложная распределенная система информационных потоков. В ряде случаев данные потоки становятся доступны в бизнес-сегментах сетей, имеющих доступ к Интернету, а иногда даже в публичных сетях.

С точки зрения персонала, ответственного за эксплуатацию технологического объекта, все в порядке, им необходимо выполнять свои функции по поддержанию надежности производственных процессов, извещать ответственных лиц по электронной почте о соответствующих событиях в технологическом контуре управления, предоставлять информацию внешним контролирующим компаниям, взаимодействовать с внутренним и внешним ремонтным персоналом и т. д.

С точки зрения ИТ-служб тоже все в порядке, инфраструктура работает, данные предоставляются в установленные сроки, пользователи обеспечены всей необходимой им информацией. С другой стороны, специалисты по информационной безопасности, рассказывают о трагических и не очень происшествиях, которые повлекли за собой или создали угрозу техногенных аварий и финансовых потерь, как прямых, так и косвенных. Так насколько реальны те угрозы, рассказами о которых наводнен Интернет и другие СМИ? Снимаются фильмы, проводятся семинары, конференции, в видео-сервисе «*Youtube*» подробно рассказывают, как вскрыть тот или иной технологический протокол или контроллер. Но это тоже еще не все.

К проблемам может привести даже не злонамеренная атака или воздействие, а просто «человеческий» фактор, когда из-за недостатка квалификации или сложности интерфейса оператор вводит некорректный параметр или меняет текущую конфигурацию.

Эффективность, удобство, безопасность сегодня, к сожалению, чаще всего реализованы только два из трех перечисленных свойств, а это снижает надежность технологического процесса в целом. Проблема возникла не вчера и была обусловлена предысторией развития архитектуры автоматизированных систем управления технологическими процессами.

Исторически промышленные сети строились на специализированных протоколах обособленно от остального информационного пространства. Проникновение в эту область IP-устройств, незаметно привело к тому, что обособленность исчезла, а принципы построения и архитектура не изменились.

Информатизация общества и технологий, в том числе и в энергетике, идет такими быстрыми темпами, что времени на подготовку и анализ всех изменений и потенциальных угроз просто не остается. Сам по себе технологический процесс претерпел минимальные изменения, современные средства позволяют увеличить динамику и скорость реакции, учесть дополнительные влияющие факторы, повысить КПД. С другой стороны, возросла вероятность появления ошибок, как прямых, так и косвенных в работе устройств и как следствие рост вероятности не технологических отказов.

Прямая ошибка – это ошибка в алгоритме работы устройства, в части его базовой функциональности. Такие ошибки должны выявляться еще на уровне заводских испытаний оборудования, но усложнение программных алгоритмов приводит к тому, что в процессе испытаний ошибка может себя не проявлять, а в рамках эксплуатации в реальных условиях – отработать.

Причиной такой ошибки может быть неточность при разработке устройства, при его настройке или в результате внешнего воздействия на устройство уже в процессе эксплуатации. Косвенная ошибка – это ошибка, возникающая не в самом устройстве управления, а на внешних устройствах, что приводит к искажению, поступающей информации (например, измерительной). В результате логика устройства управления будет работать как положено, но самому техпроцессу может быть нанесен непоправимый вред. Не технологическими отказами принято считать отказы (аварии), произошедшие из-за ошибок в работе интеллектуальных устройств и программного обеспечения.

Бытует распространённое мнение, ну раз это так опасно, вернемся к электромеханическим защитам и на этом остановимся. Все это напоминает, как десять лет назад все были уверены, что если сеть, в которой работает АСУ ТП изолировать от внешнего мира, то это решит все проблемы и информационной безопасностью можно не заниматься. Сейчас, пришло понимание, что интеллектуальное устройство уязвимо вне зависимости от того находится оно в изолированной сети или нет.

Новые технологии и сервисы (возобновляемая энергетика, электромобили, мощные накопители и т. д.) требуют от энергетиков нового качества услуг, обеспечить их, используя морально устаревшие технологии управления невозможно, так же, как и остановить прогресс. Остается тщательно прорабатывать концепцию обеспечения технического процесса в новых условиях, строить новое дерево отказов, учитывающее особенности работы программного обеспечения, закладывать элементы информационной безопасности уже на стадии проектирования. Вносить изменения в требования по эксплуатации, менять процедуры метрологического контроля. То есть в ближайшем будущем изменения должны коснуться всех процессов, связанных с эксплуатацией, контролем и управлением технологическими процессами в энергетике.

Подходы при решении задачи повышения надежности критической информационной инфраструктуры для существующих, и вновь строящихся (проектируемых) технологических объектов существенно различаются. Внести изменения в действующую архитектуру автоматизированных систем управления технологическими процессами, практически невозможно. Поэтому здесь широкое применение находят неинвазивные решения, которые гарантированно не могут повлиять или исказить существующие информационные потоки. Для строящихся (проектируемых) объектов, в свою очередь, безопасность критической информационной инфраструктуры должна гарантироваться на уровне проектных решений и обеспечивать требуемый уровень надежности объекта в целом.

Чтобы дойти до цели, необходимо сделать первый шаг. Таким шагом могло бы стать, если брать в качестве примера Российскую Федерацию, внесение изменений в

Постановление Правительства от 28 октября 2009 г. № 846 «Об утверждении Правил расследования причин аварий в электроэнергетике». В этом постановлении приведена процедура организации расследования аварий. Вопросы информационной безопасности, как одной из вероятных причин аварии не рассматриваются, и соответствующие эксперты не привлекаются. Таким образом, если реальной причиной аварии стала ошибка в работе средств вычислительной техники, объективно установить это практически невозможно. Выход предлагается простой, данное Постановление уже пережило множество редакций, однако достаточно внести изменения в ряд пунктов, и ситуация коренным образом меняется.

Если при расследовании аварий надо будет привлекать в комиссию экспертов по безопасности критических информационных инфраструктур, то они должны быть подготовлены и знакомы с работой оборудования и систем на производственных объектах. Раз состояние информационных систем, наравне с прочими эксплуатационными характеристиками станет влиять на результаты проводимого расследования, то появится необходимость в специальных эксплуатационных регламентах, предусматривающих мониторинг (в автоматизированном или ручном режиме) оборудования и систем.

Проведение периодических испытаний и контрольных проверок, как самого оборудования, так и каналов передачи данных, включая каналообразующую аппаратуру. Реализация подобных мер, повлечет за собой необходимость повышения квалификации эксплуатационного персонала и как следствие повысит культуру эксплуатации производственных объектов в целом.

Уже сегодня многие Российские корпорации и холдинги требуют включать в технические задания и проектную документацию на системы технологического управления производственными процессами разделы по информационной безопасности. Но, к сожалению, формальные требования не приводят к решению проблем, так как обычно они не учитывают специфику конкретного производственного процесса.

Системный подход к вопросам безопасности критически важных информационных инфраструктур требует учитывать эти вопросы уже на стадии формирования требований к архитектуре АСУ ТП, выбора технических средств и методов реализации процессов управления. Частная модель угроз для каждой системы в составе критически важных информационных инфраструктур должна учитывать вероятности функциональных отказов и их влияние на уровень надежности технологических процессов в целом.

Архитектура телекоммуникационной системы, обеспечивающей работу критической информационной инфраструктуры должна предоставлять необходимые информационные каналы для АСУ ТП, РЗиА и систем мониторинга, при этом гарантировать невозможность использования данной логической телекоммуникационной инфраструктуры для других целей, как в санкционированном, так и в несанкционированном режимах. Измерительные датчики должны хранить первичную информацию, определенный период времени и обеспечивать возможность трассировки алгоритмов формирования косвенных измерений.

Для технологических процессов определенного уровня стоит предусматривать независимый мониторинг работоспособности самих интеллектуальных устройств и сети передачи данных., что позволит выявлять на ранних стадиях попытки несанкционированных подключений, не предусмотренные проектом, контролировать взаимодействие контроллеров по IP-сети, как между собой, так и с внешними адресатами, определять ошибки как на самих контроллерах, или так и их работу не в соответствии с утвержденной нормативно-технической документацией.

Это далеко не полный перечень мер, которые могут быть направлены на повышение предсказуемости работы информационных систем и программно-аппаратных комплексов в критических информационных инфраструктурах. Их грамотное сочетание и применение позволит гарантировать не только сохранение надежности технологического процесса на прежнем уровне, но и в ряде случаев позволит его значительно повысить.

Актуальность задачи систематизации работы по обеспечению безопасности критически важных информационных инфраструктур уже ни у кого не вызывает вопросов. Необходимо начать планомерное построение реальной модели угроз и выработку комплекса мер (методических, организационных, технологических и информационных) по защите критически важных объектов от умышленных и непредумышленных кибератак.

Такая работа в первую очередь будет интересна самим технологам, так как позволит навести порядок с действующими решениями, выявить слабые места, и обосновать развитие современных систем управления. Руководители смогут более эффективно использовать инструменты управления рисками компаний.

Государство решит социальную задачу, в части улучшения качества оказываемых услуг населению и задачу повышения энергобезопасности страны в целом.

Литература

1. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / В. Ф. Шаньгин. – М. : ДМК Пресс, 2012. – 592 с.

2. Добротун Е. Б. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действия нарушителя / Е. Б. Добротун. – М. : Инсайд, 2016. − 42 с.