УДК 621.039.4

ОСОБЕННОСТИ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУТП ТЭС И АЭС

Э.К. АРАКЕЛЯН, А.В. АНДРЮШИН, А.П. МИНЗОВ

Научно-исследовательский университет «Московский энергетический институт»
Красноказарменная,14, Москва, 111250, Россия

Поступила в редакцию 4 февраля 2015

Проблема обеспечения безопасности автоматизированных систем управления технологическими процессами (АСУТП) возникла в 90-х гг., когда на смену отечественному оборудованию пришли зарубежные образцы с соответствующим АСУТП и программным обеспечением. Это, безусловно, увеличило вероятность скрытого управления элементами АСУТП, однако до 2010 года считалось, что закрытые промышленные сети имеют высокий уровень доверия к их безопасности. Появление инцидентов проникновения вредоносного кода StuxNet (2010 г.), Duqu (2011 г.) и особенно Regin (2014 г.) в промышленные сети повлияло на существующие взгляды создания систем защиты инфраструктуры критически важных объектов (КВО). По данным Лаборатории Касперского последний вредоносный код (Regin) направлен на скрытое управление объектами энергетики и промышленности и может быть использован киберпреступниками для достижения определенных целей в масштабах государства. Отсюда возникла необходимость создания отечественных систем АСУТП на основе аппаратных и программных элементов собственного производства и разработки новых механизмов защиты. Первую задачу (импортозамещения) решить в короткие сроки практически невозможно, но вторая задача актуальна уже сегодня, поэтому разработка новых документов, регулирующих деятельность в этой сфере деятельности, является важным этапом обеспечения защиты информации в КВО. С этой точки зрения, приказ ФСТЭК № 31 от 14 марта 2014 г. «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» является важным и своевременным регламентирующим документом.

Проблемы информационной безопасности АСУТП электростанций на базе современных программно-технических комплексов обусловлены следующими особенностями ТЭС и АЭС:

– технологический процесс ТЭС и АЭС отличается сложностью взаимосвязей между большим числом агрегатов, высокими параметрами рабочей среды, жесткими требованиями к точности их регулирования;

– значительную долю оборудования электростанций и ПТК, на базе которых созданы АСУТП, составляют оборудование и ПТК, произведенные зарубежными фирмами, особенно в последние годы при широком внедрении новых технологий производства энергии на базе газотурбинной установки (ГТУ) и парогазовой установки (ПГУ);

– имеет место тенденция к поставке основного оборудования (котлов, турбин и т.д.) со своей локальной системой контроля и управления, выполненные на различных технических средствах;

– развитие современных АСУТП ТЭС и АЭС идет в основном по пути применения территориально-распределенных АСУТП с установкой полевых контроллеров, перехода на

цифровую передачу информации, создания цифровых промышленных сетей, беспроводных систем передачи информации, интеллектуализация измерительных устройств и запорно-регулирующей арматуры.

Кроме того, переход энергетики на рыночные отношения привело к:

– созданию большого количества управляющих компаний (ОГК, ТГК и т.д.) со своими корпоративными сетями и с удаленным доступом к станциям (в основном – телефон, интернет);

– необходимости передачи большого объема информации со станционного уровня на уровень управления энергосистемой и обратно (в основном по интернету);

– возможности оперативного управления текущих режимов со стороны СО-ЦДУ(РДУ) – (по интернету).

Указанные особенности при реализации требований указанного выше приказа требуют решения ряда методических и организационных проблем, в том числе наиболее существенные следующие:

1. Информационное обеспечение АСУТП современных ТЭС в зависимости от объема выполняемых функций содержит от 5,0 до 10 – 12 тыс. единиц информации различного рода (аналоговых, дискретных и цифровых), большое число программируемых логических контроллеров (ПЛК), регуляторов и другое оборудование, выполняющее одно из основополагающих положений «Требований» к системе – защиту АСУТП и информации так, чтобы не мешать нормальному функционированию системы АСУТП при указанном объеме обрабатываемой информации, связано с большими сложностями. Например, проблема, как определить необходимый экономически и технически обоснованный объем подлежащей защите функций АСУТП и информации АСУТП.

2. Одной из основных функций АСУТП, независимо от способа ее реализации (традиционное ручное или дистанционное управление, управление на базе программно-технического комплекса (ПТК)) является обеспечение надежной работы технологических защит и блокировок, для чего в АСУТП используется проверка достоверности сигналов, как правило, по схеме «два из трех» и в редких случаях по схемам «один из двух» или «два из двух». Правда, несмотря на это, на практике нередки случаи (особенно в АСУТП на традиционных технических средствах) «ложного» срабатывания технологических защит, и реже – не срабатывания защит (что еще опаснее). Проблема, при разработке систем защиты информации – каким образом будут сосуществовать указанные системы.

3. Концепция приказа № 31 определена из начального условия проектирования, разработки и внедрения АСУТП из элементов доверенной среды. Реально это далеко не так. Всеобщий технический контроль элементов АСУТП либо технически невозможен, либо экономически невыгоден владельцу АСУТП объекта энергетики. Поэтому требуется научная проработка другой концепции, рассчитанной на переходной период до полного импортозамещения элементов АСУТП. Суть этой концепции: создание методологии разработки, внедрения и безопасной эксплуатации АСУТП, работающих в недоверенной среде.

4. Актуальной является разработка нового направления по защите АСУТП с концепцией упреждающей или проактивной защиты. Это возможно в тех случаях, когда управление объектом энергетики проводится одновременно с анализом состояния системы информационной безопасности АСУТП и системы управления объектом энергетики с последующим моделированием его будущего состояния от очередного управляющего воздействия. Во всех случаях, когда управляющие воздействия могут привести к нестационарным процессам и критическим значениям параметров объекта, системой безопасности предпринимаются согласованные с персоналом действия по выводу объекта энергетики на стационарные заданные режимы управления. Следовательно, современные защищенные от внешнего и внутреннего воздействия АСУТП должны иметь легко настраиваемую интеллектуальную надстройку, позволяющую прогнозировать и выявлять заранее процессы, которые могут привести к техногенным катастрофам. Однако такие подходы требуют серьезной научной проработки и моделирования.