Алексей МАЛЬНЕВ:

«Понимание логической структуры АСУ ТП позволяет применять комплексный подход к ее защите»

Интервью с начальником отдела защиты КСИИ АМТ-ГРУП

– Когда проблематика информационной безопасности АСУ ТП начала приобретать актуальность? Как давно ваша компания занимается этими вопросами?

– Считается, что внимание широкой общественности к вопросам защиты АСУ ТП привлек инцидент 2010 г. – «червь» Stuxnet на Бушерской АЭС Ирана. Однако государство еще раньше занималось этой проблемой. В России в 2005 г. был выпущен документ Совета Безопасности РФ «Система признаков критически важных объектов…». В 2007 г. ФСТЭК выпустил четыре документа, определяющих базовую модель угроз, методику определения актуальных угроз, требования и рекомендации по обеспечению безопасности ключевых систем информационной безопасности. США также уделяют внимание данному вопросу – с конца XX в. развивается Национальная лаборатория Айдахо, уникальный полигон площадью более 2000 км^2 для отработки решений для АСУ ТП, в том числе по их защите.

АМТ-ГРУП занимается этой темой с 2009 г. Именно тогда у нас начались первые крупные проекты по информационной безопасности в топливно-энергетической отрасли, в том числе по защите АСУ ТП. За прошедшие годы специалистами АМТ-ГРУП накоплены колоссальный опыт и компетенции в области защиты АСУ ТП. Совершенствовался подход как с позиции консалтинга (была сформирована собственная методика аудита безопасности систем АСУ ТП, выработан собственный подход к проведению аудиторских работ), так и с инженерной точки зрения – наращивались компетенции в части проектирования и внедрения технических решений по защите АСУ ТП.

– В чем специфика проекта по информационной защите АСУ ТП сравнительно с проектом по защите ИТ-систем? Каковы различия на стадии подготовки проекта (обследования, анализа защищенности)? Какова специфика применяемых технических средств?

– Различия лежат на поверхности: в АСУ ТП приоритетом является непрерывность функционирования системы. Поэтому основное внимание уделяется обеспечению целостности контрольно-измерительной информации и доступности сервисов, от которых зависит непрерывность выполнения технологического процесса. Фактически это означает абсолютно другой подход к проблематике, как с консалтинговой, так и с технической точки зрения. Кардинально отличается подход к защите АСУ ТП и со стороны заказчика: задачи ИБ считаются здесь менее приоритетными и организационных сложностей при защите АСУ ТП возникает намного больше, чем в других сферах.

Если говорить о технических средствах защиты АСУ ТП, то для них, как правило, характерны промышленное исполнение, возможность максимально прозрачной и аккуратной инсталляции в имеющуюся инфраструктуру и, главное, наличие механизмов защиты информационных потоков в АСУ ТП.

– Насколько важно использование именно специализированных средств при защите АСУ ТП?

– Понимание структуры и логических уровней АСУ ТП – крайне важная задача. Дело в том, что каждый из уровней АСУ ТП обладает собственной спецификой и степенью критичности. К примеру, если на верхние уровни АСУ ТП распространяется значительное количество традиционных угроз ИБ, то ближе к уровню контроллеров мы сталкиваемся с большей спецификой АСУ ТП. Понимание этого позволяет применять комплексный подход с использованием специализированных средств там, где это действительно необходимо.

– В какой мере в проекте по защите АСУ ТП и КСИИ есть место аутсорсингу? Насколько заказчики работ готовы переложить повседневные функции на поставщика услуг?

– В организационной структуре типичного предприятия с АСУ ТП, как правило, отсутствуют специализированные подразделения, обладающие достаточным штатом квалифицированных специалистов по ИБ. Поэтому, например, в США значительная часть предприятий отдает функции анализа инцидентов ИБ внешним организациям, специализирующимся на этих задачах, способным быстро, с заданным временем реакции, и квалифицированно определять факты тех или иных инцидентов, выдавать соответствующие рекомендации или содействовать их разрешению.

На российском рынке подобные услуги пока не развиты. В первую очередь из-за традиционного нежелания заказчиков транслировать внутреннюю информацию вовне. ■