Марина СОРОКИНА:
«Интеграция функций ИБ – важное направление развития АСУ ТП»

За последнее время значительно изменилось отношение к вопросам обеспечения безопасности инфраструктуры и защиты информации. О тенденциях, доминирующих в данном сегменте, роли нормативных требований, решениях, доступных на российском рынке, рассказала руководитель направления индустриальных решений отдела развития продуктов компании «ИнфоТеКС» Марина Сорокина.

– Как, по вашим оценкам, за прошедший год изменился рынок средств защиты АСУ ТП?

– Рынок АСУ ТП за последние два года сделал качественный переход к осознанию необходимости обеспечения защиты информации. Наличие требований регуляторов, осознанность со стороны участников рынка и реальные кейсы взломов АСУ ТП привели к повышенному спросу на средства защиты информации (СЗИ). При этом интересно отметить, что многие компании обращаются с запросами на СЗИ, которых на рынке ИБ АСУ ТП пока нет или практически нет. Точнее, СЗИ с необходимым функционалом есть, но в связи со специальными требованиями к среде эксплуатации или спецификой используемых технологий их использование в АСУ ТП невозможно. Сюда же можно отнести и запрос на защиту информации, например, для не IP-устройств, функционирующих на устаревших последовательных сетях или на современных LPWAN-каналах.

– В каком направлении развиваются технологии защиты АСУ ТП в России и мире?

– Общие тенденции связаны с движением АСУ ТП в сторону IIoT, что приводит к увеличению количества отдельно стоящих устройств и размыванию периметра. Кроме того, АСУ ТП начинают сильнее интегрироваться друг с другом и становятся базой для предоставления дополнительных сервисов или информации смежным системам. Набирают обороты цифровые модели, системы предиктивной аналитики.

– Насколько популярно использование криптографии в средствах защиты промышленных сетей?

– Криптография де-факто является стандартом для защиты любых сетей, в том числе промышленных. Для АСУ ТП целесообразнее использовать имитозащиту. Кроме того, важно правильно выбрать криптографический алгоритм, где жестко определены допустимые задержки при передаче данных, что особенно актуально для систем реального времени. Здесь ключевым параметром будет значение размера накладных расходов на передаваемую информацию: чем меньше – тем лучше. Для систем реального времени лучше использовать встраиваемые средства криптографической защиты информации (СКЗИ).

Для промышленных предприятий у ИнфоТеКС есть линейка Industrial Security, включающая как наложенные, так и встраиваемые средства защиты информации.

Наложенные средства сегодня крайне востребованы, поэтому мы предлагаем индустриальные шлюзы безопасности ViPNet Coordinator IG. Шлюзы используют технологию ViPNet VPN, которая обеспечивает безопасную передачу данных, а реализованный в ViPNet Coordinator IG межсетевой экран защищает объекты от несанкционированного доступа.

В качестве встраиваемого средства защиты мы предлагаем решение ViPNet SIES, позволяющее обеспечить защищенность устройств АСУ ТП «из коробки», реализуя концепцию secure by design. ViPNet SIES – полностью законченное и сертифицированное решение, которое подходит для защиты систем АСУ, IIoT, M2M, в том числе для защиты интеллектуальных систем учета электроэнергии.

– Есть ли в промышленных системах реального времени место для использования квантовой криптографии?

– Квантовая криптография в будущем может стать фундаментом системы информационной безопасности России. В портфеле ИнфоТеКС есть квантовая криптографическая система, выполняющая протокол квантового распределения ключей и работающая в топологии «точка-точка» ViPNet Quandor, и квантовая криптографическая система ViPNet QSS, работающая в топологии «звезда».

Система ViPNet Quandor успешно прошла ряд испытаний: в Санкт-Петербургском информационно-аналитическом центре, на сети связи между МГТС и ГВЦ ОАО «РЖД», а также на линиях связи, принадлежащих ПАО «Ростелеком». На основе ViPNet QSS была запущена Университетская квантовая сеть. ■