Руслан СТЕФАНОВ:

«В России приоритет за национальной безопасностью и импортозамещением»

Потребность в качественных системах управления технологическими процессами (АСУ ТП) растет по мере цифровой трансформации. Существенным требованием является обеспечение информационной безопасности АСУ ТП, реализованных самим производителем. О возможностях встроенных в АСУ ТП механизмов защиты мы задали несколько вопросов Руслану Стефанову, консультанту по защите АСУ ТП подразделения «Промышленная автоматизация» компании Honeywell Россия/Таможенный союз.

– Чем отличаются потребности владельцев промышленных решений в информационной защите АСУ ТП на российском и глобальном рынках?

– На российском рынке задают тон требования национальной безопасности и импортозамещения. На глобальном рынке требования формируются с учетом интересов бизнеса крупнейших игроков и их партнеров. Здесь важно определить надежного поставщика (партнера), которому можно доверить защиту критичных активов, и дальше выстраивать с ним долговременные отношения на основе сервисных контрактов, в рамках которых поставщик будет учитывать требования владельца и обеспечивать защиту от киберугроз. Основные потребности, такие как категорирование КИИ, сегментирование и защита периметра промышленных сетей, обеспечение регулярного и автоматического обновления программного обеспечения, аутсорсинг услуг защиты квалифицированным подрядчикам, приняли за прошедший год более четкие очертания под влиянием регуляторов и крупных игроков рынка.

– Как изменился российский рынок средств защиты АСУ ТП за прошедший год? Как ваша компания отреагировала на требования закона № 187-ФЗ «О безопасности КИИ»?

– Все больше и больше компаний понимают перспективы формирующегося рынка защиты АСУ ТП и предлагают свои услуги. Honeywell уже длительное время предлагает собственные продукты для защиты АСУ ТП, а также продукты ведущих в этой области производителей. Предоставление услуг по защите АСУ ТП, на наш взгляд, является перспективным направлением, так как реализация требований закона № 187-ФЗ потребует мобилизации всех имеющихся квалифицированных ресурсов на рынке. Поэтому мы предлагаем на российском рынке собственные решения для защиты АСУ ТП, в том числе Managed Security Services – услуги управления защитой, включающие предоставление проверенных нами обновлений операционных систем, антивирусного ПО и сигнатур. Такие услуги могут быть особенно востребованы компаниями, которые используют отечественные средства защиты и хотят максимально снизить риски для непрерывности своих технологических процессов.

– Какое место должны занимать требования по защите АСУ ТП в проектах по цифровой трансформации?

– Участвуя во многих проектах по цифровой трансформации, Honeywell предлагает заказчикам и решения, приносящие дополнительную прибыль благодаря повышению эффективности производства, и решения, сохраняющие эту прибыль за счет снижения киберрисков и обеспечения непрерывности бизнеса. Проекты цифровой трансформации достаточно сложные, поскольку реализуются при существующих на предприятии системах АСУ ТП и бизнес-процессах. Минимизировать киберриски при проведении такого проекта возможно при участии производителя АСУ ТП, например в рамках сервисного контракта или контракта на техническую поддержку.

– Как обеспечивается безопасность клиентских данных в случае внедрения промышленных решений?

– В 2017 г. Honeywell получила лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации. Для защиты информации реализуются такие меры, как: учет, контроль и разграничение доступа сотрудников компании в соответствии с их ролями и обслуживаемыми клиентами; обезличивание хранимых и обрабатываемых данных; шифрование данных при передаче и во время хранения; уничтожение данных после окончания срока действия контракта; обеспечение надежности при хранении и обработке данных. ■