Руслан Стефанов:

«Недопущение несанкционированного доступа – главная задача защиты АСУ ТП»

На вопросы журнала Connect отвечает Руслан Стефанов, ведущий инженер Центра комплексных услуг и проектов, ОАО «ЭЛВИС-ПЛЮС»

– Применительно к АСУ ТП существуют понятия функциональной безопасности и информационной безопасности. По опыту вашей работы, как бы вы охарактеризовали реальное состояние той и другой безопасности на отечественных промышленных объектах?

– Состояние информационной безопасности на промышленных объектах можно охарактеризовать как зачаточное. В основном используются средства защиты периметра и антивирусной защиты. Внутри периметра, как правило, защиты нет либо организована она бессистемно. Осведомленность сотрудников минимальная (Stuxnet и еще несколько известных инцидентов). Выполняются элементарные правила хранения паролей, защиты от вирусов.

С функциональной безопасностью ситуация намного лучше. Грубую оценку состояния функциональной безопасности можно получить по данным учета технологических нарушений и по анализу причин их возникновения. Эти показатели из года в год улучшаются. Однако есть ряд ключевых причин (износ оборудования, природные явления), с которыми сложно бороться. У кого-то ситуация лучше, у кого-то хуже.

– Насколько выражена специфика задач информационной защиты АСУ ТП по сравнению с защитой других классов информационных систем? Если такая специфика существует, то в чем она состоит?

– Вся специфика уже известна и не раз обсуждалась. Хотелось бы подчеркнуть, что главное отличие АСУ ТП от других информационных систем – способность оказывать ПРЯМОЕ воздействие на окружающий нас реальный мир, мир, в котором мы живем. Попав «не в те руки», такая способность может привести к драматическим последствиям. В связи с этим главной задачей защиты АСУ ТП видится недопущение несанкционированного доступа к ней, особенно к командам управления исполнительными устройствами и установкам систем противоаварийной защиты.

– В качестве угроз информационной безопасности АСУ ТП сегодня чаще всего упоминаются внешние угрозы – целенаправленные атаки. Но, возможно, есть и другие источники угроз?

– Необходимо обратить внимание на внутренние источники угроз – сотрудников, вовлеченных в хозяйственную деятельность объекта. Они могут быть заинтересованы в различных экономических махинациях. Для этого им требуется доступ к информации об учете ресурсов.

– Что можно сказать о современном состоянии технологий информационной защиты и методической базы в этой области? Насколько они достаточны для нейтрализации актуальных угроз ИБ АСУ ТП?

– Накопленный в технологически развитых странах опыт позволяет существенно сократить разрыв между технологиями информационной защиты, методической базой и актуальными угрозами ИБ АСУ ТП, который существовал еще несколько лет назад. Это способствует нейтрализации большей части известных угроз. Тем не менее продолжается совершенствование мер защиты от угроз, связанных с безопасностью промышленных протоколов, целенаправленных долговременных атак с привлечением крупных ресурсов (APT). В России такая работа обратила на себя внимание государства только в последнее время, и это позволило начать скоординированную подготовку нормативно-правовых документов с учетом опыта всех участников рынка информационной безопасности. ■