Алексей КОСИХИН:
«Среди отечественных компаний растет заинтересованность в получении услуг ИБ из облака»

Интервью с руководителем направления по работе с ТЭК компании «Инфосистемы Джет»

– От чего следует сегодня защищать АСУ ТП? Можно ли считать угрозу внешнего несанкционированного воздействия наиболее актуальной?

– Чтобы понять, как и от чего защищать АСУ ТП, нужно определить основные источники угроз. Их чаще всего четыре. Первый – деятельность иностранных разведывательных и специальных служб. Тут следует вспомнить понятие «кибервойна», в армиях различных стран мира создаются специализированные подразделения. Второй источник – лица (или группы), действующие в корыстных или иных целях. Инциденты ИБ АСУ ТП могут наступать в результате действий уволенных или недобросовестных сотрудников, использующих возможности софта, скрытые на уровне программного кода, хакерских атак, вирусов, случайных взломов и пр. Третий источник связан с деятельностью конкурирующих структур, стремящихся улучшить свои позиции за счет дестабилизации работы других предприятий. К четвертому источнику относятся террористические организации: в связи с тем, что «порог вхождения» для взлома снижается год от года, у них появляется возможность использовать высокотехнологичные инструменты (купленные на «черном» рынке), которые интуитивно понятны и легкодоступны.

Угроза внешнего несанкционированного воздействия сохраняет свою актуальность, и на первый план выходят угрозы, связанные со специализированными вирусами, создаваемыми под определенные типы АСУ ТП, и использованием злоумышленниками недекларированных возможностей прикладного ПО и систем SCADA.

– Когда, при каких условиях можно говорить о том, что АСУ ТП защищается комплексно?

– Задача создания системы ИБ АСУ ТП условно делится на три части: организационную, техническую и организационно-техническую. Первая предполагает создание концепции безопасности АСУ ТП на уровне бизнеса. Разрабатывается пакет документов, регламентирующих подход к обеспечению защиты. В рамках второй части внедряются средства защиты, требующие минимального вмешательства сотрудников. Обычно это межсетевые экраны, средства обнаружения вторжения и защиты от несанкционированного доступа, VPN и антивирусы. На третьем этапе внедряют средства, помогающие оценивать состояние защищенности АСУ ТП, выявлять и оперативно реагировать на инциденты, связанные с ИБ. Обычно это системы класса SIEM и различные сканеры безопасности.

Большинство компаний, занимаясь безопасностью АСУ ТП, выполняют только первую часть либо первую и вторую, но эшелонированный и комплексный подход требует выполнения и организационно-технической части.

– У компании есть опыт обеспечения защиты АСУ ТП на предприятиях разных отраслей. Возможно ли создание неких универсальных сценариев защиты или проекты скорее индивидуальны?

– Мы выполнили ряд проектов по защите АСУ ТП в компаниях ТЭК и нескольких промышленных предприятиях. Полученный опыт позволил нам выработать общий подход к обеспечению ИБ АСУ ТП. Он дает возможность компаниям уже на начальной стадии работы ознакомиться с общей картиной проекта и эффективно контролировать его дальнейшие этапы.

Специфика бизнеса и технологических процессов каждого предприятия накладывает свой отпечаток на разрабатываемые документацию, схемы подключения и настройки средств защиты. Поэтому мы адаптируем общий подход под каждую компанию. Основной упор делается на надежность системы ИБ и использование средств защиты, адаптированных под защиту АСУ ТП.

– Насколько распространена практика получения заказчиками безопасности АСУ ТП как сервиса?

– Услуга, называемая «безопасность как сервис», появилась на российском рынке недавно. В большинстве компаний штат сотрудников ИБ-подразделений составляет пять-шесть человек, а обслуживать им приходится до 20–25 различных решений. Возникает необходимость пополнять штат высококвалифицированными специалистами, занимающимися ИБ технологических сетей. Поэтому среди отечественных компаний растет заинтересованность в услугах ИБ-аутсорсинга и получении услуг ИБ из облака. Многие из них уже готовы отдавать на аутсорсинг ИБ критичных систем, включая мониторинг и реагирование на инциденты. Это позволит компаниям удерживать систему управления ИБ на должном уровне, своевременно реагировать на возникновение новых угроз, на атаки и инциденты, проводить донастройку средств защиты информации. ■