Василий НОСАКОВ:
«Достигнут принципиально новый уровень защищенности критичных производственных сегментов»

Василий НОСАКОВ,
директор департамента информационной безопасности, АМТ-ГРУП

– Идет время, как, по-вашему, меняется ли ситуация в области информационной безопасности АСУ ТП?

– Недавно мы задались целью проверить, насколько актуален «разогрев» темы защиты АСУ ТП и какова степень заинтересованности предприятий этого сегмента рынка в обеспечении ИБ.

Были проанализированы отчеты авторитетных организаций, занимающихся изучением уязвимостей и инцидентов ИБ в АСУ ТП, рассмотрен опыт нашей компании и других предприятий, реализовавших проекты по защите информации в АСУ ТП. В результате мы пришли к выводу, что внимание к вопросам защиты АСУ ТП явно недостаточное. В области защиты критически важных объектов наметилось отставание от ряда развитых стран. Вместе с тем нельзя не заметить и ряд позитивных тенденций: наличие проблемы признано всеми участниками рынка; государственные структуры, регуляторы, законодатели начали серьезную проработку вопроса. Все это способствует тому, чтобы перейти наконец от набора формальных, не связанных между собой инициатив и требований по защите АСУ ТП к решению конкретных задач и реализации проектов по защите АСУ ТП.

– Какие именно законодательные инициативы имеются в виду? Есть ли какие-то временные рамки в части их реализации?

– Мы стали свидетелями появления проекта Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации». В нем определены требования к владельцам КСИИ, обозначены зоны ответственности регуляторов, приведены основные требования к защите и оценке защищенности объектов информационной инфраструктуры страны, а также по обнаружению, предупреждению и ликвидации последствий компьютерных инцидентов.

Сам факт выхода законопроекта является знаменательным событием, говорящим о том, что государство не только озаботилось решением вопросов защиты критической информационной инфраструктуры, но и начинает переходить от слов к делу. Определен конкретный срок вступления в силу закона – с 1 января 2015 г. Надеемся, что к этому моменту будут проработаны и подзаконные акты, без которых реализация данного закона невозможна.

– Изменился ли ваш взгляд на проблематику после получения практического опыта в подобных проектах?

– Да, изменился. Во-первых, к каждому проекту нужен индивидуальный подход, так как и сами системы АСУ ТП, и их реализация в каждой из организаций уникальны. Во-вторых, очень многое зависит от качества первоначального аудита, в ходе которого определяются основные задачи по защите АСУ ТП, приоритеты их выполнения, намечаются возможные подходы к реализации технических решений. В-третьих, необходимо использовать специализированные технические средства защиты, особенно на среднем и нижних уровнях АСУ ТП. На нижних уровнях АСУ ТП это обусловлено спецификой применяемых устройств, технологий и протоколов, связанной с повышенными требованиями к отказоустойчивости, гарантированной доставке сообщений и др. Производители таких специализированных средств защиты зачастую являются и производителями оборудования самих АСУ ТП. Для внедрения подобных решений необходима экспертиза в части построения систем передачи данных АСУ ТП и в других смежных областях.

– Есть ли у вас какие-то практические наработки и успехи в области защиты АСУ ТП?

– Да, есть. В первую очередь хочется отметить, что нами были отработаны в лаборатории и внедрены уникальные решения, позволяющие реплицировать промышленные информационные потоки критичных систем АСУ ТП в менее защищенные корпоративные сегменты сети. При этом полностью исключается возможность несанкционированного доступа из корпоративного сегмента сети в критичные производственные сегменты. Кроме того, мы разработали принципиально новый подход к дизайну защищенных периметров критически важных объектов. Решение позволяет связывать между собой фактически полностью изолированные промышленные сегменты через открытые каналы связи, исключая большую часть внешних угроз, характерных для открытых сетей типа Интернет. Фактически мы достигли принципиально нового уровня защищенности критичных производственных сегментов и в ближайшее время представим это решение на рынке в качестве готового продукта. ■

AMT GROUP

ИСКУССТВО ИНТЕГРАЦИИ

КОРПОРАТИВНЫЕ СЕТИ СВЯЗИ И ПЕРЕДАЧИ ДАННЫХ

ВИДЕОНАБЛЮДЕНИЕ

ЗАЩИТА АСУ ТП

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МОНИТОРИНГ И УПРАВЛЕНИЕ IT-ИНФРАСТРУКТУРОЙ

ВИДЕОКОНФЕРЕНЦСВЯЗЬ

СИТУАЦИОННЫЕ ЦЕНТРЫ

СИСТЕМЫ ХРАНЕНИЯ И ОБРАБОТКИ ДАННЫХ

+7 (495) 725-7660

www.amt.ru

Реклама

БИЗНЕС - ЭТО ЛЮДИ