Николай ДОМУХОВСКИЙ:

«Сейчас все объекты КИИ РФ проходят испытание на прочность»

О текущем состоянии рынка ИБ-решений и сервисов, а также его будущем мы поговорили с заместителем генерального директора по научно-технической работе УЦСБ Николаем Домуховским.

– Насколько успешно, по вашим оценкам, проходят проекты комплексной защиты отечественных промышленных предприятий? Каких средств автоматизации для ускорения этих проектов не хватает?

– Не думаю, что проблема именно в средствах автоматизации. Повышение сложности и увеличение сроков обусловлены скорее тем, что только при создании СБОКИИ подразделения ИТ, автоматизации, связи и безопасности впервые выстраивают тесную взаимную работу. Это существенно меняет привычные процессы. Кроме того, нередко требуется модернизация информационной или инженерной инфраструктуры, чтобы обеспечить корректное функционирование средств СБОКИИ, что требует больших временных ресурсов. Не стоит забывать и про бюджеты: создание такой масштабной системы – это значительные капитальные затраты, не всякое предприятие способно выделить их единовременно. Поэтому проекты разбиваются на отдельные очереди и система строится поэтапно.

– Как, на ваш взгляд, можно защитить предприятие от атак через цепочку поставок?

– Для этого требуется активное участие самого разработчика или поставщика ПО. Что конкретно делать, достаточно подробно изложено в государственном стандарте по безопасной разработке ПО. Самое главное – не нужно забывать, что ответственность разработчика заканчивается не в момент выпуска нового релиза или обновления ПО, а в момент его успешной доставки потребителю.

– Как вы оцениваете уровень соответствия российских промышленных организаций требованиям Закона № 187-ФЗ?

– Практически все субъекты КИИ стараются выполнить требования Закона № 187-ФЗ.

Сейчас все объекты КИИ РФ проходят испытание на прочность в рамках беспрецедентных атак со стороны различных группировок. Это заставляет многих задуматься об адекватности их модели угроз и средств, которые выделяются на обеспечение ИБ. Думаю, что в ближайшее время многие предприятия озаботятся повышением уровня защищенности их информационных систем.

– Как на процесс построения защиты на предприятиях промышленности влияет импортозамещение?

– В целом программных СЗИ отечественного производства достаточно, но с оборудованием дело обстоит гораздо хуже. Даже если не принимать в расчет потенциальные проблемы с производством отечественных процессоров, далеко не все отечественные программные СЗИ поддерживают работу на них.

– Что будет определять развитие рынка средств защиты АСУ ТП в течение ближайших двух лет?

– Конечно, текущая геополитическая ситуация. Необходимо усиливать импортозамещение, обеспечивать поддержку альтернативных (не x86) архитектур, чтобы иметь возможность использовать оборудование, созданное в азиатских странах. В целом на рынке оборудования (особенно чипов) сейчас много изменений – Intel и AMD уже далеко не монополисты, в этом направлении появилось множество стартапов либо, наоборот, пришли зрелые компании (например, Alibaba group).

– В каком направлении ваша компания будет развиваться в 2022 г.?

– Мы думаем, что в 2022-м будут очень востребованы услуги аудита ИБ, проведения пентестов, услуги SOC, создание или модернизация систем ИБ (не только объектов КИИ), а также услуги безопасной разработки ПО (DevSecOps). Наша компания предлагает все перечисленное – на этом мы и сконцентрируемся. ■