Андрей ПОМЕШКИН:
«Наш козырь – оптимальные решения в сфере защиты информации»

В Новосибирской области создается межвузовская учебная лаборатория по проблемам информационной безопасности, на базе которой планируется осуществлять переподготовку специалистов и проводить семинарские занятия для студентов. Преподавателями и авторами курса по защите информации на критически важных объектах станут сотрудники компании «Системы информационной безопасности». В ноябре компания проводит в Новосибирске конференцию по проблемам безопасности платежных систем, включающую мастер-классы и демонстрацию решений. О других инициативах и проектах интегратора, приоритетах в области защиты критически важных объектов нашему корреспонденту рассказал директор ООО «Системы информационной безопасности» Андрей ПОМЕШКИН.

– Какие объекты следует относить к категории критически важных с точки зрения информационной безопасности?

– Необходимо обеспечивать защиту информации на промышленных, энергетических, транспортных, пищевых предприятиях, в частности по производству питьевой воды, в учреждениях здравоохранения, службах МЧС. Особое место в этом ряду, на мой взгляд, должны занимать ИТ-системы, проектируемые для госорганов, например СМЭВ. Включение подобных систем, на основе которых строится взаимодействие государства и общества, в перечень критически важных объектов позволит повысить уровень защиты циркулирующей в них информации.

– С какими типовыми угрозами и рисками в области защиты информации сталкиваются ваши заказчики в госсекторе?

– Основных угроз, на мой взгляд, три: недоступность сервисов, нарушение целостности данных и утрата доверия к системам, сценариям и регламентам их работы. Недоступность сервисов в сфере госуслуг, сбои при обмене данными при межведомственном взаимодействии способны вызвать недоверие к органам власти. Нарушение целостности данных, приводящее к искажению информации, наиболее опасно в условиях чрезвычайных ситуаций.

Серьезную проблему при взаимодействии госструктур с гражданами представляет расхождение заявленных функций и реализованных на базе ИТ-систем, которое может снижать доверие к государству.

Распространенными причинами возникновения подобных угроз являются некачественное исполнение обязательств разработчика, взятых на себя государством или уполномоченной организацией, случайная подмена сценариев в условиях, когда большинство ИТ-систем для региональных органов власти находится в тестовой эксплуатации, уязвимость ПО, на котором работают программисты, ошибки при написании программных кодов и т. д.

– Какая роль при выборе решений заказчиком отводится сотрудникам вашей компании на этапе обсуждения будущего проекта?

– Большой проблемой для заказчика является выбор оптимального решения для обеспечения защиты систем или инфраструктуры, поскольку у него нет целостного представления о процессах, связанных с ИБ. Специалисты нашей компании владеют ситуацией на рынке, ориентируются в нормативно-правовых требованиях и придерживаются комплексного подхода к решению задач в сфере ИБ. Предложить заказчику соответствующее решение, позволяющее оптимизировать его расходы, – одна из обязанностей интегратора.

Зачастую нам приходится демонстрировать заказчику, уверенному в изолированности своей технологической среды, насколько уязвимы объекты его инфраструктуры: вирусы проникают даже на станки с ЧПУ. Уровень современного технологического оборудования сопоставим с уровнем развития компьютерных решений, поэтому информационная безопасность одинаково важна и для офисных приложений, и для АСУ ТП. Если нам удается убедить в этом заказчика, ему легче принимать решение о выделении средств на эти цели.

– Какой проект, реализованный вашей компанией, вы могли бы выделить и почему?

– В рамках одного из проектов по созданию защищенного сегмента СМЭВ по заказу региональных органов власти мы обеспечили безопасность передаваемой информации, используя дополнительные функции имеющегося оборудования и программных продуктов. Благодаря этому не пришлось закупать дорогостоящие специализированные системы и были сэкономлены значительные бюджетные средства. ■