Владимир АКИМЕНКО:
«Защита АСУ ТП – это спланированная целенаправленная работа»

Принятый прошлым летом Федеральный закон № 187-ФЗ «Об обеспечении безопасности КИИ» вступил в силу 1 января 2018 г. Чтобы понять, как он повлияет на российский рынок услуг информационной безопасности, мы задали несколько вопросов **АКИМЕНКО Владимиру Викторовичу**, руководителю Центра кибербезопасности критических инфраструктур АО «ЭЛВИС-ПЛЮС».

– Как обеспечивалась информационная безопасность АСУ ТП промышленных объектов до принятия Закона № 187-ФЗ «Об обеспечении безопасности КИИ»? Насколько часто приходилось учитывать при защите АСУ ТП требования приказа ФСТЭК России № 31? Какие проекты в этой сфере были реализованы вашей компанией ранее?

– Часть организаций, подпадающих под действие Закона № 187-ФЗ «Об обеспечении безопасности КИИ», особенно крупных, уже имеют свои локальные нормативные документы, регламентирующие порядок и требования к обеспечению защиты информации, в том числе на уровне технологических информационных систем. Однако, по нашему опыту, при подготовке заказчиком технических заданий в них, как правило, включались и требования приказа № 31 ФСТЭК России. Стоит отметить, что требования нормативных документов регуляторов, в том числе названного приказа, все больше рассматриваются как важные методические инструменты, позволяющие реализовать эффективные меры по снижению рисков, связанных с нарушением функционирования организации и обусловленных воздействием на ее информационные ресурсы и активы.

ЭЛВИС-ПЛЮС активно занимается вопросами защиты информации технологических систем и критически важных объектов (КВО) с 2010 г. За это время компания выполнила работы по аудиту, проектированию и внедрению систем защиты информации АСУ ТП для ПАО «ФСК ЕЭС», АО «СибурТюменьГаз», ЗАО «РУСАЛ Глобал Менеджмент Б.В.», ряда подразделений и дочерних обществ ПАО «НК «Роснефть», других организаций и предприятий.

– Что для вашей компании меняет Закон № 187-ФЗ? Потребуется ли вашим клиентам что-то переделывать и во что это может обойтись владельцам объектов критической информационной инфраструктуры?

–Учитывая довольно большое количество отраслей, подпадающих под действие Закона № 187-ФЗ, ожидаем, что количество обращений к нам заказчиков возрастет. Даже на первых этапах работ по определению состава объектов КИИ и их категорированию потребуется привлечение специализированных организаций. Нашу задачу я вижу не только в том, чтобы обеспечить соответствие формальным требованиям, но и в том, чтобы объяснить заказчику необходимость реализации этих требований; показать, как это повлияет на его бизнес, его конкурентоспособность; указать на дополнительные преимущества, которые заказчик может получить, интегрируя меры безопасности в основной бизнес-процесс.

Любая переделка требует двойных затрат: сначала нужно что-то сломать, потом сделать заново. Это неэффективно. Все механизмы защиты должны быть гибкими. Наша задача – повысить эффект, сохранив инвестиции. Поэтому любую систему защиты мы рассматриваем как гибкую, адаптивную систему, способную максимальным образом парировать актуальные угрозы.

Сколько нужно потратить на ИБ? Вопрос и простой, и сложный. Сколько, например, нужно потратить

на автоматизацию бизнес-процесса? Столько, сколько необходимо, чтобы итоговый эффект от ее внедрения в определенной перспективе превышал затраты на ее реализацию. Аналогичный подход с оценкой рисков и ущерба может использоваться и при оценке затрат на ИБ. Кстати, такой подход применяется, в частности, при проведении категорирования объектов КИИ.

Важными моментами, на которые мы обращаем внимание при создании различных систем безопасности, являются:

- интегрированность: система защиты должна встраиваться в бизнес-процесс, должна стать его частью и обеспечивать его стабильность, надежность, в том числе в условиях наличия угроз ИБ;
- комплексность и целостность: защита должна реализовываться взаимосвязанным набором мер и средств, минимизирующим риски реализации актуальных угроз по всем векторам атак;
- эффективность: система защиты должна не только минимизировать существующие риски, но и создавать дополнительные преимущества, повышающие управляемость, контролируемость и результативность процессов деятельности организации.

– Насколько, по вашим наблюдениям, российские предприятия готовы к взаимодействию с ГосСОПКА?

– Несомненно, у предприятий интерес к взаимодействию с ГосСОПКА есть, как и готовность к нему. Всем понятно, что против общего врага бороться лучше сообща. Поэтому элементы ГосСОПКА будут развертываться не только на значимых объектах КИИ, но и в организациях, не имеющих таких систем. Полагаю, что количество организаций, которые будут готовы активно участвовать в данном процессе, учитывая определенную, в том числе экономическую, выгоду для себя, постепенно будет расти.

– Есть ли на российском рынке необходимый набор технических решений для построения корпоративных центров реагирования на кибератаки? Какими продуктами ваша компания пользуется для этого?

– Рынок давно предлагает различные решения, в том числе ориентированные на взаимодействие с региональными и ведомственными центрами ГосСОПКА в соответствии с требованиями ФСБ России, которые определены «Методическими рекомендациями по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» и содержат необходимые рекомендации по взаимодействию, а также перечень передаваемых в рамках функционирования системы сведений. Но при этом нужно понимать и оценивать готовность заказчиков использовать и применять такие средства. У всех она разная. Наша компания мультивендорная, поэтому мы ориентируемся на потребности и возможности заказчиков, предлагая им различные варианты и реализуя наиболее оптимальные решения.

– Как коррелирует деятельность государства по Закону № 187-ФЗ с программой «Цифровая экономика» в части вопросов информационной безопасности? Насколько «Цифровая экономика» повлияет на обеспечение информационной безопасности АСУ ТП, учитывая, что центр компетенции по ИБ находится в ведении Сбербанка?

– Цели и задачи Закона № 187-ФЗ довольно плотно коррелируют с программой «Цифровая экономика» в части вопросов информационной безопасности. Этот закон решает часть задач обеспечения ИБ цифровой инфраструктуры, развиваемой в рамках данной программы. Но это лишь небольшая часть задач. Сама программа покрывает гораздо больший пласт вопросов, начиная с развития и стимулирования отечественных разработок и заканчивая вопросами стандартизации и повышения ответственности за нарушения в области ИБ, например, введение с 2020 г. ответственности за неприменение сертифицированных криптографических алгоритмов при организации любого защищенного обмена по каналам связи. Кроме того, программой заложено увеличение доли используемых российских продуктов и средств защиты информации, продолжающее политику импортозамещения и государственного регулирования сферы обеспечения ИБ.

Что касается последнего вопроса, думаю, что создание центра компетенции по вопросам обеспечения ИБ госпрограммы «Цифровая экономика» на базе какой-то отраслевой организации обусловит определенный перекос в сторону соответствующей отраслевой специфики. Представляется, что общей координацией развития этой части программы должны заниматься специализированные институты в области обеспечения ИБ, а центры компетенции должны создаваться на базе отраслевых некоммерческих объединений.

В заключение хочу отметить, что ЭЛВИС-ПЛЮС активно участвует в обсуждении, анализе, апробации и учитывает в своей работе текущие и перспективные тенденции развития информационных технологий и технологий безопасности. Качественное выполнение работ обеспечивается штатом сертифицированных специалистов высокой квалификации по всем направлениям деятельности в области ИБ. Компания также принимает участие в разработке и развитии стандартов и современных подходов к обеспечению ИБ: АО «ЭЛВИС-ПЛЮС» входит в состав технических комитетов ТК122 «Стандарты финансовых операций», ТК26 «Криптографическая защита информации» и рабочих групп по подготовке руководящих документов ФСБ России и ФСТЭК России. ■