Алексей МАЛЬНЕВ:

«Четкая нормативно-правовая база становится основным драйвером развития ИБ на объектах АСУ ТП»

На вопросы журнала Connect отвечает Алексей МАЛЬНЕВ, начальник отдела защиты КСИИ, АМТ-ГРУП

– Насколько востребованы решения в сфере защиты АСУ ТП? Какие наблюдаются тенденции в данной тематике?

– Защита АСУ ТП сейчас находится в списке наиболее актуальных тем в ИБ как в России, так и за рубежом. Для этого есть ряд причин, самые главные из которых заключаются в общем размере рынка ИБ АСУ ТП, сохранении непрерывности функционирования производственных процессов, очевидном отставании ИБ АСУ ТП от актуальных угроз и возрастающем внимании государства и регуляторов к данной тематике. За последние два-три года кардинально поменялся характер спроса и, как следствие, предложения: от решений по защите АСУ ТП требуется наличие понятного для производственников и прозрачного для систем АСУ ТП функционала, а также баз знаний о контрольно-измерительных потоках информации АСУ ТП и т. д. Но, главное, спрос характеризуется требованием к наличию специализированного и комплексного подхода проектных организаций к защите АСУ ТП, опыта в решении задач ИБ АСУ ТП, знания отраслевых стандартов и законодательства в данной области. С учетом высочайшего уровня ответственности владельцев (менеджеров) на предприятиях АСУ ТП в равной степени для них важны соответствие требованиям законодательства, регуляторов, отраслевых стандартов и реальное повышение уровня ИБ АСУ ТП при минимизации рисков для непрерывности производства.

– В каких отраслях проекты ИБ АСУ ТП наиболее востребованы?

– На мой взгляд, какого-то явного преимущества отдельной отрасли в объеме спроса к решениям по защите АСУ ТП сейчас не наблюдается (по крайней мере, в относительном исчислении). Разумеется, задача актуальна для предприятий ТЭК, поскольку в России данная отрасль является локомотивом экономики и доминирует в общем объеме производимой продукции. Именно поэтому ТЭК в числе первых получил законодательное определение (№ ФЗ-256) необходимости выполнения мер информационной безопасности. Но фактически активный спрос сейчас характерен для всех отраслей. Особенно это касается предприятий и систем, категорированных как критически важные объекты (КВО) и ключевые системы информационной инфраструктуры (КСИИ), – это телекоммуникационные холдинги государственного масштаба, предприятия ТЭК, объекты химической промышленности, системы управления транспортом, предприятия добывающих отраслей. Пожалуй, пока можно выделить несколько меньший спрос со стороны отраслей машиностроения и пищевой промышленности, хотя естественный процесс информатизации в конце концов затронет все отрасли без исключения. Например, суточное прерывание работоспособности систем управления отгрузки товарами на предприятии (заводе) может вызвать миллионные потери для владельцев бизнеса.

Единственная причина, почему проекты защиты ИБ АСУ ТП пока не очень востребованы в некоторых отраслях и на конкретных предприятиях, заключается в длительном жизненном цикле функционирования оборудования и наличии большого парка устаревшего оборудования. С новым витком модернизации производства, централизации и информатизации функций управления производственными процессами задачи ИБ АСУ ТП станут актуальными не меньше, чем в самых передовых с точки зрения ИБ отраслях.

– Какие нормативно-правовые тенденции наметились в области ИБ АСУ ТП?

– В последнее время наблюдались существенные изменения (точнее, тенденции) в нормативно-правовой области ИБ АСУ ТП. Все последние годы мы жили в условиях отсутствия четкой взаимосвязи между законодательным уровнем, уровнем регуляторов и уровнем отраслевых стандартов (в дополнение к постановлениям Правительства и указам Президента). До сих пор все руководствовались на законодательном уровне № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса», ст. 11, на уровне регуляторов – нормативно-методическими документами ФСТЭК, в области отраслевых стандартов встречаются документы разного уровня проработки (иногда их нет вовсе).

Сегодня появилась надежда на исправление ситуации. В 2012 г. Совет Безопасности выпустил дорожную карту «Основные направления государственной политики в области обеспечения безопасности АСУ ТП КВО Российской Федерации», определяющую основные этапы развития государственной системы информационной безопасности для объектов КВО. В августе 2013 г. опубликован проект Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации». Этот законопроект, пожалуй, может стать наиболее важным правовым документом в области ИБ АСУ ТП за последние годы. Согласно данному законопроекту (предположительно он вступит в силу с 1 января 2015 г.) критические системы информационной инфраструктуры будут поделены на три уровня критичности (по аналогии с категорированием ФСТЭК КСИИ), определятся зоны ответственности основных регуляторов ФСТЭК и ФСБ, будет прописан алгоритм взаимодействия объектов критической инфраструктуры и государственных центров предотвращения компьютерных атак. Практика западных стран (в первую очередь США) показывает, что четкая нормативно-правовая база становится основным драйвером развития ИБ на объектах АСУ ТП, поэтому появление данного законопроекта, на мой взгляд, явление сугубо позитивное. Однако важно не доводить дело до абсурда, когда выполнение требований законодательства может стать экономической катастрофой для предприятий. Другими словами, регуляторам также нужно учитывать баланс задач и приоритетов бизнеса и ИБ на предприятиях АСУ ТП. ■

> Защита АСУ ТП сейчас находится в списке наиболее актуальных тем в ИБ как в России, так и за рубежом.

Новости

Identity Manager для среднего бизнеса

Компания «Инфосистемы Джет» вывела на рынок новый продукт Jet inView Identity Manager – систему автоматизации управления учетными записями и доступом.

Традиционные IdM-решения, которых на рынке большинство, представляют собой своего рода «конструктор» – система собирается индивидуально под каждого конкретного заказчика, чтобы максимально соответствовать его бизнес-процессам. Однако такое решение слишком дорого для средних компаний. Были попытки предлагать на рынке «коробочные» IdM-решения, однако в силу ограниченного функционала и невозможности адаптации к особенностям бизнеса они не подходили большинству заказчиков.

Компания «Инфосистемы Джет» решила предложить рынку собственное решение для компаний со штатом от 500 до 2500 сотрудников. Продукт Jet inView Identity Manager основан на технологической платформе IBM Security, которая позволила предоставить достаточно полную функциональность решения, возможность масштабирования, а также отказоустойчивость и производительность. Платформа была дополнена возможностями интеграции с различными корпоративными системами, в том числе российских производителей, – на сегодня имеется 40 штатных коннекторов. Кроме того, в систему заложены наиболее востребованные процессы управления доступом. На данный момент таких процессов 12: «прием на работу», «перевод по должности», «увольнение», «запрос/отзыв прав» и др., они запускаются либо на основании данных кадровой системы, либо вручную. Пользователям доступны более 30 отчетов о состоянии прав доступа, активных и согласованных заявках, о различных процессах и объектах. Имеются также дополнительные отчеты, необходимые для расследования инцидентов и ИТ-аудита.

По утверждению разработчиков, Jet inView Identity Manager решает 80% проблем управления доступом за 20% стоимости типового IdM-решения. Объем рутинной работы по исполнению заявок сокращается на 60%, а сотрудники получают необходимые права доступа за несколько минут.