Защита АСУ ТП: проект или стиль жизни?

Алексей КОСИХИН,
руководитель направления по работе с ТЭК Центра информационной безопасности компании «Инфосистемы Джет»

Проблема защиты критически важных объектов (КВО) еще некоторое время назад широкой публике была знакома по большей части как одна из самых зрелищных фантазий голливудских сценаристов и режиссеров. И немудрено – мировой кинематограф представляет благодарному зрителю целую плеяду блокбастеров, ключевые антигерои которых – злодеи новой формации. В последние годы кинематографические кибертеррористы с завидным постоянством демонстрируют таланты к эффектной организации техногенных коллапсов национального масштаба, экологических катастроф, масштабных обвалов фондовых рынков, взломов информационных систем и манипулированию данными различных спецслужб и т. п. При этом сама идея борьбы с киберпреступностью, столь увлекательно популяризированная, имеет под собой вполне реальные жизненные обоснования.

Секреты национальной безопасности

Во-первых, даже разовое нарушение нормального режима работы технологических установок некоторых компаний (спровоцированное умышленно или непреднамеренно) может оказаться чревато катастрофическими последствиями – многомиллионным ущербом, рисками возникновения ситуаций, угрожающих жизни и здоровью населения целых регионов. Чего стоит, например, авария на Саяно-Шушенской ГЭС, в результате которой погибли десятки человек… Аналогичные нарушения могут быть спровоцированы и в системах управления, как в небезызвестной истории с вирусом Stuxnet, выведшим из строя иранские центрифуги, обогащающие уран. Тогда обошлось без человеческих жертв, но развитие иранского ядерного проекта в целом застопорилось. А если представить, что разговор идет об объекте, еще более важном в рамках национальной безопасности? Для таких организаций безопасность систем технологического управления имеет первостепенное значение.

Во-вторых, с практической точки зрения многие отечественные компании не уделяют достаточного внимания защите АСУ ТП, зачастую ограничиваясь применением технологий межсетевого экранирования, что подтверждается результатами подавляющего большинства тестов на уязвимость, с которых традиционно начинается любой проект по защите АСУ ТП. Демонстрируя уязвимость обследуемых систем, наши эксперты разными способами получают доступ непосредственно к серверам управления технологическими процессами, к управлению ключевыми агрегатами и т. п. Например, через Wi-Fi-сети (в том числе нелегально организованные сотрудниками в личных целях), незакрытые дыры в сетевом периметре, с использованием методов социальной инженерии и т. д.

Таким образом, резкий всплеск интереса к данной тематике отнюдь не случаен и обеспечение безопасности критически важных объектов входит сегодня в список самых обсуждаемых тем в отечественной законотворческой среде и различных сферах бизнеса. Флагманом в этом направлении традиционно выступил энергетический комплекс. Затем на тему защиты собственных АСУ ТП более пристальное внимание обратили нефтедобывающие и нефтеперерабатывающие организации, предприятия отечественной промышленности, транспортные компании и т. д.

Защита АСУ ТП — дело не одного дня

Оперируя понятием «проект по защите АСУ ТП», мы имеем в виду некую совокупность мероприятий (согласованных по цели, задачам, месту и времени), направленных на нейтрализацию внутренних и внешних угроз и минимизацию ущерба от их возможной реализации. Наш опыт показывает, что подходить к созданию системы безопасности автоматизированных систем управления технологическими процессами следует комплексно, с учетом нескольких уровней мер: административного, процедурного и программно-технического.

Главной целью мер административного уровня, в рамках которого руководством организации предпринимаются действия общего характера, является формирование программы работ по обеспечению ИБ АСУ ТП в соответствии с общей концепцией защиты. Основу такой программы традиционно составляет пакет документов, позволяющий регламентировать высокоуровневый подход к обеспечению ИБ и описывающий политику развития системы безопасности АСУ ТП в целом.

Процедурный уровень ориентирован на человеческий фактор. Его основная цель – определение и выполнение требований по

обеспечению безопасности компонентов АСУ ТП за счет создания и поддержания режима ИБ АСУ ТП.

На программно-техническом уровне внедряются средства, предназначенные для управления доступом, обеспечения целостности и безопасного межсетевого взаимодействия, антивирусной защиты, эффективной оценки состояния защищенности АСУ ТП, выявления и оперативного реагирования на инциденты ИБ. К таким средствам относятся системы класса SIEM и различные сканеры безопасности.

> Использование термина «проект» применительно к задаче по обеспечению ИБ АСУ ТП не вполне корректно. Правильнее использовать слово «программа» — оно точнее отражает масштабность и длительность процесса. Эта программа включает в себя «пласты», «накрывающие» всю АСУ ТП, и отдельные элементы — «кубики», нацеленные на решение более локальных задач. И «пласты», и «кубики» могут строиться в различном порядке, не мешая друг другу.

Таким образом, использование термина «проект» в классическом его значении применительно к задаче по обеспечению ИБ АСУ ТП не вполне корректно. В данном контексте равильнее использовать слово «программа» – оно точнее отражает масштабность процесса и его растянутость во времени.

Безопасная 3D-«геометрия»

Если попытаться такую программу визуализировать, то она будет включать в себя масштабные «пласты», накрывающие всю АСУ ТП, и отдельные элементы – «кубики», нацеленные на решение более локальных задач (например, контроль администраторов). К первой группе относятся:

- базовый уровень – архитектура АСУ ТП: в идеальном случае требования ИБ необходимо учитывать на этапе проектирования и разворачивания АСУ ТП. Но на практике это редко возможно, так как о безопасности систем управления критически важных объектов подавляющее большинство игроков отечественного рынка стали задумываться лишь в последние два-три года, а функционирующие у них АСУ ТП гораздо «старше». Иными словами, их проектировали и разворачивали без учета современных требований ИБ. Таким образом, на архитектурном уровне нам нередко приходится сталкиваться с необходимостью проведения фрагментарной «реконструкции» прямо на работающей АСУ ТП (так, например, проводится оптимизация информационных потоков);
- сетевая безопасность: возможные изъяны в проектировании АСУ ТП с точки зрения обеспечения сетевой безопасности можно свести к минимуму за счет внедрения дополнительных средств защиты (IPS, межсетевых экранов, VPN и т. п.);
- антивирусная безопасность, реализованная с учетом требований АСУ ТП;
- контроль доступа, аутентификация.

Роль «кубиков» в этой схеме играют средства защиты, внедрение которых требует относительно меньших ресурсов, а отдача от них может быть получена в более сжатые сроки. Например, средства для контроля привилегированных пользователей, позволяющие контролировать администраторов, подрядчиков и аутсорсеров с точки зрения легитимности предпринимаемых ими действий, а не только в части аутентификации. Вторым «кубиком», внедрение которого можно запускать на самых начальных этапах работы, можно считать сканеры уязвимостей, адаптированные для работы в технологическом сегменте.

Наша практика показывает, что такое «геометрическое» разделение вовсе не накладывает каких-либо жестких ограничений с точки зрения очередности их выполнения. К примеру, и масштабные «пласты», и более компактные «кубики» могут строиться в различном порядке, не мешая друг другу. Более того, мы часто сталкиваемся с ситуациями, когда системы контроля администраторов или сканирования уязвимостей внедряются одними из первых, а результаты их работы используются для корректировки общего направления работ по созданию полноценной системы безопасности АСУ ТП.

Секрет концепта — в дозировке рисков

Описанная концепция обеспечения ИБ АСУ ТП отличается гибкостью, что позволяет кастомизированно формировать очередность этапов, реализуемых в рамках комплексной программы по защите каждой отдельной АСУ ТП. В данном случае ключевым параметром, влияющим на очередность закрываемых проблем, является величина возможного ущерба в результате того или иного ИБ-риска, характерного для АСУ ТП.

Например, наиболее значимые риски связаны с проникновением внешнего нарушителя внутрь защищаемого периметра, поскольку в этой ситуации невозможно предсказать, каковы его цели. С равной долей вероятности мы можем иметь дело как с хакером-«игроком» (для которого важен сам факт взлома системы защиты), так и с целенаправленной атакой на системы управления АСУ ТП – здесь риск остановки АСУ ТП более чем очевиден. При этом риск проникновения злоумышленника в защищаемый периметр извне – один из самых распространенных для любого вида АСУ ТП. К числу специфических рисков, но не менее значимых для жизнеспособности АСУ ТП относится группа рисков, возникающих вследствие использования неадаптированных средств защиты. Например, большинство антивирусов не понимает протоколы, по которым работают АСУ ТП, опознают их как вредоносный код и блокируют. Существуют также риски, обусловленные уровнем зрелости самой АСУ ТП. В частности, риск взлома извне более вероятен для АСУ ТП, реализованной на современной промышленной платформе, что связано с увеличенным кругом лиц, имеющих к ней доступ, – это и представители вендора (удаленно обновляющие платформу), и специалисты интегратора (внедрявшие платформу и, возможно, продолжающие ее модернизацию). С другой стороны, если АСУ ТП работает на платформе, разработанной индивидуально, всегда есть риск снижения ее работоспособности, обусловленный невозможностью оперативно устранить какие-либо неполадки в силу отсутствия на рынке специалистов нужной квалификации.

Следовательно, к наиболее важным с точки зрения ИБ относятся: во-первых, внешний периметр, так как именно он позволит отсеять львиную долю всех возможных внешних атак на АСУ ТП; во-вторых, серверы управления как наиболее критичный элемент инфраструктуры, отвечающий за работу всей автоматизированной системы управления; в-третьих, диспетчерские рабочие станции, с которых можно вводить ряд ключевых команд: например, отключить систему автоматической сигнализации, поднять до максимума или опустить до минимума ряд критически важных для работы аппаратной части АСУ ТП параметров и т. д.; в-четвертых, контроллеры – это уровень более низкий, чем серверы управления или диспетчерские рабочие станции, но не менее важный, ибо позволяет управлять всевозможными датчиками, заслонками и прочими устройствами.

Каким путем пойдем, товарищи?..

Защиту АСУ ТП часто пытаются приравнивать к стандартному разовому проекту в области информационной безопасности (аналогичному, например, внедрению систем класса DLP или IdM, нацеленных на устранение конкретных, четко описанных проблем, с прогнозируемыми критериями в части их эффективности и окупаемости), что, на наш взгляд, не вполне правильно. Как мы уже говорили, построение ИБ АСУ ТП – весьма продолжительный процесс, связанный с постоянным мониторингом существующих рисков и их оценкой, внедрением средств защиты (в том числе таких, чья окупаемость прогнозируется только в долгосрочной перспективе), соответствующей донастройкой уже внедренных средств и т. п. Это обусловлено, с одной стороны, непрерывно расширяющимся спектром угроз безопасности АСУ ТП, с другой – с логическим изменением инфраструктуры самих АСУ ТП (появлением новых сегментов, требующих защиты). Следовательно, в контексте темы ИБ АСУ ТП логичнее говорить не столько о работах, ограниченных во времени или стоимости, сколько о создании своеобразной идеологии, принимаемой организацией в качестве стратегического пути развития ИБ.

Таким образом, приступая к защите АСУ ТП, стоит учитывать, что созданная система защиты потребует поддержки, донастройки и постоянного контроля. В большинстве компаний штат сотрудников ИБ-подразделений составляет пять-шесть человек, а обслуживать им приходится до 20–25 различных решений. Это ставит организации перед необходимостью пополнять штат высококвалифицированными специалистами, занимающимися ИБ технологических сетей.

> В контексте темы ИБ АСУ ТП логичнее говорить не о работах, ограниченных во времени или стоимости, а о своеобразной идеологии, в соответствии с которой организация планирует стратегию ИБ. Это новый стиль жизни, подразумевающий постоянное развитие созданной системы защиты.

Логичным ответом российского рынка на потребность организаций в минимизации ресурсов (бюджет, штат сотрудников и т. п.), затрачиваемых на поддержку безопасности АСУ ТП на должном уровне, стало появление услуги, называемой «безопасность как сервис». Среди отечественных компаний растет заинтересованность в услугах ИБ-аутсорсинга и аутстаффинга, а также в получении услуг ИБ из облака. Многие из них уже готовы отдавать на аутсорсинг ИБ критичных систем, в том числе мониторинг и реагирование на инциденты. Это позволит удерживать систему управления ИБ на должном уровне, своевременно реагировать на возникновение новых угроз, на атаки и инциденты, проводить донастройку средств защиты информации. ■