Защита технологических процессов: чем и куда движется отрасль

Р.Н. Хайретдинов (ГК InfoWatch)

Проанализирована ситуация в области кибербезопасности АСУТП с позиции требований регулятора, количества реальных инцидентов, оценки рисков. Показаны реальные шаги в направлении увеличения защищенности промышленных систем и сдерживающие данное направление факторы.

Ключевые слова: кибербезопасность, АСУТП, инцидент, риск, информационная безопасность.

Защита АСУТП — относительно свежее направление в информационной безопасности (ИБ). До сих пор разговоров о защите гораздо больше, чем реальных проектов. Первые сообщения об успешных кибератаках на промышленные и энергетические предприятия датированы 2009–2010 гг. И на рынке до сих пор нет как реального спроса, так и полноценных предложений.

Двигателем новых проектов в ИБ обычно являются одна из трех причин — инциденты, оценка рисков или требования регуляторов. На сегодняшний день ни одна из этих причин не является двигателем рынка из-за небольшого числа доказанных инцидентов, отсутствия доверенной статистики и невнятной позиции многочисленных регуляторов как отраслевых, так и федеральных.

Надежда на активное регулирование

Большинство профессионалов по защите АСУТП сходятся во мнении, что рынок защиты промышленных предприятий совершит рывок только при явном требовании регуляторов к предприятиям не только иметь такие системы, но и проходить проверки. Ключевым нормативным документом, регламентирующим вопросы обеспечения безопасности области АСУТП, является Приказ № 31 ФСТЭК России «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»

Ранее выпущенный ФСТЭК набор методических документов (2007–2009 гг.), ряд из которых под грифом «ДСП», также признается актуальным, несмотря на некоторое их устаревание, но в разъяснениях ФСТЭК к применению 31-го приказа сообщается, что они также могут применяться, но только в части, не противоречащей 31-му приказу. Поэтому на сегодняшний день при построении процессов защиты АСУТП следует пользоваться именно 31-ым Приказом.

Другие регулирующие документы также декларируют актуальность защиты АСУТП. Например, 68-ая статья «Стратегии национальной безопасности» утверждает: «Одним из главных направлений РФ на среднесрочную перспективу определяет технологическую безопасность. С этой целью совершенствуется государственная инновационная и промышленная политика, определяются в качестве безусловного приоритета инновационного развития национальной экономики фундаментальная и прикладная наука, образование, совершенствуется федеральная контрактная система и система государственного заказа на подготовку высококвалифицированных специалистов и рабочих кадров, развивается государственно-частное партнерство в сфере науки и технологий, создаются условия для интеграции науки, образования и промышленности, проводятся системные исследования в интересах решения стратегических задач национальной обороны, государственной и общественной безопасности, а также устойчивого развития страны».

В Проекте Доктрины информационной безопасности РФ в статье 18 говорится: «Обеспечение информационной безопасности РФ в области государственной и общественной безопасности направлено на повышение защищенности критической информационной инфраструктуры РФ и устойчивости ее функционирования, включая совершенствование механизмов предупреждения и обнаружения угроз информационной безопасности и ликвидации последствий их реализации»

Что останавливает?

«Навесные» (то есть «не встроенные») системы ИБ плохо работают в устаревших АСУТП, которые проектировались и внедрялись, когда не было еще никаких кибер-рисков. К тому же даже для внедрения «навесных» решений необходимо остановить АСУТП, что довольно непросто, если вообще возможно.

Сегодня защиту от кибератак на «промышленные» системы разрабатывают и предлагают в основном те же компании, которые выпускают и традиционные средства защиты «офисных» систем. Однако требования защиты АСУТП отличаются от требования по защите «офисных» или «финансовых» систем. На первое место в приоритетах выходит доступность, оставляя привычную конфиденциальность на последнем месте. Действительно, например, для электростанции не столь важно, какие данные из системы управления могут украсть хакеры, лишь бы они не нарушили ее работоспособность.

К тому же в различных отраслях промышленности системы автоматизации могут иметь различную архитектуру. Например, в атомной энергетике, нефтеперерабатывающей отрасли или на транспорте требуется повышенная безопасность, применяются архитектуры АСУТП с резервированием, средства и системы автоматизации, имеющие соответствующие сертификаты и разрешения на применения в ответственных приложениях, защищенные протоколы передачи данных. Поэтому и универсальных «специалистов по защите АСУТП» быть не может, слишком важен при защите контекст конкретной отрасли.

На сегодняшний день еще не состоялась встреча двух экспертиз — АСУТП и кибербезопасности. Специалисты, пришедшие из промышленной автоматизации,

не обладают нужной экспертизой в кибербезопасности, а киберзащитники пока не набрались опыта в конкретных отраслях промышленности. Нынешнее состояние экспертизы: киберзащитники работают в привычных им IP-сетях, а специалисты по АСУТП — в сетях промышленных. Поэтому, если посмотреть на нечастые пока проекты по анализу защищенности АСУТП, то они не опускаются ниже уровня SCADA, с которым исторически знакомы пен-тестеры (pen-test, penetration test — анализ системы на проникновение). То есть пока чаще всего речь идет об исследовании возможностей проникновения по IP-сетям на управляющие компьютеры и серверы. Однако для хакера проникнуть на сервер — это успешный пен-тест, а для системы промышленной автоматизации такое проникновение не представляет никакой опасности, поскольку выполнить хоть какую-то команду на изменение с управляющего сервера не так-то просто. Можно, конечно, «украсть» какую-то информацию с этих серверов или компьютеров, но такая «атака» обычно критична для финансовых систем или систем обеспечения государственных услуг, а промышленным системам она не опасна.

От пен-тестов к защите

Однако каково бы не было нынешнее состояние технологической экспертизы и требования регуляторов, мы не можем не работать над инструментами и методиками отражения будущих кибератак. Наши геополитические противники не скрываясь создают кибервойска, и одним из самых вероятных направлений кибердара являются критически важные системы, в частности, энергетика и транспорт. Так что эффективная защита критичных объектов от кибератак и кибертеракторов — насущная задача, если не сегодняшнего, то совершенно точно завтрашнего дня.

Прежде всего, надо поменять отношение «защитников» к ответственности за работу своих решений. Когда решение для защиты АСУТП выпускает производитель антивирусов, обновление ПО которого раз в несколько лет «кладет» тысячи компьютеров по всему миру, то надо начинать волноваться. Если при сбое офисного компьютера его просто перегрузят или, в крайнем случае, переустановят, то сбой в системе промышленной автоматизации — это взрыв, пожар, утечка ядовитых или радиоактивных веществ.

Далее надо распространить на системы защиты принятый в АСУТП принцип наличия и беспрекословного соблюдения регламентов на все случаи жизни. Дя предельно высокого уровня ответственности (человеческие жизни) в критичных системах это должно стать обязательным.

Специализированные технические решения необходимо иметь на всех уровнях: диспетчерском (SCADA), управления (программируемые контроллеры) и “полевой” (полевые устройства). На этом этапе важно обеспечить обнаружение угроз ИБ (проникновение, злонамеренное ПО, некорректная работа управляющих систем) и реагирование на них как в корпоративных сетях, так и в технологических и инженерных системах, а также в технических средствах охраны.

Из-за высокого уровня ответственности, а значит, нетерпимости к сбоям и ложным срабатываниям систем защиты, пока принципиально не определено, кто будет отвечать за сбои в системах защиты. Производители АСУТП обычно не разрешают сторонним производителям вторгаться в автоматизированные их оборудованием системы, поэтому, даже имея в своей продуктовой линейке антивирусы и системы обнаружения вторжений, производители средств защиты АСУТП не могут включить их в режим защиты, то есть блокирования определенных команд. Зачастую для запуска системы защиты в активный режим требуется временная остановка системы или ее элементов, а любое несанкционированное с производителем изменение внедренной технологической системы немедленно приводит к отмене гарантий. Поэтому пока чаще всего системы защиты работают в пассиве, анализируя команды постфактум и сообщая оператору о подозрительной активности. То есть, это по определению никакая не защита, а лишь система информирования оператора об аномалиях в технологической системе. Такой подход пока примиряет потребность в защите и большой (именно для АСУТП) уровень ложных срабатываний промышленных антивирусов и систем обнаружения вторжений.

Многие специалисты по АСУТП утверждают, что в существующих условиях готовы ставить в активный (то есть блокирующий команды) режим только системы защиты, полностью интегрированные в технологический процесс, а значит, от производителя средств промышленной автоматизации, а не от именитых ИБ-вендоров. Это связано с приоритетами защиты АСУТП — доступностью и защитой всего ТП. Поэтому наиболее эффективными представляются не «навесные» средства, которые заказчик готов рассматривать только в пассивных режимах, а решение «защищенного ТП из одних рук с гарантией и ответственностью». Возможно, мы скоро услышим о поглощениях крупными производителями систем промышленной автоматизации ИБ-компаний или о лицензировании ими технологий и продуктов.

Заключение

Пока на рынке больше конференций на эту животрепещущую тему, чем реальных проектов. Да и те редкие проекты, что сейчас проходят — не про защиту, а про исследование защищенности. Однако такую важную часть ИБ, имеющую отношение не к данным и даже не к деньгам, а к человеческим жизням и базовым системам жизнеобеспечения, нельзя пускать на самотек, пусть и ведомый «невидимой рукой рынка». Свое веское слово должны сказать регуляторы всех уровней, а также производители самих систем технологической автоматизации.

Хайретдинов Рустэм Нилович *– руководитель проекта Appercut, заместитель генерального директора ГК InfoWatch.*
Контактный телефон (495) 22-900-22.
Http://www.infowatch.ru