Владимир ДРЮКОВ:

«Ростелеком-Solar готов решать задачи больших федеральных заказчиков, в том числе по защите АСУ ТП»

«Ростелеком» с покупкой Solar Security приобрел большое количество компетенций, связанных в том числе с безопасностью АСУ ТП. О ключевых проблемах и перспективах отрасли мы поговорили с Владимиром Дрюковым, директором центра мониторинга и реагирования на кибератаки Solar JSOC компании Ростелеком-Solar.

– Что может предложить Ростелеком-Solar владельцам АСУ ТП?

– Сейчас тематика безопасности АСУ ТП получила новый импульс к развитию. Ее основным драйвером на данный момент является Федеральный закон «О критической информационной инфраструктуре». Деятельность компании в сфере защиты АСУ ТП включает два основных направления (хотя ими не ограничивается). Первое нацелено на то, чтобы помочь заказчику разобраться в рисках и угрозах текущего состояния АСУ ТП. Этот процесс проходит под эгидой категорирования объектов критической информационной инфраструктуры. В зависимости от конкретных объектов (например, в энергетике) эта задача может иметь совершенно различную сложность, однако в общем и целом она сводится к тому, чтобы понять, как устроен конкретный технологический сегмент сети, какие риски информационной безопасности он в себе несет и каким образом их можно устранить или компенсировать.

Дальше это направление распадается на два: первое – система активной защиты или система специализированной защиты АСУ ТП, которую необходимо внедрить, настроить и сопровождать, для того чтобы АСУ ТП корректно функционировали и все вектора угроз были закрыты.

Второе – тематика ГосСОПКА, а также мониторинг, анализ, реагирование и ликвидация последствий тех инцидентов, которые выявляются в сети АСУ ТП. На каждом из этих направлений есть свои подходы и задачи. В первом случае мы говорим о реализации интеграционных проектов по построению комплексных систем защиты АСУ ТП и их эксплуатации. Во втором – о более классических проектах Security Operations Center (SOC), но с акцентом на тематику АСУ ТП, с учетом ее специализированных систем и сценариев атак.

– Что вы можете предложить субъектам КИИ в рамках проведения процедуры категорирования принадлежащих им объектов?

– Проекты, связанные с Законом № 187-ФЗ, состоят из типовых этапов. Первый этап включает обследование или аудит. Прежде всего мы помогаем определить, относится ли юридическое лицо к субъектам КИИ. У многих организаций эта задача сейчас вызывает серьезные затруднения.

Второй этап – разобраться с процессами в соответствующих сферах деятельности. Речь в данном случае идет не только о бизнес-процессах, но и о технологических и других, перечисленных в постановлении. Необходимо установить взаимосвязь между процессами и информационными системами, АСУ или ИТКС. Иногда несколько процессов взаимодействуют с одной и той же системой, и тогда приходится заниматься их укрупнением. Заказчики редко готовы к реинжинирингу процессов, однако мы все же рекомендуем вносить в них определенные изменения.

На следующем этапе осуществляется сбор информации, необходимой для категорирования объектов КИИ, после чего мы помогаем провести категорирование.

Затем субъекту КИИ необходимо перейти к формированию требований к системе защиты информации. Здесь на помощь приходят соответствующие приказы ФСТЭК – № 235 и № 239. Мы вместе с заказчиком следуем процедуре: техническое задание, моделирование угроз и все остальные этапы построения СУИБ

и выполнения требований приказов. В завершение мы осуществляем поставку, наладку и внедрение систем защиты. Мы готовы выполнять все этапы под ключ, но, разумеется, это зависит от потребностей и собственных возможностей каждого заказчика.

– Есть ли у вас завершенные проекты по категорированию субъектов КИИ?

– Да, у нас есть разные проекты, касающиеся нескольких отраслей. Одним из самых сложных был проект по практической реализации требований № 187-ФЗ в одной из компаний электросетевого комплекса РФ.

У заказчика была развитая распределенная инфраструктура. В ходе работ было изучено 259 объектов (подстанции разного класса напряжения, структурные подразделения и связанные с ними системы), 33 процесса основной деятельности, более 200 систем. В результате выделено 15 объектов защиты, среди которых пять значимых объектов КИИ и десять объектов, которым не была присвоена категория значимости, однако собственник принял решение об их защите.

После выделения объектов КИИ в соответствии с приказом ФСТЭК от 22.12.2017 № 236 были составлены акты о категорировании и по методике, рекомендованной регулятором, разработаны модели угроз.

Далее, для построения системы безопасности значимых объектов КИИ были разработаны подсистемы безопасности, релевантные выделенным актуальным угрозам, и выбраны технические средства защиты информации, которые мы протестировали на совместимость с системами АСУ заказчика. Было рассмотрено три варианта реализации этой задачи: стенд на стороне заказчика, инфраструктура на стороне вендора АСУ ТП и тестирование на реальной инфраструктуре заказчика. В итоге был выбран самый сложный вариант – развертывание на реальной сетевой инфраструктуре энергетической компании.

На выходе получен эскизный проект подсистем безопасности 15 объектов и спроектирован корпоративный проект ГосСОПКА.

Это первый проект для энергетики, в рамках которого удалось пройти все этапы построения КИИ в соответствии с № 187-ФЗ и дойти до создания технорабочего проекта. Взаимодействие с вендорами АСУ ТП позволило создать типовой проект по обеспечению безопасности КИИ для сетевых энергетических компаний, включающий использование встроенных систем безопасности АСУ ТП.

– Какие отрасли наиболее активны в области защиты своих систем?

– Самую большую активность в этом отношении проявляют отрасли промышленности, энергетики и топливно-энергетического комплекса. Причины во втором и третьем случае достаточно понятны: во-первых, эти отрасли уже сталкивались с киберугрозами, есть подтвержденные вектора атак, и мировой опыт показывает, что есть случаи, когда злоумышленники разрабатывают ВПО специально для этих отраслей. Речь идет о BlackEnergy, теперь переживающем новую жизнь, Industroyer и Triton – об APT, которые описывались исследователями разных стран.

Во-вторых, эти отрасли из всех сетей АСУ ТП являются наиболее зрелыми в вопросах информационной безопасности. Они были отнесены к КВО, и еще на этом этапе они в рамках приказа № 31 ФСТЭК уже начали огромную работу по подготовке своей инфраструктуры и приведению ее в соответствие с требованиями информационной безопасности. Несколько специфичнее картина в атомной промышленности, но там действительно ведется большая работа. Остальные скорее понемногу догоняют, но сложно перечислить отрасли, где бы работа не велась совсем. Вектор защиты технологических процессов воспринимается всерьез всеми компаниями на рынке.

– Насколько сформирован российский рынок услуг центров мониторинга по защите АСУ ТП?

– Пока что мало какие из центров мониторинга подходили к тематике АСУ ТП. Одна из главных причин – это то, что для данного сегмента характерны специфичные вектора угроз, требующие от SOC достаточно редкой профильной экспертизы по тематике АСУ ТП.

Второе – производственники с большой неохотой дают на подключение даже средний уровень АСУ ТП, поэтому возможность получить какой-то опыт в этой области во многом зависит от того, насколько заказчик доверяет центру мониторинга. Поэтому проработка практических кейсов также идет с большим скрипом. В результате получается парадоксальная картина, когда экспертиза в тематике АСУ ТП и в тематике SOC сочетаются буквально в двух-трех компаниях. Остальные пока продолжают ориентироваться исключительно на коммерческий рынок, корпоративные сети и нижний уровень сегмента АСУ ТП.

Кроме того, важно понимать, что защита АСУ ТП – это, как правило, стратегические проекты огромной емкости. Например, средняя энергетическая компания – это 1000 объектов по всей территории страны, каждый из которых требует мониторинга со стороны SOC. Такое количество объектов подразумевает, что компания должна быть готова выделить очень большую команду, до 30–40 человек, для обслуживания этого заказчика. При этом сейчас даже сервис-провайдеры находятся в условиях серьезного кадрового голода. Поэтому все они трижды думают, стоит ли ввязываться в большой проект, например в энергетике или ТЭК, и смогут ли они «проглотить этого слона» целиком, когда проект станет полностью федеральным. В этом нам несколько проще, чем всем остальным, – в первую очередь потому, что мы тесно сотрудничаем с вузами, благодаря чему формируется серьезный кадровый резерв. Мы действительно ежегодно кратно увеличиваем штат Solar JSOC и готовы поддерживать этот темп, закрывая задачи больших федеральных заказчиков, в том числе по защите АСУ ТП. ■