ЗАЩИТА АСУ ТП В РОССИИ: НОВЫЕ ТРЕБОВАНИЯ ФСТЭК

Евгений Дружинин
habrahabr.ru/company/pt/blog/242803/

Российские организации, ответственные за регулирование в области безопасности, до поры до времени не уделяли внимания уязвимостям промышленных систем, однако приказ ФСТЭК № 31 от 14 марта 2014 года обещает коренным образом изменить ситуацию.

Нельзя сказать, что раньше в России безопасность АСУ ТП (SCADA) совсем не регулировалась. С 2007 года процессы ИБ на основных критически важных объектах регламентируются требованиями, предъявляемыми к «ключевым системам информационной инфраструктуры» (КСИИ), однако методические указания в этом документе имеют ограничения по распространению: предприятия, которым они адресованы, должны быть внесены в специальный перечень. В этом списке КСИИ могли оказаться и банки, и любые другие организации, но при этом не учитывались особенности применения АСУ ТП как систем реального времени, а также тенденции развития IT-инфраструктур (к примеру, работа в визуализированных средах). Отделить АСУ ТП, учесть специфическую архитектуру и слабые места таких систем — задача требований, сформулированных в приказе № 31.

Часто российское нормотворчество упрекают в том, что оно оторвано от передового международного опыта и не соответствует последним тенденциям. Чтобы проверить это предположение, мы сравнили требования приказа ФСТЭК № 31 с ведущими зарубежными стандартами в области систем промышленной автоматизации, а именно:

- семейством отраслевых стандартов NERC Critical Infrastructure Protection (NERC CIP);
- семейством стандартов ISA/IEC 62443 Industrial Automation and Control Systems Security;
- рекомендациями NIST SP 800-82 «Guide to Industrial Control Systems (ICS) Security» и NIST SP 800-53 «Security and Privacy Controls for Federal Information Systems and Organizations».

Что в приказе ФСТЭК № 31 есть уже сейчас

Разработка и документирование правил и процедур (политик) обеспечения безопасности (эти меры защиты идут под номерами на 0). Это важные меры: любой процесс обеспечения безопасности, причем не только информационной, начинают строить с тщательного документирования всех процедур.

Требования к защите среды виртуализации (ЗСВ). Технологии виртуализации позволяют оптимизировать ресурсы, однако порождают новые угрозы. Понятно, что снижение издержек интереснее борьбы за безопасность, поэтому критически важные системы в целом и АСУ ТП в частности очень быстро оказываются в не совсем безопасных облаках, и этот процесс необходимо как-то контролировать. Соответствующие пункты в приказе № 31 можно только приветствовать, а вот в перечисленных нами зарубежных стандартах вопросы защиты виртуальных сред не рассмотрены.

Обучение и отработка действий пользователей в случае возникновения нештатных (непредвиденных) ситуаций (ДНС). Повышение осведомленности персонала уменьшает как минимум риски, связанные с социальной инженерией. Репетиция «плана спасения» важна также для понимания сотрудниками своей роли в процессах управления инцидентами безопасности.

Требования по безопасной разработке ПО (ОБР). Код в программном обеспечении АСУ ТП зачастую низкого качества, а на большинстве критически значимых предприятий можно обнаружить уязвимости 10—15-летней давности. Обновления часто не устанавливаются в принципе, что обусловлено множеством факторов, начиная от непрерывности технологического процесса и заканчивая неосведомленностью сотрудников об угрозах. Поэтому наилучшее решение — принимать всевозможные меры для исправления ошибок в АСУ ТП на этапе разработки. Подобные требования практически не отражены в зарубежных стандартах, что еще раз говорит в пользу авторов российского документа.

Требования по инцидент-менеджменту (ИНЦ) и анализу угроз безопасности (УБИ). Данные требования составляют суть риск-ориентированного подхода, отраженного в приказе № 31. Их наличие означает формирование защиты на основании характерных для системы рисков: это позволяет учитывать новые угрозы и улучшать процессы обеспечения ИБ.

Что хотелось бы увидеть

Скорейшее появление детальных рекомендаций и методических указаний для специалистов ИБ и аудиторов. Сейчас приказ ФСТЭК № 31 — это достаточно высокоуровневый документ.

Разделение на сетевом уровне корпоративной ЛВС и технологических сетей по аналогии с IEC-62443-2-1 и NIST SP 800-82. Требование о необходимости сегментирования ЛВС в приказе присутствует (ЗИС-17), однако в соответствующем методическом документе наилучшим решением будет явно отметить необходимость отделения технологических сетей от корпоративных.

Рекомендации по построению безопасной архитектуры компонентов АСУ ТП с учетом разделения на уровни, как это сделано в стандартах IEC-62443-2-1, NIST SP 800-82: нижний уровень — полевой, средний — ПЛК, верхний уровень — SCADA.

Инвентаризация компонентов АСУ ТП. Подобное требование есть во всех рассмотренных документах. При этом инвентаризация предусматривает не только идентификацию компонентов, участвующих в технологических процессах, но и хранение дополнительной информации, позволяющей определить их назначение, степень значимости и т. п. Данная процедура имеет одно из первостепенных значений для риск-ориентированного подхода, поэтому мы ожидаем ее описания в дальнейших ревизиях документа.

Проверка персонала перед предоставлением допуска к работе с АСУ ТП. Подобные требования есть в NERC CIP и ISA/IEC 62443, но в текущую версию приказа № 31 не вошли.

Мероприятия, связанные с увольнением персонала. Не самые радостные, но необходимые действия, включающие блокирование учетных записей, смену паролей и т. п., прописаны в ISA-62443-2-1 и NERC-CIP. Говорят, что бывшие следователи лучше всех умеют уничтожать улики, а экс-сотрудник КВО, хорошо знакомый с технологическим процессом, может быть значительно опаснее нарушителя со стороны. Хотелось бы в дальнейших версиях приказа № 31 увидеть требования к мероприятиям, связанным с увольнением сотрудников КВО.

В целом, несмотря на отдельные шероховатости, документ соответствует лучшим международным стандартам и практикам в области обеспечения информационной безопасности АСУ ТП, а в отдельных пунктах вводит самые современные требования, необходимость в которых как раз назрела.

Более подробное сопоставление требований приказа ФСТЭК № 31 с аналогичными пунктами международных стандартов представлено на сайте: ***ptsecurity.ru/lab/analytics/***