РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ НЕФТИ И ГАЗА
ИМЕНИ И.М.ГУБКИНА

ВЫСШАЯ ШКОЛА ЭКОНИМИКИ
НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Кризисное управление технологическими процессами (ТП)

АКАДЕМИК АКАДЕМИИ КРИПТОГРАФИИ РОССИИ
А.П. БАРАНОВ
baranov.ap@yandex.ru

ДОЦЕНТ НИУ ВШЭ
П.А. БАРАНОВ
pbaranov@hse.ru

baranov.ap@yandex.ru pbaranov@hse.ru

Кризис подхода о тотальном импортозамещении в системах управления ТП

1. Автоматизированная система управления (АСУ) техническим устройством (SCADA), как ЛВС с удаленным или без него внешним подключением

2. Сервер данных на нижнем уровне ТП с помощью фирменных датчиков и протоколов взаимодействия

3. Сервер обработки данных в режиме реального времени – есть в открытом исходном коде

4. Человеко-машинный интерфейс (HMI) и система логического управления – требуется доскональное знание ТП

5. База данных реального времени с системой сравнения с ранее наработанными режимами – фирменная

6. Прикладное ПО – генерация отчетов, внешние интерфейсы для обмена данными между SCADA и другими приложениями – фирменное развитое

baranov.ap@yandex.ru pbaranov@hse.ru

Сертификация SCADA - отечественного и внешне разработанного ТП по требованиям ИБ

1. Для полностью отечественного ТП сейчас может быть разработана SCADA в России за разумные деньги и время с ее сертификацией по ИБ
2. Для собранного по собственной схеме ТП с применением импортных комплектующих (если для датчиков имеется протокол взаимодействия) возможно создание АСУ с его аттестацией по ИБ
3. Для готового покупного ТП нет данных по ЛВС, за исключением, может быть, системы внешнего управления

baranov.ap@yandex.ru pbaranov@hse.ru

ИБ в SCADA-системах

1. Как и в любых компьютерных системах ИБ – конфиденциальность, целостность, доступность
2. Специфическая особенность SCADA – массовость датчиков, ограниченное число пользователей и относительная стабильность ПО сервера обработки данных и управлением при возможной текучести системы представления отчетности
3. Локальное размещение ЛВС и возможно компактная контролируемая зона
4. Удаленное управление на основе общенациональных сетей
5. Контролируемый и ограниченный персонал эксплуатирующий и обслуживающий SCADA и возможный внутренний нарушитель в ТП
6. Сертификация по ИБ в системе ФСТЭК по действующим нормативам. Известны SCADA с открытым кодом ПО

baranov.ap@yandex.ru pbaranov@hse.ru

Проблемы сертификации по ИБ и требования к представляемым материалам

1. В отличие от информационно-аналитических систем АСУ ТП в области ИБ имеет приоритет не конфиденциальность, а целостность и доступность
2. Целостность в данном случае это отсутствие НДВ и неизменность (фиксированность ПО) или контролируемая корректировка прикладного ПО
3. Доступность к АСУ не только эксплуатантам, но и датчикам. Резервирование серверных компонент фактически – надежность
4. Требования по доступности со стороны регуляторов разработаны слабо. (ТИЭР для ЦОДов здесь не подходят)
5. Аттестация на НДВ аппаратной части в случае импортных компонент проблематична

baranov.ap@yandex.ru pbaranov@hse.ru

Особенности сложившейся практики аттестации АСУ ТП по ИБ

1. В настоящее время аттестуется система АСУ ТП в целом по общей схеме: модель угроз → блокирование с помощью СЗИ → оценка эффективности защиты

2. Оценки эффективности защиты строятся на основе сертификатов на отдельные элементы взаимодействия и их защиты

3. Оценить защищенность от НДВ датчиков или тайм-закладок в большом разнообразии типов весьма трудно. В датчиках могут присутствовать микросхемы типа ASIC

4. Операционные системы подвергаются сертификации также как обычные, так же, как и СЗИ, работающие с или в этих ОС

5. Практически отсутствуют на рынке предложений крупные блоки ПО, аттестованные по ИБ такие как ОС, криптопровайдеры реального времени, совокупность средств отображения данных включая 3D- представление и т.д.

baranov.ap@yandex.ru pbaranov@hse.ru

Поэтапное повышение уровней ИБ – способ обоснования применения импортных составляющих АСУ ТП

1. Ранжирование угроз и парирование на начальном этапе только наиболее острых
2. Например: внешнее управление по общепринятым телекоммуникационным протоколам через шифраторы с обязательной инкапсуляцией пакетов
3. Организационные меры контролирующей зоны размещения ЛВС и контроль персонала
4. Частичная проверка на НДВ доступного и наиболее чувствительного ПО
5. Инструментальная проверка аппаратной части или использование отечественных, сертифицированных аппаратных средств
6. Тестирование вновь приобретаемого оборудования на таймерные или ситуационные закладки
7. Выявление возможности управления SCADA из вне по радиоканалу

baranov.ap@yandex.ru pbaranov@hse.ru

Построение кризисной системы блокировки опасных режимов

1. АСУ ТП с применением импортных компонент без детальных описаний работы и текстов ПО невозможно аттестовать по требованиям ИБ
2. Осуществление полного импортозамещения, как показывает опыт IT-отрасли длительный и пока малоуспешный процесс
3. Наибольший ущерб приносит выход ТП на разрушительные критические уровни. Выявление признаков опасных ситуаций
4. Построение трассы и констатация движения к критическому состоянию (КС) важнейшая задача анализа ТП
5. В качестве первоочередной задачи повышения устойчивости ТП к разрушению можно пытаться построить относительно простую систему отслеживания движения ТП к кризисному состоянию
6. Ограниченную по функциям антикризисную систему предлагается строить на отечественной элементной базе
7. Необходимо рассмотреть вопрос о приостановлении страховки ТП для которых не проведена аттестация SCADA по вопросам ИБ

Спасибо за внимание

baranov.ap@yandex.ru