innoSTage
группа компаний

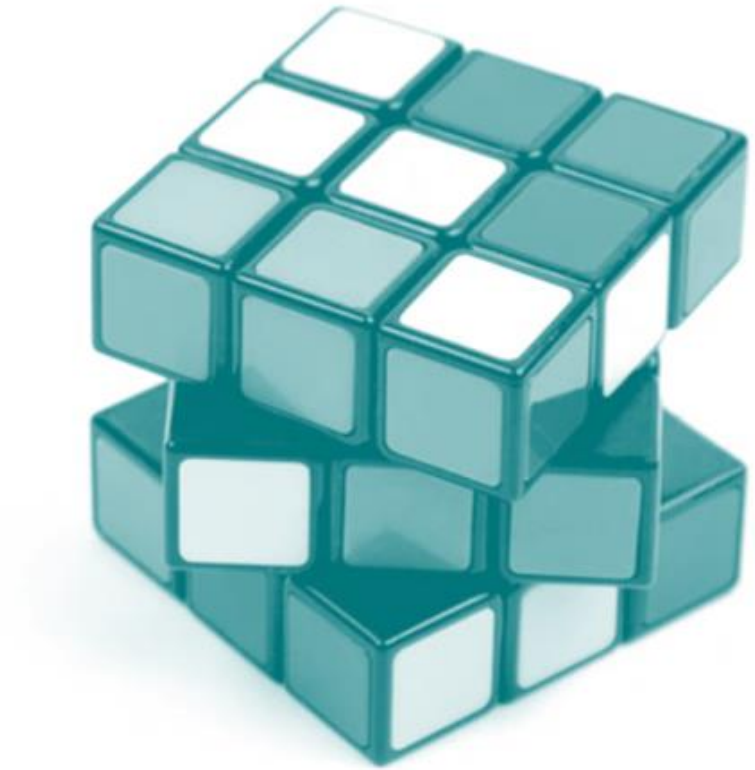
Практический опыт внедрения решений ИБ на промышленных объектах: особенности, проблемы, решения

Айрат Мухаметшин,
Ведущий инженер отдела кибербезопасности АСУ ТП

Проблематика

Срывы сроков внедрения:
– можно было избежать?

Как быть и что делать?



Содержание

№.	Блок	Тайминг
1.	Аналитика • отраслевая специфика • отличия • причины и предпосылки	3 мин
2.	Практики внедрения • действующее производство vs новое строительство • небольшие объекты vs «большие стройки»	9 мин
3.	Выводы и рекомендации	3 мин
	Блок вопросов и ответов	5 мин

Аналитика

- *факторы и предпосылки*
- *специфика*
- *новое строительство*
  vs действующее производство

Факторы и предпосылки

Режимность и повышенные требования безопасности	Изначально большие сроки работ
Взаимозависимость технических решений ИБ и автоматизации	Изменения решений на этапе СМР и ПНР = данность
Внедрение решений по ИБ после решений по автоматизации	Накопительный эффект ошибок и изменений
Деятельность по ИБ не генерирует прибыль	Процессы производства всегда в приоритете
Финансовые реалии не совпадают с производственными	Пролонгация договоров на внедрение

«Технология» vs «Корпорат»: внедрение решений ИБ

innostage
группа компаний

Организация работ

Сложнее процедура допуска к работам	Больше времени на «сопутствующие» организационные процессы
Критичность затрагиваемых сервисов	Сложнее процедура согласования ППР, больше заинтересованных сторон, сложнее оценка рисков
Зависимость от графика функционирования производства	Сжатые сроки реализации
Разделение зон ответственности за критические и значимые объекты, инфраструктуру совместного использования	Дополнительные согласования

«Технология» vs «Корпорат»: внедрение решений ИБ

innoStage
группа компаний

Интеграция средств защиты

Нет итоговой картины информационных потоков

- необходимость накопления статистики функционирования, анализ состояний
- длительная опытная эксплуатация средств защиты

Состояние инфраструктуры объектов

- тщательное (многоступенчатое) тестирование настроек
- мониторинг ресурсоемкости и оценка совместимости

Действующее производство и новое строительство

innoStage
группа компаний

Отличия и специфика

№	Факторы	Действующее	Новое
1	Ограниченность сроками технологического останова	✓	
2	Ограниченность сроками запуска		✓
3	Единовременная работа множества подрядчиков		✓
4	Согласование работ с технологическими регуляторами и сторонними организациями	✓	✓
5	Работы в условиях действующего производства (ТОУ «на режиме»)	✓	
6	Внешние объективные обстоятельства	✓	✓
7	Недостаточная осведомленность персонала об инфраструктуре		✓

Практики внедрения

- У вас были срывы сроков при внедрении решений ИБ?
- Нет, пока ни одного не было…
- Будут!

С чем столкнулись?

Нефтеперерабатывающий завод

Действующее производство

- ПИР СЗИ АСУ ТП в объеме завода
- Внедрение 1 очереди

- отсутствие технической поддержки на АСО
- необходимость тестирования АВЗ с разработчиком ПТК
- досрочный выход из технологического останова

- Теплоэлектроцентраль
- Установка каталитического крекинга

- Нельзя расширить функционал до проектных значений (кол-во VLAN)
- длительные переговоры с разработчиком ПТК, ожидание останова

- 1 подрядчик
- 1 разработчик средств защиты
- 2 разработчика ПТК

- по результатам АНЗ не приняты меры >> ожидание следующего ТО
- внедрение МЭ на действующей установке >> усложнение ППР и процедуры согласования

От старта до окончания работ - 2 года

Цифровая подстанция

С чем столкнулись?

innoStage
группа компаний

Новое строительство

- ПИР СЗИ ЦПС
- Внедрение

- Система телемеханики
- РЗА
- Сети связи

- 4 подрядчика
- 2 службы заказчика
- 1 Генеральный подрядчик

- «поздний старт» разработки решений по ИБ
- пересечение этапов проектирования ИБ и внедрения АСУ ТП
- изменение проектных решений на этапе ПНР
  - новый канал связи
  - изменение перечня объектов взаимодействия
  - изменение плана адресации
- внедрение АСУ ТП и РЗА «ушло вперед»
  - отсутствие специалистов на местах
- электротехническая часть ПС в опытной эксплуатации на момент внедрения ИБ

Последствия

Цифровая подстанция

Система защиты ЦПС принята в постоянную эксплуатацию

Опоздание на 4 месяца

- дисбаланс сроков реализации между подрядчиками
- неготовность инфраструктуры к внедрению решений ИБ
- корректировка проектных решений «на ходу»
- ужесточение условий допуска к работам – согласование технологических окон с РДУ СО ЕЭС

Проектно-изыскательские работы

Нефтехимический комплекс

- Новое строительство
- ПИР СЗИ АСУ ТП
- Внедрение СЗИ АСУ ТП
- Технологические установки
- ПС-500 кВ

Состояние объекта:

- наличие временных сетей связи, операторных
- часть решений ИБ спроектировано в смежных разделах ПД
- лицензии на ПО и оборудование закуплены, активированы

Причины:

- не проработаны требования по ИБ в задании на проектирование
- избыточность проектных требований

Следствие:

- «зоопарк» средств защиты
- избыточность решений
- средства защиты в каждой поставке разных подрядчиков

Итог:

- исправить существующее положение дел
- привести инфраструктуру ИБ к единообразию

Нефтехимический комплекс

Внедрение

Состояние объекта

- объект стал действующим (поэтапный запуск производства)
- отдельные объекты уже функционируют

С чем столкнулись

- требование максимального использования созданной инфраструктуры
- необходимость согласования отдельных настроек ПТК АСУ ТП
- различия в требованиях доступности сервисов
- реализация архитектуры взаимодействия по промышленным протоколам

Нефтехимический комплекс

Внедрение

Как решали

- дооснащение МЭ >> поэтапное переключение
- согласование настроек >> через подрядную организацию-интегратора АСУ ТП
- различия требований доступности сервисов >> корректировка и согласование плана работ
- особенности функционирования промышленных протоколов >> поиск решения «на ходу»

На данный момент

- приведение инфраструктуры к единообразию (объединение разрозненных сервисов)
- инфраструктура дооснащена до проектных показателей
- согласование установки и настройки решений по ИБ (наложенных, встроенных)

Нефтехимический комплекс

Архитектура взаимодействия с промышленными протоколами

Дано

- АСДУЭ
- протокол PRP
- взаимодействие с верхним уровнем

Задача обеспечения

- непрерывности передачи данных
- защиты взаимодействия
- отказоустойчивости

Проблема

- две независимые сети – одновременная дублированная передача данных
- резервирование на уровне взаимодействия с MES не предусмотрено
- сервисы ИБ и сервисы автоматизации – по PRP протоколу

Нефтехимический комплекс

Работа с промышленными протоколами

Решение

виртуализация кластеров МЭ (1 физический МЭ = 1 виртуальный кластер) >>

- виртуальное разделение потоков
- стек коммутаторов для кластера МЭ
- 1 виртуальный кластер обслуживает один канал
- резервирование на уровне отдельного МЭ

Обеспечение «бесшовной» передачи данных в корпоративный сегмент

Выводы и рекомендации

Проблема

Архитектурные ограничения

Решение

Четкое формулирование требований не только к обеспечению ИБ, но и к инфраструктуре

Преимущество

- Единообразие архитектуры ИБ
- Устранение проблем межсистемной интеграции

Проблема

1. Несогласованность работ подрядных организаций
2. Различие требований в доступности сервисов

Решение

- Разработка ППР всеми заинтересованными сторонами
- Единый центр принятия решений

Преимущество

Минимизация задержек сроков реализации

Проблема

Накопительное
отставание по срокам реализации

Решение

Максимальное информирование
заинтересованных
сторон

Преимущество

- Повышение
эффективности
деятельности
- Минимизация задержек
сроков реализации

innoStage
группа компаний

Благодарю за внимание!

Контакты:

Ayrat.Mukhametshin@innostage-group.ru

innostage-group.ru

Facebook

Instagram