КРОК

Обеспечение ИБ АСУ ТП: архитектура и рекомендации по внедрению

Евгений Дружинин
Ведущий эксперт по информационной безопасности КРОК

Ключевые изменения в требованиях

Указ №250:

- Наличие структурного подразделения, отвечающего за ИБ, обнаружение и реагирование на атаки
- Организация обнаружения и реагирования на компьютерные атаки
- С 1 января 2025 года запрет на использование средств защиты информации из недружественных стран

Указ №166:

С 1 января 2025 г. запрет на использование иностранного ПО на значимых объектах КИИ

Необходимость:

- ускоренной модернизации ЗОКИИ
- поиска эффективного подхода к реализации законодательных требований
- эффективного обеспечения защищенности ЗОКИИ в процессе эксплуатации

Сложности реализации на предприятиях

- Ограниченное время на поиск альтернативных решений ПО и средств защиты информации (СЗИ)
- Увеличение сроков поставок оборудования
- Риск расширения перечня недружественных стран
- Необходимость выполнения однотипных задач каждым предприятием
- Риск усиления гетерогенности (разнородности) решений в отрасли
- Необходимость формирования и поддержки компетенций работников, ответственных за обеспечение безопасности АСУ ТП

Централизованный подход к обеспечению безопасности ЗОКИИ (АСУ ТП)

Цели:

- Исполнение нормативных требований по защите ЗОКИИ
- Снижение временных и финансовых затрат на реализацию и модернизацию систем безопасности ЗОКИИ
- Повышение эффективности процессов эксплуатации и обслуживания систем безопасности ЗОКИИ

Принципы реализации:

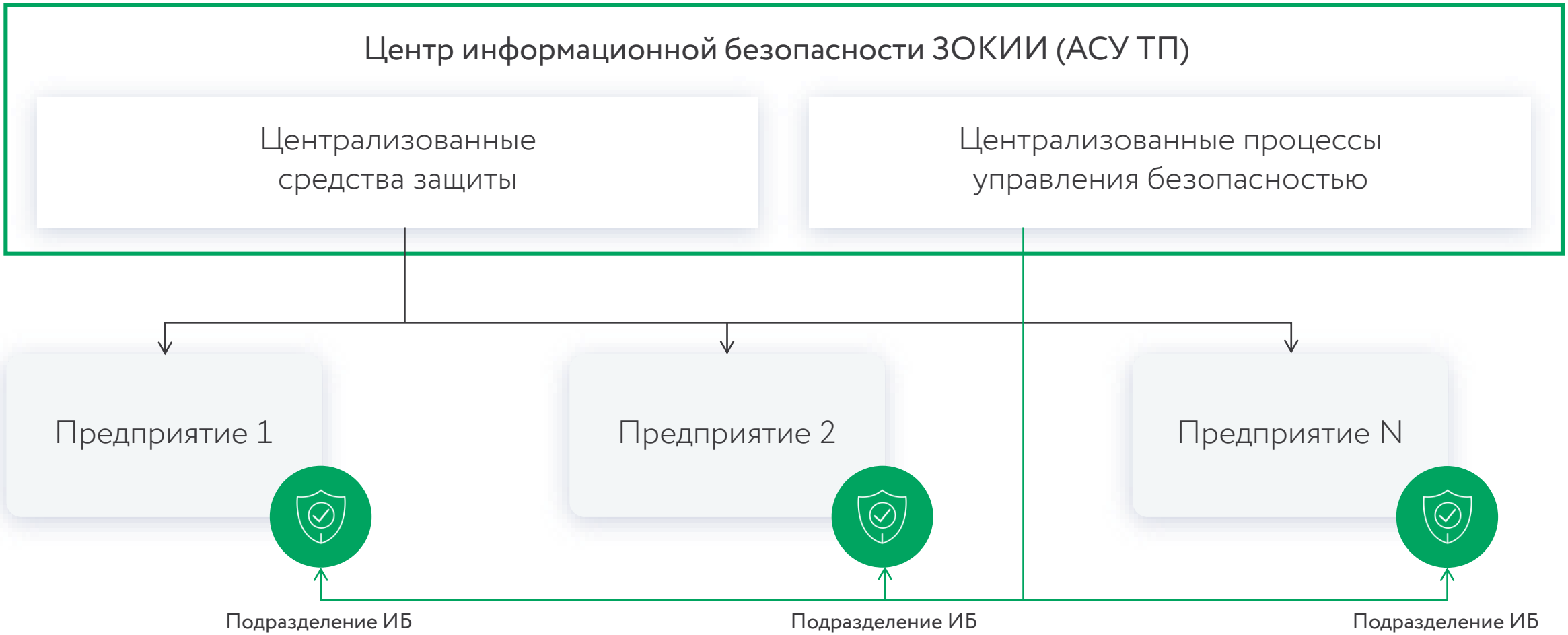
- Централизация архитектуры
- Унификация (стандартизация) внедряемых решений и централизованно предоставляемых услуг ИБ
- Оптимизация распределения функциональных обязанностей между головным и дочерними подразделениями

Преимущества:

- Усиление отраслевого контроля за безопасностью ЗОКИИ
- Оптимизация кадровых ресурсов, задействованных в процессах обеспечения безопасности ЗОКИИ
- Ускорение процессов проектирования, внедрения и модернизации систем безопасности ЗОКИИ

КРОК

Схема централизованной отраслевой модели обеспечения безопасности ЗОКИИ (АСУ ТП)



КРОК

Централизованные услуги безопасности, предоставляемые центром информационной безопасности (ЦИБ)

Контроль безопасности состояния ЗОКИИ

Выявление и расследование инцидентов ИБ

Устранение последствий инцидентов ИБ

Эксплуатация и обслуживание средств защиты

Предоставление рекомендаций
по реагированию на инциденты ИБ

Тиражирование типовых программно-аппаратных комплексов (ПАК) , предназначенных
для обеспечения безопасности,
по производственным дивизионам

КРОК

Пошаговый план до 2025 г.

Пилотная зона. Концепт

Формирование комплексного архитектурного подхода:

- Концепция
- Детализация
- Стандартизация
- Унификация

До конца 2023 г.

Тиражирование решения

Адаптация типовых решений и документов под оставшиеся предприятия

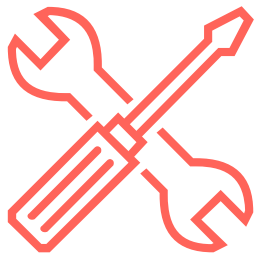
До 2025 г.

Типичные технические проблемы на уровне предприятий

Отсутствие защищенной сетевой архитектуры

(отсутствие отделения ЗОКИИ от ОКИИ, запутанные сетевые топологии, наличие небезопасных точек взаимодействия с внешними системами …)

Встроенные механизмы защиты компонентов ЗОКИИ **либо не настроены, либо настроены неправильно**



Неготовность инфраструктуры к внедрению средств защиты

(потребность в прокладке СКС, установка дополнительных шкафов, подключение инженерной инфраструктуры)

Проблема обеспечения совместимости СЗИ с АСУ ТП

Конкретные примеры сложностей при установке СЗИ на производстве

Проблемы диагностики и функционирования прикладного ПО АСУ ТП после установки СЗИ

Отказы / некорректная работа ПО АСУ ТП

Кейс 1:
существенное падение производительности ПО АСУ ТП

Кейс 2:
после обновления компонентов защиты на сервере занят весь объем оперативной памяти ОЗУ

Кейс 3:
после установки компонентов защиты не запускается ПО АСУ ТП

Рекомендации КРОК

1. создайте стенды, полностью эмулирующие работу АСУ ТП
2. выполните полнофункциональное тестирование совместимости
3. проводите обновление ПО и СЗИ в разное время с фиксацией корректного функционирования

КРОК

Заражение вредоносным ПО АСУ ТП на момент установки СЗИ

Наличие активного заражения

Множество кейсов, когда по итогам установки компонентов защиты на объектах заказчика было найдено ВПО

Рекомендации КРОК

1. проведите инсталляцию компонентов защиты на всех серверах и АРМ АСУ ТП в режиме мониторинга
2. выявите и проанализируйте результаты мониторинга ВПО
3. удалите ВПО и установите обновления безопасности
4. переключите компоненты защиты в активный режим работы

КРОК

Устранение проблем типовой установки и настройки средств защиты

Проблемы типовой установки / настройки СЗИ

Проблемы настройки источников событий ИБ для SIEM на старых версиях Windows

Одинаково настроенные ОС с идентичным набором ПО

Кейс 1: на Windows XP
С одного события идут, с другого — неизвестная ошибка

Рекомендации КРОК

- Если вы столкнулись с аналогичными проблемами:
  - снимите образ с АРМ / сервера
  - разверните его в тестовой среде
  - проведите глубокий анализ по выявлению причин в лабораторных условиях

КРОК

Типовые проблемы сетевой сегментации

Проблемы сегментации

Кейс 1: корпоративная и технологическая сети физически находятся в одной плоской сети, при этом отсутствуют межсетевые экраны и маршрутизаторы

Кейс 2: ЗОКИИ находятся в единой сети с другими системами АСУ ТП

Рекомендации КРОК

- Выполните физическое разделение корпоративной и технологической сетей
- Проведите сегментацию технологической сети, с учетом категорирования АСУ ТП
  Для этого:
  - проведите инвентаризацию оборудования АСУ ТП
  - выполните перепроектирование сетей
  - модернизируйте сеть с учетом категорирования АСУ ТП
- Актуализируйте проектную документацию

КРОК

Виды испытаний

1 Тестовые испытания уровня **«Вендор АСУ ТП — Вендор СЗИ»**

2 Тестовые испытания уровня **«Интегратор — Вендор СЗИ»**

3 Тестовые испытания уровня **«Интегратор — Заказчик»**

Тестовые испытания уровня «Интегратор — Вендор СЗИ/Заказчик»

Кто?

Рабочая группа «Интегратор — Вендор СЗИ» + Заказчик (опционально)

Где?

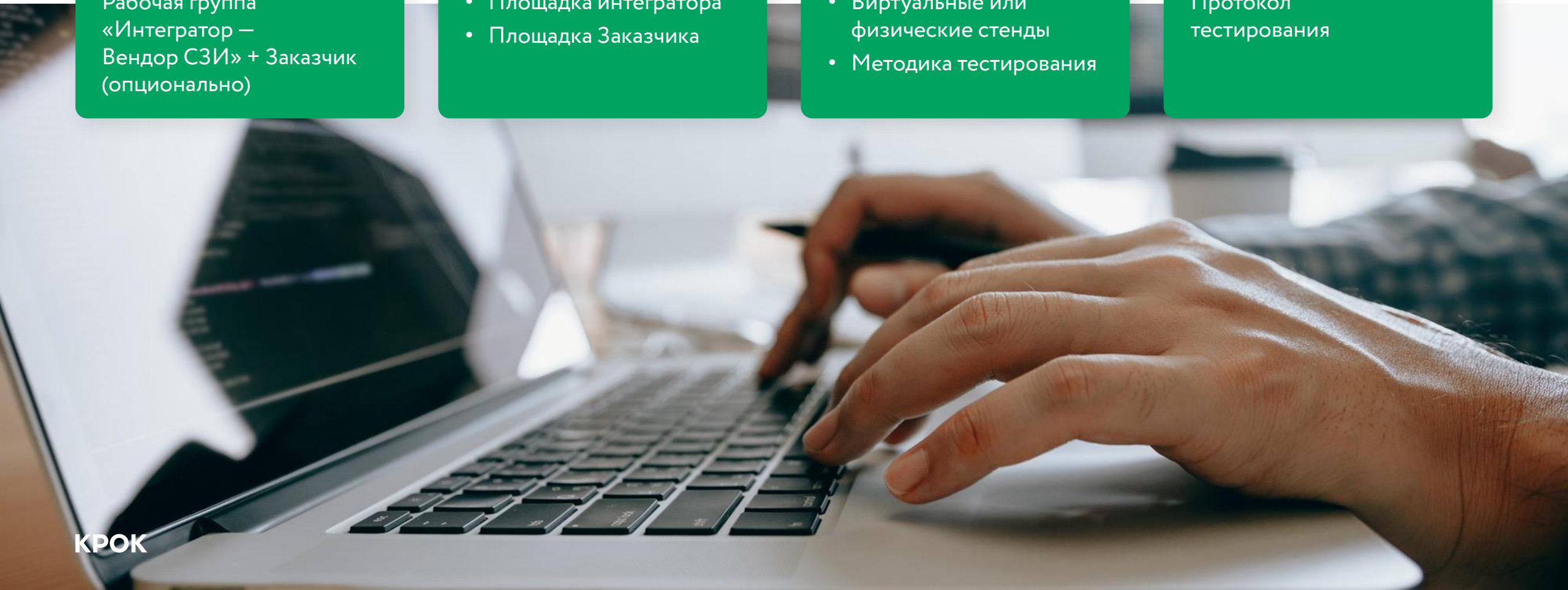
- Площадка интегратора
- Площадка Заказчика

На основании чего?

- Виртуальные или физические стенды
- Методика тестирования

Какой результат?

Протокол тестирования



КРОК

Чем мы можем помочь?

- Построим централизованную модель управления защитой ЗОКИИ
- Внедрим СЗИ «под ключ»
- Выполним тестирования на совместимость
- Предоставим техподдержку
- Подключимся на необходимую стадию работ

Резюме

Преимущества работы с КРОК

Преимущества интегратора
на проектах работают команды ИБ, инфраструктуры, телекоммуникации

1500+
проектов по ИБ

Команда инженеров ИБ + АСУ ТП

Практический опыт построения безопасности для ЗОКИИ

КРОК

Узнать о решениях ИБ КРОК

Нужна квалифицированная помощь
в реализации требований по защите ЗОКИИ?

Свяжитесь с нами!

Евгений Дружинин
Ведущий эксперт по информационной безопасности КРОК

Полина Мельник

Менеджер по продвижению решений
ИБ КРОК
ТГ: @polinameln
pomelnik@croc.ru

111033, Москва,
ул. Волочаевская, д. 5, корп. 1