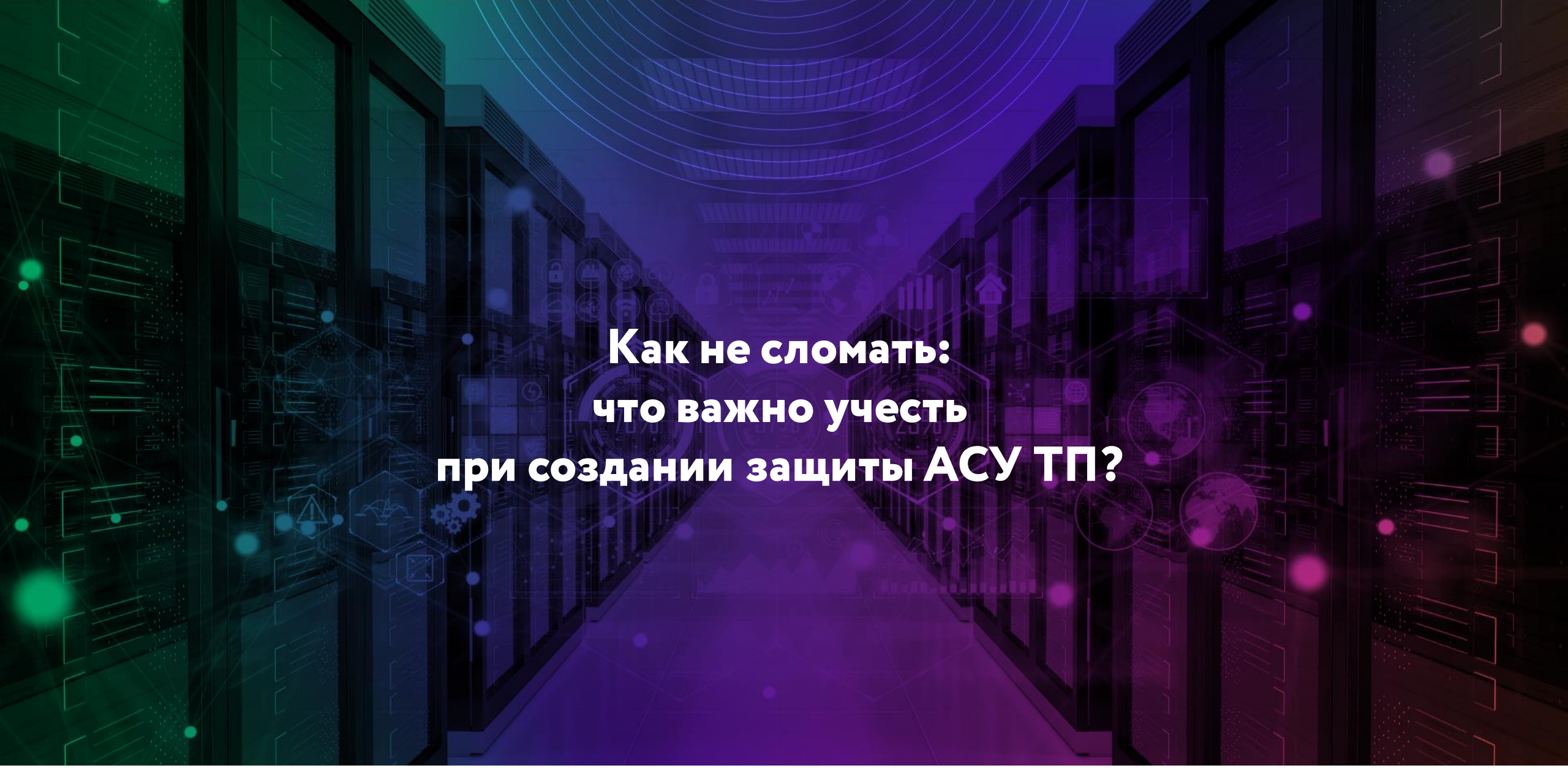
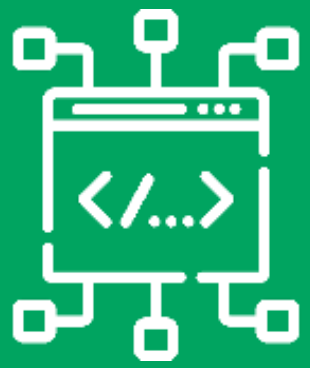


Как не сломать: что важно учесть при создании защиты АСУ ТП?

КРОК

Области повышенного внимания

1. Целевая архитектура безопасности
2. Типичные технические ограничения
3. Обеспечение совместимости с компонентами АСУ ТП
4. Внедрение и эксплуатация – лучшие практики



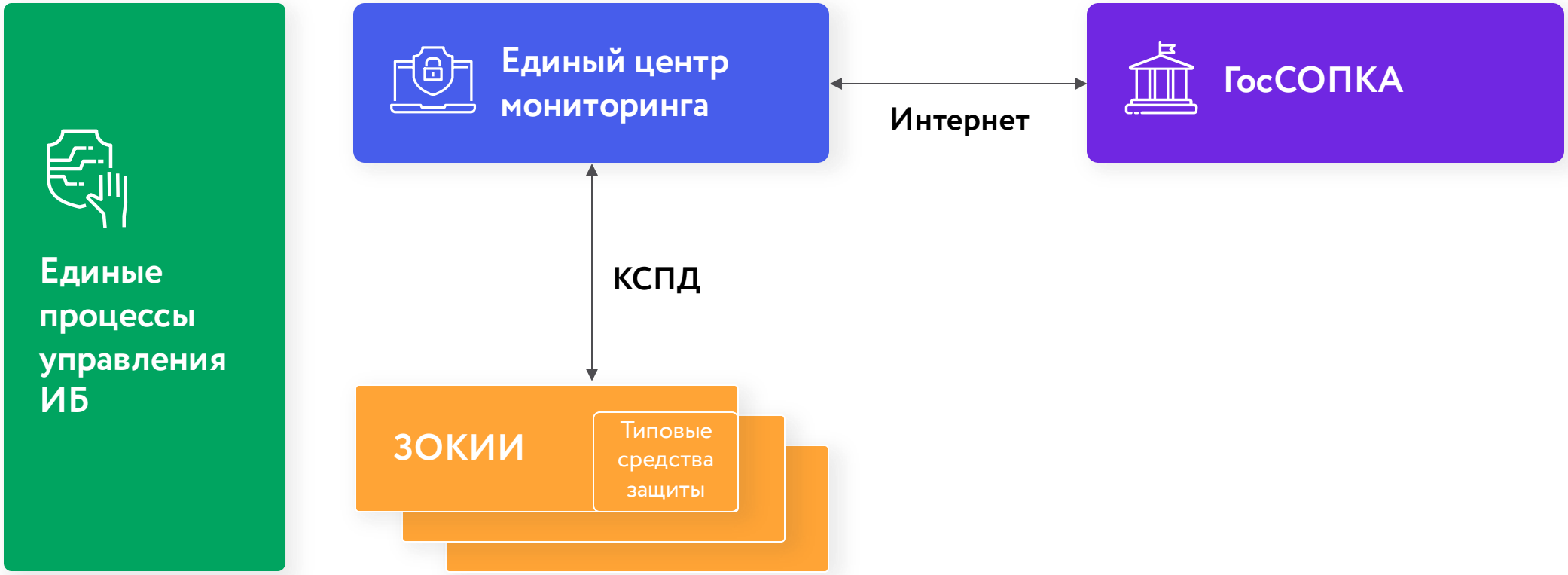
Характеристики оптимального целевого состояния

1. **Наличие единого центра мониторинга** защищенности ЗОКИИ

2. **Стандартизация решений** для защиты ЗОКИИ

3. Максимальное **использование механизмов безопасности**, встроенных в компоненты ЗОКИИ

Типовая целевая архитектура централизованной системы защиты ЗОКИИ



Типичные технические проблемы

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)

Полное или частичное **отсутствие средств защиты**

Предпосылки необходимости модернизации инфраструктуры

Недостаточная пропускная способность каналов связи

Ограниченность вычислительных ресурсов

Отсутствие сегментирования ЗОКИИ от смежных систем

Использование устаревших и уязвимых ОС

Необходимость **наличия инженерной инфраструктуры** для внедрения типового решения

(СКС, инженерные системы, портовая емкость, шкафы для оборудования)

Ограничения этапа модернизации

Необходимость **согласования с производителями АСУТП**, осуществляющими гарантийную или сервисную поддержку

Необходимость **выделения технологических окон для настроек** (влияние сезонности и пр.)

Необходимость **проектирования и закупок**

Рекомендуемый подход к реализации

Стадия 1

- Глубокое технические обследование
- Выявление архитектурных недостатков
- Формирование типового технического решения
- Формирование требований к модернизации существующей инфраструктуры
- Модернизация существующей инфраструктуры (длительный процесс!)

Стадия 2

- Формирование требований к адаптации типового решения
- Адаптация типового решения к особенностям конкретных ЗОКИИ
- Формализация процессов управления ИБ
- Определение необходимой численности персонала ИБ
- Внедрение технических решений и организационных процессов

Вопросы технической совместимости средств защиты и компонентов АСУ ТП

Как и чем подтвердить совместимость СЗИ с компонентами АСУ ТП?

Наши **системы отсутствуют в перечне** совместимых с СЗИ, что делать?

Могут ли **обновления СЗИ** повлиять на функционирование АСУ ТП?

Наши системы **на гарантийной поддержке** вендора АСУ ТП, как нам установить там СЗИ?

У нас **старые системы**, возможно ли получить для них официальное подтверждение совместимости?

КРОК

Четыре кита процесса обеспечения надежной совместимости

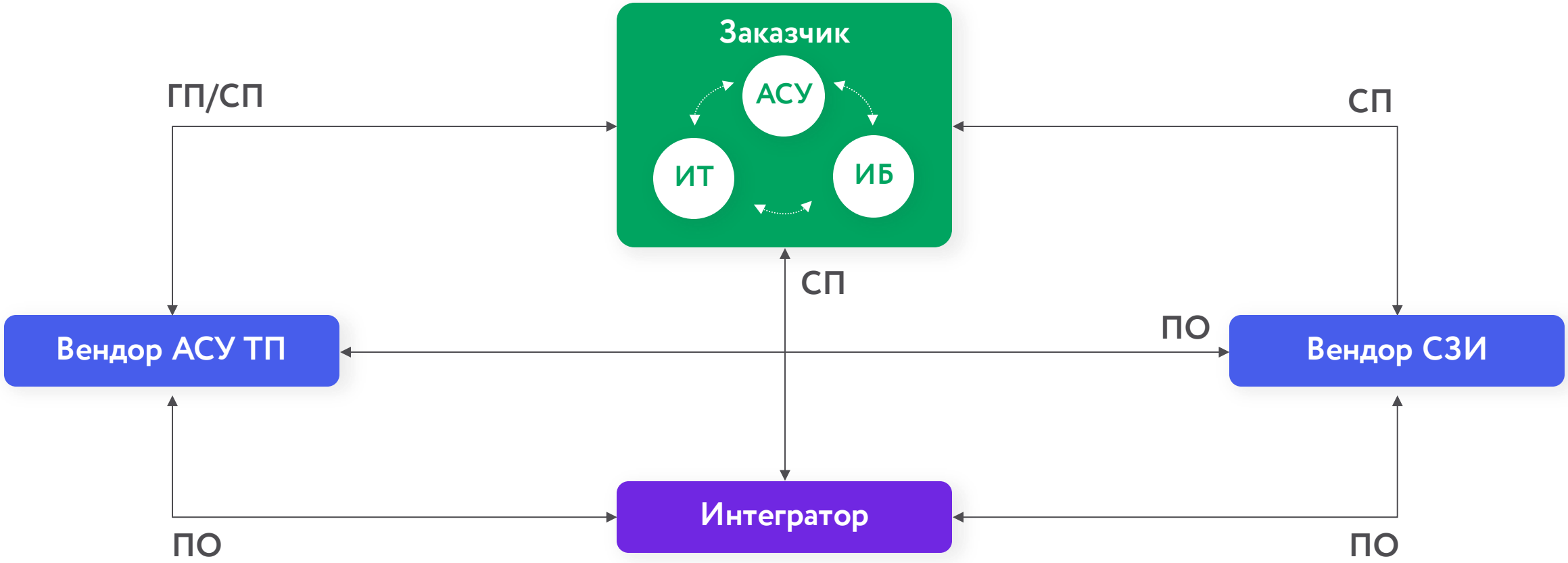
Налаженные отношения между вовлеченными сторонами

Лучшие практики по установке и эксплуатации

Внешняя сервисная поддержка

Тестовые испытания

Вовлекаемые стороны



СП – сервисная поддержка **ГП** – гарантийная поддержка **ПО** – партнёрские отношения

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»

Кто?

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

Где?

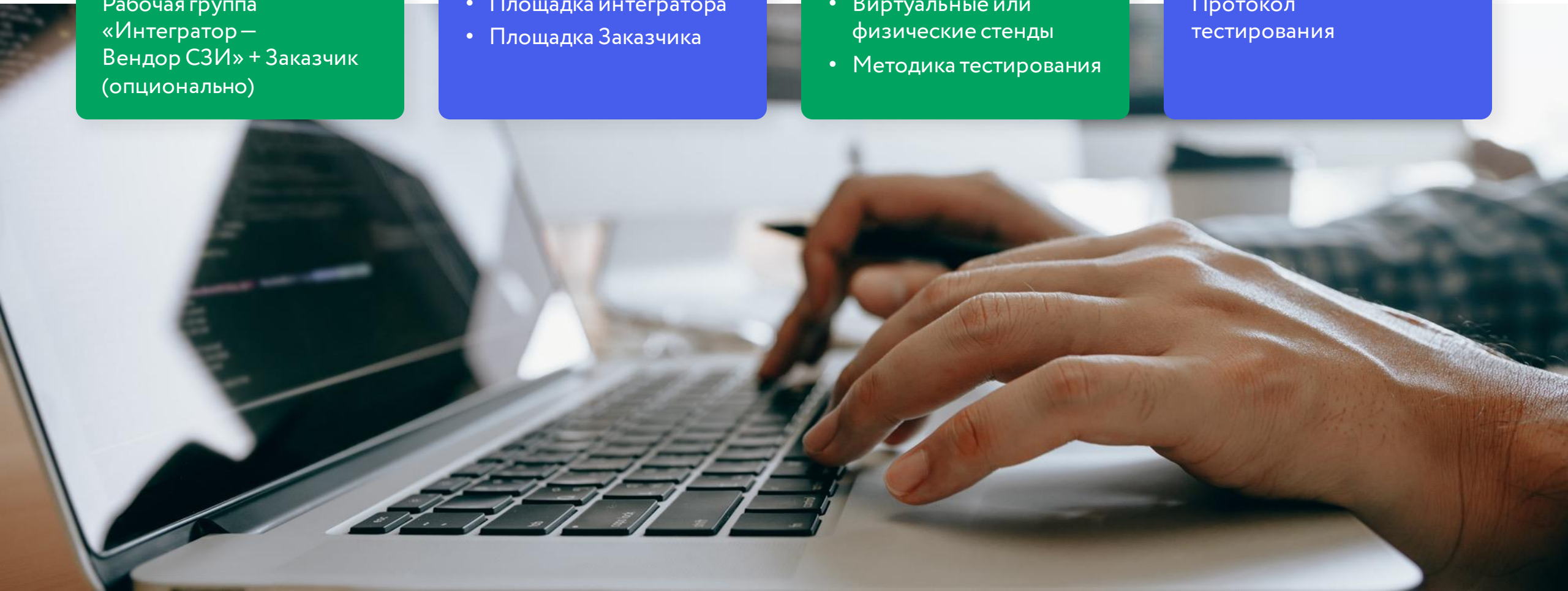
- Площадка интегратора
- Площадка Заказчика

На основании чего?

- Виртуальные или физические стенды
- Методика тестирования

Какой результат?

Протокол тестирования



Лучшие практики по установке СЗИ

- Установка в режиме мониторинга на резервный компонент (при наличии)
- Настройка исключений
- Проверка работоспособности
- Оценка производительности
- Перевод в режим блокировки с дальнейшим обнаружением

КРОК

Лучшие практики по эксплуатации

Мониторинг работоспособности, включая интеграцию с SIEM

Резервное копирование АРМ и серверов

Тестирование восстановления из резервных копий

Наличие стендов для тестирования обновлений

КРОК

ИНТЕГРИРУЕМ БУДУЩЕЕ

Евгений Дружинин
Ведущий эксперт по
информационной безопасности

+7 (495) 974-22-74
+7 915 197-86-85
edruzhinin@croc.ru

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