TELECOM INTEGRATION
innostage group

Безопасность АСУ ТП на практике: «Воздушный зазор» vs современные угрозы. Как экономить на ИБ? Практика интегратора ИТ/ИБ

Авраменко Дмитрий

Руководитель центра компетенций комплексной экспертизы ИБ

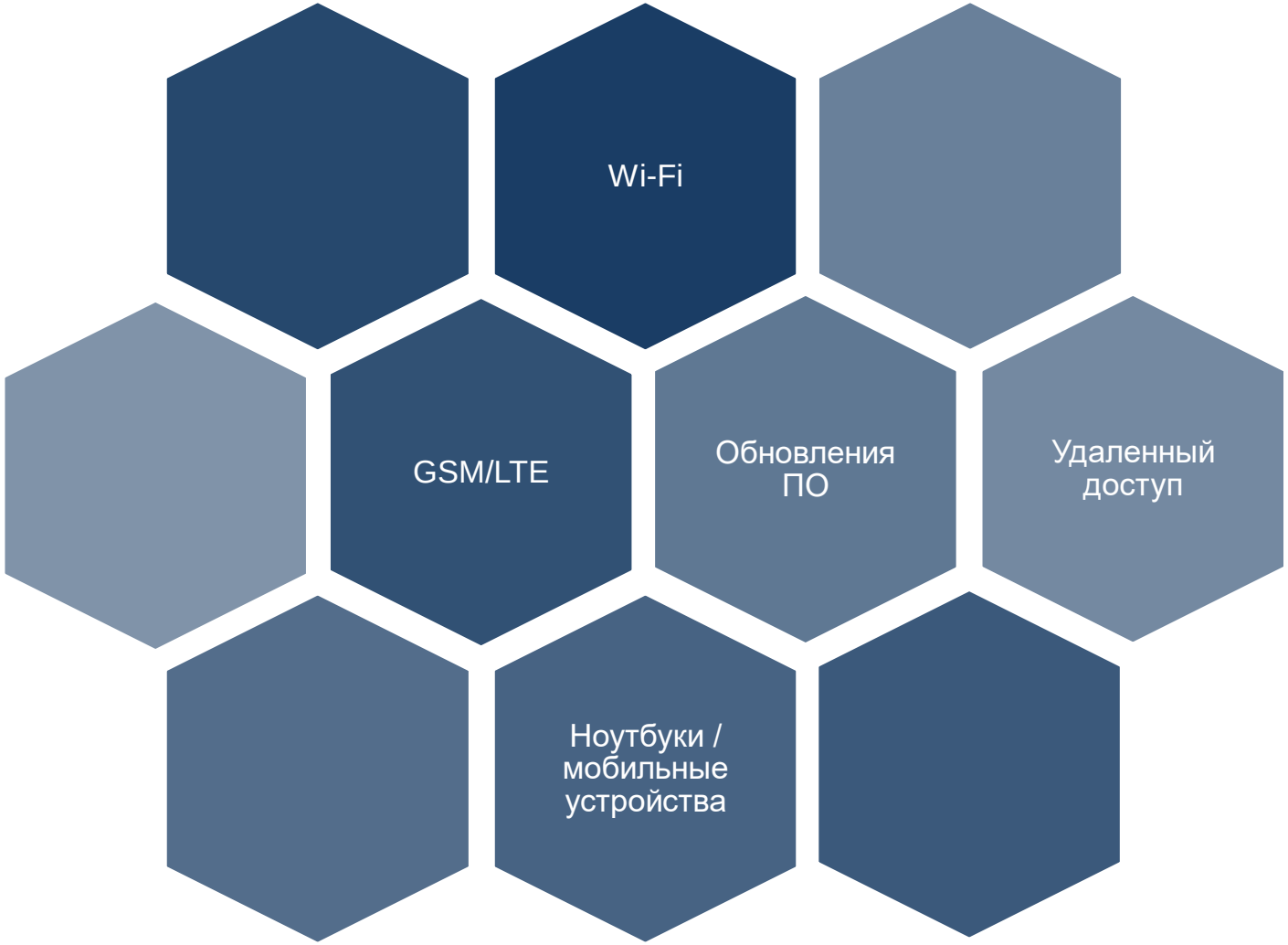
Уровень защиты российских предприятий

50+ % Признают, что кибератака с большой вероятностью будет успешной

50+ % Подтверждают, что риск имеет критические последствия

10+ % Утверждают, что смогут противостоять целевой атаке

«Воздушный зазор»?



Источники угроз промышленных предприятий

	Источник угрозы	Примеры, цели, задачи
Целевые атаки	Террористы, криминал	• Проникновение в технологическую сеть и организация несанкционированного доступа с целью его перепродажи • Развертывание вредоносного ПО, шантаж, получение выкупа
	Конкуренты	• Конкурентная борьба • Нарушение работы бизнеса, ущерб деловой репутации, кража технологических секретов
	Кибервойска	• Атаки спецслужб, как следствие международной конфронтации
	Подрядчики и персонал	• Имеют полный доступ к АСУ ТП, в том числе удаленный • Могут быть мотивированы к мошенничеству и саботажу

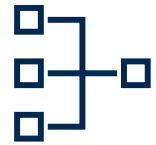
«Совместимость» ИБ с экономией

Как «нужно» экономить на ИБ: вредные советы

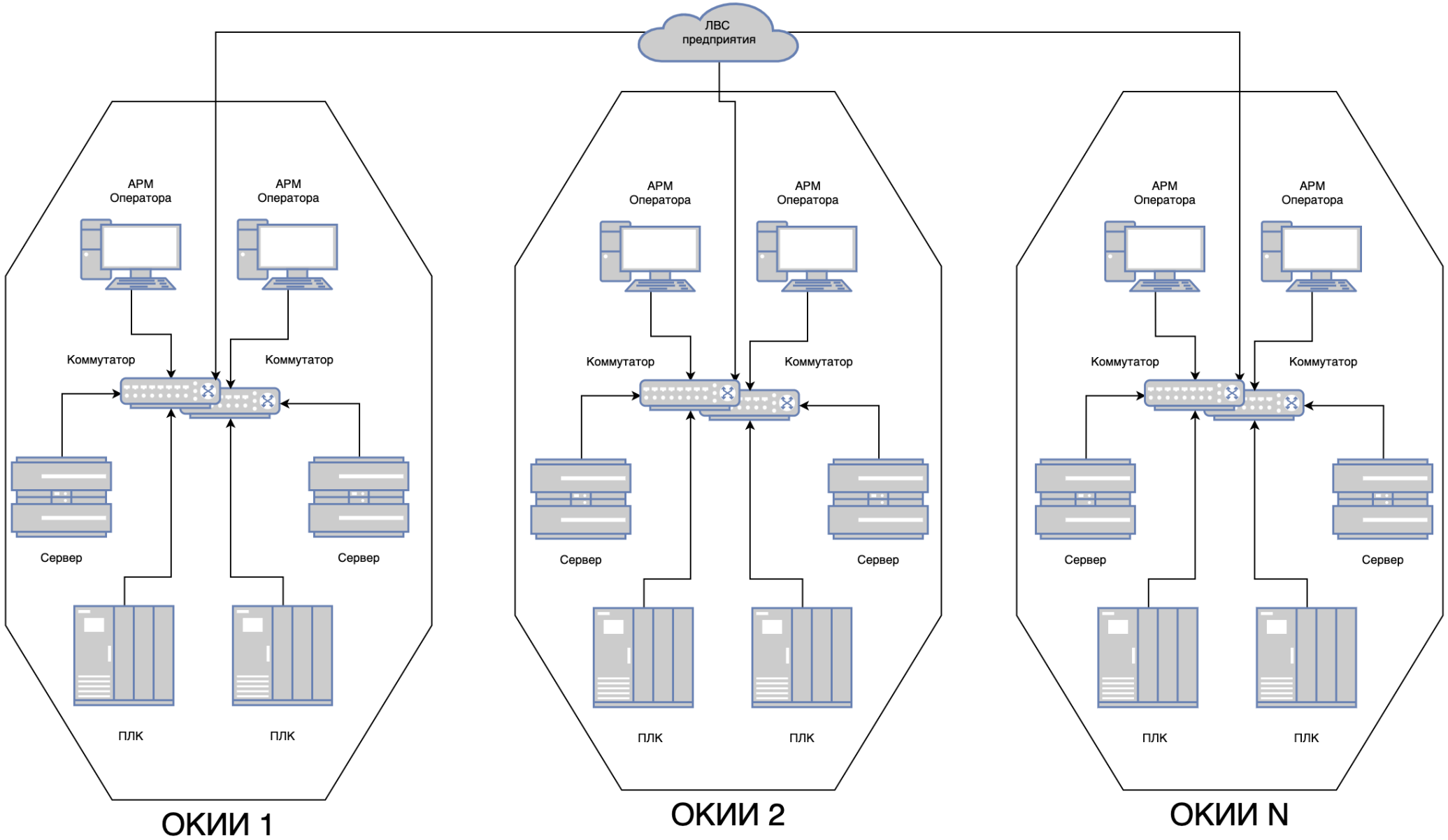
Как «нужно» экономить на ИБ: категорирование

Проблематика

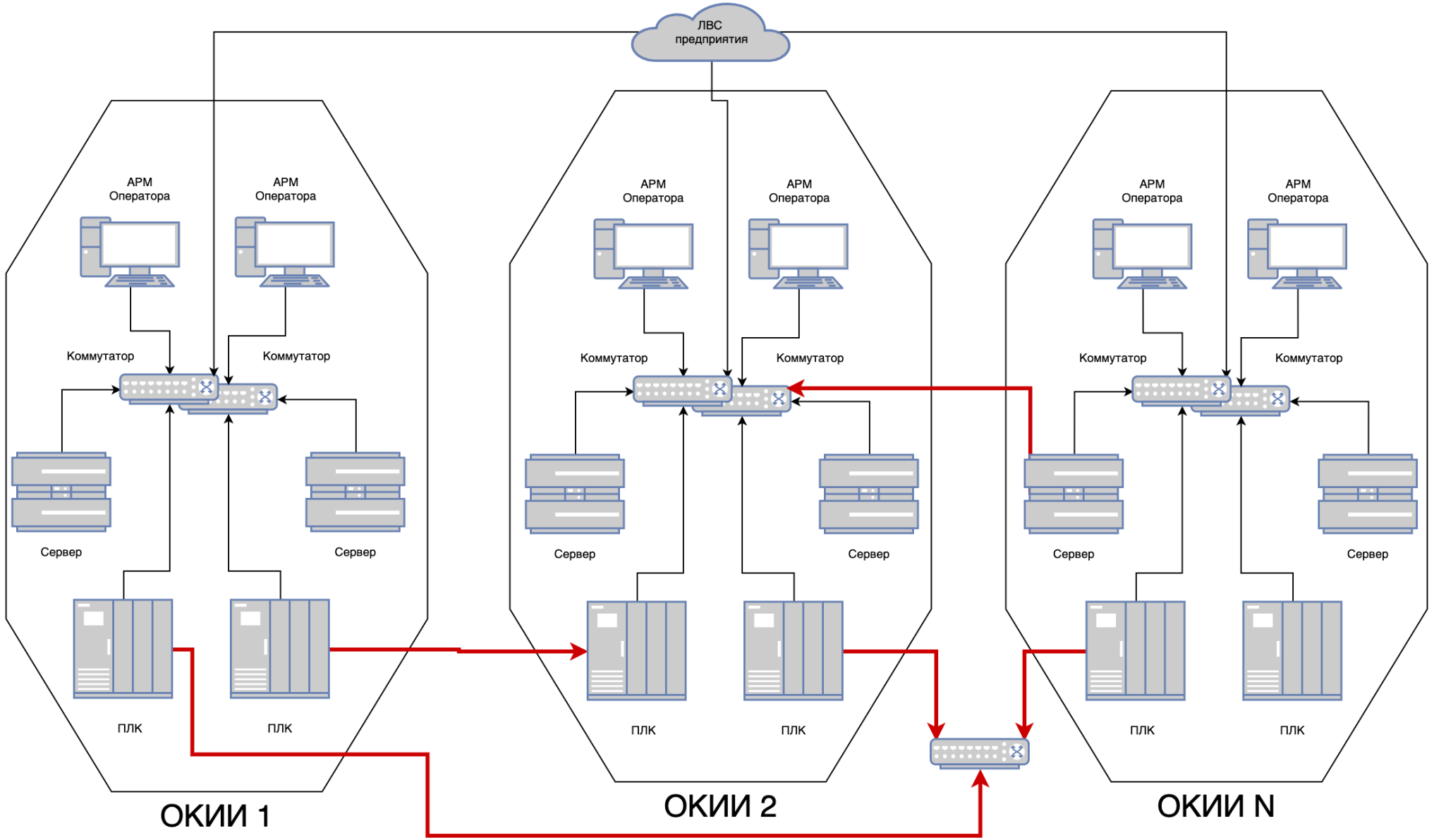
- «Размытость» границ объектов КИИ;
- Сегментировать (/) нельзя (/) объединить;
- Безопасность при взаимодействии ОКИИ между собой и внешними системами



Деление на подсистемы «в лоб»



Но в реальности все сложнее…



«Размытость» границ объектов КИИ

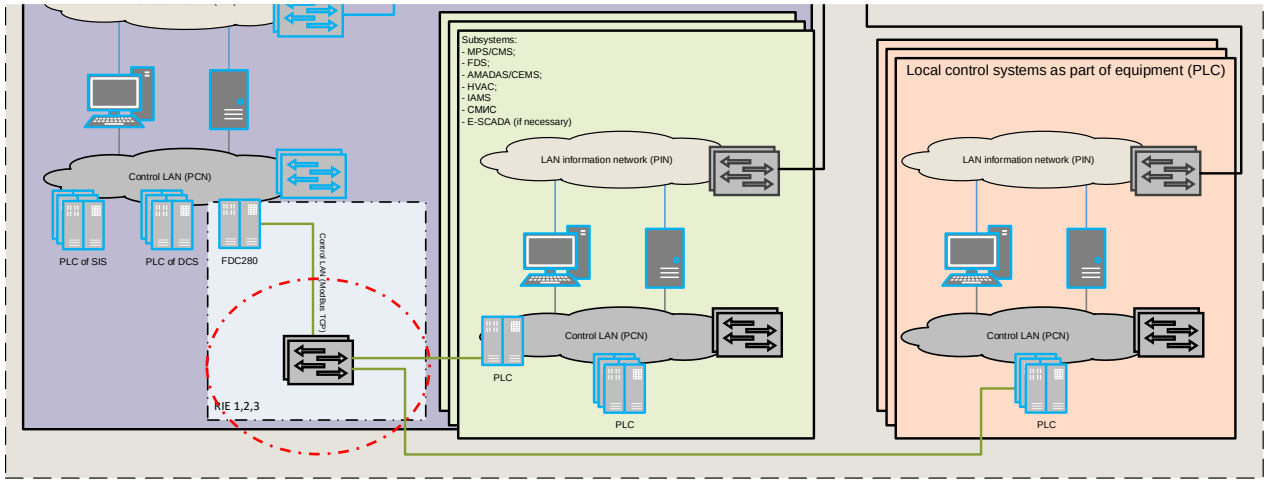
Выделение ОКИИ по «формальному» признаку: система = ОКИИ

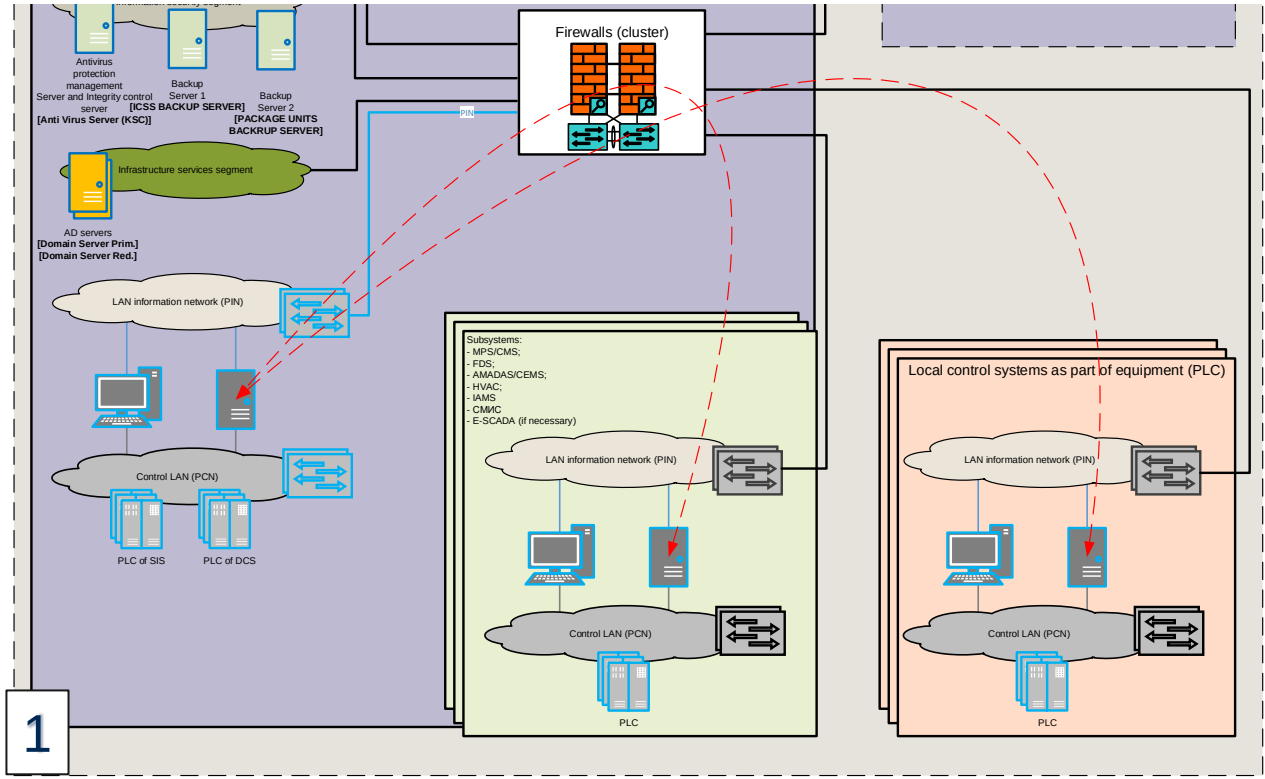
Может не повезти – ОКИИ разделяется только «на бумаге».

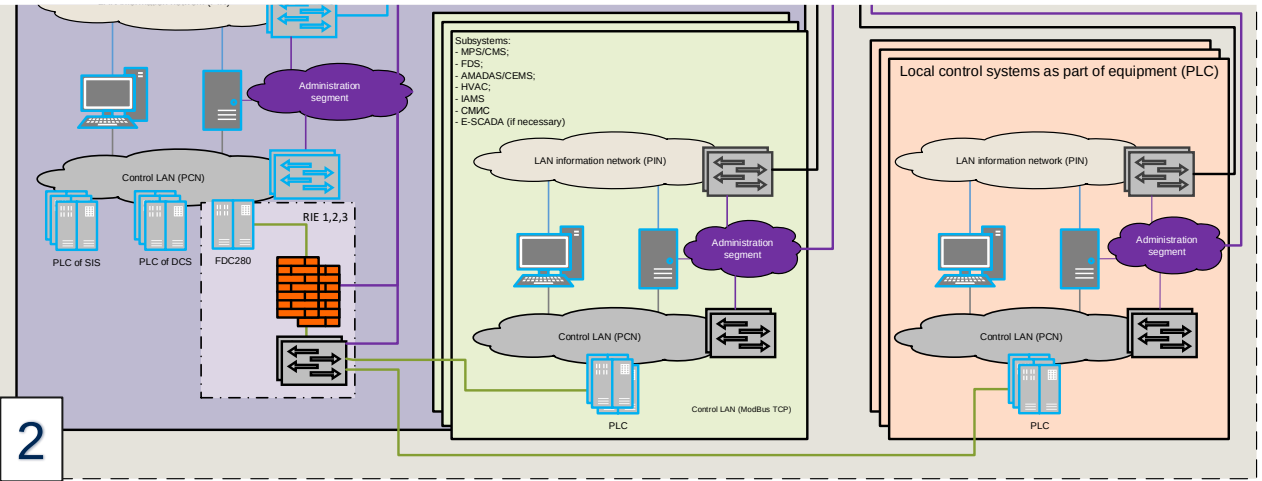
Варианты:

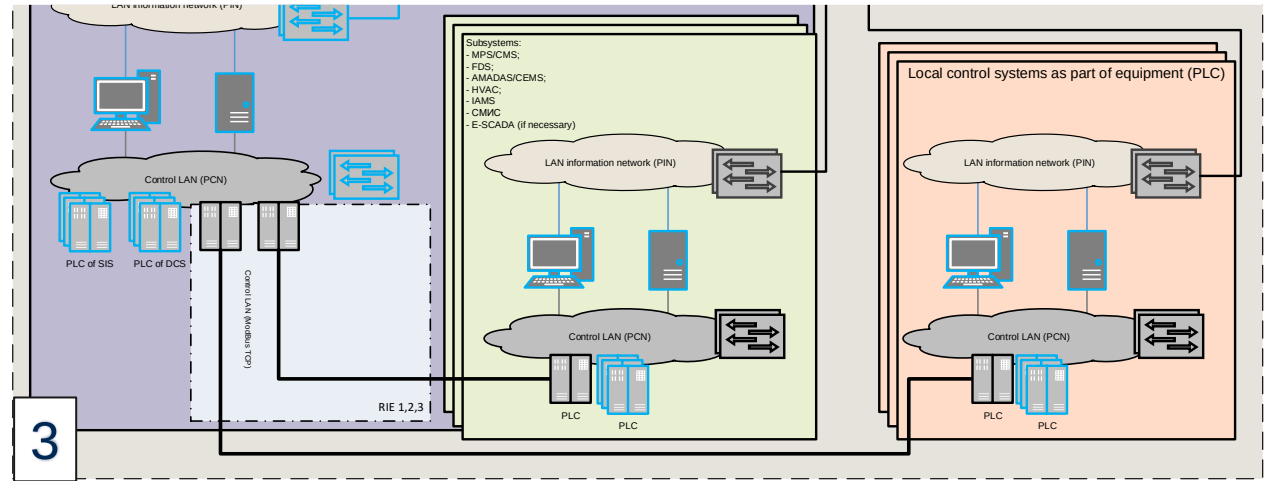
1. Разработка архитектуры сети при **создании/модернизации ОКИИ**
2. Разработка решения по «разделению» ЛВС и контролю, мониторингу сетевых взаимодействий **для действующих ОКИИ**
3. Объединение нескольких ОКИИ в один ОКИИ при невозможности сегментации сети или контроля сетевых взаимодейсвтий

Сегментировать (?) нельзя (?) объединить



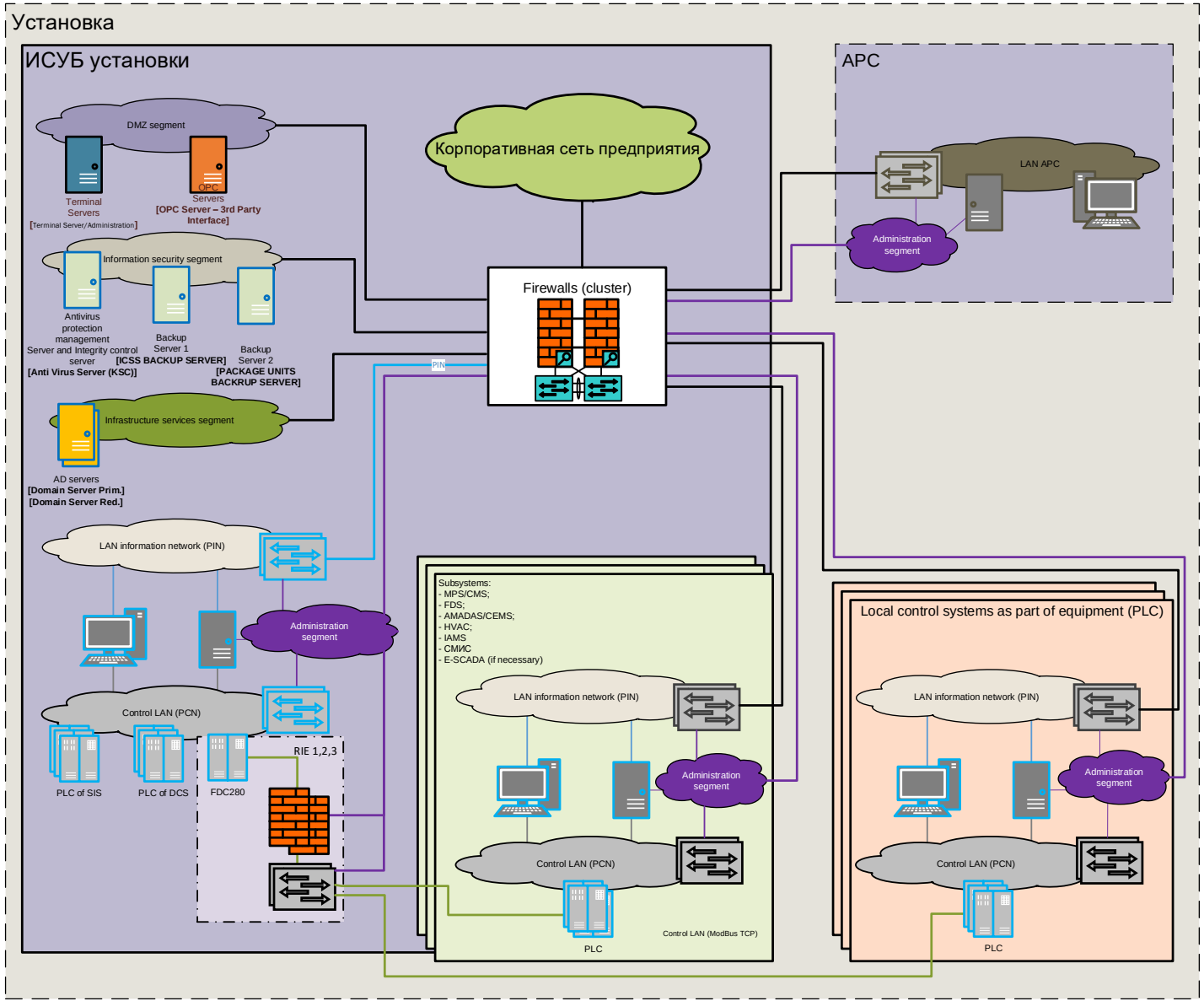


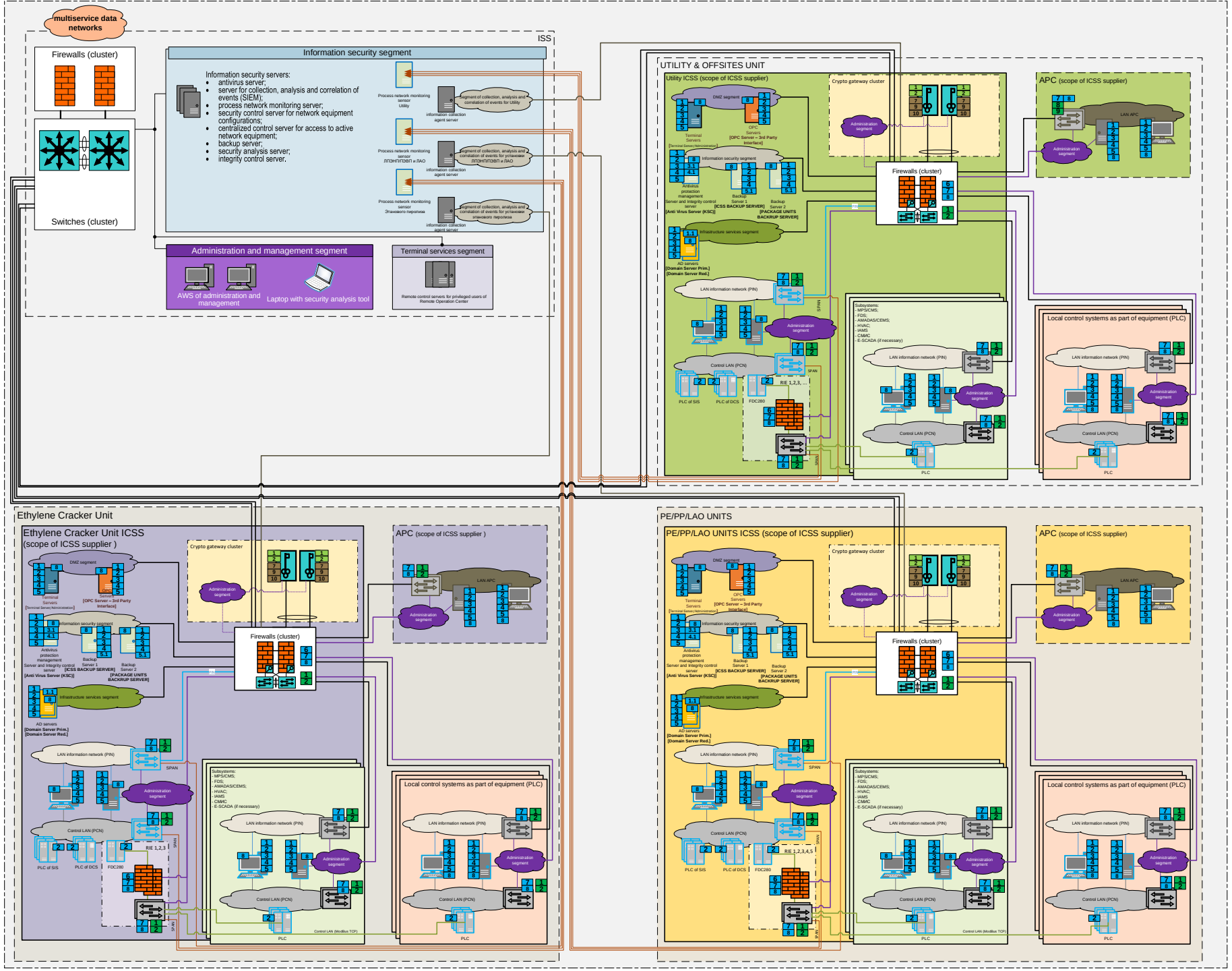




Безопасность при взаимодействии ОКИИ между собой и внешними системами

TELECOM INTEGRATION
innostage group



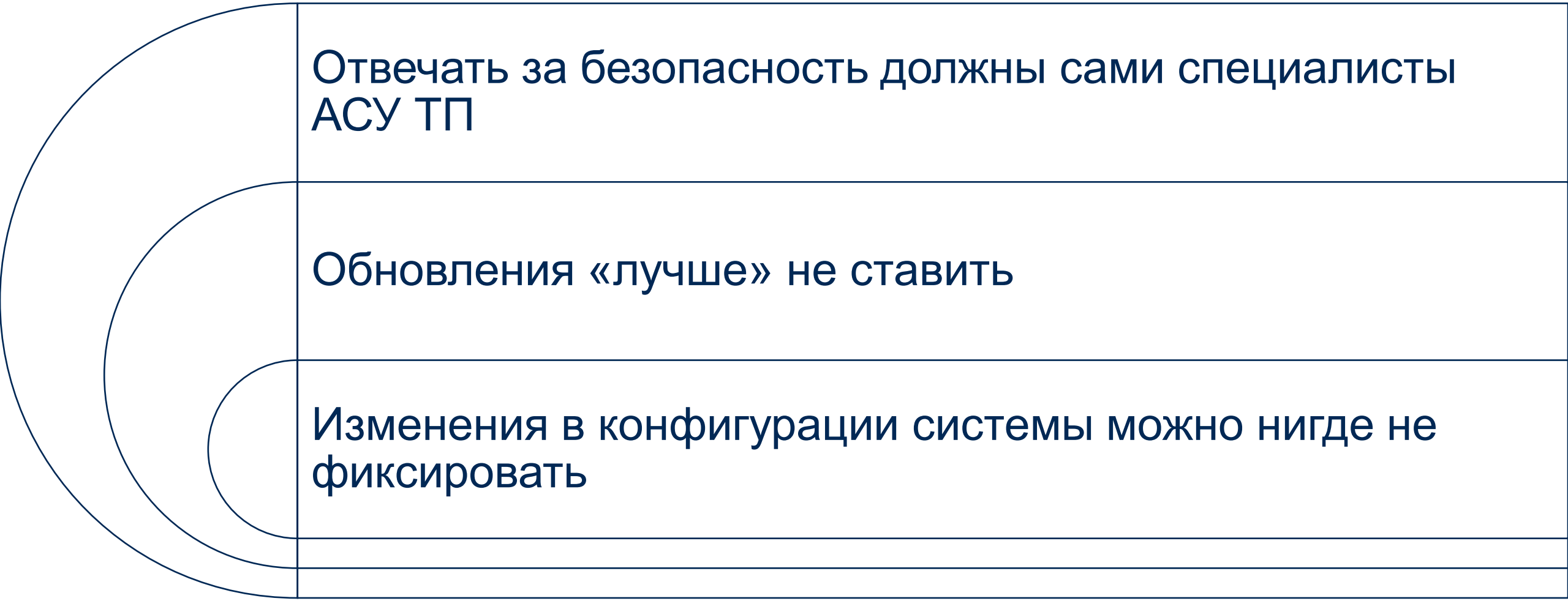


TELECOM INTEGRATION
innostage group

Как «нужно» экономить на ИБ: защита ОКИИ

- Комплексный проект на все ОКИИ – это дорого
- Кто строит/строил объект – лучше знает как защищать
- Единые требования/стандарты/унификация – это дорого, т.к. снижает конкуренцию

Как «нужно» экономить на ИБ: эксплуатация ОКИИ



Ситуации с реальных объектов

«Перестарались» с дроблением объектов КИИ

5 отдельных ОКИИ:

- АСУ турбиной №1
- АСУ турбиной №2
- АСУ турбиной №3
- АСУ котлами-утилизаторами №1, №2, №3
- АСУ и контроля общестанционным оборудованием

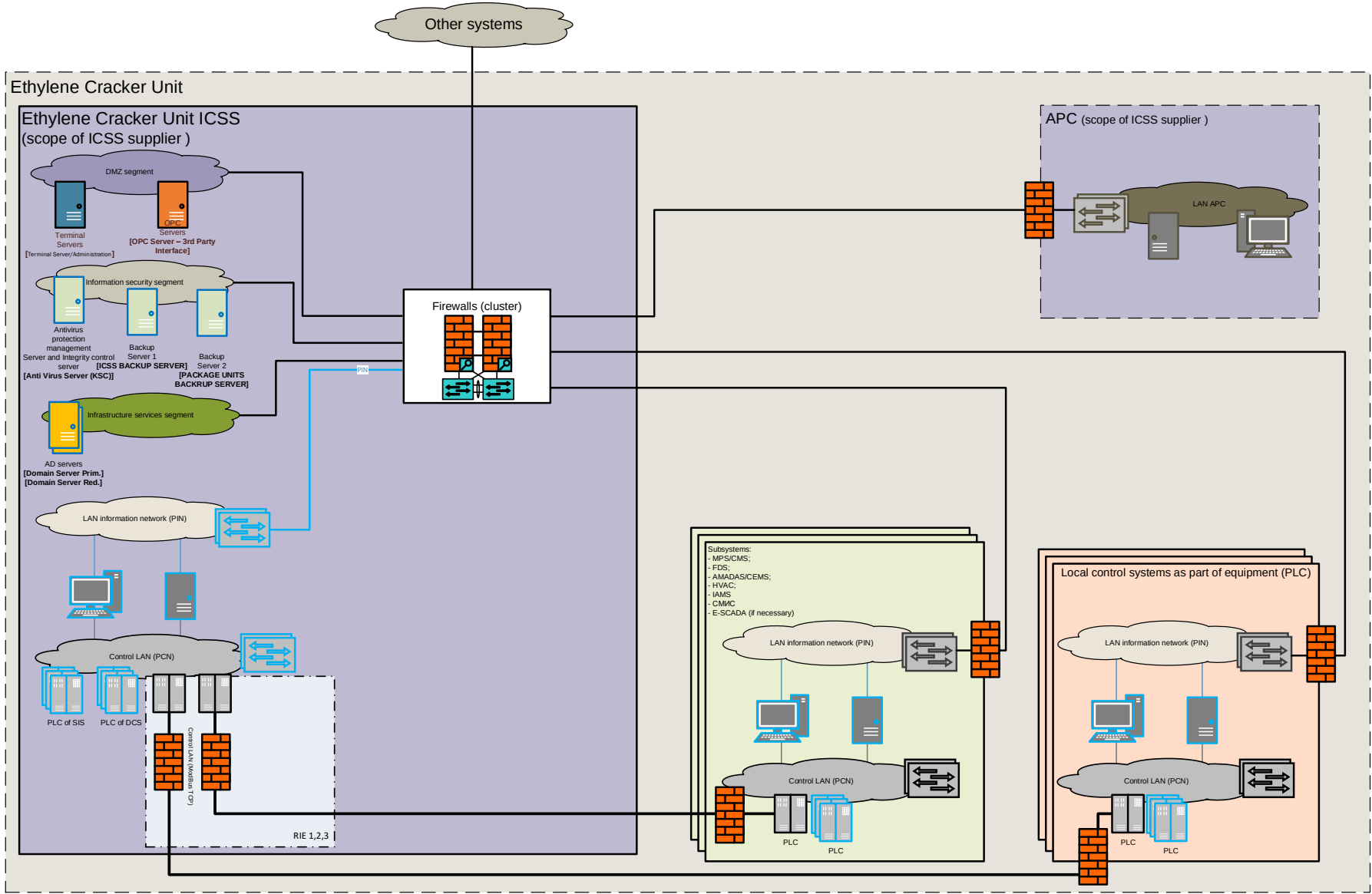
НО:

- Общие рабочие места операторов/диспетчеров
- Общая инженерная станция
- Общее сетевое оборудование
- Общие серверы

1 ОКИИ

Все через «МЭ»

Каждое «внешнее» соединение должно защищаться МЭ =



«Скрытая» инфраструктура

- Как разместить на 4х физических серверах 15 серверов, которые функционируют в системе?
- Как данные попадают на один сервер с 5 отдельных ОКИИ?
- Как один инженер удаленно обслуживает все «изолированные» ОКИИ?
- …

«Домашние» версии ОС и ПО, игры…

- Windows 7 Домашняя/Максимальная
- Avast Free antivirus/Premium Security
- Kaspersky Free | Internet Security
- Half-life, CS 1.5

«Зоопарк» средств защиты

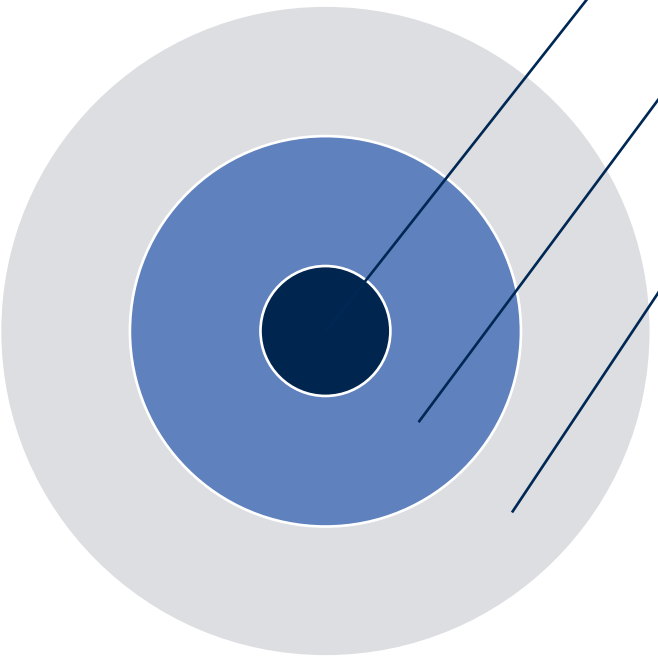
- АВЗ: Kaspersky, Dr. Web, SEP, Trend Micro, Nod32
- МЭ: Cisco, D-Link, Siemens, Hirschmann…
- СРК: Акронис, Veritas, Veeam…

Советы для экономии на ИБ

Обеспечение безопасности должно выполняться на всех этапах жизненного цикла

- Обеспечение безопасности объектов КИИ – обязанность Субъекта КИИ
- Обеспечение безопасности – составная часть работ при создании ОКИИ
- Объект КИИ запускается в эксплуатацию совместно с системой защиты

Подход к оптимизации затрат на обеспечение ИБ при строительстве новых объектов



Уровень ОКИИ

- Встроенные СрЗИ ПТК
- Агенты наложенных СрЗИ
- Сенсоры анализа сетевого трафика
- + Защита периметра ЛВС ОКИИ

Поставщик ПТК ОКИИ

Уровень произв. площадки

- Защита периметра ЛВС ОКИИ
- Сканеры анализа защищенности
- Серверы централизованного управления СрЗИ
- Агенты системы сбора, анализа и корреляции событий ИБ

Уровень предприятия

- Централизация серверов управления СрЗИ
- Сервер системы сбора, анализа и корреляций событий ИБ

Поставщик СОИБ ОКИИ

Зоны ответственности при проектировании СОИБ ОКИИ

Стадия	Результат	Ответственный
Формирование требований к ОБИ ОКИИ	Модель угроз ИБ ОКИИ Технические требования к ОБИ ОКИИ	Проектировщик СОИБ ОКИИ
Архитектура СОИБ ОКИИ	Эскизный проект СОИБ ОКИИ	Проектировщик СОИБ ОКИИ
Проектирование СОИБ на уровне ОКИИ	ТП и РД на СОИБ конкретного ОКИИ в соответствии с ТТ и архитектурой СОИБ ОКИИ	Поставщик ПТК ОКИИ + контроль проектировщика СОИБ ОКИИ
Проектирование СОИБ на уровне произв. площадки	ТП и РД на СОИБ ОКИИ произв. площадки	Проектировщик СОИБ ОКИИ
Проектирование СОИБ на уровне предприятия	ТП и РД на СОИБ ОКИИ предприятия	Проектировщик СОИБ ОКИИ

А что с действующими производствами?

Шаг за шагом приходим к единой масштабируемой СОИБ…

Замена антивируса на действующем производстве

- 350+ рабочих станций и серверов
- От win XP/2003 до windows 10/2016
- 5+ отдельных производств со своей архитектурой
- Тестирование 40+ различных конфигураций ОС и ППО
- Ежемесячное тестирование и выпуск проверенных обновлений
- 3 месяца на замену антивирусного ПО

Резюме

- ✓ Единый подход к обеспечению ИБ предприятия
- ✓ Масштабируемость СОИБ ОКИИ
- ✓ Оптимизация затрат на эксплуатацию СОИБ ОКИИ

Спасибо за внимание!
Вопросы?

Dmitry.Avramenko@innostage-group.ru
innostage-group.ru