ITSF

XIII ЦИФРОВОЙ ФОРУМ

Обеспечение кибербезопасности на объектах электросетевого комплекса: особенности и практический опыт реализации

Айрат Мухаметшин
АО «АйСиЭл - КПО ВС»

Дмитрий Павлюкевич
ОАО «Сетевая компания»

Содержание

- *Инфраструктура энергоснабжения в призме нормативной базы*
- *Электросетевой комплекс как объект атаки*
- *Тенденции обеспечения кибербезопасности в энергетике*
- *Целевое состояние ИБ*
- *Проблематика построения СОИБ на электросетевых объектах*
- *Практический опыт реализации СОИБ на электросетевом объекте*

О компании

- Полный спектр ИТ услуг
- 27 лет в индустрии
- 130 сервисных центров по всей России
- 500 заказчиков в России и за рубежом
- 3 000 - численность сотрудников

Сетевая Компания

- Объекты уровней напряжения 0,4 - 500 кВ
- Топ-10 крупных электросетевых компаний
- 11 филиалов
- 374 подстанции 35 кВ - 500 кВ
- 67 800 км^2 - площадь территории оказываемых услуг

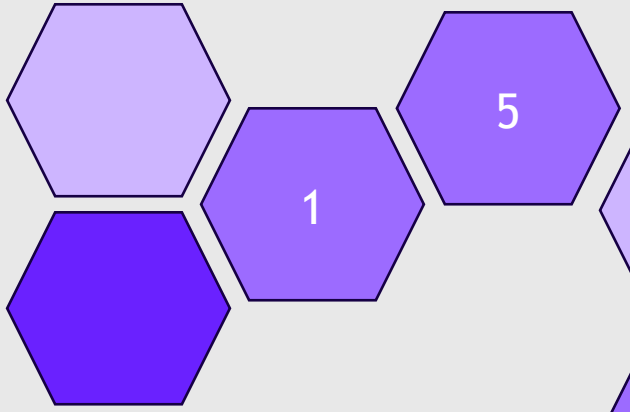
О чем речь?

- *Электросетевой комплекс как объект критической информационной инфраструктуры*
- *Кибербезопасность в электроэнергетике: вчера, сегодня, завтра*
- *Построение системы защиты на примере цифровой подстанции*

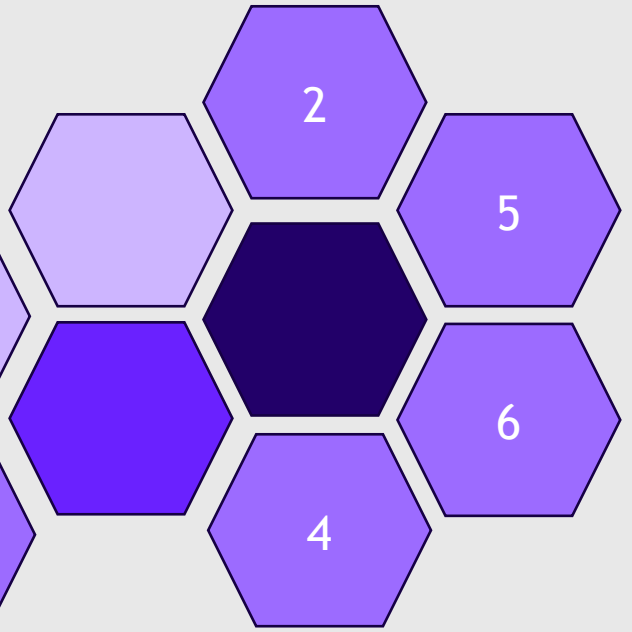
Электросетевой комплекс как объект критической информационной инфраструктуры

- Инфраструктура энергоснабжения в призме нормативной базы
- Электросетевой комплекс как объект атаки
- Объект защиты: ключевые особенности

Инфраструктура энергоснабжения в призме нормативной базы



ФЗ-187 «О безопасности ОКИИ»

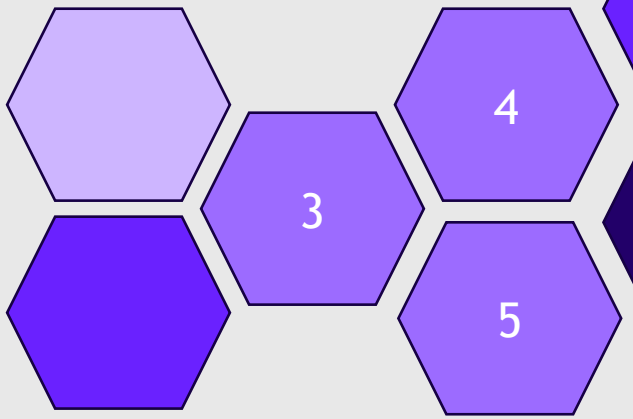


ПП РФ № 127 «О порядке категорирования»

Банковский сектор

ОПО / ООПО / ЧОПО

Документы отраслевого Регулятора

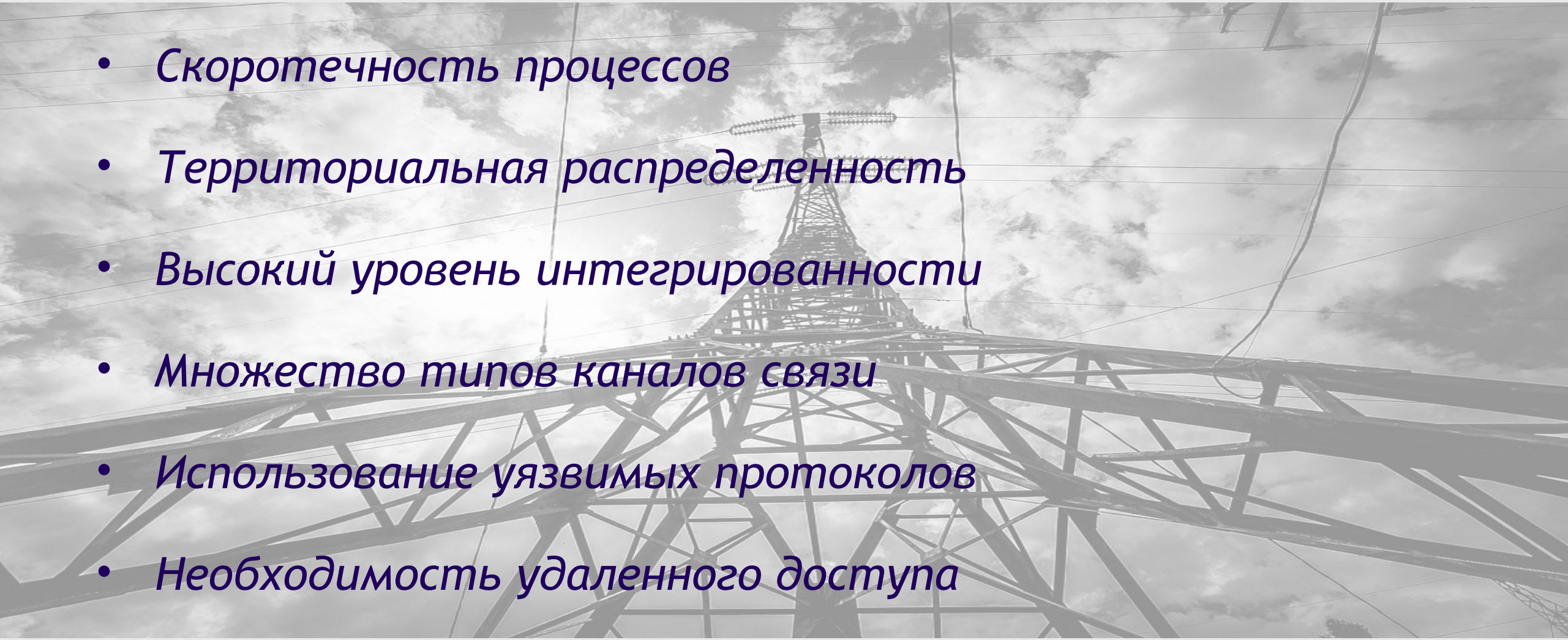


Документы технологического Регулятора

Электроэнергетика

1. Нарушение проведения клиентами операций по банковским счетам
2. Нарушение функционирования объектов жизнедеятельности
3. Ущерб жизни и здоровью людей
4. Возникновение ущерба субъекту КИИ
5. Возникновение ущерба бюджетам РФ
6. Возникновение ущерба окружающей среде

Объект атаки: ключевые особенности



- Скоротечность процессов
- Территориальная распределенность
- Высокий уровень интегрированности
- Множество типов каналов связи
- Использование уязвимых протоколов
- Необходимость удаленного доступа

Объект атаки: ключевые особенности

История актуальности вопроса

Таргетированная фишинговая email атака. Использование макросов, встроенных в файлы Office

Вредоносное ПО скомпрометировало 3 региональных центра управления

Привело к деструктивным последствиям на подстанциях

В результате отключения электроэнергии сотни тысяч домов остались без электричества

Физический урон:

- *удаленное управление выведено из строя*
- *отключение на 7 110 кВ и 23 35 кВ подстанциях*
- *отключение э/энергии в 5 регионах на 6 часов*

Кибер-урон:

- *прошивки RTU изменены*
- *диспетчерские ПК атакованы и «затерты»*
- *DDOS атака на колл-центры*

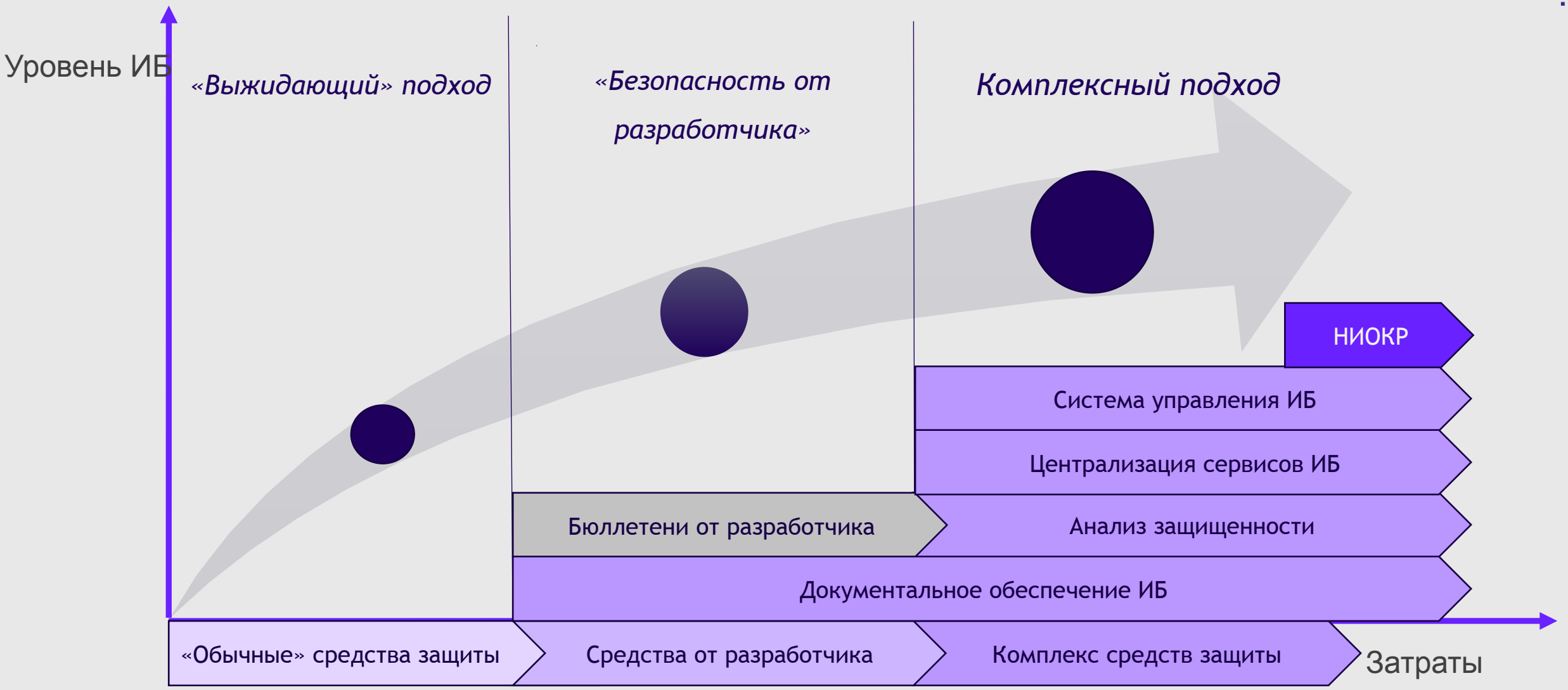
Кибербезопасность в электроэнергетике: вчера, сегодня, завтра

- *Электроэнергетика и кибербезопасность: растем и развиваемся вместе*
- *Тенденции обеспечения кибербезопасности*
- *Определение целевого состояния*

Электроэнергетика и кибербезопасность: растем и развиваемся вместе

ТРЕНДЫ:

Эволюция подхода к обеспечению кибербезопасности



Определение целевого состояния

- *Риск-ориентированный подход к обеспечению ИБ*
- *Единство архитектуры компонентов*
- *Нет зависимости от разработчиков ПТК и средств защиты*
- *Контроль состояния защищенности*
- *Обеспечение непрерывности процессов в условиях кибератак*

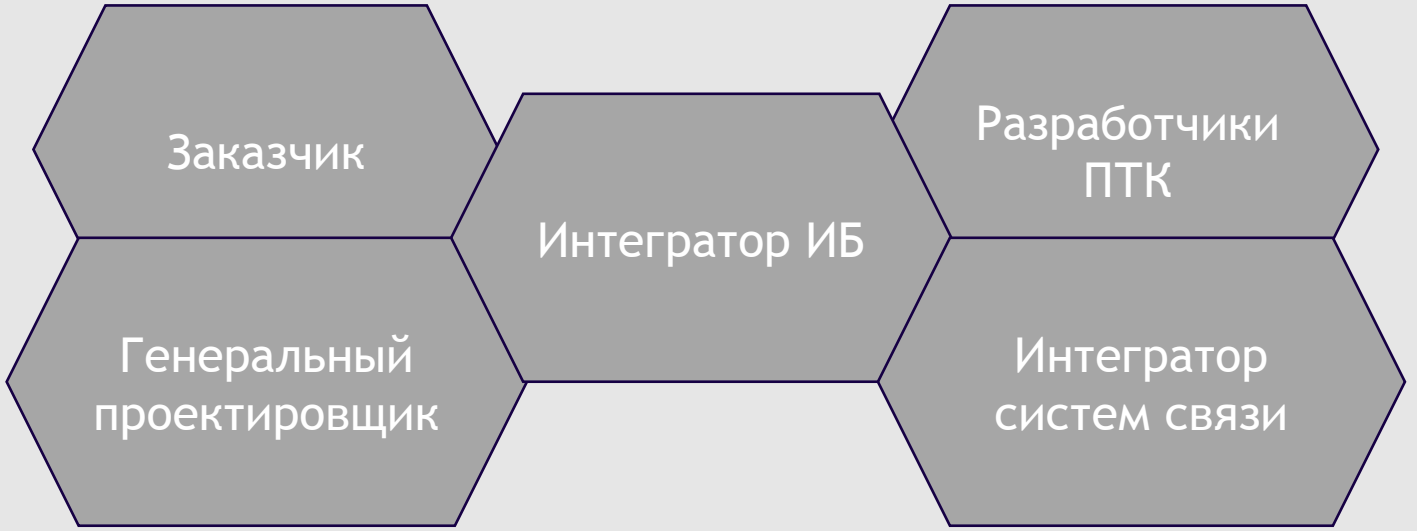
Построение системы защиты на примере цифровой подстанции

- *Защита систем электросетевого комплекса: суровые будни ИБ*
- *Построение СОИБ на электросетевых объектах: теория и практика*
- *Реализация системы защиты на ЦПС «Портовая»*

Построение СОИБ на объектах электросетевого комплекса

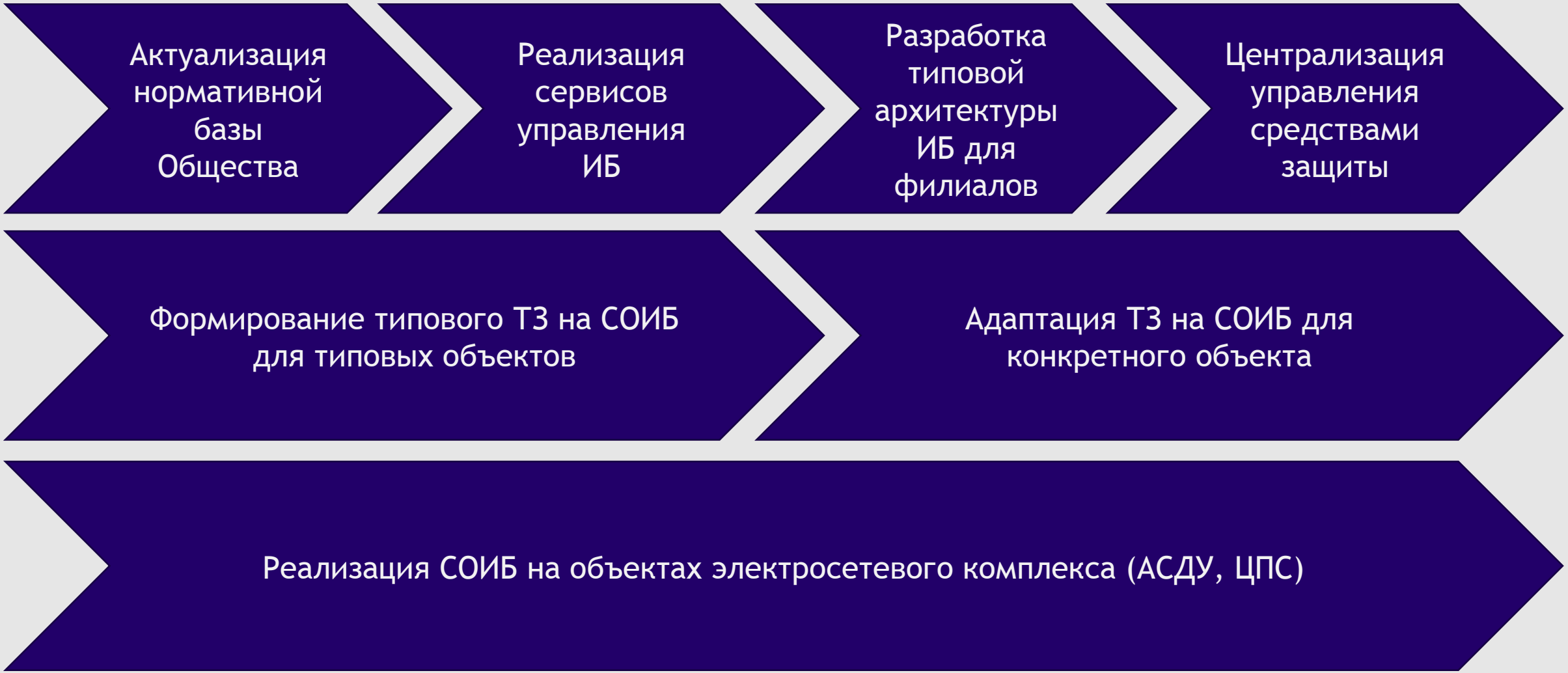
- *Определение типовых схем подключений и матрицы взаимодействия*
- *Реализация сервисов управления ИБ*
- *Типизация объектов и архитектуры СОИБ*
- *Централизация управления средствами защиты*

ИБ электросетевого комплекса: суровые будни системной интеграции



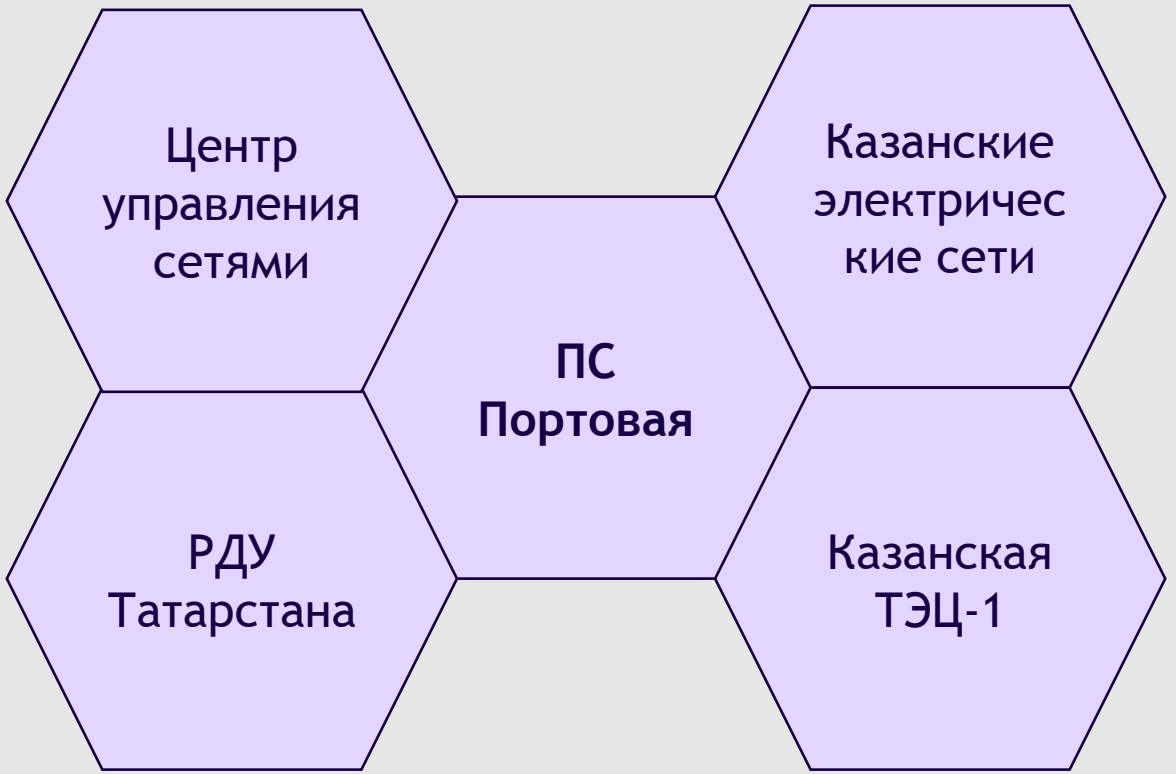
Проектирование отдельных компонентов ЦПС «под ключ»	Нет общей картины информационного обмена
Не выбран поставщик оборудования	Отсутствие возможности определить настройки безопасности
Настройки на этапе проектирования не определены	Работа «по месту» и «по факту» → Коллизии
Проектирование решений ИБ после основных разделов	Накладки графиков внедрения → Увеличение сроков реализации
Пуско-наладка отдельных компонентов ПТК до «точки подключения в ЛВС»	Несогласованность плана IP-адресации

Построение СОИБ на объектах электросетевого комплекса на примере ОАО «Сетевая компания»



Построение СОИБ на ПС «Портовая»

- *Цифровая подстанция*
- *110/6 кВ*
- *Категория значимости: 3*
- *Потребителей: > 2000 тысяч*



О проекте

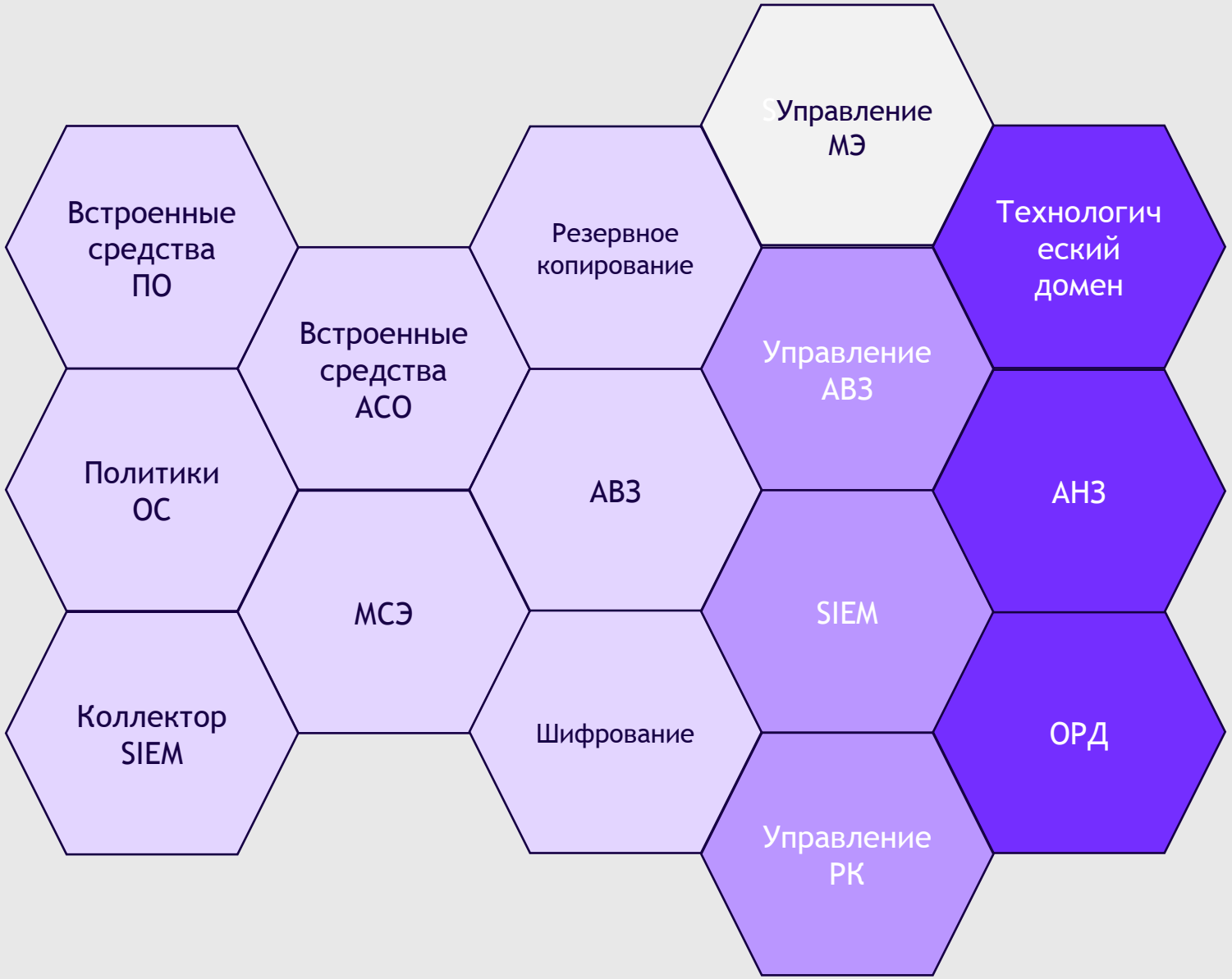
- *Переход к концепции цифровой подстанции*
- *Разработка решений по ИБ после формирования решений в части ПТК*

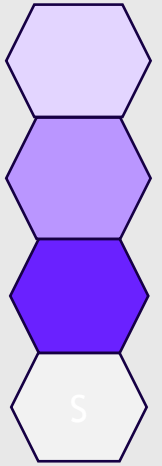
Текущее состояние: подготовка к этапу опытной эксплуатации

Планируется:

- *Анализ защищенности*
- *Приемо-сдаточные испытания*
- *Ввод в эксплуатацию*

Проектные решения





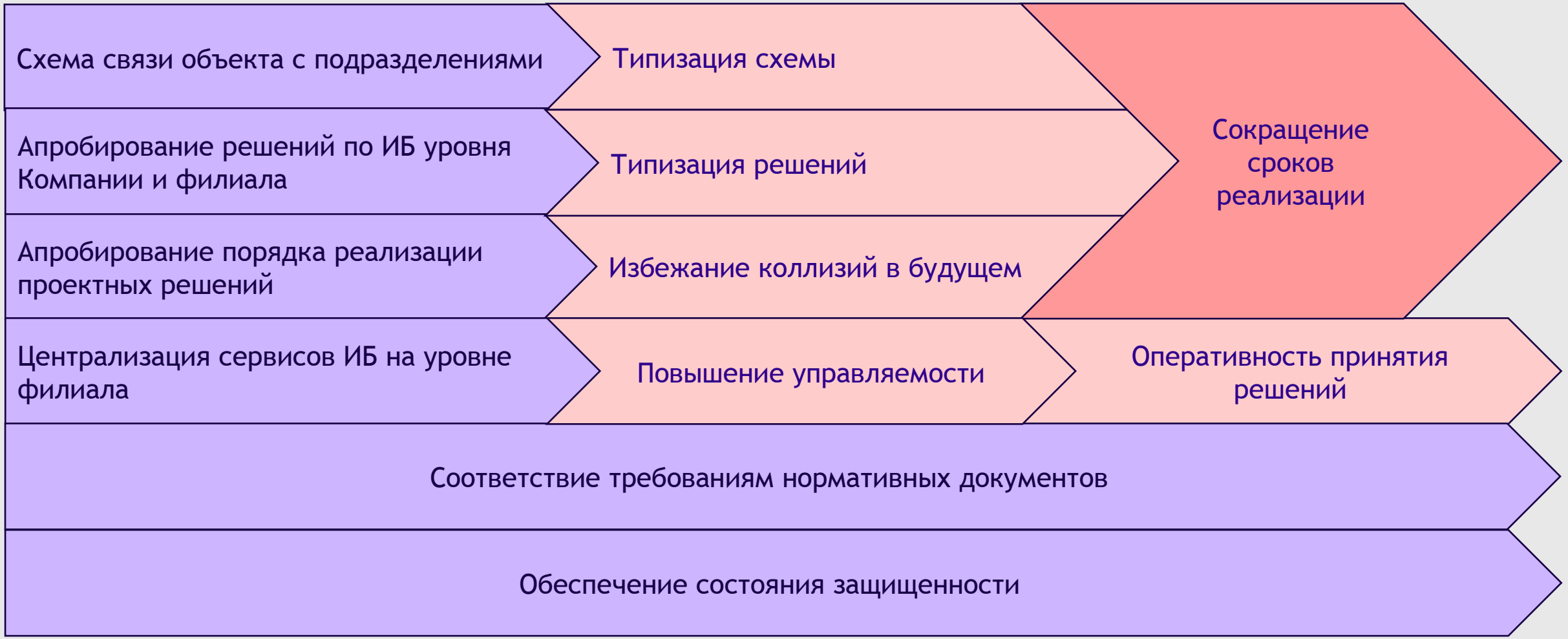
ПС
Портовая

Филиал Казанские электрические сети

Управление ОАО «Сетевая компания»

Планируемые решения

Итоги проекта



Спасибо за внимание!