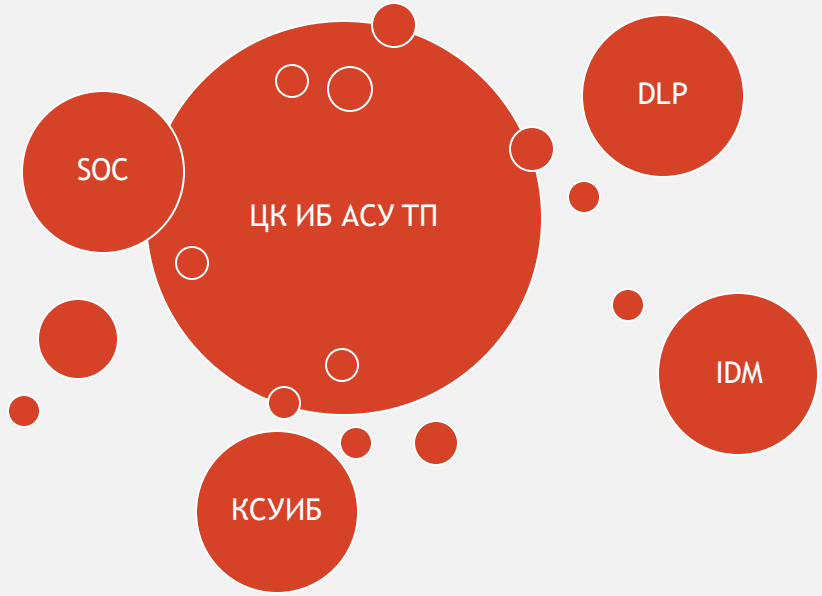
ICL SYSTEM TECHNOLOGIES

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

Дмитрий Авраменко

Руководитель Центра компетенций ИБ АСУ ТП

ICL SYSTEM TECHNOLOGIES



- 28 лет проектного опыта и экспертизы
- Центр компетенций информационной безопасности АСУ ТП
- Центр мониторинга и реагирования на компьютерные инциденты

kaspersky
Industrial Cybersecurity
partner

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 объекте электросетевого комплекса

О чем речь?

- Электросетевой комплекс как «объект» КИИ
- 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

ICL SYSTEM TECHNOLOGIES

ФЗ-187 «О безопасности ОКИИ»

ПП РФ № 127 «О порядке категорирования»

Документы отраслевого Регулятора

Документы технологического Регулятора

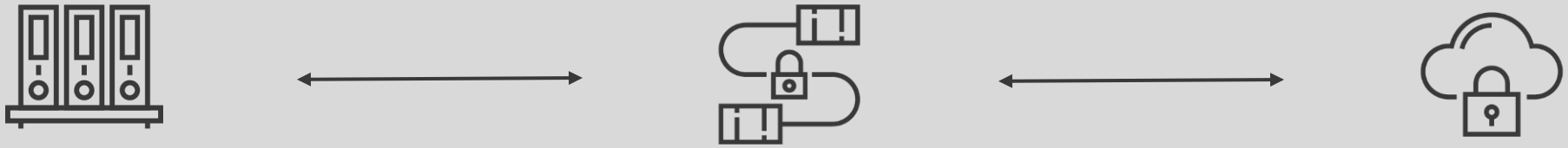
Банковский сектор	ОПО/ООПО/ ЧОПО	Электроэнергетика
1,5	3,4,5	2,3,4,5,6

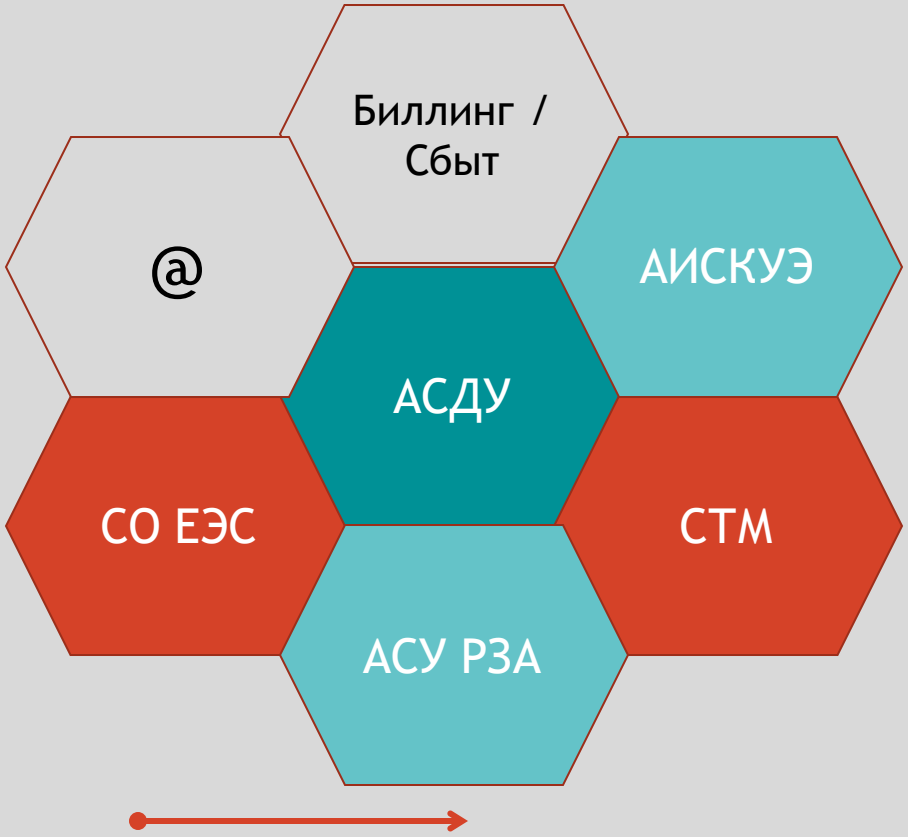
1. Нарушение проведения клиентами операций по банковским счетам
2. Нарушение функционирования объектов жизнедеятельности
3. Ущерб жизни и здоровью людей
4. Возникновение ущерба субъекту КИИ
5. Возникновение ущерба бюджетам РФ
6. Возникновение ущерба окружающей среде

Объект атаки: ключевые особенности

ICL SYSTEM TECHNOLOGIES

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





Каналы связи

- Собственные каналы
- Сеть сотовой связи
- Арендованные каналы

Объект атаки: ключевые особенности

ICL SYSTEM TECHNOLOGIES

Кибербезопасность в электроэнергетике: вчера, сегодня, завтра

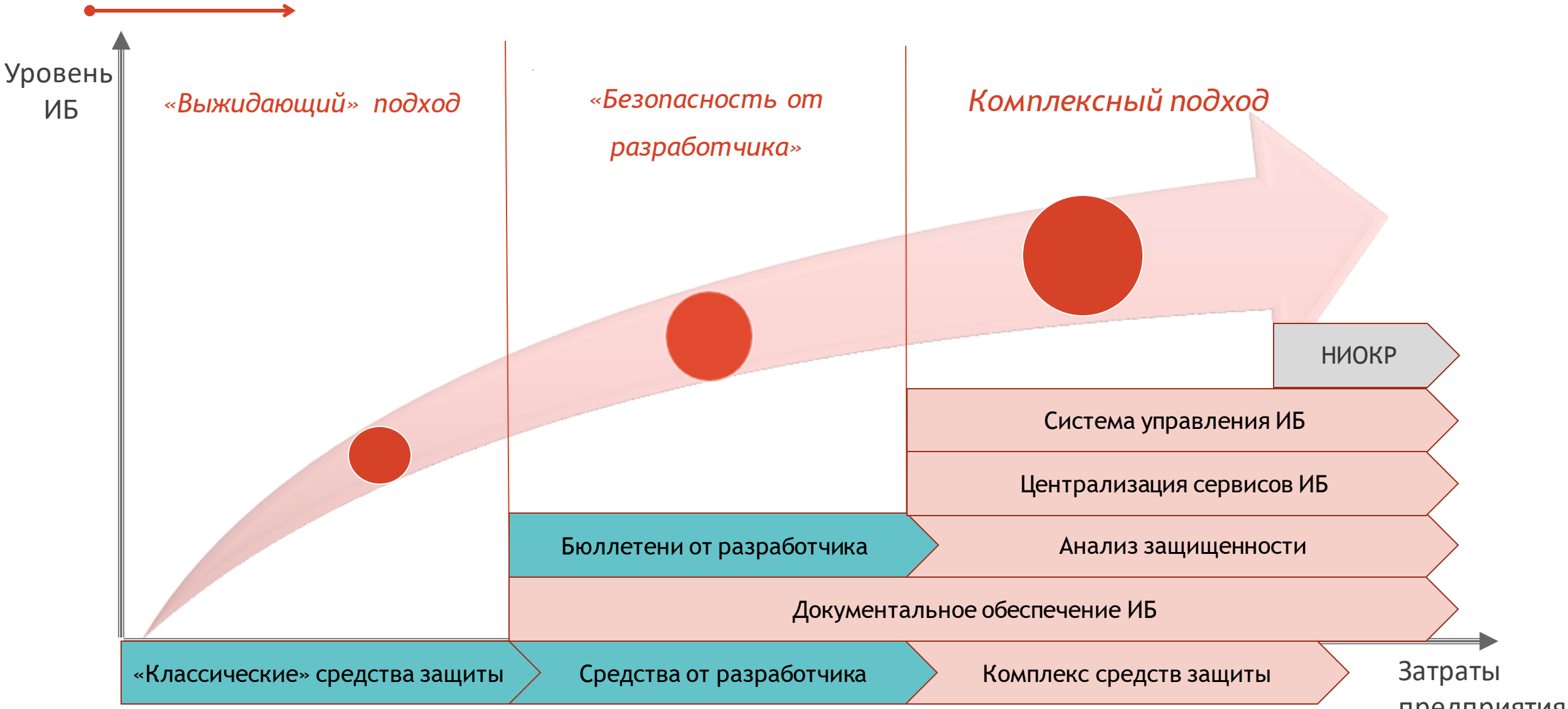
- *Электроэнергетика и кибербезопасность: растем и развиваемся вместе*
- *Тенденции обеспечения кибербезопасности*
- *Определение целевого состояния*

Электроэнергетика и кибербезопасность: растем и развиваемся вместе

ICL SYSTEM TECHNOLOGIES

«Эволюция» подхода к обеспечению кибербезопасности

ICL SYSTEM TECHNOLOGIES



Определение целевого состояния

ICL SYSTEM TECHNOLOGIES

- 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

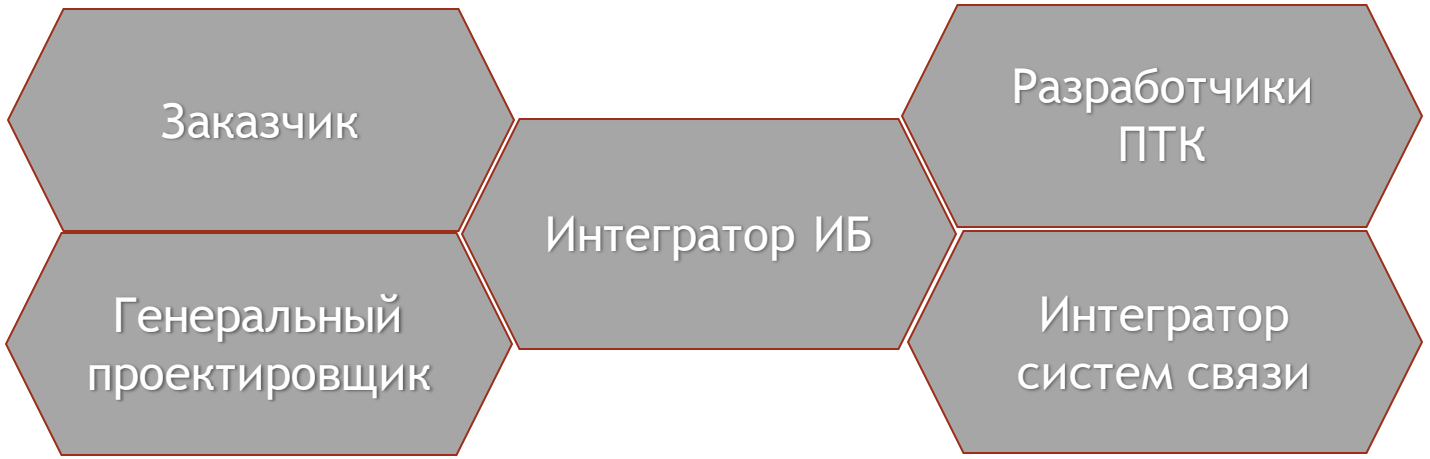
- *Защита систем электросетевого комплекса: суровые будни ИБ*
- *Построение СОИБ на электросетевых объектах: теория и практика*
- *Реализация системы защиты на ЦПС*

Построение СОИБ на объектах электросетевого комплекса

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

ИБ электросетевого комплекса: суровые будни системной интеграции

ICL SYSTEM TECHNOLOGIES



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

ICL SYSTEM TECHNOLOGIES

Актуализация нормативной базы Общества

Реализация сервисов управления ИБ

Разработка типовой архитектуры ИБ для филиалов

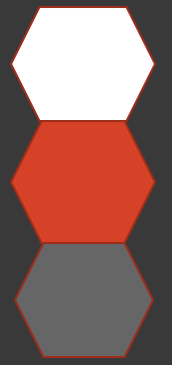
Централизация управления средствами защиты

Формирование типового ТЗ на СОИБ для типовых объектов

Формирование типовых требований к порядку создания объектов

Реализация СОИБ на объектах электросетевого комплекса (АСДУ, ЦПС)

Проектные решения



ЦПС

Филиал

Документальное обеспечение

Итоги проекта

ICL SYSTEM TECHNOLOGIES

Спасибо за внимание!