# Создание системы обеспечения ИБ АСТУ электросетевой компании

Дмитрий Ярушевский
CISA, CISM
Руководитель отдела Кибербезопасности АСУ ТП
АО «ДиалогНаука»

ДиалогНаука

Тел.: +7 (495) 980 67 76
http://www.DialogNauka.ru
Dmitry.Yarushevskiy@DialogNauka.ru

# АО «ДиалогНаука»

Системный интегратор в области информационной безопасности, успешно работающий на рынке более 20 лет.

АО «ДиалогНаука» выполняет проекты по разработке, созданию и внедрению систем обеспечения информационной безопасности в банковской, энергетической, промышленной, оборонной и других отраслях.

# О чем вообще речь?

АСТУ – автоматизированная система технологического управления (распределительными электрическими сетями)

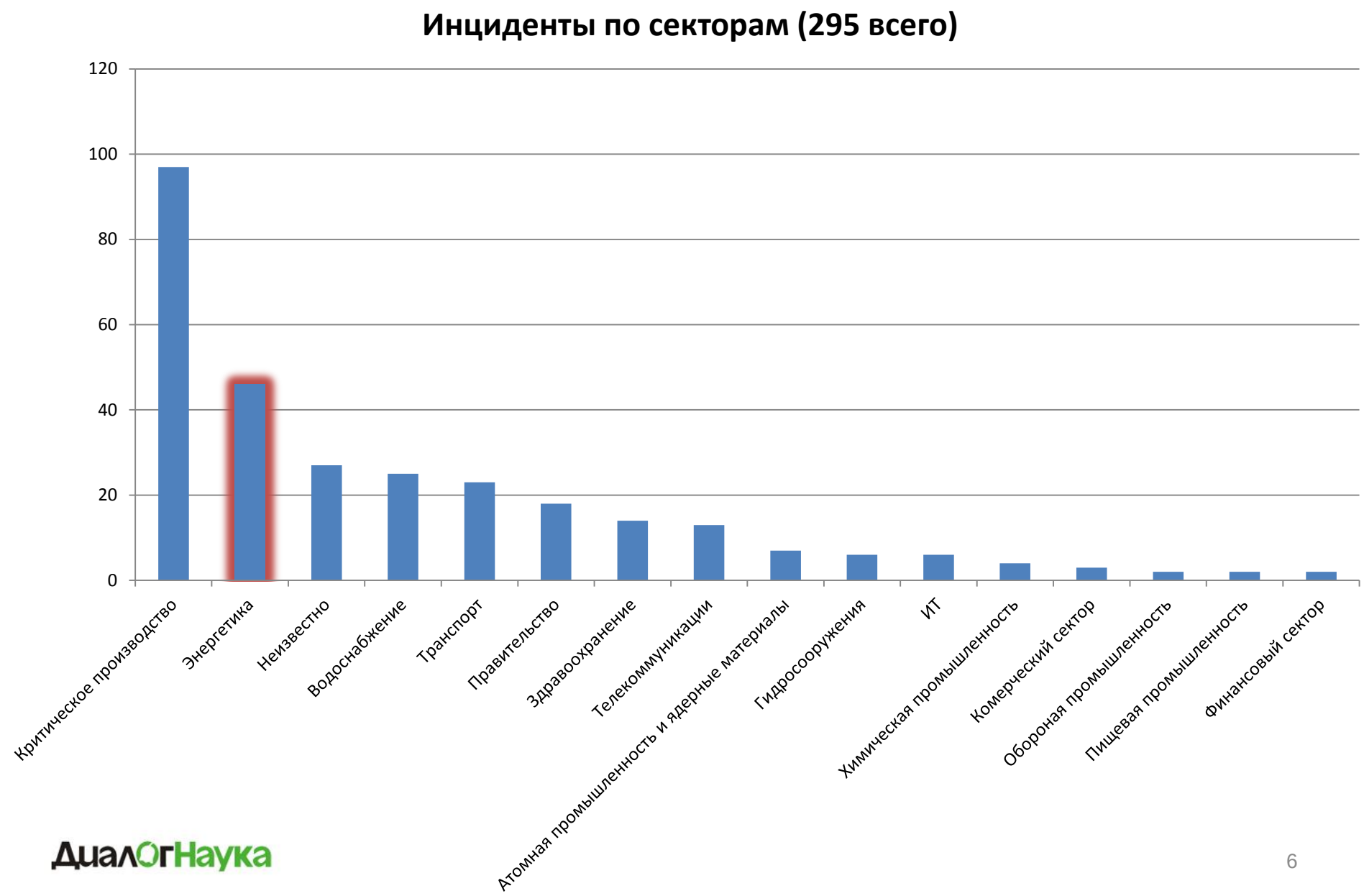
# О чем вообще речь?

- Системы диспетчерско-технологического и системы оперативного управления;
- АИСКУЭ/АИСТУЭ;
- Управление заявками;
- Системы релейной защиты и автоматики;
- Системы управления и мониторинга первичного электрооборудования;
- Системы управления и мониторинга оборудованием связи, инженерными системами, сигнализациями;
- И т.д.


ДиалОгНаука

# Немного страшных историй…

# Данные отчета ICS-CERT за 2015 г.



# Атака на энергосеть Украины, 2015

**BlackEnergy**: Выведено из строя оперативно-диспетчерское управление, отключено напряжение на 7 ПС 110кВ и 23 ПС 35кВ.
**Результат**: 5 регионов без электричества 6 часов

# Мирный атом под угрозой

## German nuclear plant suffers cyber attack designed to give hackers remote access

share

The Gundremmingen plant is run by the German utility RV

27 APRIL 2016 • 12:29PM

TECHNOLOGY NEWS | Mon Oct 10, 2016 | 10:39am EDT

## IAEA chief: Nuclear power plant was disrupted by cyber attack

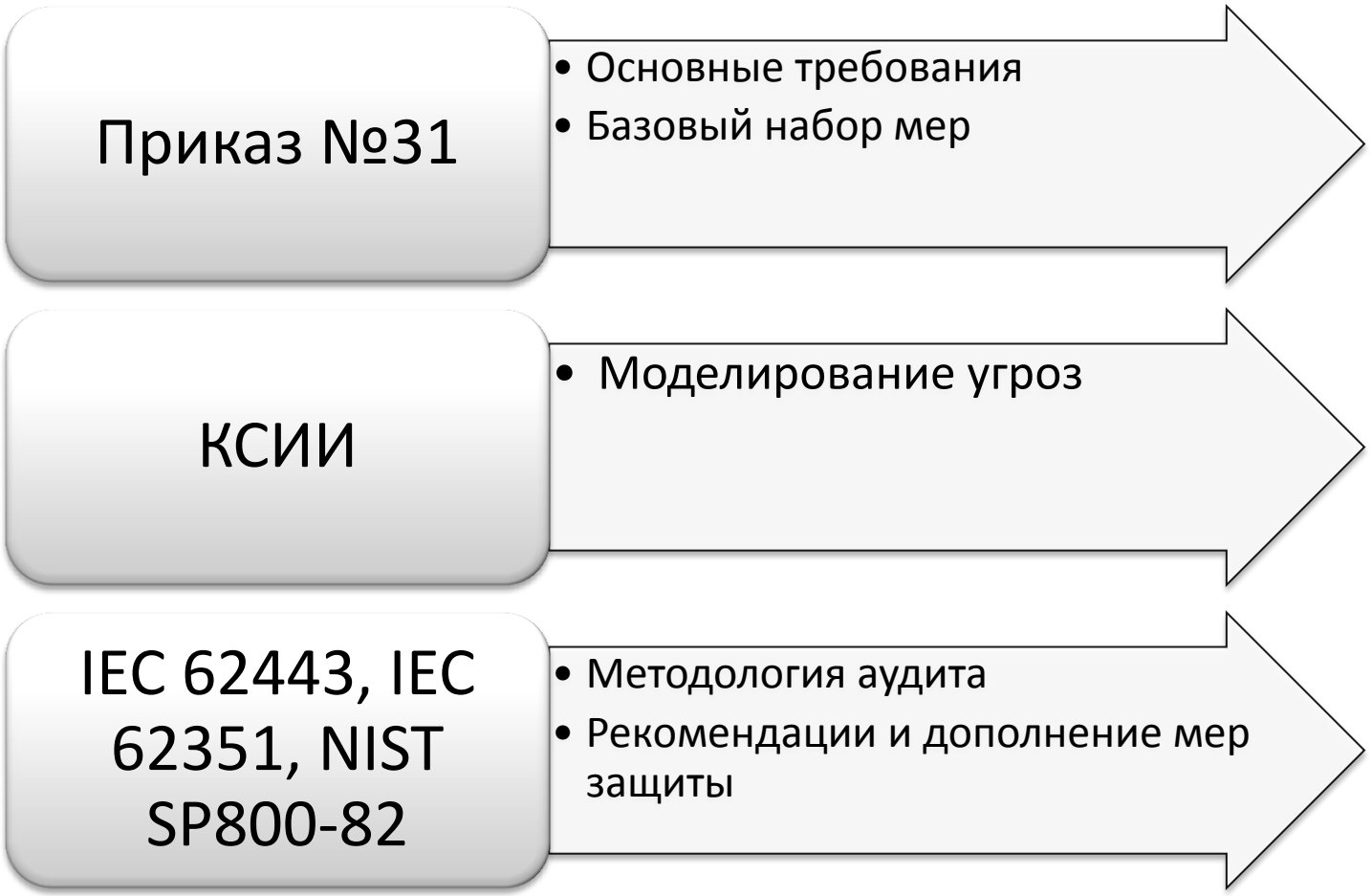

International Atomic Energy Agency (IAEA) Director General Yukiya Amano smiles as he waits for a board of governors meeting to begin at the IAEA headquarters in Vienna, Austria June 6, 2016. REUTERS/Heinz-Peter Bader

# «Суровые хакеры на службе ЦРУ, АНБ и других страшных букв»

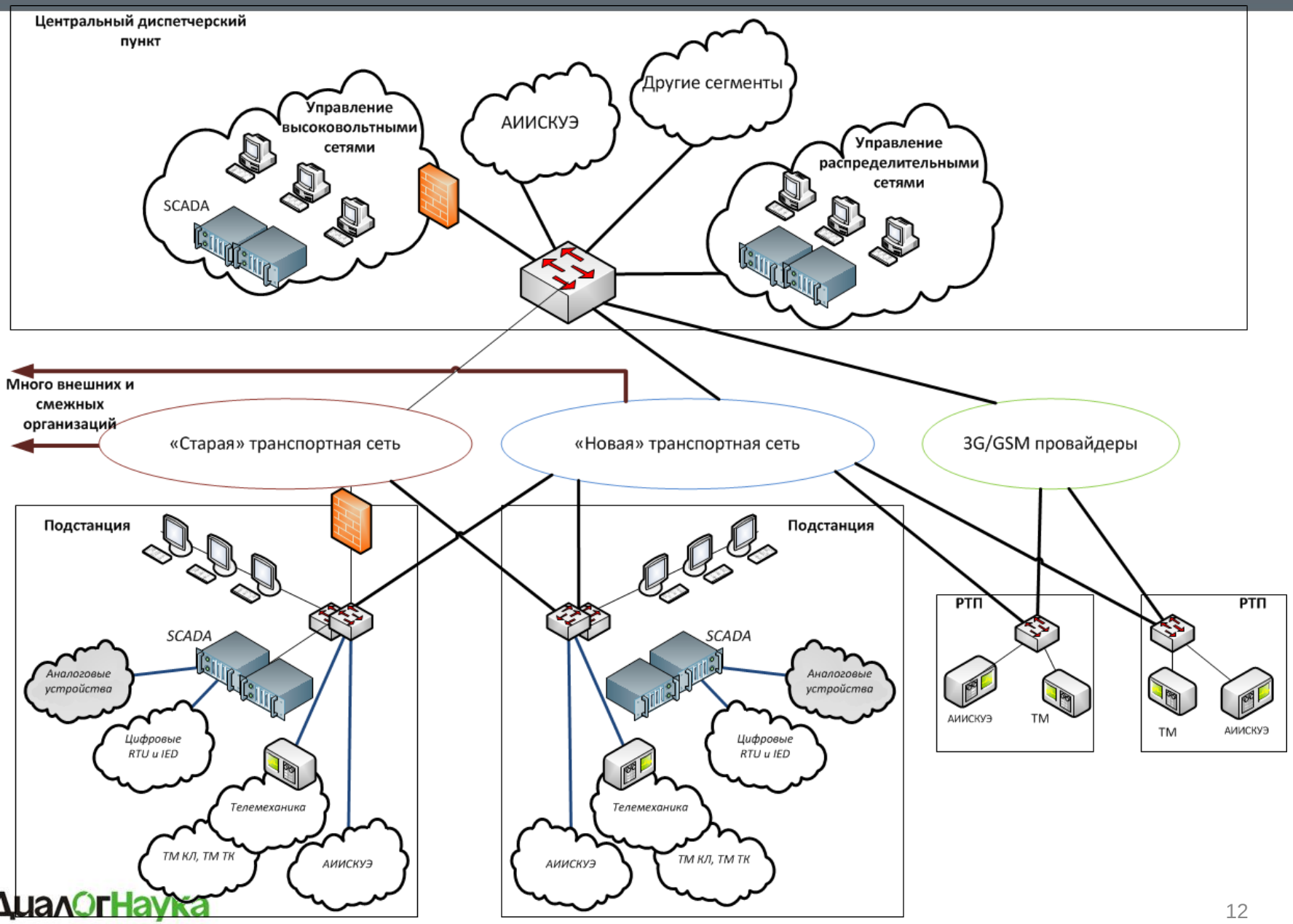

Фото: https://ics.kaspersky.ru/ru/conference-ru/

# …и перейдем к делу

# Методическая база

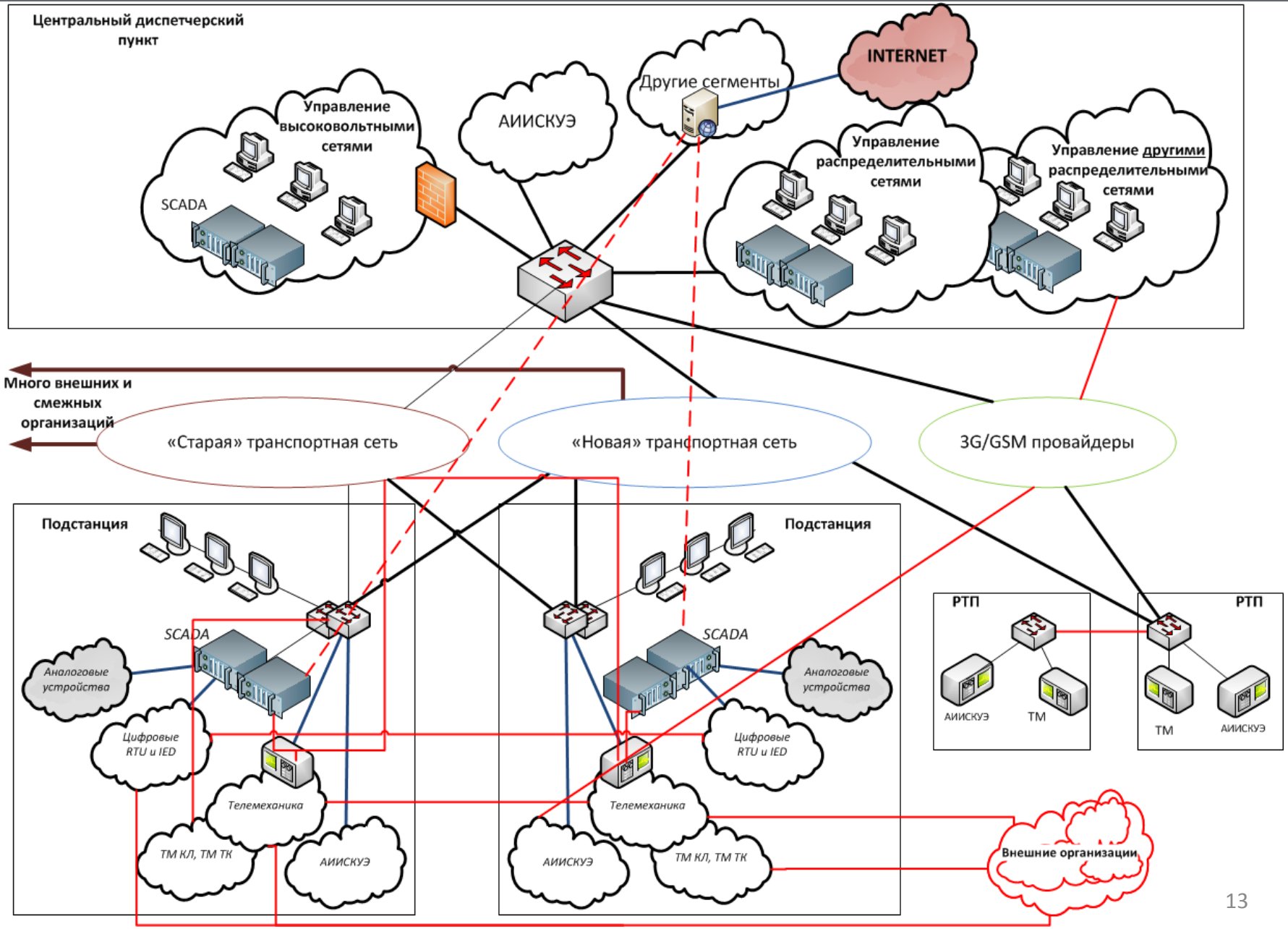


# Результаты документального аудита




ДиалОгНаука

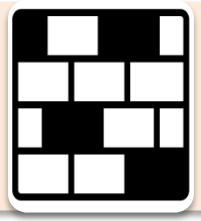
# Инструментальный аудит и «внезапные открытия»



# Примеры выявленных уязвимостей

Незащищенный удаленный доступ к SCADA-серверам через Интернет

Вредоносное программное обеспечение

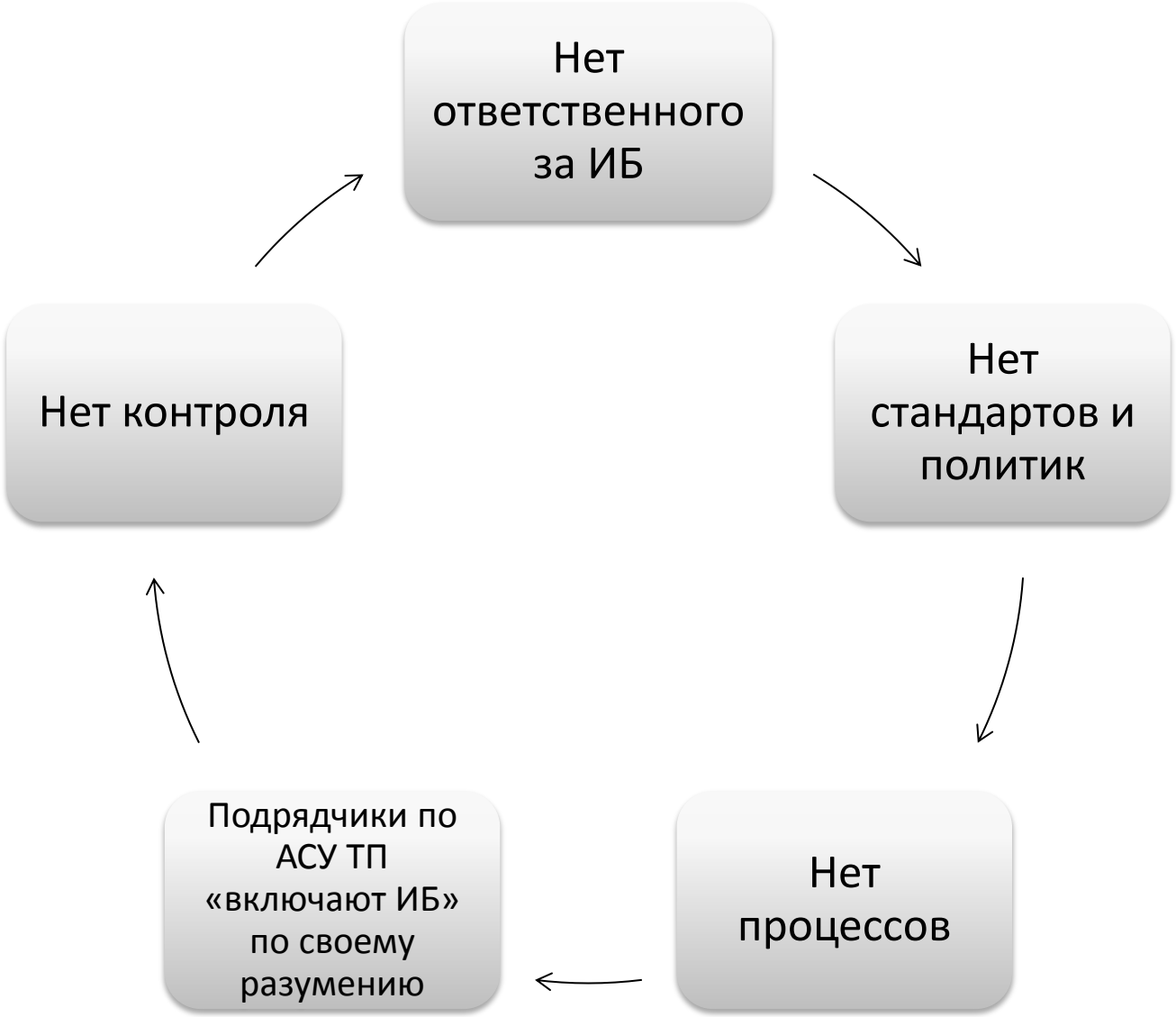


Отсутствие правил МЭ (permit any any), или отсутствие самих МЭ, имеющихся в документации

Неконтролируемые и слабо (не) документированные связи на нижнем уровне

Пароли, установленные подрядчиками при создании системы

# Ключевые поводы для беспокойства



# Ключевые поводы для беспокойства

## Сетевая архитектура

- Множество «горизонтальных» связей
- Незащищенные смежные и внешние подключения
- Недокументированное подключение к Интернет
- МЭ “permit any any” или вообще отсутствие МЭ

## Угрозы

- НСД
- Сетевые атаки
- Распространение вредоносного ПО
- Сетевые штормы
- Подключение нелегальных устройств

# Ключевые поводы для беспокойства

## Отсутствие защиты на уровне endpoint

- Отсутствие антивируса
- Старые версии ОС + нет обновлений
- Нет контроля портов в/в и съемных устройств
- Пароли

## Угрозы

- НСД
- Вредоносное ПО, в т.ч. «древнее»
- Bad USB и прочие целенаправленные атаки
- Возможность создания неконтролируемых подключений

# Ключевые поводы для беспокойства

## Удаленные РТП/ТП/СП

- de facto неконтролируемая зона
- Отсутствие контроля портов сетевого оборудования
- Слабая аутентификация
- Отсутствие контроля целостности и подлинности

## Угрозы

- НСД, в т.ч. ко всей сети
- Модификация ПО и проектов ПЛК

# Ключевые поводы для беспокойства

## Технологическое управление

- Слабая аутентификация
- Отсутствие контроля целостности и подлинности

## Угрозы

- НСД к управлению
- Модификация ПО и проектов ПЛК

# Ключевые задачи

Внедрение процессов ИБ

Защита сети

- Сегментирование и защита периметра
- Обнаружение/блокирование сетевых атак, червей и т.п.

Защита конечных устройств

- Защита от вредоносного ПО
- Аутентификация и контроль доступа (в т.ч. удаленных ПЛК)

Технологический трафик

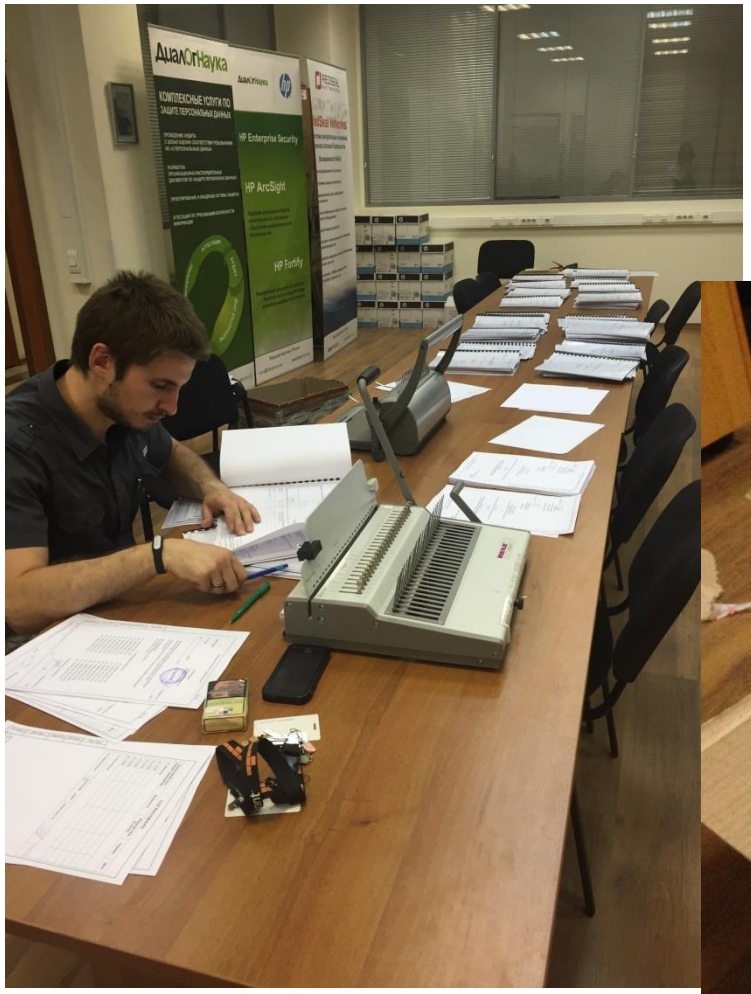
- Обеспечение целостности
- Обнаружение несанкционированных действий

Наблюдаемость

- Мониторинг событий ИБ
- Мониторинг

# Организационная поддержка

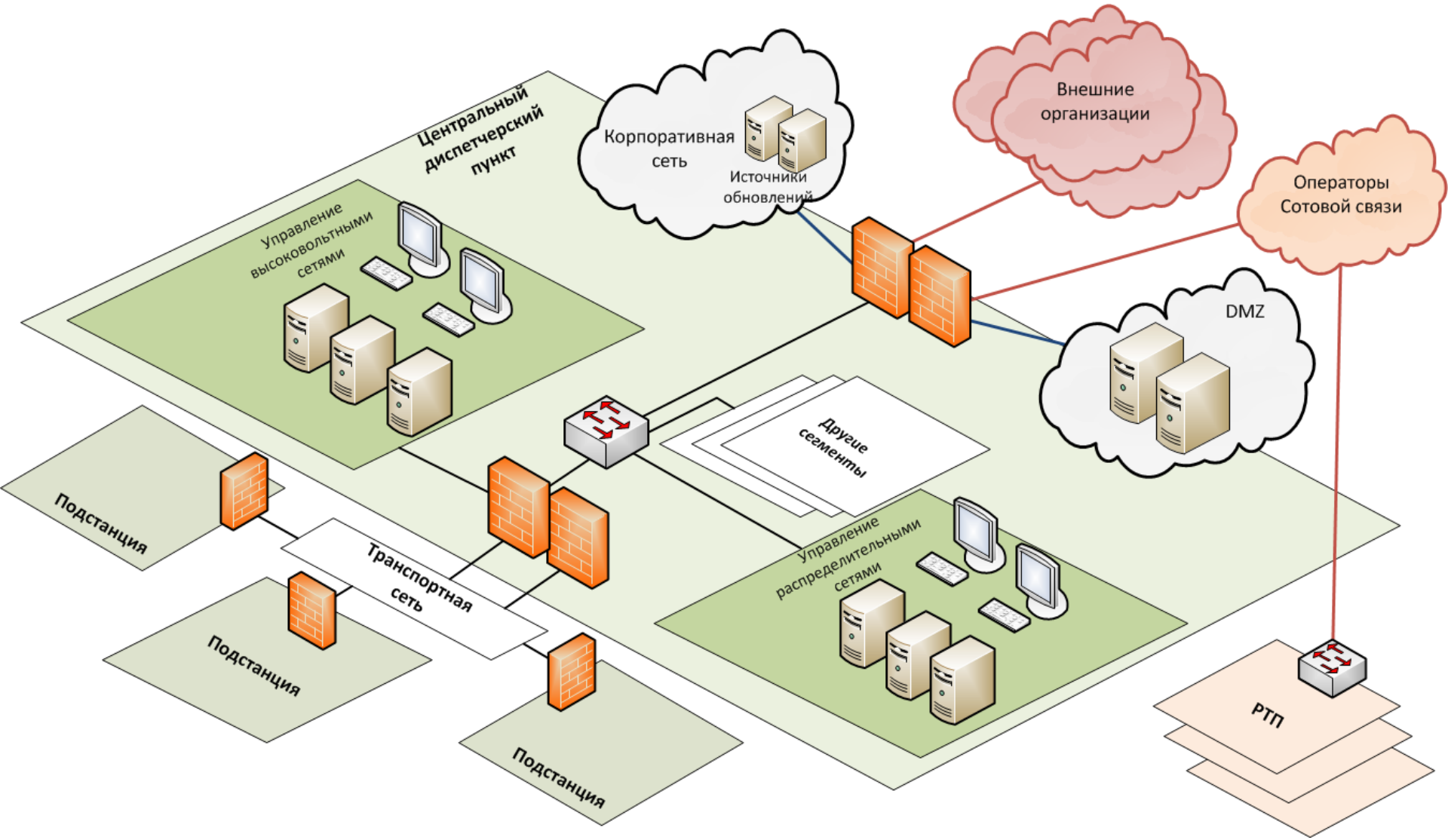
# Организационная поддержка




# Защита сети

- Требования к архитектуре
- Сегментация и периметр
- Мониторинг
- Плавный ввод политик и отсекаем «лишнее»
- Защита связи с удаленными узлами

# Защита сети


Центральный диспетчерский пункт
Управление высоковольтными сетями
Корпоративная сеть
Источники обновлений
Внешние организации
Операторы Сотовой связи
DMZ
Другие сегменты
Управление распределительными сетями
Подстанция
Транспортная сеть
Подстанция
Подстанция
РТП

# Технологический трафик

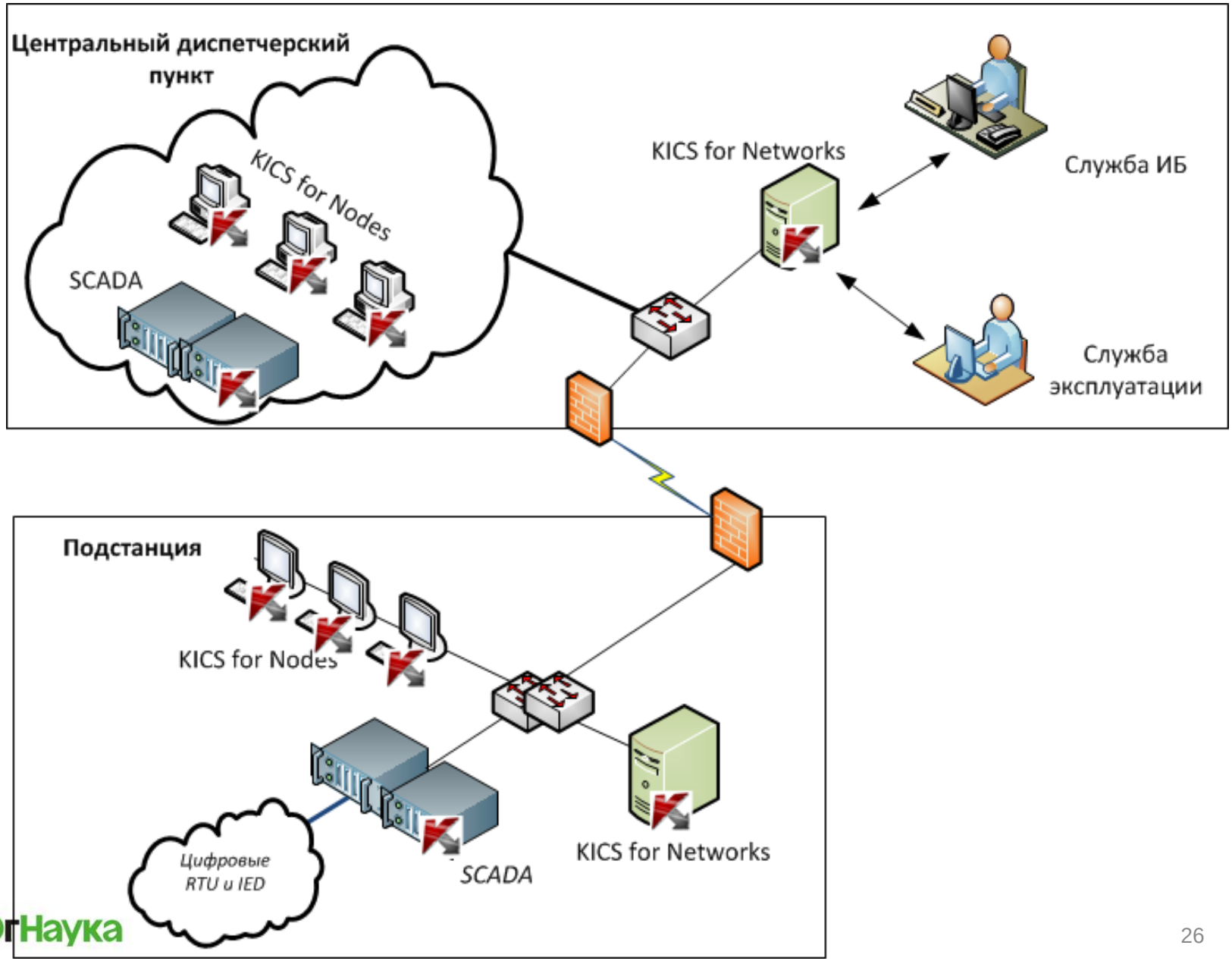
Не навреди!

Целостность

Подлинность

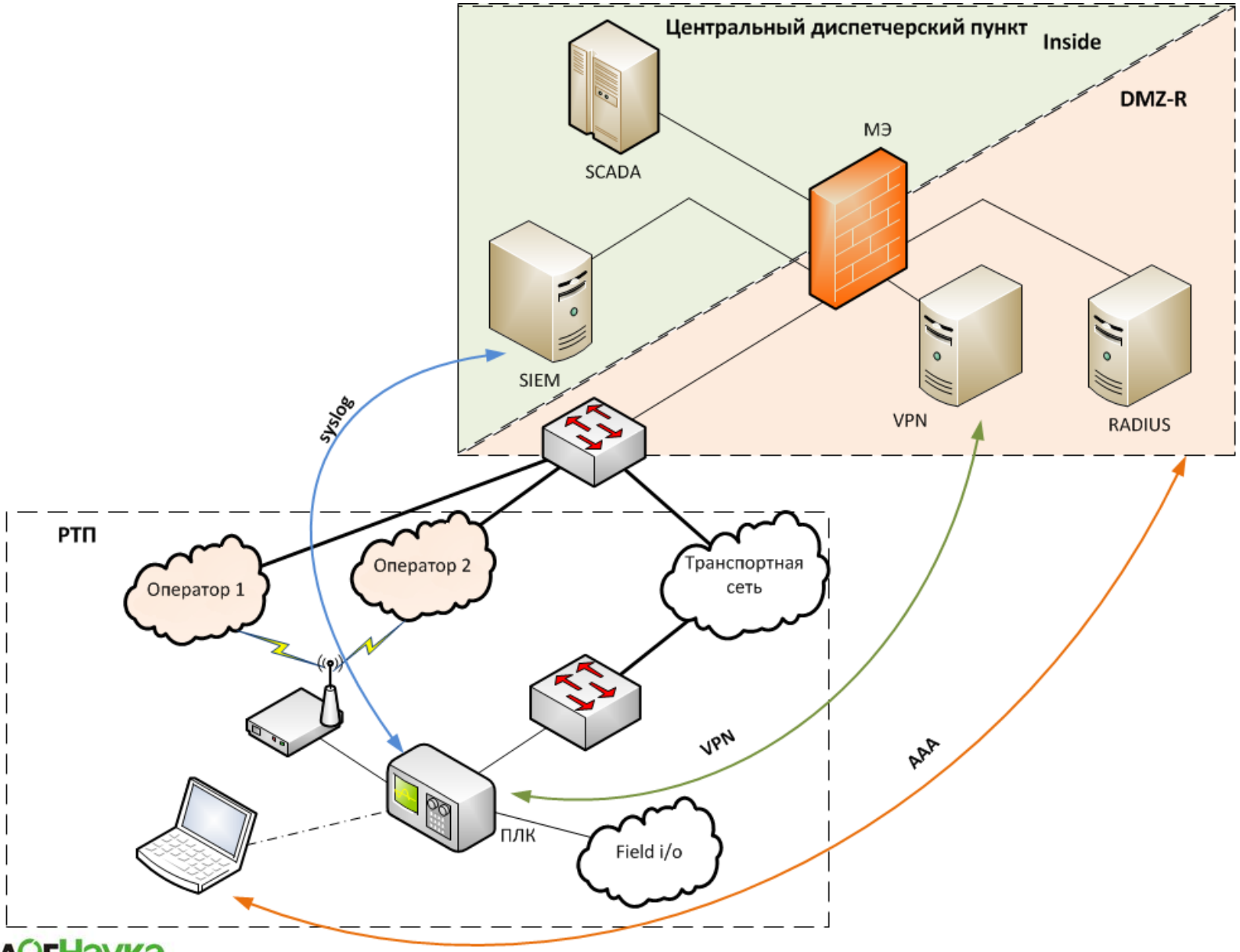
Едим слона по кусочкам

# ПС

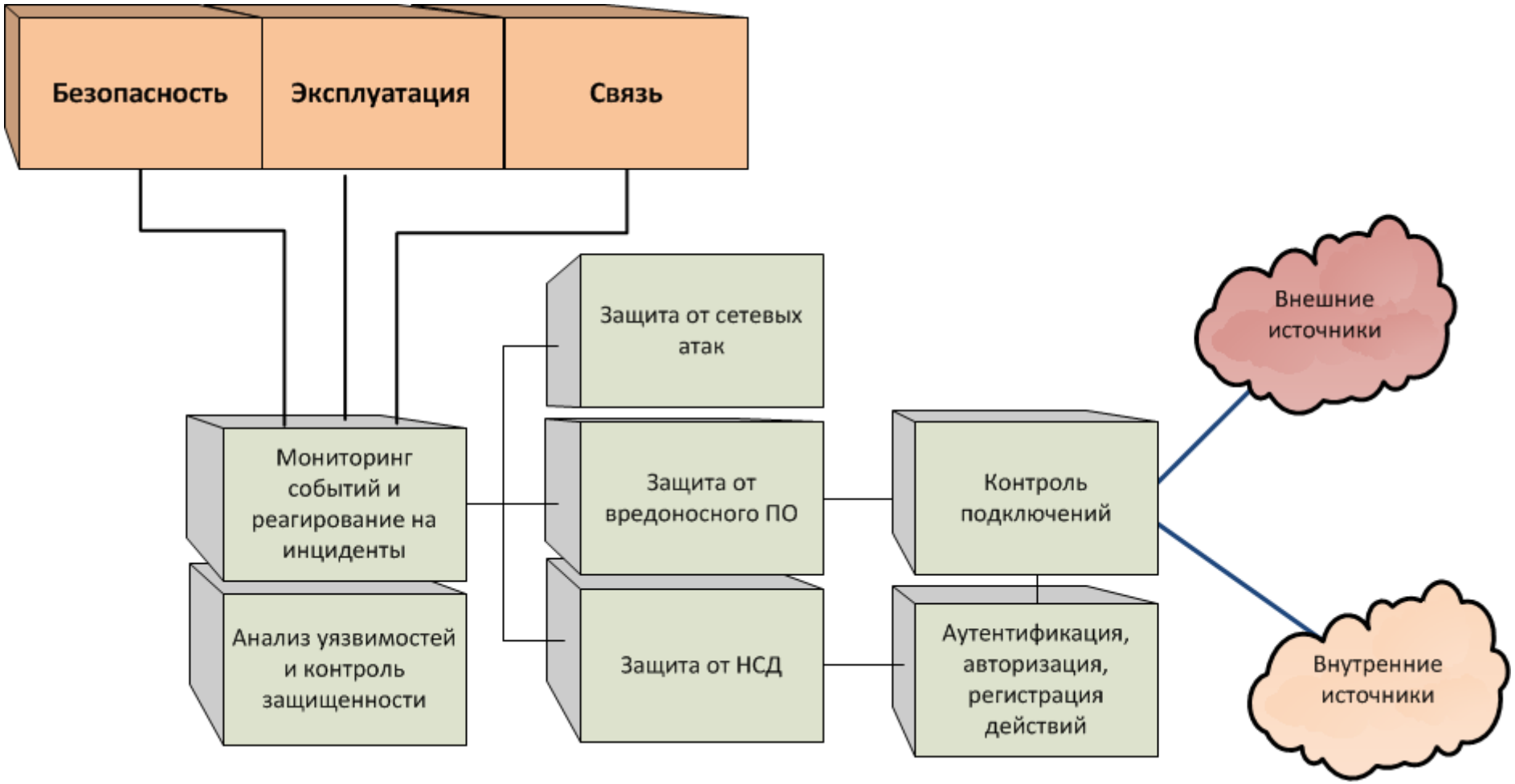



ДиалОгНаука

# РТП


Центральный диспетчерский пункт
Inside
DMZ-R
МЭ
SCADA
SIEM
VPN
RADIUS
syslog
РТП
Оператор 1
Оператор 2
Транспортная сеть
VPN
AAA
ПЛК
Field i/o

# Мониторинг и управление



# Минимизация рисков

Использование лучших решений и мировых практик

Отказоустойчивая архитектура

Резервирование ключевых компонент

Резервные схемы работы

Плавное внедрение политик ИБ в ходе опытной эксплуатации

# Основные сложности

Отсутствие ответственных за ИБ

«Исторически сложившаяся» сетевая архитектура и инфраструктура

Отсутствие типовых решений по автоматизации и телемеханизации

Быстрые изменения в АСТУ без общего контроля и надзора в части ИБ

# Направления развития

# Спасибо за внимание!