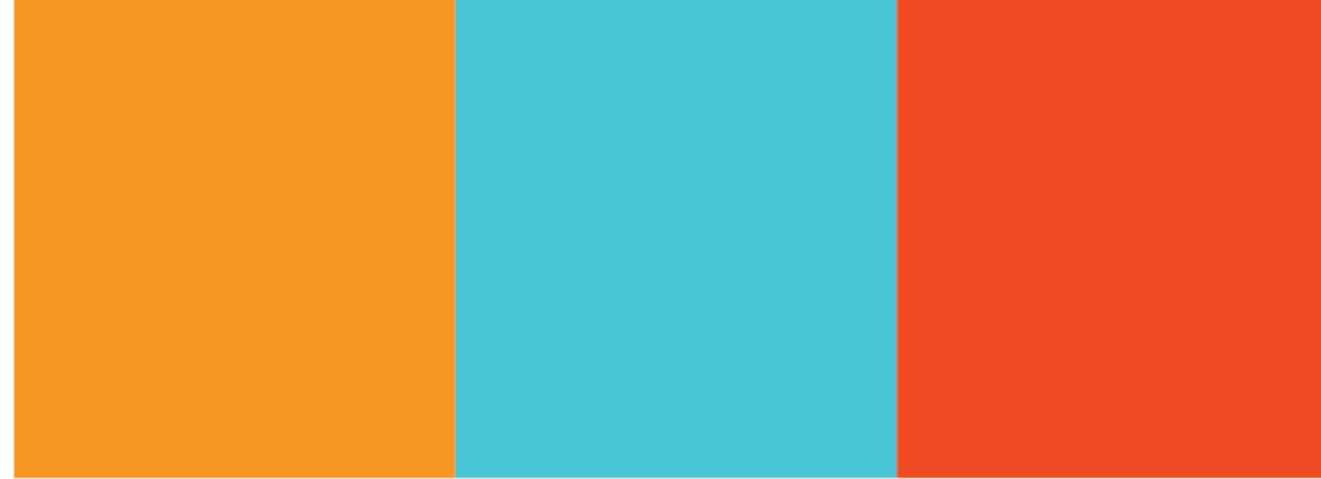




initi

from diversity to uniformity



ИНИТИ СОЛО – универсальная система операционной поддержки пользователей.

Учамприн Андрей

ООО “ИНИТИ” Директор по развитию бизнеса

+7 (977) 600 5000

a.uchamprin@initi.ru

<http://www.initi.ru>

ЗАДАЧИ

Обеспечение высокой готовности всей ИКТ инфраструктуры

- мониторинг состояния всего ИКТ оборудования в режиме реального времени
- автоматизация поиска первопричины аварий с целью сокращение времени устранения неисправностей
- расстановка приоритетов при устранении аварий
- прогнозирование мест возможных отказов

Обеспечение эффективной работы ИКТ инфраструктуры

- технологический учет всей инфраструктуры
- выявление неиспользуемых ресурсов
- обоснованное планирование развития и закупок
- отслеживание актуальных конфигураций сетевого оборудования
- определение технического состава используемых сервисов

Обеспечение поддержки принятия решений и прозрачности на всех уровнях управления

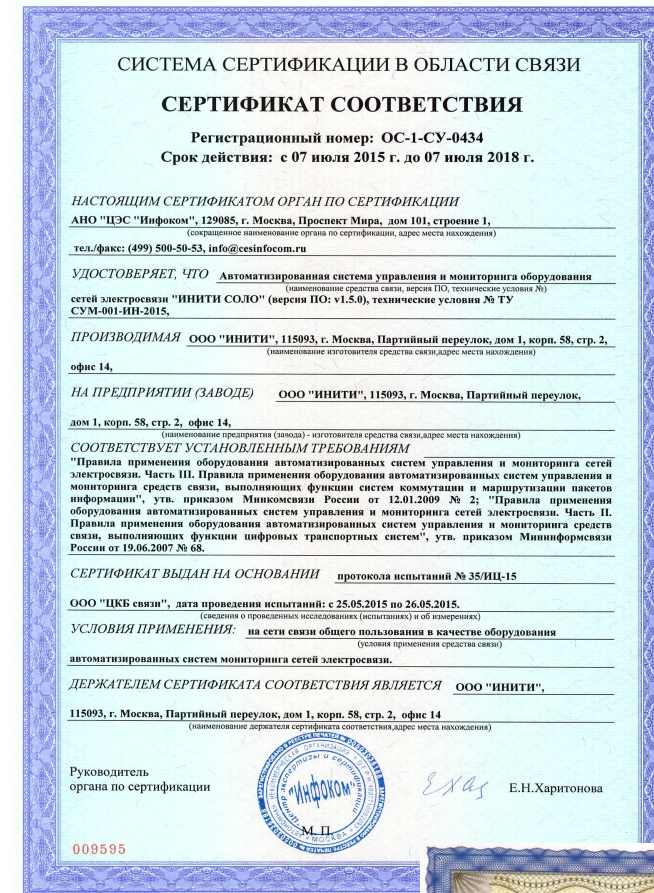
- создание единого центра мониторинга, управления и диспетчеризации для контроля всех технологический доменов ИКТ инфраструктуры
- повышение эффективности работы инженеров за счет унификации рабочих мест
- построение вертикали управления на основе введенных регламентов и прав доступа
- ведение единой базы данных для формирования операционной и управленческой отчетности

Почему необходима единая система? Типичные проблемы.

- Отсутствует охват всех технологических доменов – нет целостного контроля, невозможность контроля SLA ИКТ сервисов;
- Отсутствует единая база технического учета – невозможность определить критичность сбоя и его влияние на оказываемые ИКТ сервисы;
- Отсутствуют автоматические механизмы поиска первопричины – высокий процент пропуска уведомлений, большое время восстановления сбоев, невозможность автоматизации процессов обслуживания;
- Отсутствуют механизмы прогнозирования сбоев – потери на простои, которых можно было избежать;
- Отсутствуют механизмы управления мощностями – неэффективная утилизация оборудования, избыточные потери на ЗИП (не то и не там);
- Невозможность подключения не ИТ и устаревшего оборудования – отсутствие полноценного контроля над ситуацией;
- Сложная и ресурсоемкая архитектура – невозможность масштабирования текущего решения.

Почему “ИНИТИ СОЛО” – о компании

- 100% Российская компания
- Год основания 2007
- Число сотрудников 50+
- Решение включено в Реестр Российского ПО
- Решение включено в реестр ПАО “Ростелеком”
- Локальная разработка, служба технической поддержки
- Не используется третьестороннего коммерческого ПО
- Подтверждённая база заказчиков в РФ и за рубежом
- Наличие локальной партнёрской базы
- Решение используется рядом ведущих иностранных производителей



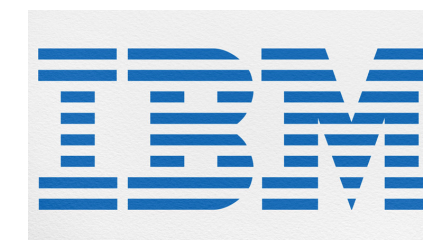
Почему “ИНИТИ СОЛО” – особенности решения

- Независимое ядро системы (зарегистрировано отдельно)
- Работа в высоконагруженных системах с большим количеством событий
- Использование технологий параллельных вычислений и EEDA
- Работа на x86 архитектуре и открытых ОС (Linux)
- Поддержка работы на защищённых ОС (Astra Linux)
- Русифицированный полнофункциональный web интерфейс
- Наличие русскоязычной пользовательской документации
- Возможность разработки сторонних модулей
- Интеграция с внешними системами и оборудованием

Почему "ИНИТИ СОЛО" – некоторые Заказчики и Партнёры



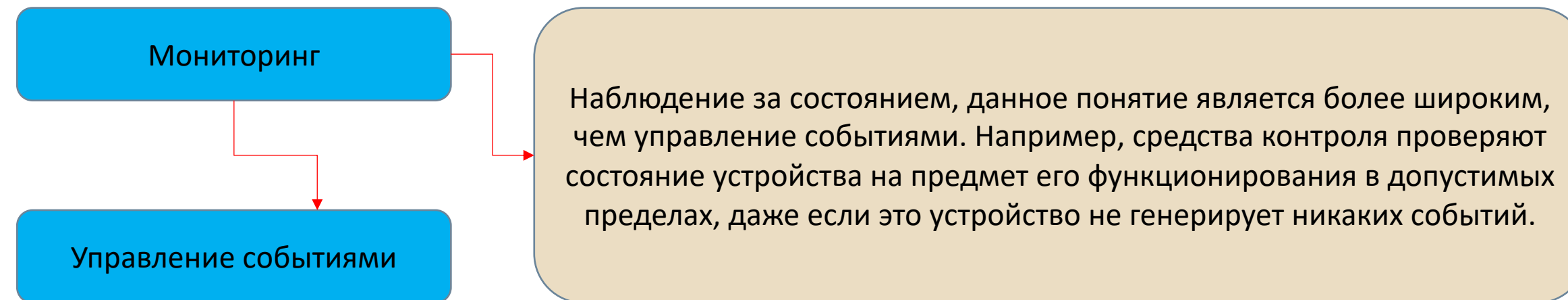
Федеральное
казначейство



РОСАТОМ

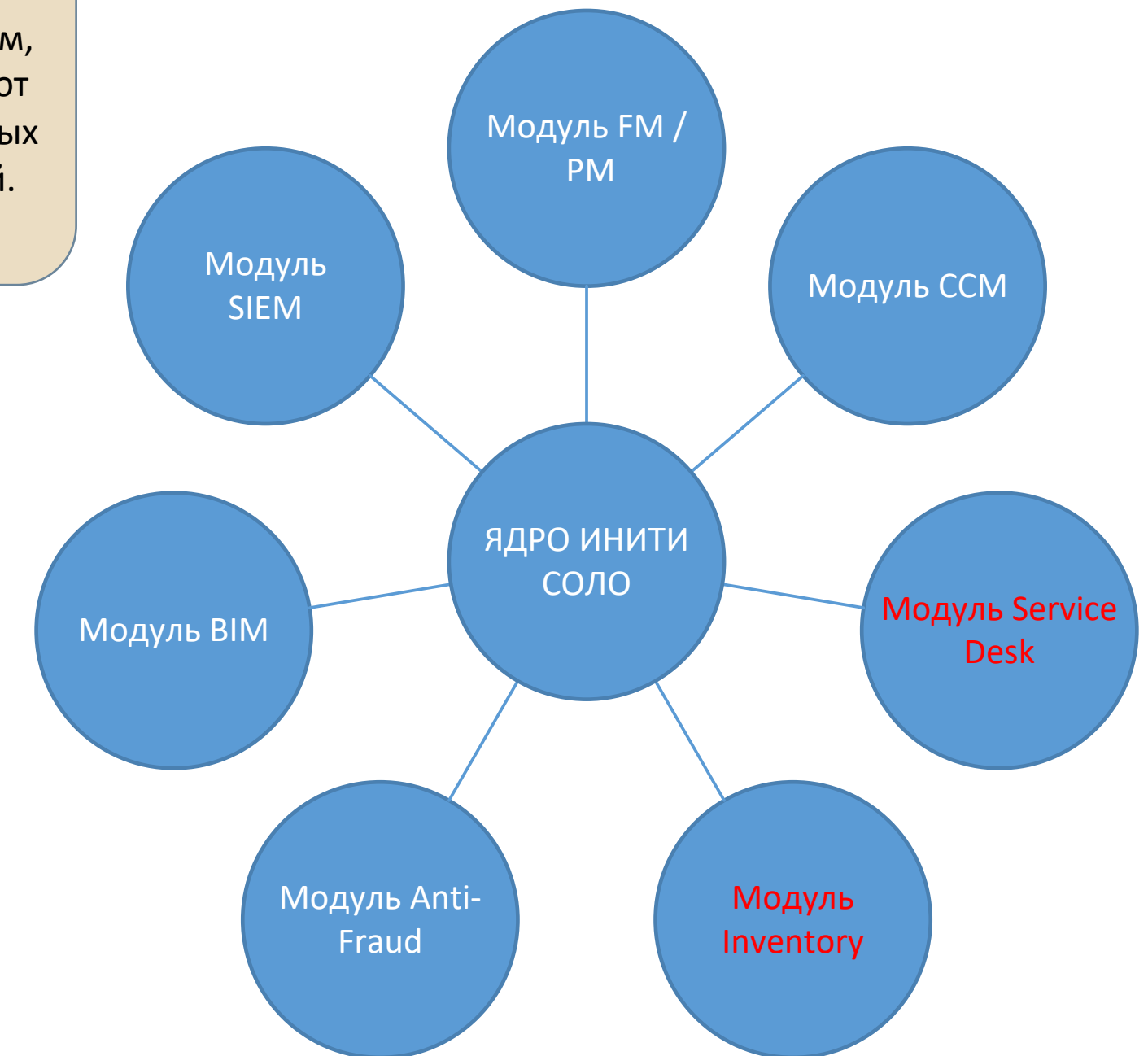


Какие процессы автоматизируем



- Раннее обнаружение инцидентов
- Повышение рациональности мониторинга автоматизированных процедур
- Раннее оповещение о необходимости обновления процедур или ресурсов
- Основа для автоматизации процедур эксплуатации

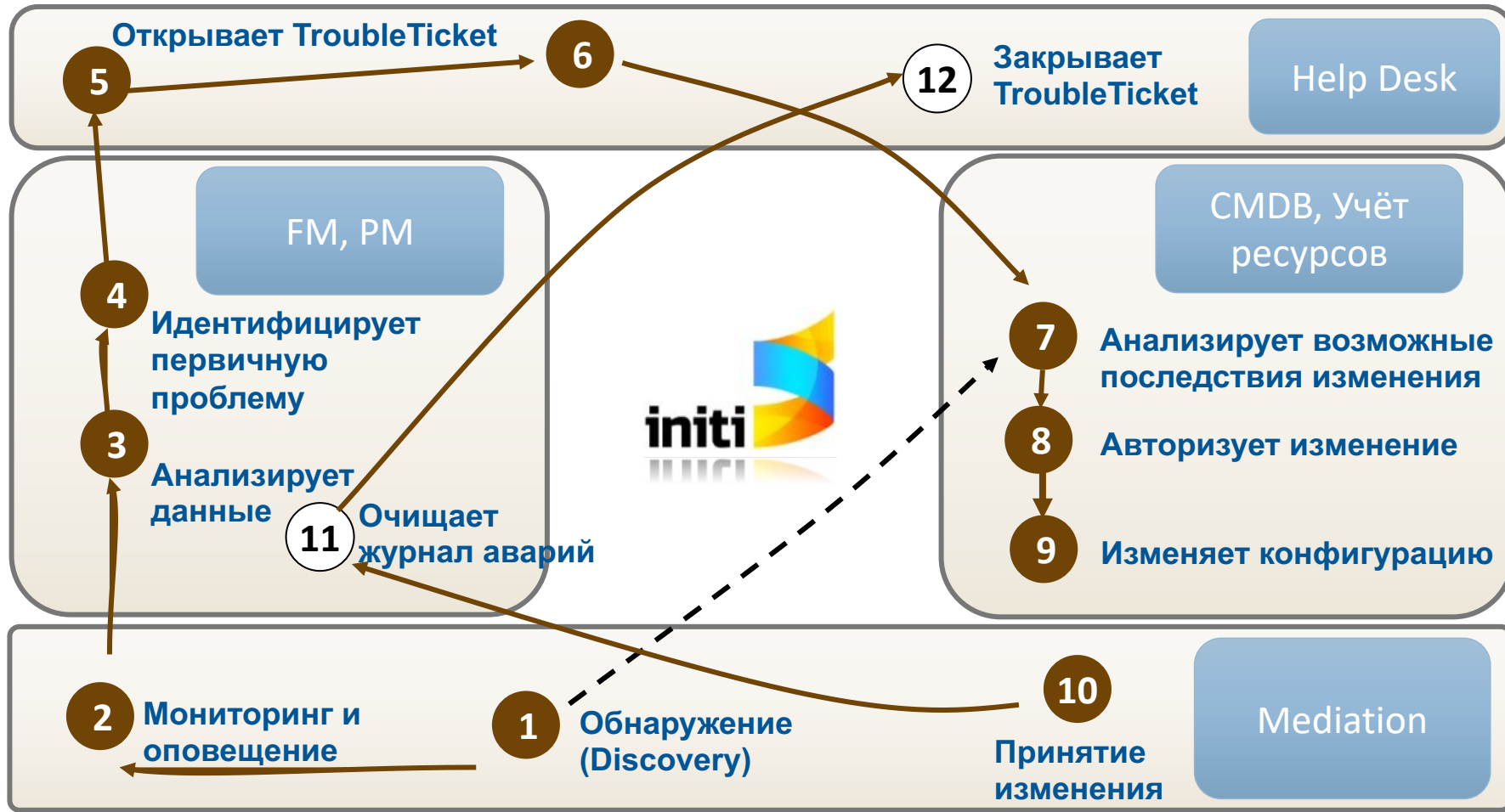
- Независимое ядро системы (зарегистрировано отдельно)
- Модуль мониторинга / сбора и анализа производительности
- Модуль контроля конфигураций оборудования
- Модуль оценки негативного влияния сбоя на бизнес-процессы
- Модуль Anti-Fraud
- Модуль SIEM



В разработке:

- Модуль Service-Desk (на данный момент используется ядро Naumen Service Desk)
- Модуль Inventory (на данный момент используется ядро Naumen Inventory)

Цель – замкнутый цикл автоматизации

[illegible]

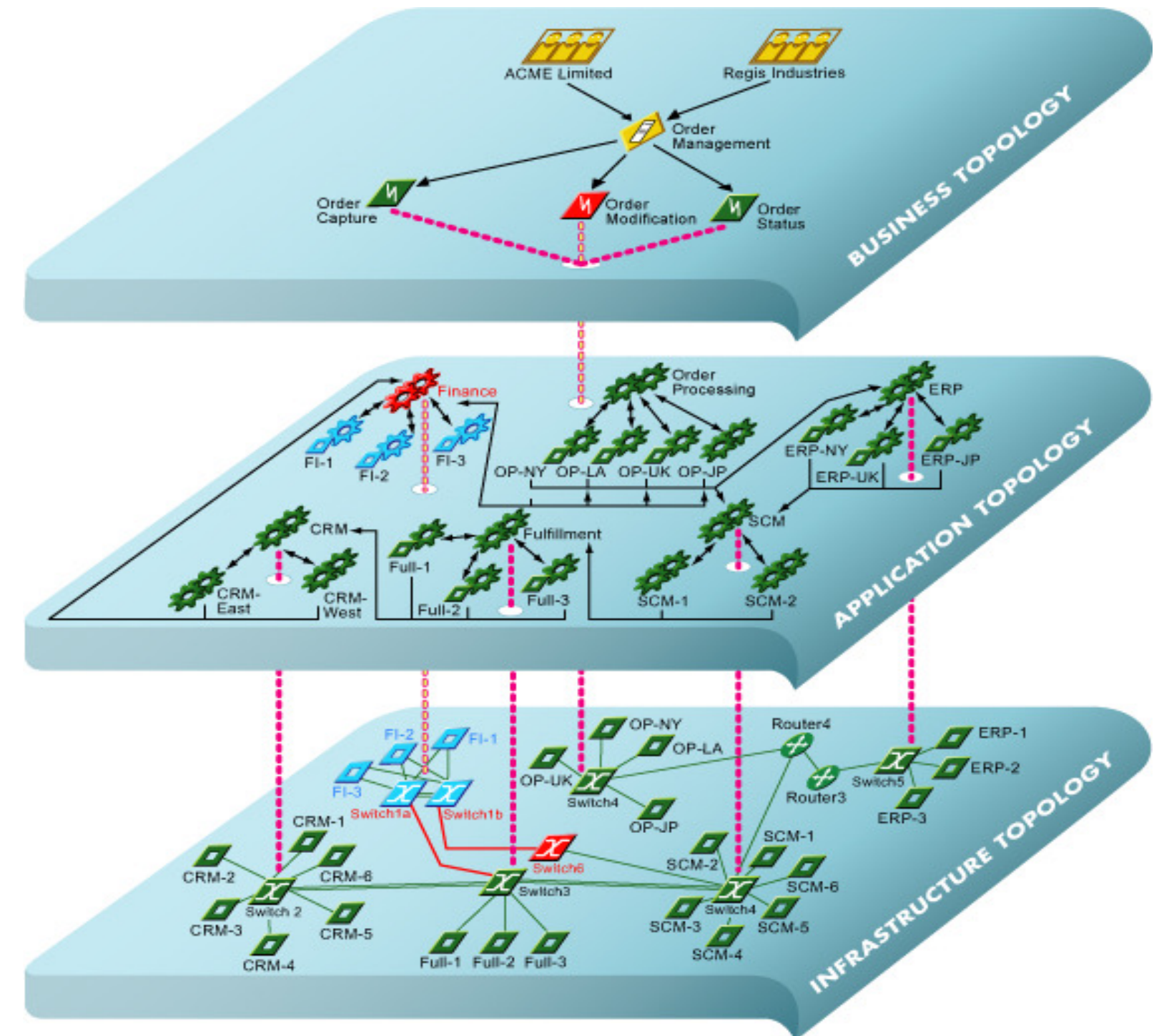
Сквозной мониторинг недоступности сервиса

От аварии к затронутому сервису:

- Сквозная корреляция аварий на сетевой и логической топологии с сервисом включая все уровни ИТ-инфраструктуры
- Автоматическое определение первопричины недоступности сервиса на всех уровнях, с проецированием ключевой аварии на сервис
- Автоматическое раскрытие и мониторинг приложений
- Автоматическое раскрытие и мониторинг физической и логической топологии ИТ-инфраструктуры.

Механизмы корреляции:

- На базе раскрытой топологии и модели сервисов
- Встроенные в модель механизмы корреляции
- Настраиваемые правила корреляции на базе правил



От проблемы в инфраструктуре к сервису

Использование ресурсно-сервисной модели для достижения максимальной отказоустойчивости ИТ-сервисов компании:

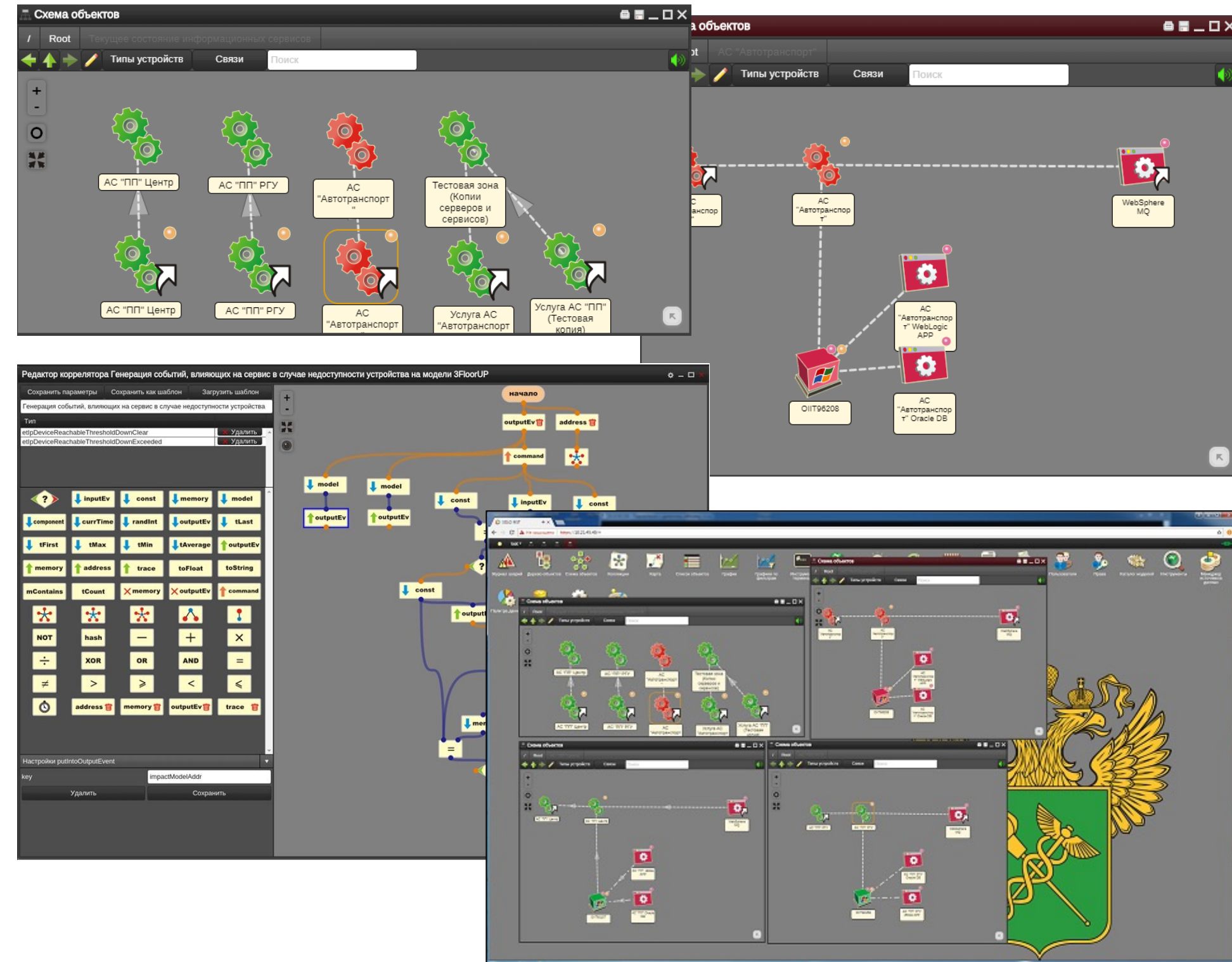
- Сокращение времени на выявление затронутых аварией сервисов
- Оперативное уведомление ответственных за эксплуатацию аварийных объектов лиц, при аварии на сервисе или при приближении к пороговым значениям прогноза аварийных ситуаций

Удобный интерфейс конфигурации сервисов:

- Минимальные трудозатраты на реализацию сервисно-ресурсной модели внутри системы
- Конфигурация сервисов и правил корреляции через единый графический интерфейс пользователя
- Настройка прогнозов недоступности сервиса с оповещением операторов о возможных проблемах на сервисе

Сквозной анализ влияния на сервис:

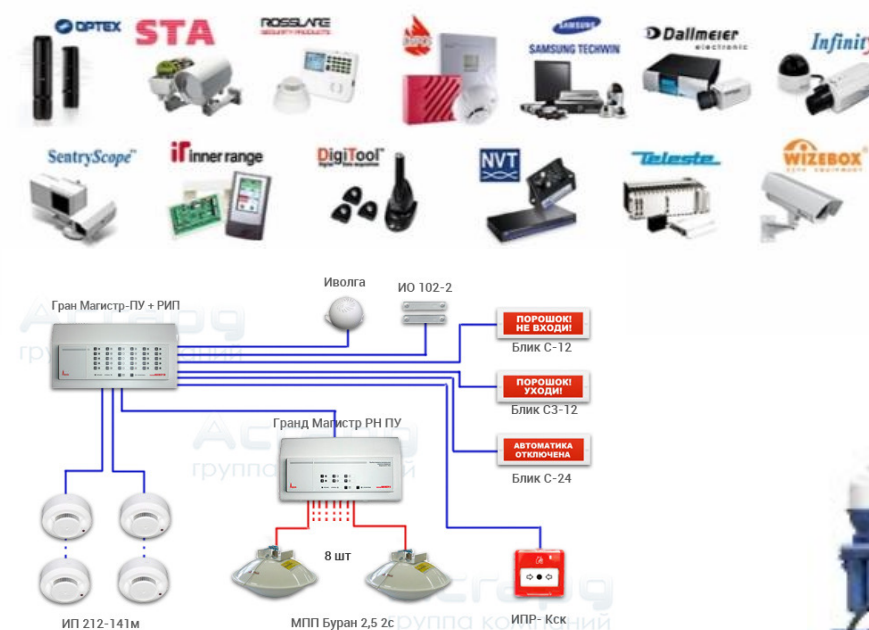
- Возможность перехода с аварии на сервисе к первопричине отсутствия услуги.
- Возможность отслеживать всю цепочку влияния на сервис



Первоочередные эффекты от внедрения

Сбор разнородных событий в едином решении:

- Сообщения оборудования IP сетей, транспортных сетей, сетей передачи данных, оборудования сетей спутниковой связи
- Сообщения тех. процессов: Контроллеры, АСУТП, SCADA
- Сообщения оборудования электрообеспечения, кондиционирования, датчиков
- Сообщения БД, приложений, систем хранения данных
- Сообщения подсистем информационной безопасности – межсетевые экраны, антивирусы, DLP и пр..



Консолидация данных:

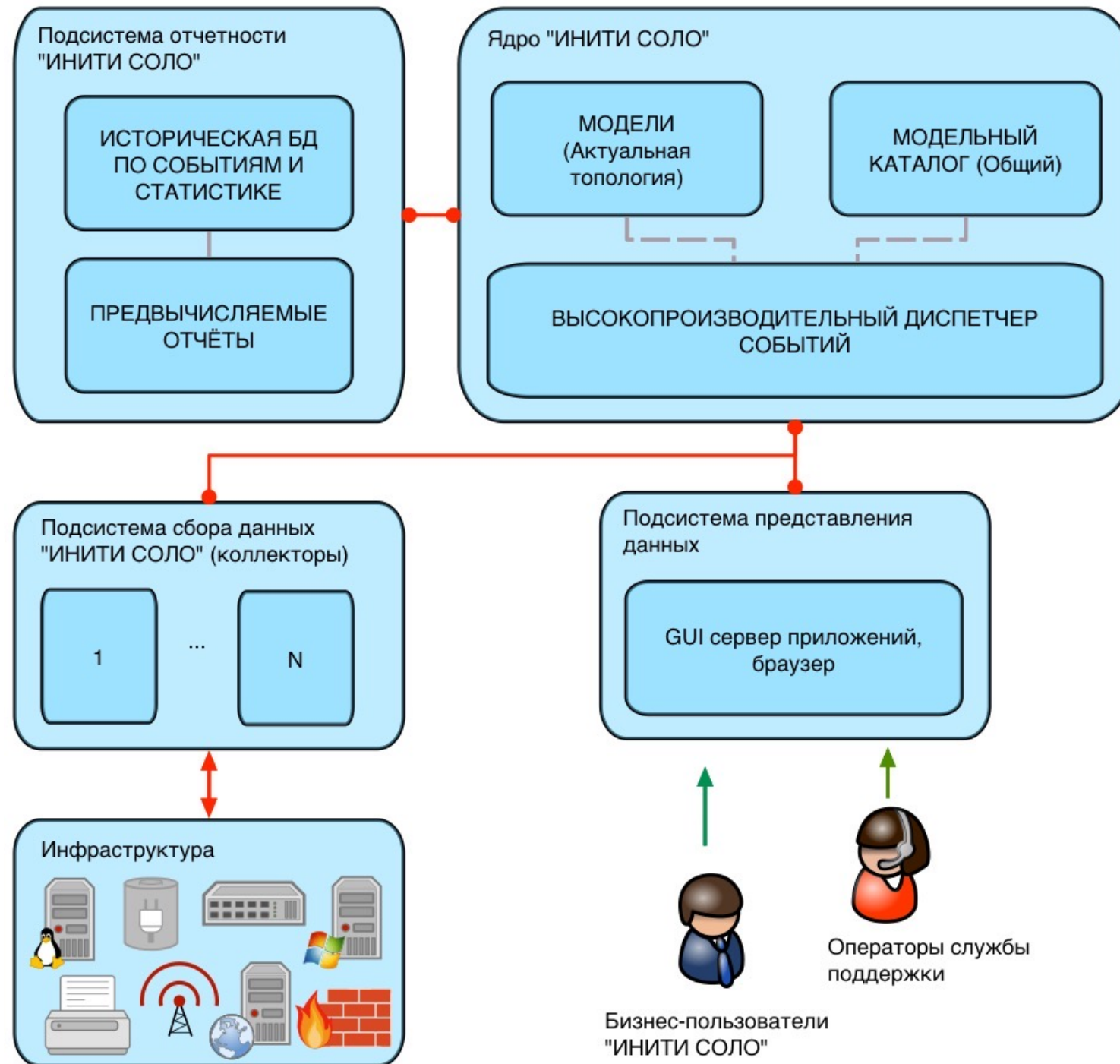
- Информация из разных систем управления?
- Представление в едином интерфейсе системы управления неисправностями и контроля производительности оборудования?
- Предоставление единого интерфейса с геоинформационной системой?
- Универсальный инструмент для дежурной смены службы эксплуатации и руководства
- Исключение возможности манипулирования или искажения информации?



Техническая информация



Структура "ИНИТИ СОЛО"

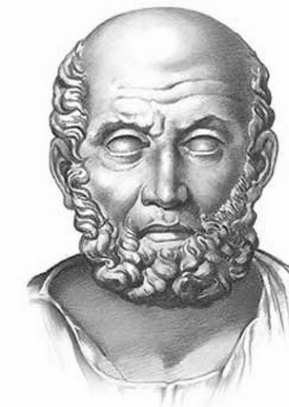
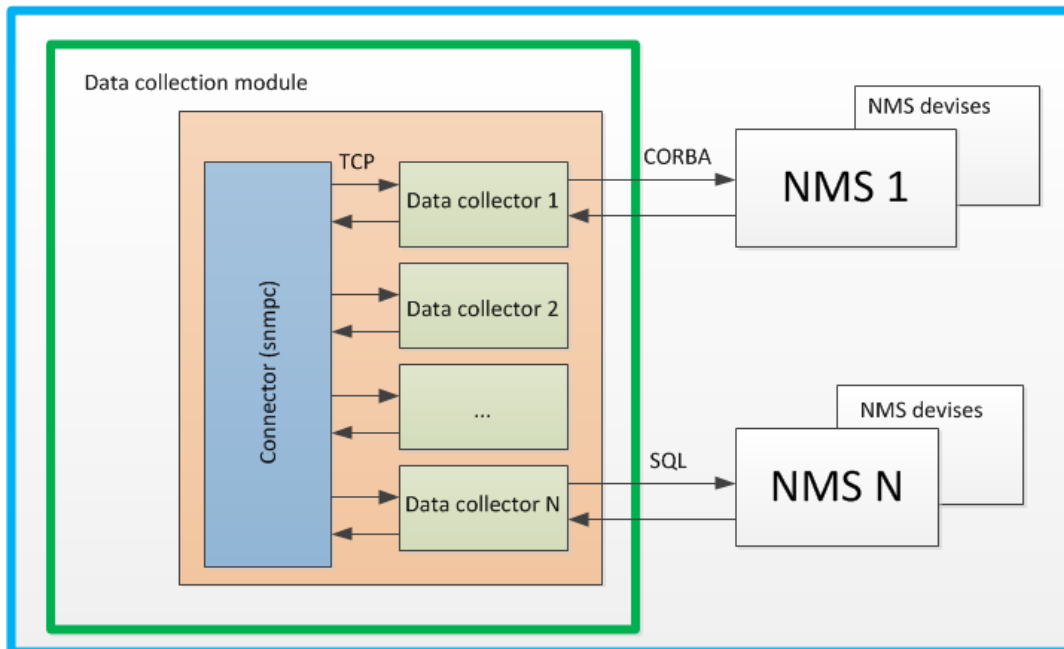


- Уровень сбора данных (Коллекторы)
- Уровень нормализации данных (Диспетчер событий)
- Ядро системы (Core):
 - Модельный каталог
 - Модель инфраструктуры
 - Обработка событий
- Уровень представления (GUI)
- Высокая производительность ядра (10000+ EPS)
- Реализация отказоустойчивой и распределённой "облачной" структуры
- Возможность реализации иерархической сложноподчинённой инсталляции
- Многопользовательский портал с гибкими возможностями назначения зон видимости
- Любая x86 архитектура, поддержка работы в виртуальных средах
- Высокопроизводительная БД для работы с большим количеством устройств (более 150 000 на одно ядро)
- Открытые задокументированные API для интеграции с внешними системами
- Полностью WEB – based интерфейс (не требуется установка специализированного ПО), в том числе и на мобильных устройствах

Уровень сбора данных – любой цифровой протокол

Единая платформа для сбора и нормализации данных с большого количества разнородных источников

- Используется универсальный механизм автообнаружения устройств: SNMP v1,2,3, CLI, интеграция с системами управления, сбор первичной информации от систем инвентаризации и пр..
- Ограничение путём использования гибкой системы фильтров (единичный объект, подсети, типы устройств, OID, класс устройств, именование и пр..)
- Поддерживается многопоточность процесса
- Поддерживается объединение данных от различных источников в одной модели
- Поддерживается пост-процессинг



ГИППОКРАТ
460-370 до н. э.

«НЕ НАВРЕДИ!»

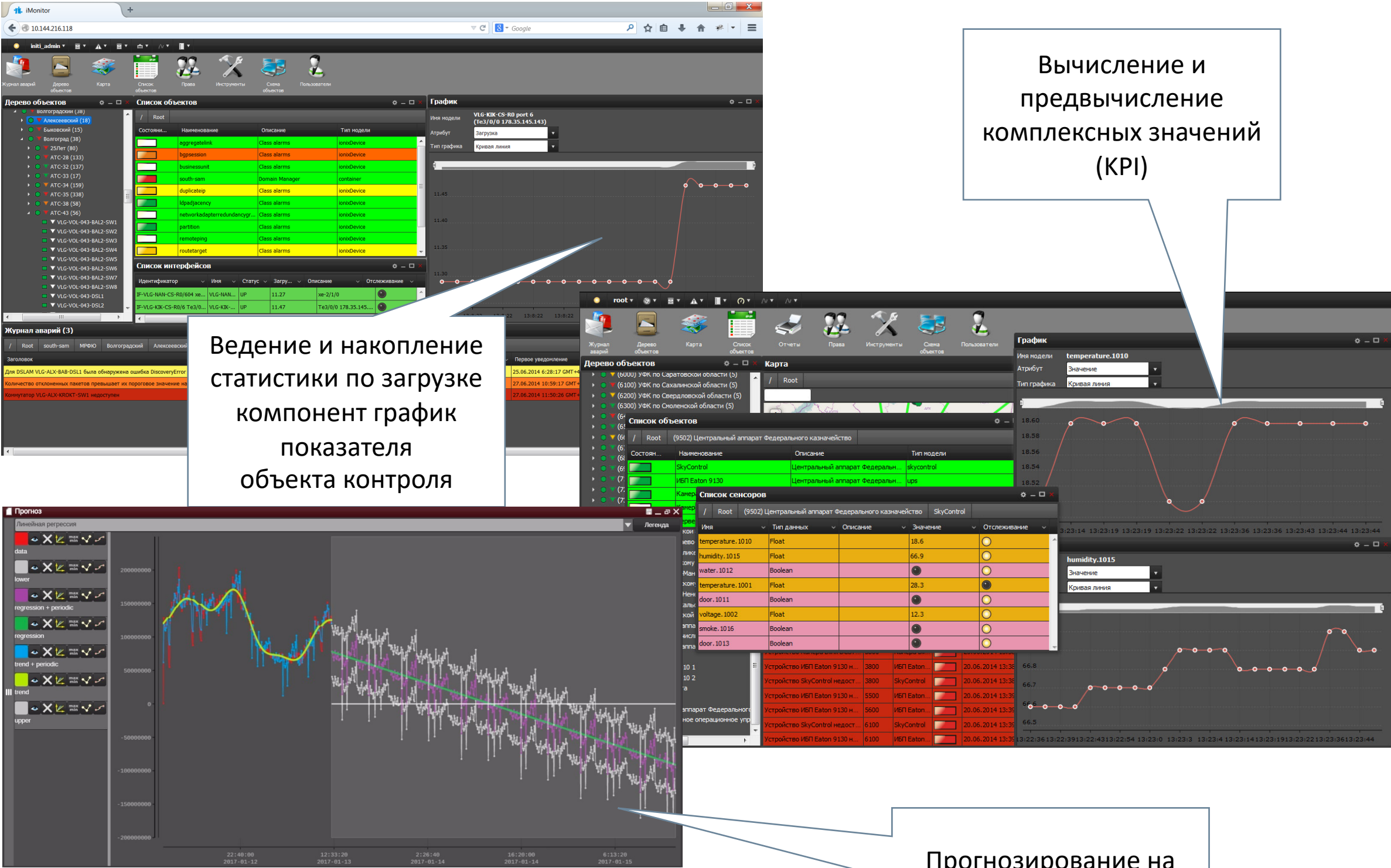
- Access Control, Authentication, DLP, IDS/IPS системы
- IP/MPLS сети, транспортные сети, радио-, ATM и пр..
- SAN сети и их компоненты (СХД, FC-коммутаторы, сервера)
- Приложения, СУБД и пр..
- Журналы событий серверов и рабочих станций
- Межсетевые экраны
- Периферийное оборудование (принтеры, сканеры и пр..)
- Сканеры уязвимостей
- Системы инвентаризации и asset-management
- Системы web фильтрации
- Технологическое оборудование и системы управления
- Прочее любое оборудование, доступное по цифровым протоколам

Мониторинг и сбор данных

Система работает в двух режимах:

- Активный опрос
- Сбор и анализ “сырых” событий

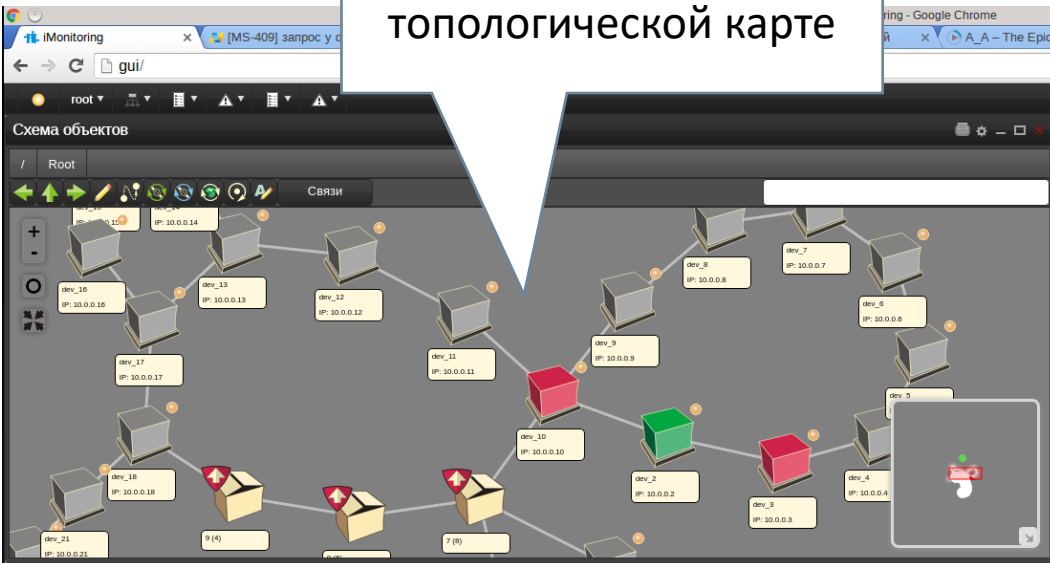
НЕКОТОРЫЕ ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ	
CORBA	SNMP
DB Link	TELNET
FTP	TMF
HTTP-HTTPS	Vendor API (Java, Perl, ...)
LOG	WebServices
OPC	WMI
SMB	XML
Modbus	Netbus
*Flow	TS 32.432
TS 32.435	И многое другое...



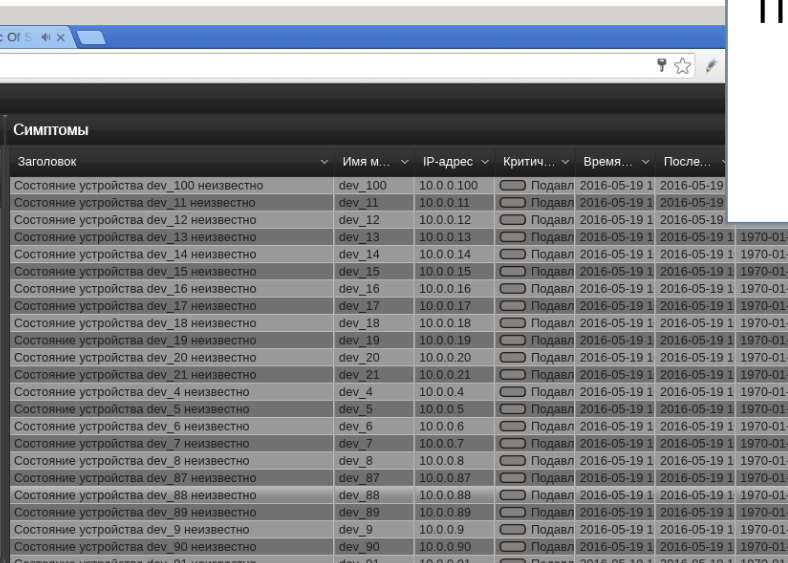
Интеллектуальный поиск первопричины сбоя (RCA)

- Автоматическая корреляция (на основе встроенных математических методов)
- Возможность создания **собственных правил** корреляции.

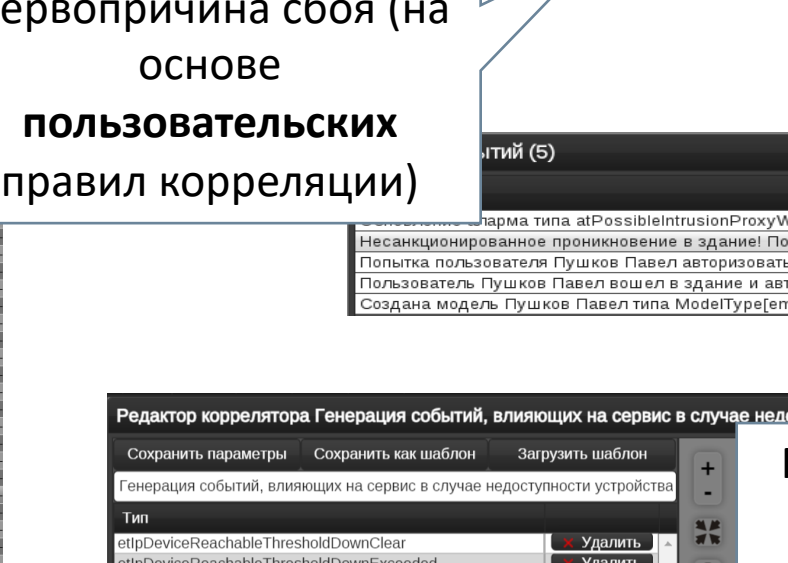
Первопричина сбоя на топологической карте



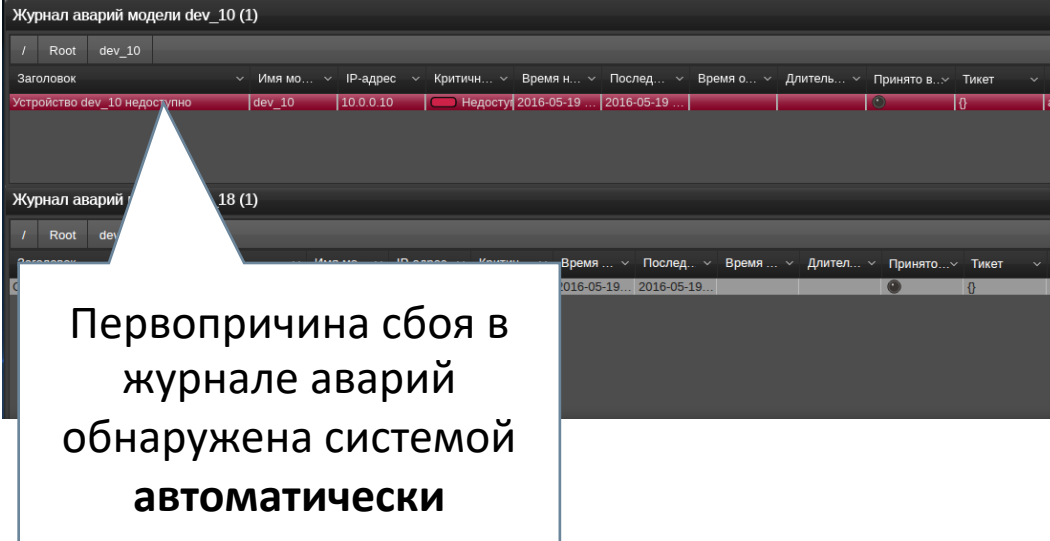
Первопричина сбоя (на основе пользовательских правил корреляции)



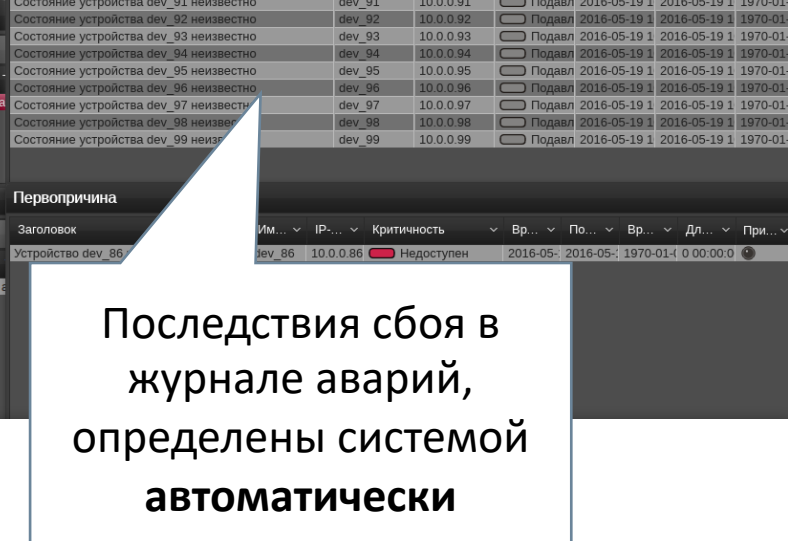
События, породившие сбой (на основе правил корреляции)



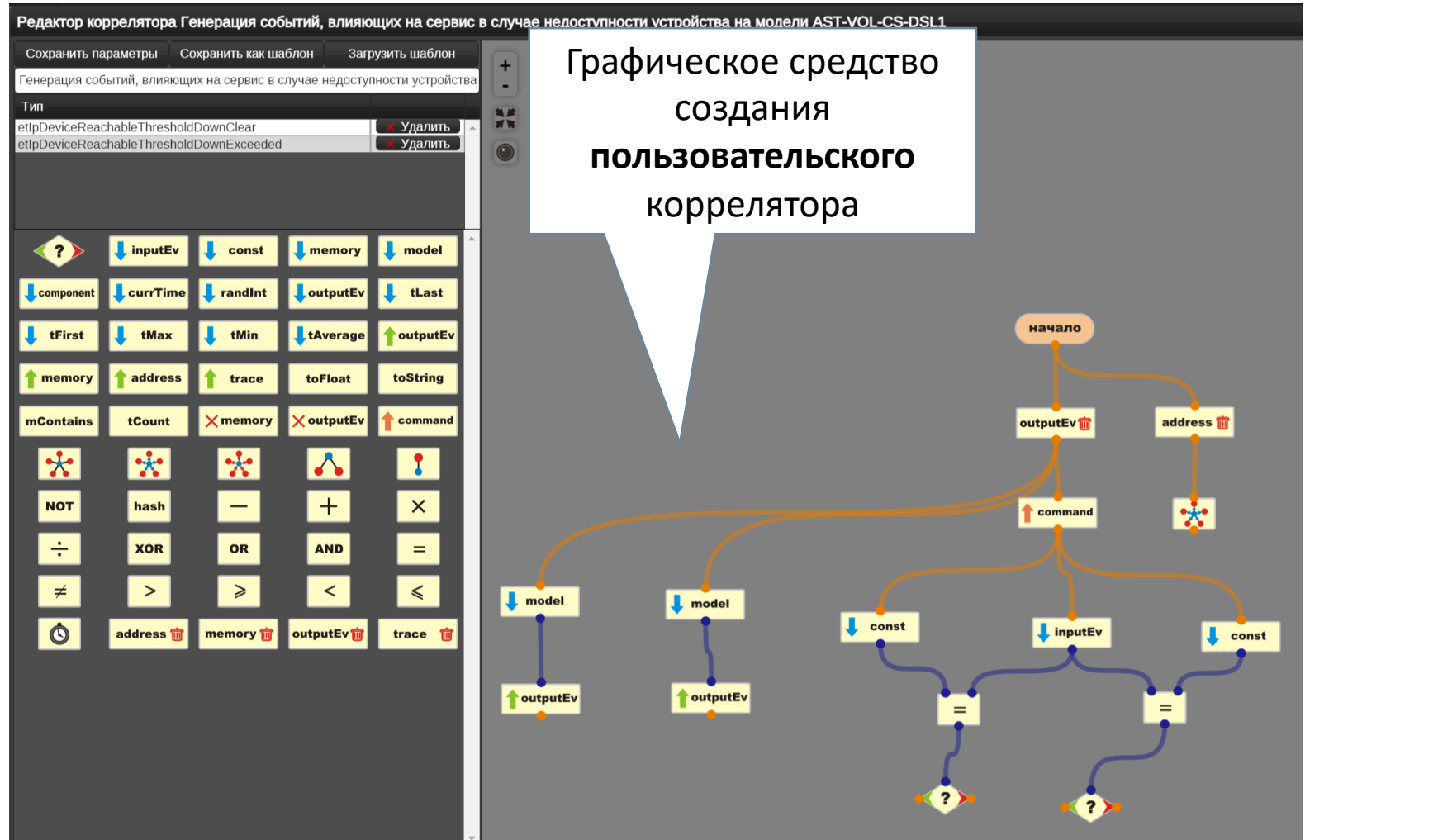
Первопричина сбоя в журнале аварий обнаружена системой автоматически



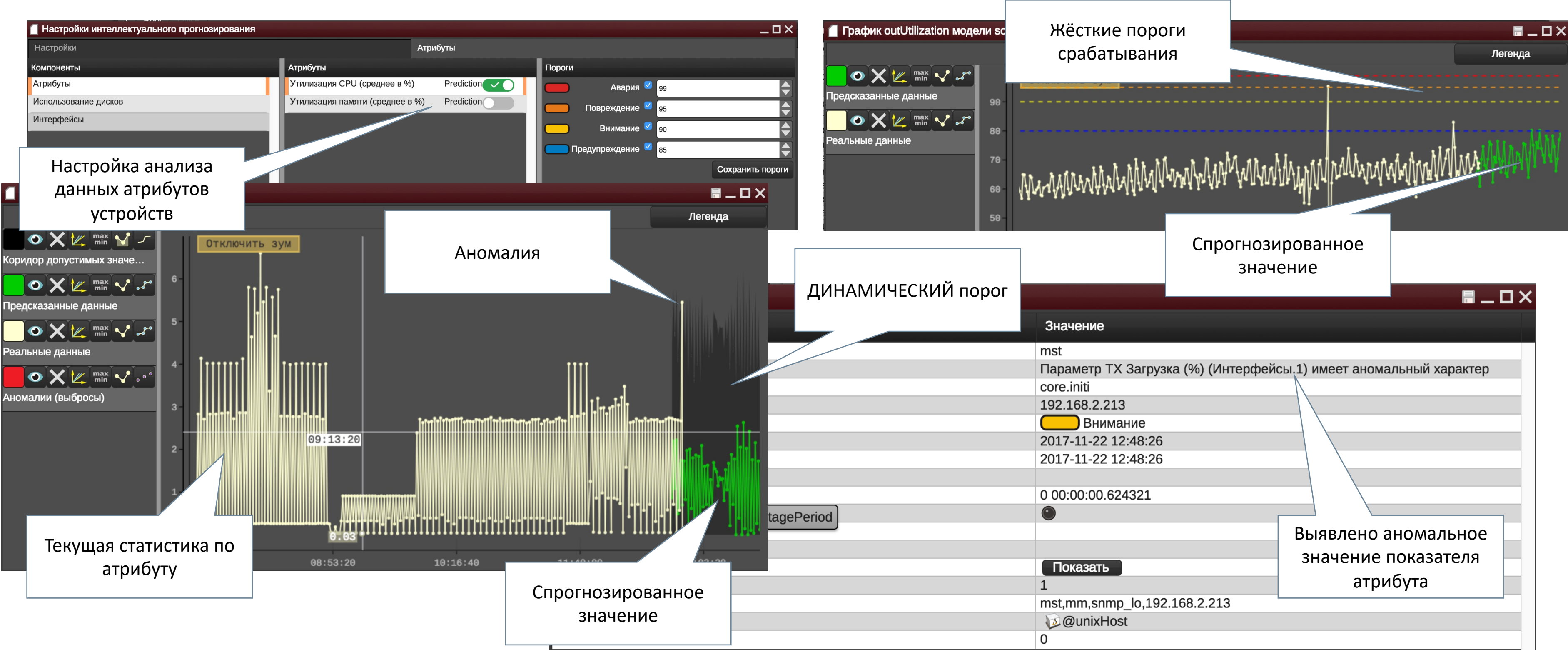
Последствия сбоя в журнале аварий, определены системой автоматически



Графическое средство создания пользовательского коррелятора



Интеллектуальный анализ данных, выявление аномалий



Конструктор отчётов, подсистема отчётности

Система имеет гибкий графический конструктор отчётов

Менеджер отчетов

Топ N устройств с максимальн...

Топ N самых популярных аварий (за

Доступность по устройствам

Топ N устройств с минимальной

Топ N аварийных устройств

Подробный отчет по авариям

Список отчётов по запросу

Примеры отчётов

Палитра данных

График

Круговая

Гистограмма

Пузырьковая

Топ

Воронка

Пирамида

Колонка

Радар

Тепловая карта

Таблица

Спидометр

Текст

Выбор вида или представления для отчёта

Менеджер источников данных

FileSystems... Dynamic)

Топ N устройств с максимальн...

PS(qTech, by Device, Dynamic)

CPU, MEM(J... BRAS, by Device,

PS,FAN(Jun... Dynamic)

Текст: Отчет за период (c no)

Severities view

CPU(Cisco, by Device, Dynamic)

Real-time view

Топ N устройств с максимальн...

CPU(edgeC... sw4, by Device,

Memory(Cisco, by Device, Dynamic)

Доступность всех устройств

CPU, Temp(... by Device, Dynamic)

Подробный отчет по авариям (от

CPU(edgeC... sw3, by Device,

Топ N устройств с минимальной

Топ N Аварийных устройств за

modelsData

Availability

CPU(Host, by Device, Dynamic)

CPU(qTech switch, by Device,

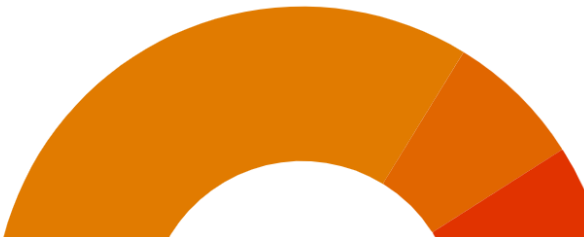
Количество аварий по типам (за

PS,FAN(Jun... BRAS, by Device,

Инвентарный состав

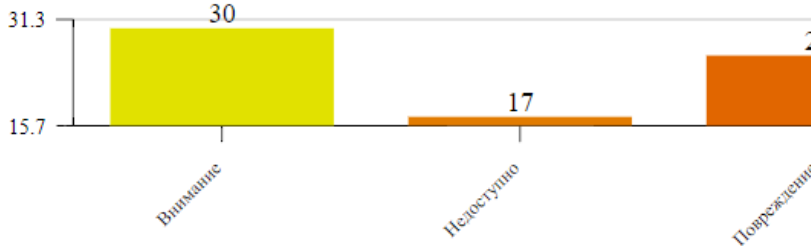
Предрасчитываемые данные

Топ N используемых интерфейсов

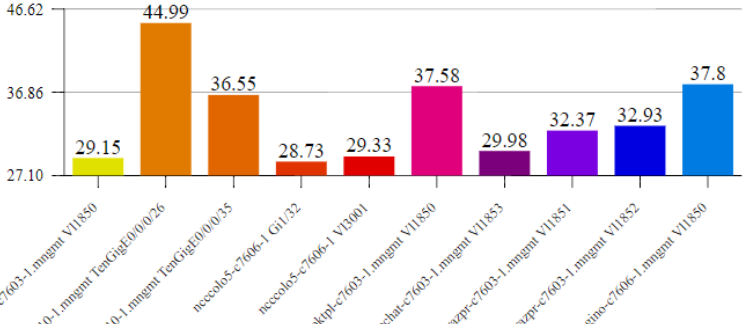


Аварии по критичности за ден

Отчет по устройству(ам) за период с 2017-11-05 17:40:14 по 2017-11-05 17:40:14



Отчет по устройству(ам) за период с 2017-11-05 17:52:29 по 2017-11-06 17:52:29



Устройство	Имя интерфейса	Alias	Тип интерфейса	Скорость интерфейса	Используемость (%)
lubyan-c7603-1.mgmt	TenGigE0/0/0/26	\$ncc-asr9010-1:TenGigE0/0/0/26\$		100000000000	47.77
ncc-asr9010-1.mgmt	TenGigE0/0/0/26	\$lubyan-c7603-1:TenGigabitEthernet1/1\$		100000000000	44.99
strogino-c7606-1.mgmt	V11850	17/1592, ISVN MosMetro, 300M, 100M		10000000	37.8

Интеграция с внешними OSS/BSS системами

Система обладает документированным открытым API

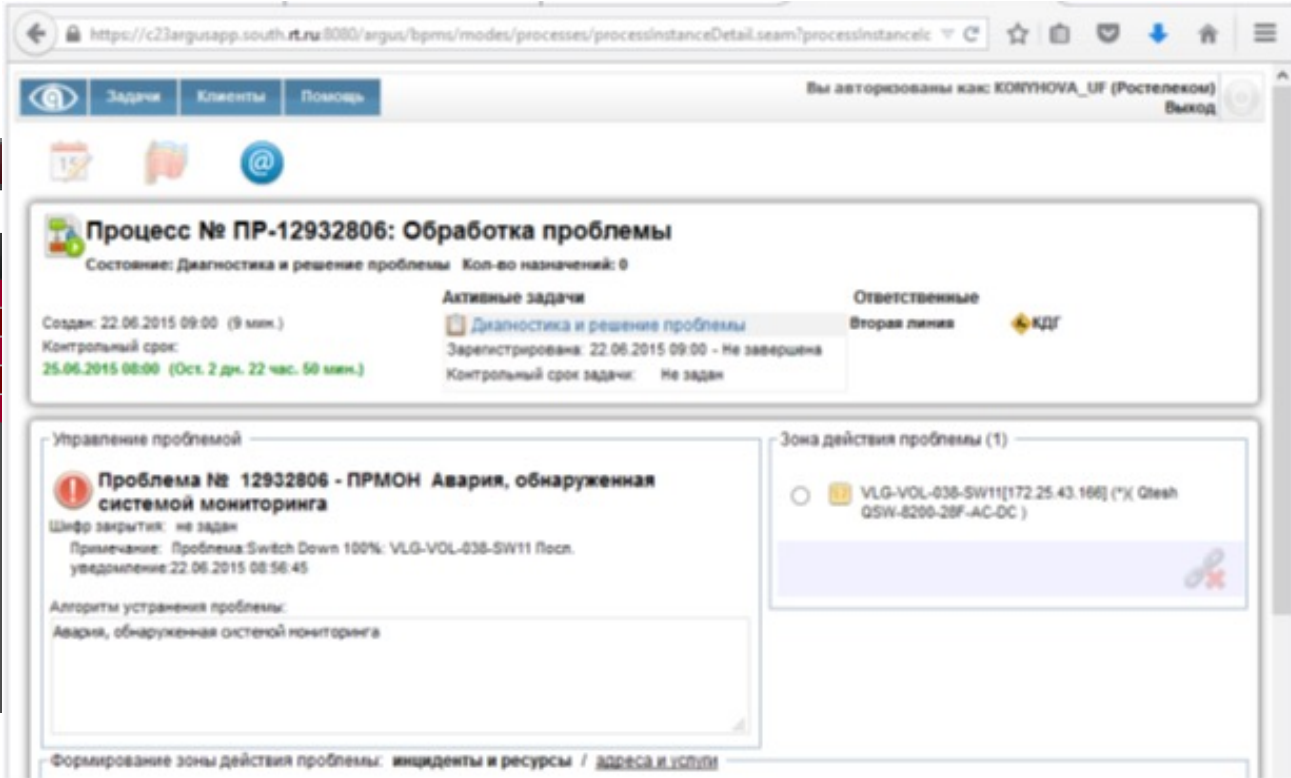
Журнал аварий пользователя root (5)

10.10.250.*

Заголовок	IP-адрес	Время начала	Последнее изме...	Принято в работу	Тикет	Затронуто физических лиц	Затронуто юридических лиц	Количество
Устройство KRD-NBG-GZVK2-SW недоступно	10.10.250.59	2016-06-22 13:32:44	2016-06-22 15:38:44	●	1156291805	0	12	1
Устройство KRD-TPS-96-1-2-DSL недоступно	10.10.250.222	2016-06-22 10:24:11	2016-06-22 15:39:41	●		0	12	1
Устройство KRD-TPS-VKV19-2-SW недоступно	10.10.250.45	2016-06-22 3:33:13	2016-06-22 10:25:08	●	1156150964	0	10	1
Устройство KRD-TPS-BKHM6-SW недоступно	10.10.250.49	2016-06-21 20:33:34	2016-06-22 10:25:08	●	1156063086	0	21	1
Устройство KRD-TPS-LNGR7-SW недоступно	10.10.250.148	2016-06-21 10:25:08	2016-06-22 10:25:08	●	1155822615	0	0	1

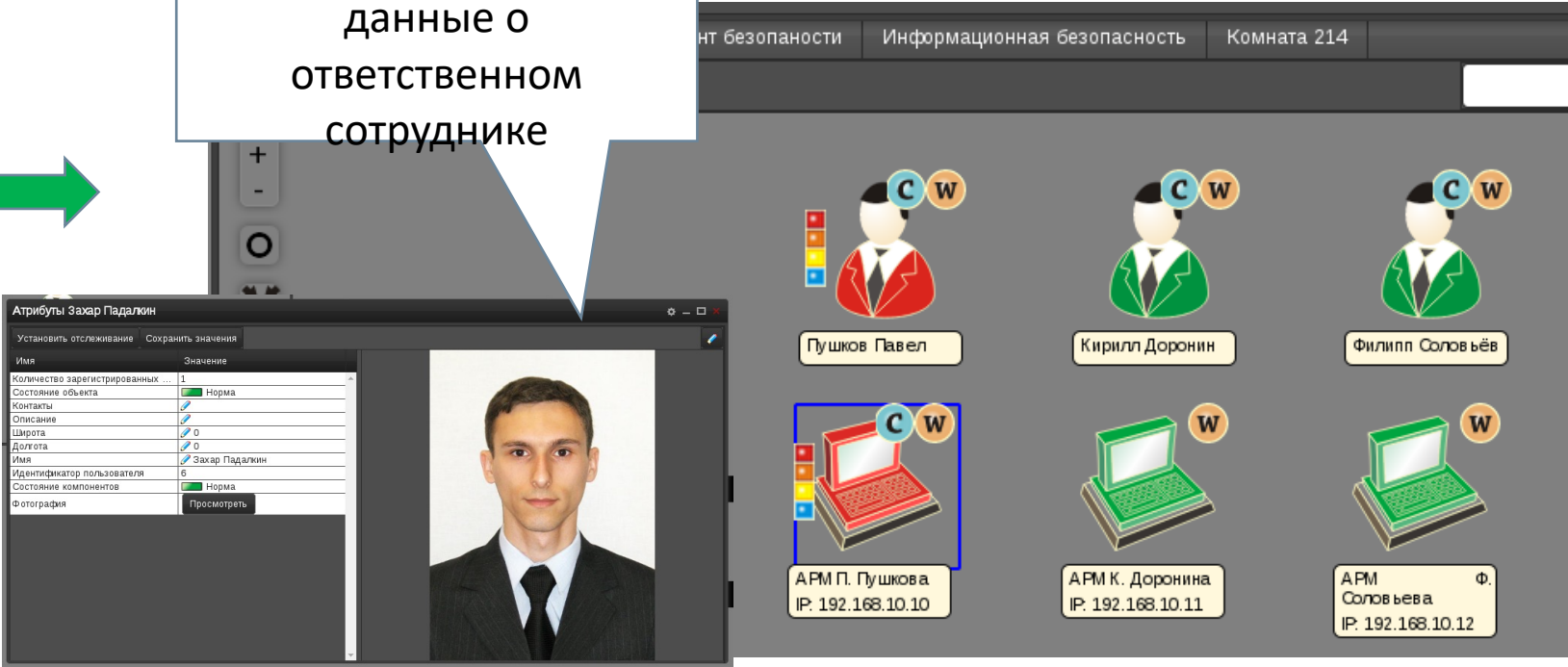
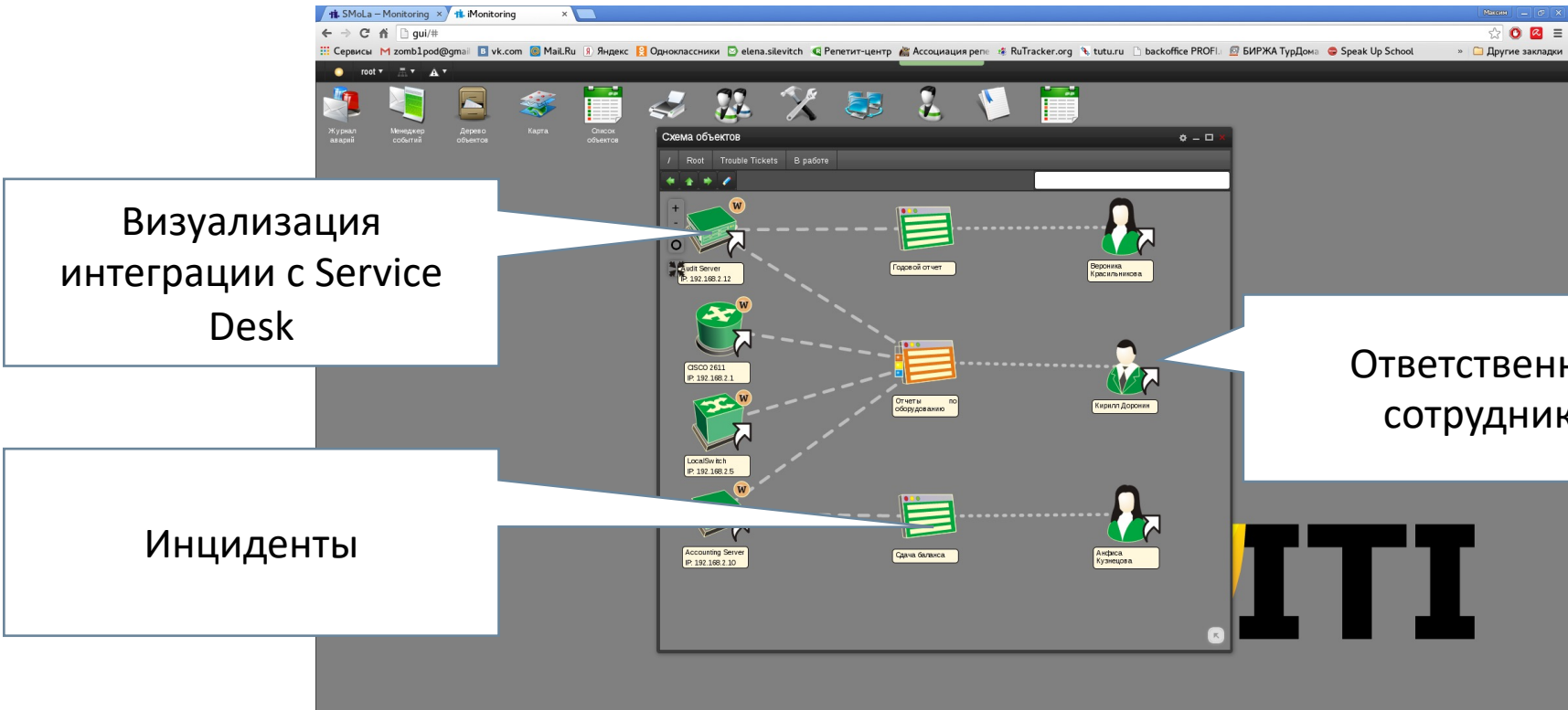
Интеграция с Service Desk

Номер инцидента



По клику переход в Service Desk на данный инцидент (SSO)

По клику переход – данные о ответственном сотруднике



Интеграция с внешними OSS/BSS системами – пример Naumen

ИНИТИ СОЛО имеет продуктивный адаптер к решениям Naumen SD и TU

Дерево объектов

▼ Root (51)

▶ 00001 головной (1)

▼ Депо (15)

▶ Электродепо 'Бутово' (5)

▶ Электродепо 'Варшавское' (...)

▶ Электродепо 'Владыкино' (31)

▼ Электродепо 'Выхино' (40)

▶ 2001-001 (8)

▶ 2001-002 (8)

▼ 2001-003 (8)

▶ A43/65197 головной (6)

▶ A43/65198 головной (6)

▶ A44/66393 (4)

▶ A44/66394 (4)

▶ A44/66395 (4)

▶ A44/66396 (4)

▶ A45/67197 (4)

▶ A45/67198 (4)

▶ 2001-004 (8)

▶ 2001-005 (16)

▶ 2001-006 (8)

▶ 2001-007 (8)

▶ 2001-008 (8)

▶ 2001-009 (8)

▶ 2001-010 (8)

▶ 2001-011 (8)

▶ 2001-012 (8)

Схема объектов

/ Root Депо Электродепо 'Выхино' 2001-003 A43/65197 головной

← ↑ → Типы устройств Связи Поиск

Объект в системе мониторинга

По клику обзор атрибутов объекта

Данные из ТУ

Карточка объекта в ТУ

Имя: Media screen A43/65197-2

Описание:

Атрибуты Media screen A43/65197-2

Иконка	
Картинка для карты	
Пороги	
Наблюдения	
Корреляторы	
Прогнозы	
Утилизация CPU (среднее в %)	31
Задержка (мс)	0
Идентификатор	4f3d0e6631b8f8325ed34ce53ed75cfd4d9f987675f455ac784b...
Задержка данных (мс)	-1
MAC-адрес	0C:73:EB:C0:14:06
Утилизация памяти (среднее в %)	44
Потеря данных (пакеты/с)	19.31551
Потеря пакетов	0
Пропуск кадров (шт)	-1
Поврежденный поток (шт)	-1
Серийный номер	VN24BAAI208002547
Сервер	
Идентификатор сервера	
Состав сервера	
Контракт	
Заставка	
Карточка	1817570
URL	udp://@239.255.1.1:31337
Значение vMOS (баллы)	1
Версия ПО	0.2.8777 9fe75d9
Вагон	A43/65197
На линии	
Состав	2001-003
Название линии	Таганско-Краснопресненская линия
Депо	Электродепо 'Выхино'

 ИНИТИ

Интеграция с внешними OSS/BSS системами – пример Naumen

ИНТИ СОЛО имеет продуктивный адаптер к решениям Naumen SD и TU

Медиаэкран

✎ Редактировать

✕ Удалить

↔ Изменить статус

↕ Изменить тип

В эксплуатацию

Информация об оборудовании

Основная информация

Редактировать

Дата монтажа:

Инвентарный номер:

Серийный номер:

IP-адрес:

MAC-адрес:

Диагональ экрана:

Вагон:

Позиция в вагоне:

Статус:

Пользователи:

ВН24ВAAI222003634

A44/66016

1

Установлено

Конфигурация

Редактировать

Версия ПО:

Состояние в мониторинге:

0.2.8777 9fe75d9

Доступно

Финансы

Редактировать

Стоимость без НДС, руб.:

НДС, руб.:

Стоимость с НДС, руб.:

102699.03

18485.83

121184.86

Штрих-код:

Печать

Медиаэкран

VN24BAAI222003634

Файлы

Добавить файл

Данные от системы мониторинга

Финансовая информация

Карточка объекта в ТУ

QR код по объекту (SN + инвентарный номер + именование)

Интеграция с внешними OSS/BSS системами – пример Naumen

ИНТИ СОЛО имеет продуктивный адаптер к решениям Naumen SD и TY

Комментарии

История

История изменений

Показывать историю вложенных объектов

[Выберите вид]

Сохранить вид

Сортировка...

Фильтрация...

Экспорт списка

Обновлять список

Дата и время	Инициатор	Описание
06.06.2018 08:13	system	Объект 'Медиаэкран' изменен: IP-адрес: '10.90.29.4' -> '10.90.29.53'.
06.06.2018 01:02	system	Объект 'Медиаэкран' изменен: Состояние в мониторинге: 'Недоступно' -> 'Доступно'.
06.06.2018 00:05	advimport	Объект 'Медиаэкран' изменен: Время последнего импорта: '05.06.2018 11:45'.
05.06.2018 23:32	system	Объект 'Медиаэкран' изменен: Состояние в мониторинге: 'Доступно' -> 'Недоступно'.
05.06.2018 11:45	advimport	Объект 'Медиаэкран' изменен: Время последнего импорта: '04.06.2018 23:32'.
05.06.2018 08:13	system	Объект 'Медиаэкран' изменен: IP-адрес: '10.90.29.11' -> '10.90.29.4'.
05.06.2018 05:32	system	Объект 'Медиаэкран' изменен: Состояние в мониторинге: 'Недоступно' -> 'Доступно'.
05.06.2018 04:02	system	Объект 'Медиаэкран' изменен: Состояние в мониторинге: 'Доступно' -> 'Недоступно'.

Сервер

Редактировать

Удалить

Изменить статус

Изменить тип

В эксплуатацию

Параметры объекта

Связанные объекты

Информация оборудования

Основная информация

Конфигурация

Данные от системы мониторинга – установленное ПО

Используемые лицензии

Штрих-код:

Печать

Сервер 123436554

Логирование истории изменений по объекту

Данные от системы мониторинга – установленное ПО

Используемые лицензии

Привязка контрактов на поставку / поддержку и пр..

Расположение в стойке / 'этажном плане и пр..

Карточка объекта в TY

Объекты учета

Расписания

Финансы

Договоры

Активности

Оргструктура

Справочники

Настройки

Затраты

Бюджетирование

Список фактических затрат

Показывать историю вложенных объектов

[Выберите вид]

Сохранить вид

Сортировка...

Фильтрация...

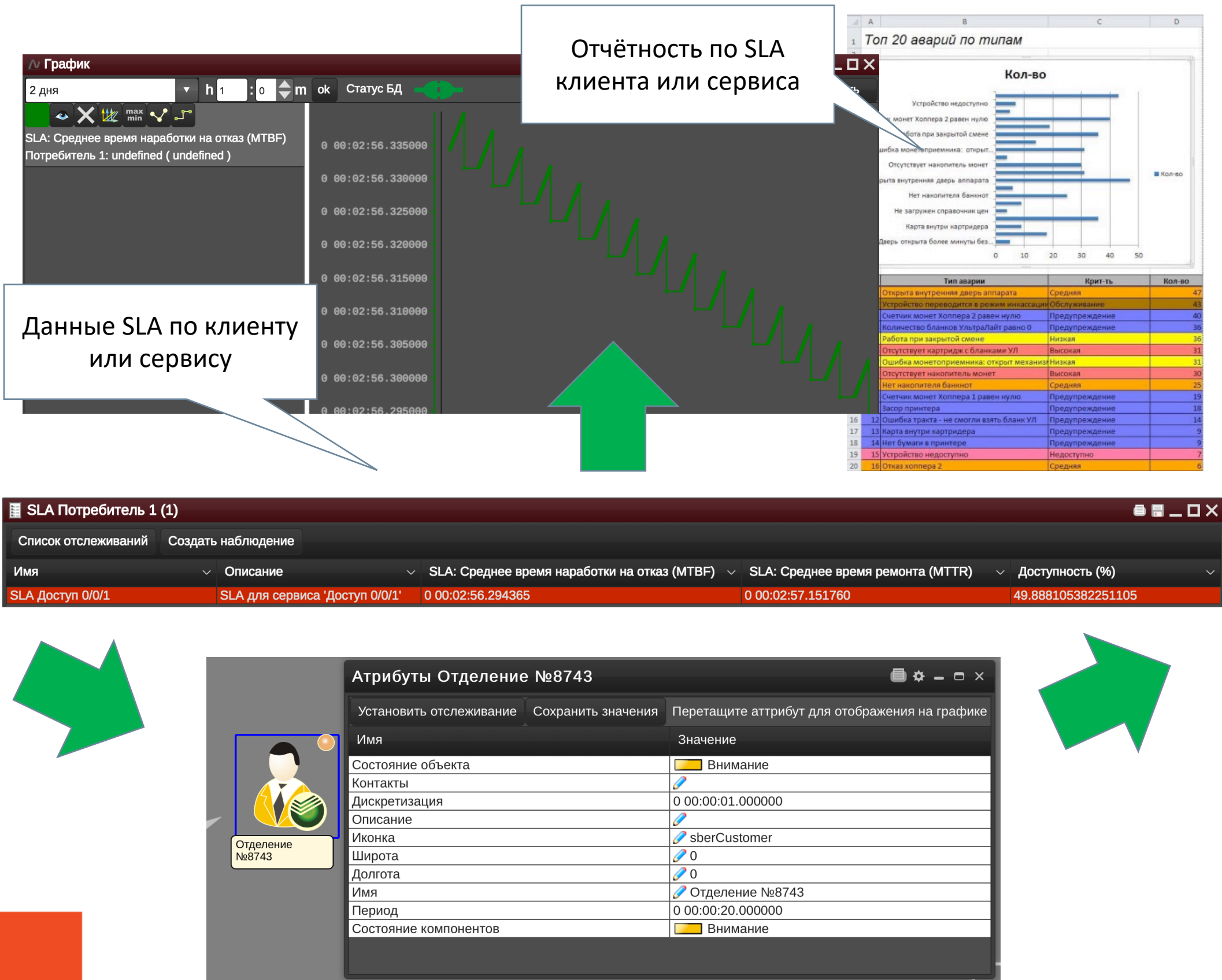
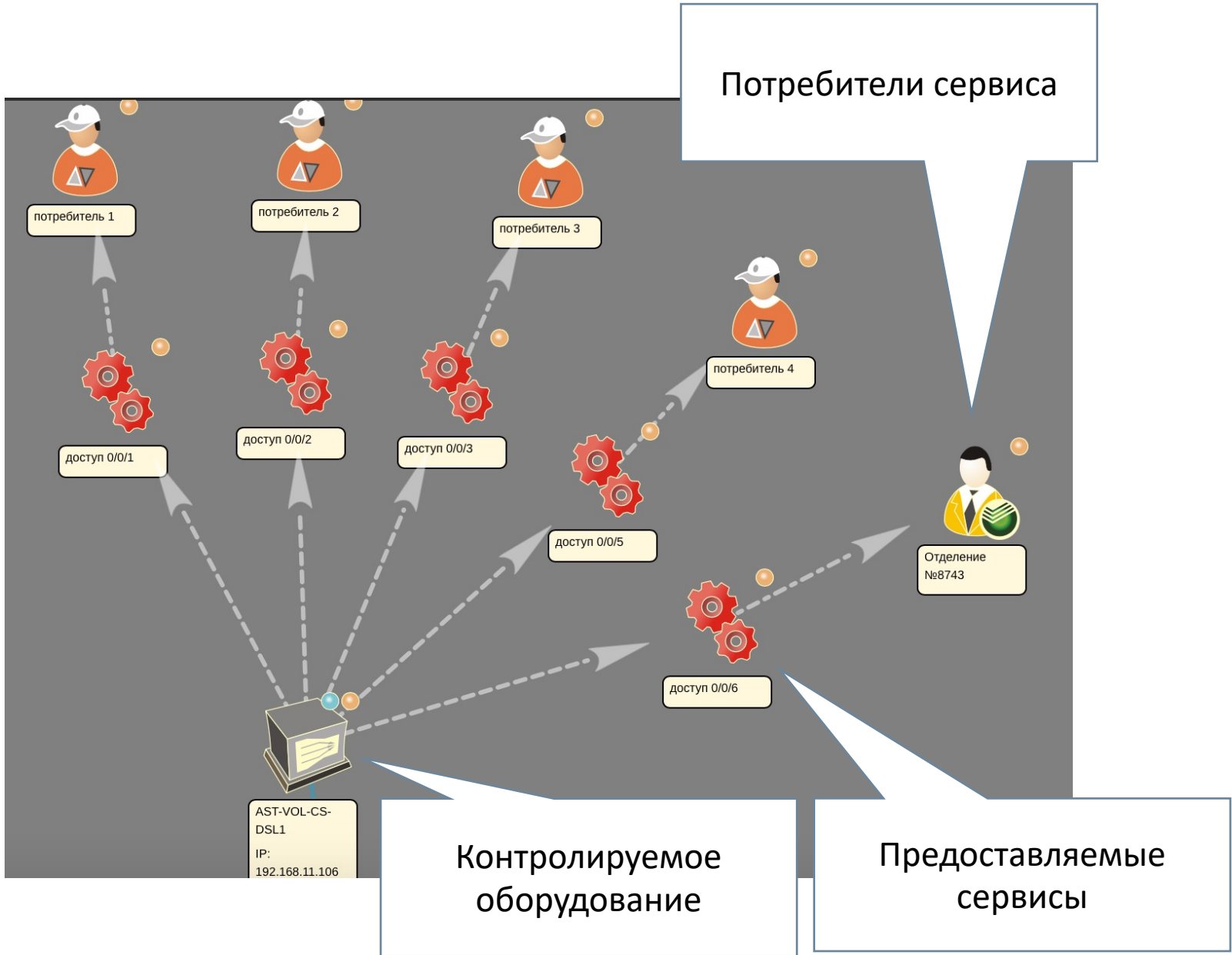
Экспорт списка

Дата	Название	Договор	Бюджет	Статья бюджета	Категория	Сумма, руб.
26.03.2018	Услуги по монтажу оборудования	№886181	Бюджет на 2018	2. Оборудование медиаплатформы, Бюджет на 2018	Операционные	2000000
21.03.2018	Закупка запасных медиаэкранов	№4484m	Бюджет на 2018	2. Оборудование медиаплатформы, Бюджет на 2018	Капитальные	1800000

Всего объектов в списке: 2, строк на странице: 20

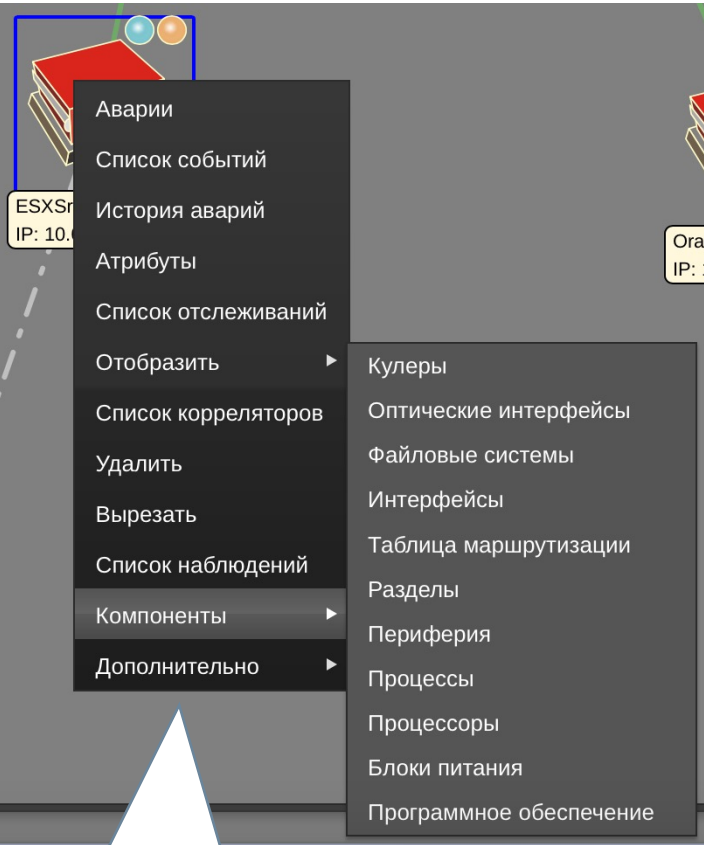
Сервисно-ресурсная модель

Контроль сервисов, предоставляемых внешним или внутренним пользователям, Контроль подрядчиков

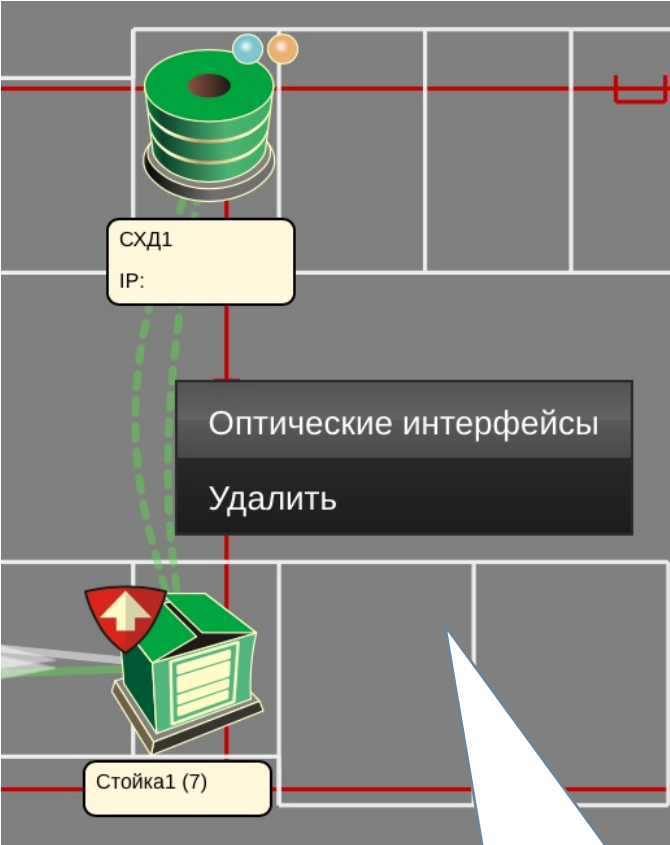


Мониторинг ИТ оборудования и сервисы

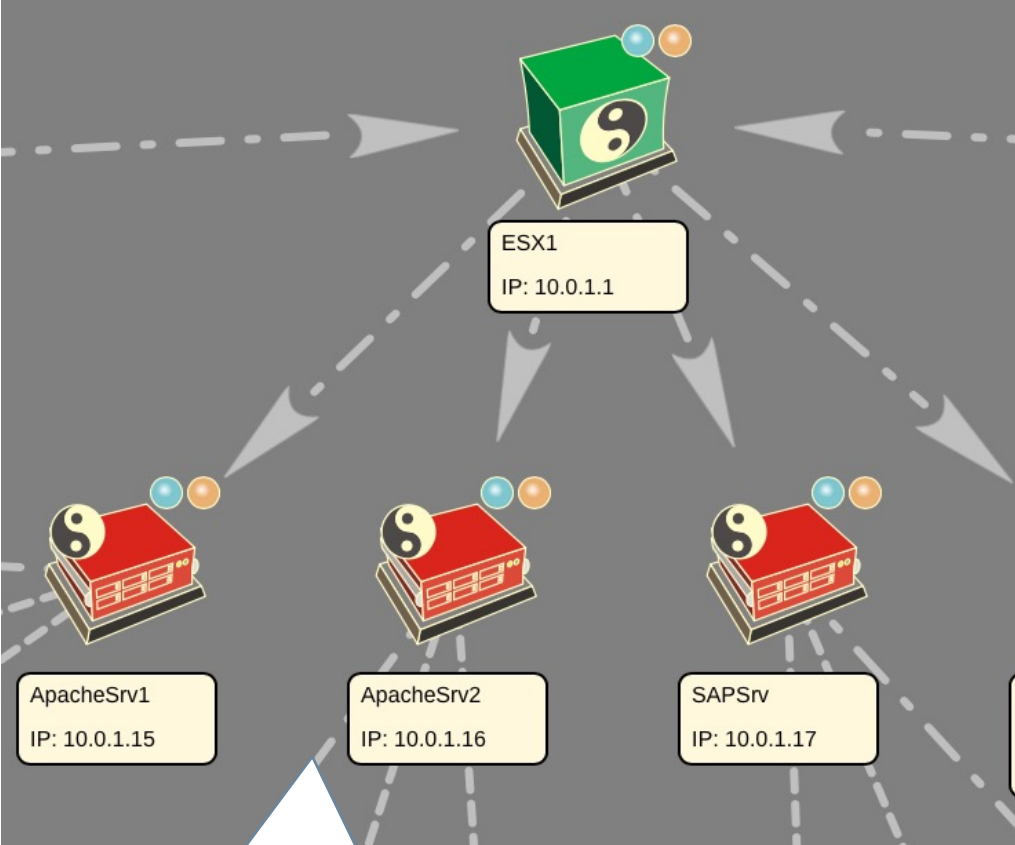
Сервера, системы виртуализации, СХД, приложения, периферийные устройства



Серверное оборудование



СХД и компоненты SAN



Средства виртуализации

Разделы ApacheSrv1 (4)

Названи...	Имя	Файловая ...	Точка мон...	Объем ди...	Используй...	Свободно...	Флаги
/dev/sdb1	/dev/sdb1	ext3	/home	78228453	0	0	
/dev/sda3	/dev/sda3	linux-sw		0	0	0	
/dev/sda2	/dev/sda2	ext4	/	2055443	0	0	
/dev/sda1	/dev/sda1	ext4	/boot	0	0	0	boot

Компоненты ОС

Табличные пространства kurs (47)

Связи

Список отслеживаний

Табли...	Файл	Физическ
USERS	+DG_DATA/kursupg/datafile/users.294.888230985	918
USERS	+DG_DATA/kursupg/datafile/users.302.888231031	4387
USERS	+DG_DATA/kursupg/datafile/users.298.888231009	1728
USERS	+DG_DATA/kursupg/datafile/users.300.888231019	7057
USERS	+DG_DATA/kursupg/datafile/users.292.888230975	2442
USERS	+DG_DATA/kursupg/datafile/users.305.888231047	4539
USERS	+DG_DATA/kursupg/datafile/users.299.888231015	6440

kursupg.south.rt.ru

kursupg

ing Needed Count

point Incomplete Count

ation Count

62177

1160938

0.0031009408000000002

36

37

24282037

0

48.08660348719999

3321888768

2258352

o (%)

s

1

2106055

0

19300352

1.9301089013000001

atio (%)

d Ratio (%)

ible Mem Per SQL Stmts

ible Mem Per User

ible Mem Stored Obj

12802752

6413680640

3070233168

0

669222

0

Детальный мониторинг ПО

Мониторинг пользовательских действий

Step No.	Command	URL	Value	Step status	Message	Description	Time
1	newSession			1	ok		
2	implicitlyWait			1	Message: POST /session/0cc266f6-3435-43c5-a93a-0c93f3c39001/timeout/implicit_wait did not match a known command		
3	get	http://10.29.6.40:8080/RostelPoints/login.jsf		1	Message: Reached error page: about:neterror?e=proxyConnectFailure&u=http%3A//10.29.6.40%3A8080/RostelPoints/login.jsf&c=UTF-8&f=regular&d=Firefox%20%D0%B0%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B5%D0%BD%20%D0%BD%D0%B0%20%D0%B8%D1%81%D0%BF%D0%BE%D0%BB%D1%8C%D0%B		

Детализация выполнения скрипта (эмулирующих действий)

Детализация выполнения скрипта (эмулирующих действий), включая снимок экрана

Execution Information

Start Time	Mon Oct 02 13:03:27 GMT+03:00 2017
End Time	Mon Oct 02 13:03:30 GMT+03:00 2017
Duration (hh:mm:ss)	00:00:03
Expected CAPs	21
Executed CAPs	1
CAP Execution (mills)	3011
Event Handler CAPs	0
Failed CAPs	1

Test Suite Information

Test Name	fullTest
Status	FAILED

Application Under Test (AUT) Information

Test Name	testCRM
Configuration	testCRM@localhost
Hostname	localhost
AUT Arguments	

Execution Stack

Navigation: Prev Next Error (ALT - Left, ALT - Right)

- fullTest - IS (nested error) - 0:00:00.640
- ub_app_activate - TC (nested error) - 0:00:00.640
- activate AUT - CAP (failed) - 0:00:00.343

Application - Activate

Activation Method [String]: NW

Error Details

Type: Action Error

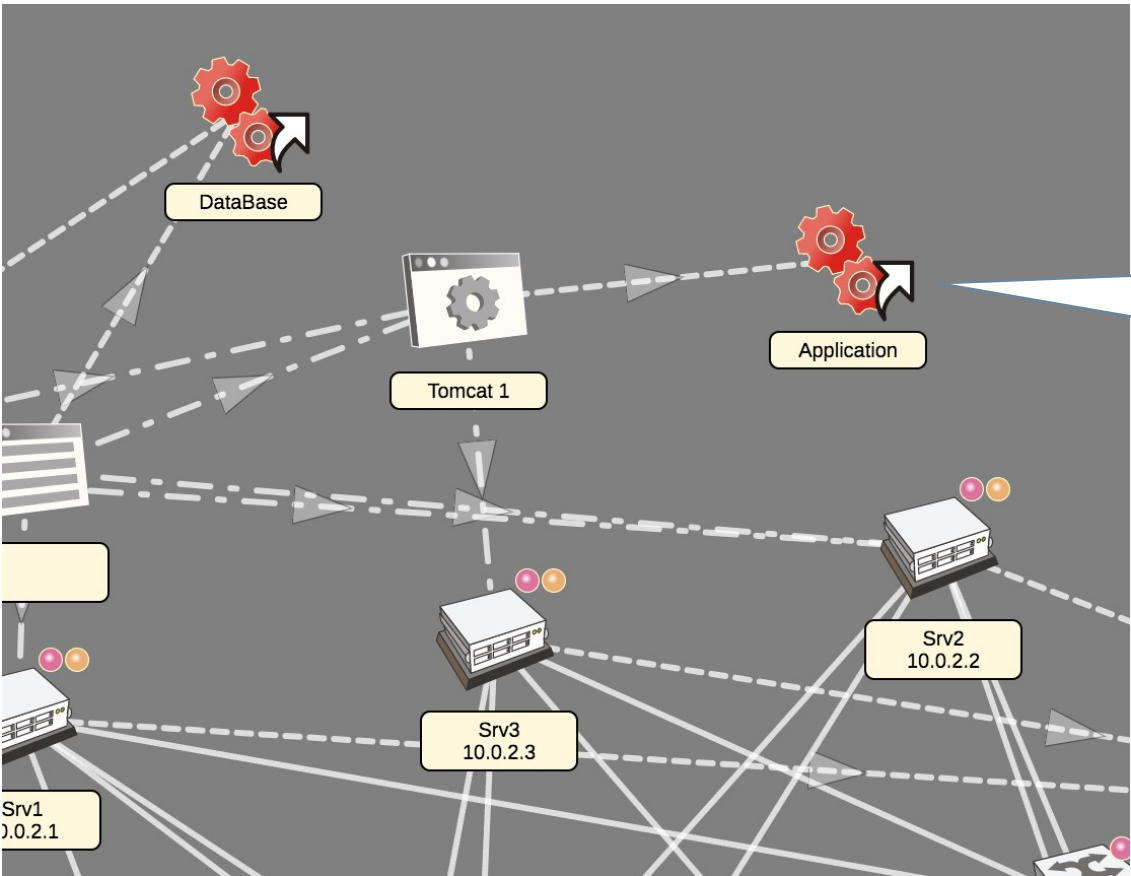
Description: Execution Error: "Window activation failed."

Screenshot



Timestamp: Mon Oct 02 13:03:29 GMT+03:00 2017

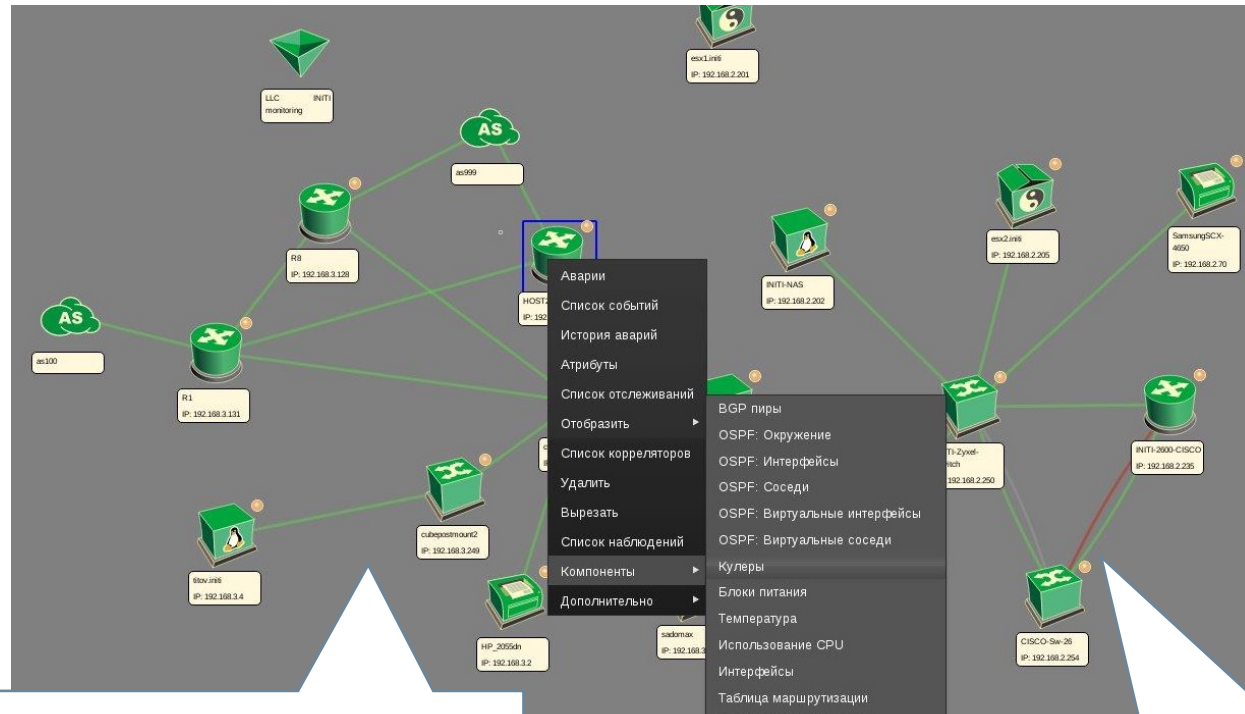
- Default Events Handler - Events Handler (ok) - 0:00:00.297
- login - TC (not tested)
- locateClient - TC (not tested)
- checkTableAndCloseApp - TC (not tested)



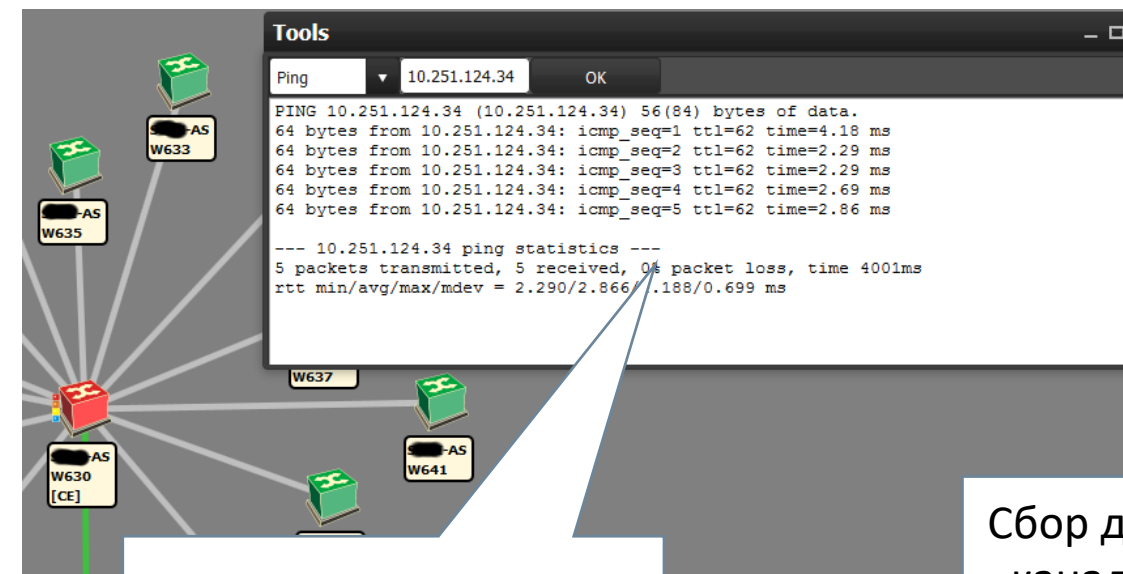
Маппирование сбоя на сервисную модель ИТ сервиса

Мониторинг сетевой инфраструктуры

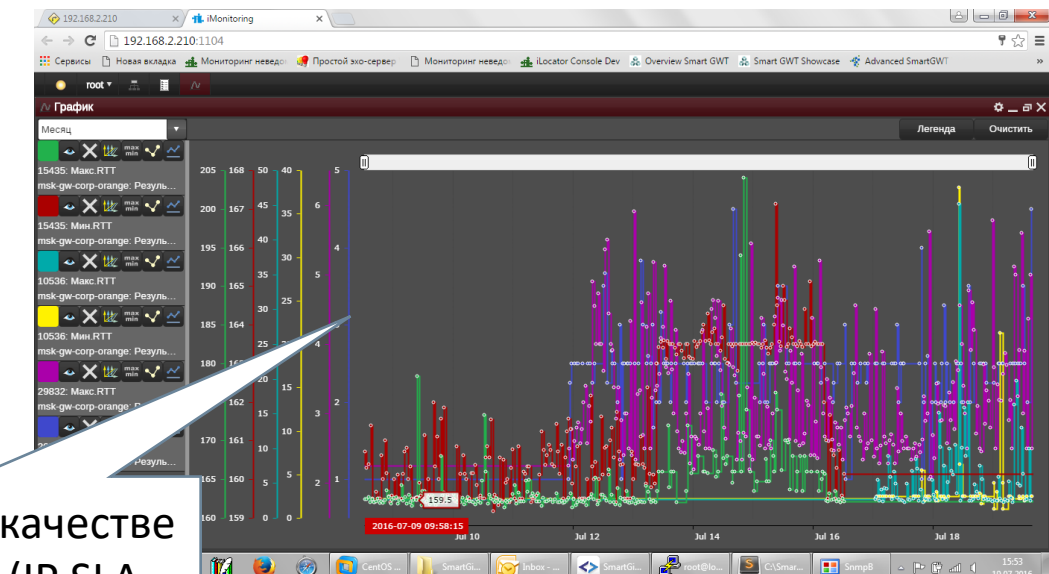
Мониторинг и поиск первопричины сбоя в различных сетевых инфраструктурах (IP/MPLS, SDH/WDM, RRL и пр..)



Автоматическое построение топологии

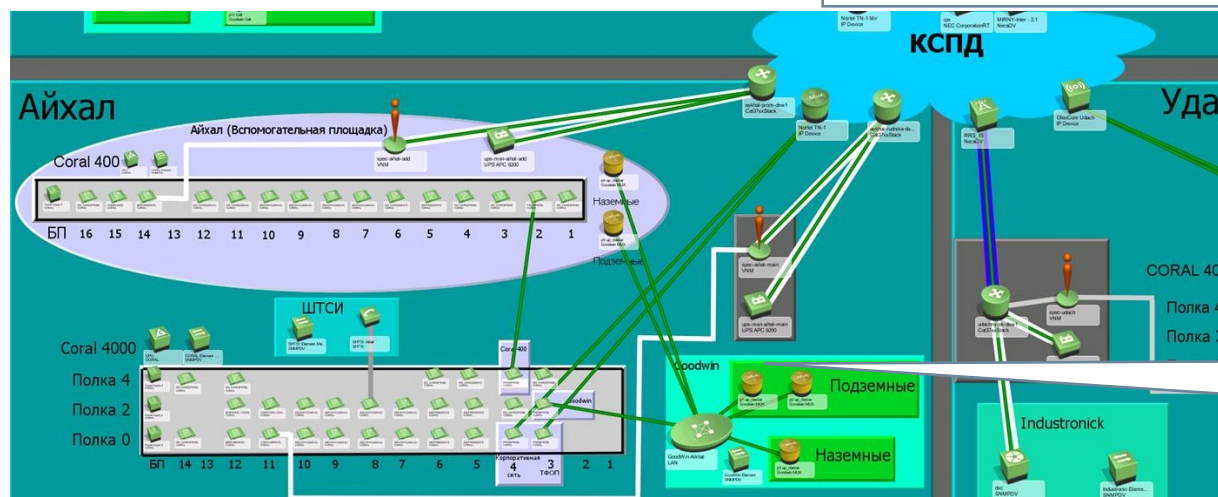


Контекстный запуск утилит по диагностике



Сбор данных о качестве каналов связи (IP SLA, QoS, TWAMP и пр..)

Сбор и ведение конфигураций оборудования



Отслеживание изменений конфигураций

Мониторинг телефонных станций

Контроль изменения конфигураций		оборудования	
Дата/Время изменения		Дата/Время изменения	
2015-10-27 16:36:45.000000 (GMT+3)		2015-10-27 16:36:45.000000 (GMT+3)	
2015-10-27 16:31:24.000000 (GMT+3)		2015-10-27 16:31:24.000000 (GMT+3)	
2015-10-27 16:31:06.000000 (GMT+3)		2015-10-27 16:31:06.000000 (GMT+3)	
2015-10-27 16:30:59.000000 (GMT+3)		2015-10-27 16:30:59.000000 (GMT+3)	
2015-10-27 16:29:39.000000 (GMT+3)		2015-10-27 16:29:39.000000 (GMT+3)	
2015-10-27 16:29:31.000000 (GMT+3)		2015-10-27 16:29:31.000000 (GMT+3)	
2015-10-27 16:29:31.000000 (GMT+3)		2015-10-27 16:29:31.000000 (GMT+3)	
snmp-server enable traps ppoe	99	95 snmp-server enable traps bstun	
snmp-server enable traps ipmobile	100	96 snmp-server enable traps dial	
snmp-server enable traps isakmp policy add	101	97 snmp-server enable traps dsp card-status	
snmp-server enable traps isakmp policy delete	102	98 snmp-server enable traps atm subif	
snmp-server enable traps isakmp tunnel start	103	99 snmp-server enable traps ppoe	
snmp-server enable traps isakmp tunnel stop	104	100 snmp-server enable traps ipmobile	
snmp-server enable traps ipsec cryptomap add	105	101 snmp-server enable traps ipsec cryptomap delete	
snmp-server enable traps ipsec cryptomap delete	106	102 snmp-server enable traps ipsec cryptomap attach	
snmp-server enable traps ipsec cryptomap attach	107	103 snmp-server enable traps ipsec cryptomap detach	
snmp-server enable traps ipsec cryptomap detach	108	104 snmp-server enable traps ipsec tunnel start	
snmp-server enable traps ipsec tunnel start	109	105 snmp-server enable traps ipsec tunnel stop	
snmp-server enable traps ipsec tunnel stop	110	106 snmp-server enable traps ipsec too-many-sas	
snmp-server enable traps ipsec too-many-sas	111	107 snmp-server enable traps voice poor-qov	
snmp-server enable traps voice poor-qov	112	108 snmp-server enable traps dnis	
snmp-server enable traps dnis	113	109 snmp-server host 192.168.3.104 public	
snmp-server host 192.168.2.104 public	114	110 snmp-server host 192.168.3.112 public	
snmp-server host 192.168.2.112 public	115	111 snmp-server host 192.168.3.113 public	
snmp-server host 192.168.2.113 public	116	112 snmp-server host 192.168.3.4 public	
snmp-server host 192.168.2.4 public	117	113 snmp-server host 192.168.3.9 public	
snmp-server host 192.168.2.9 public	118	114 snmp-server host 192.168.3.6 public	
snmp-server host 192.168.3.6 public	119	115 !	
!	120	116 !	
!	121	117 dial-peer cor custom	

Мониторинг сетевой инфраструктуры – IP/MPLS

Мониторинг и поиск первопричины сбоя в различных сетевых инфраструктурах (IP/MPLS, SDH/WDM, RRL и пр..)

Общие объекты и компоненты MPLS сети:

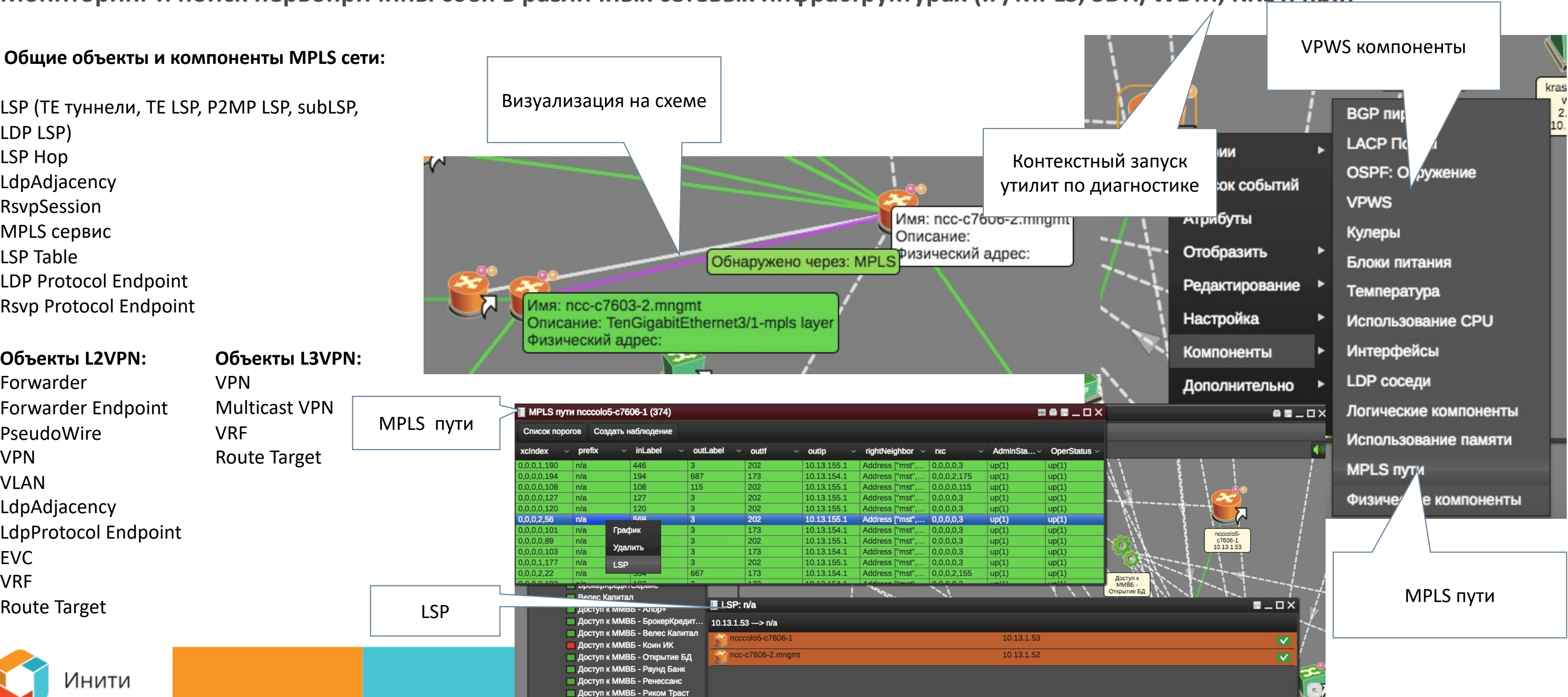
LSP (TE туннели, TE LSP, P2MP LSP, subLSP, LDP LSP)
LSP Hop
LdpAdjacency
RsvpSession
MPLS сервис
LSP Table
LDP Protocol Endpoint
Rsvp Protocol Endpoint

Объекты L2VPN:

Forwarder
Forwarder Endpoint
PseudoWire
VPN
VLAN
LdpAdjacency
LdpProtocol Endpoint
EVC
VRF
Route Target

Объекты L3VPN:

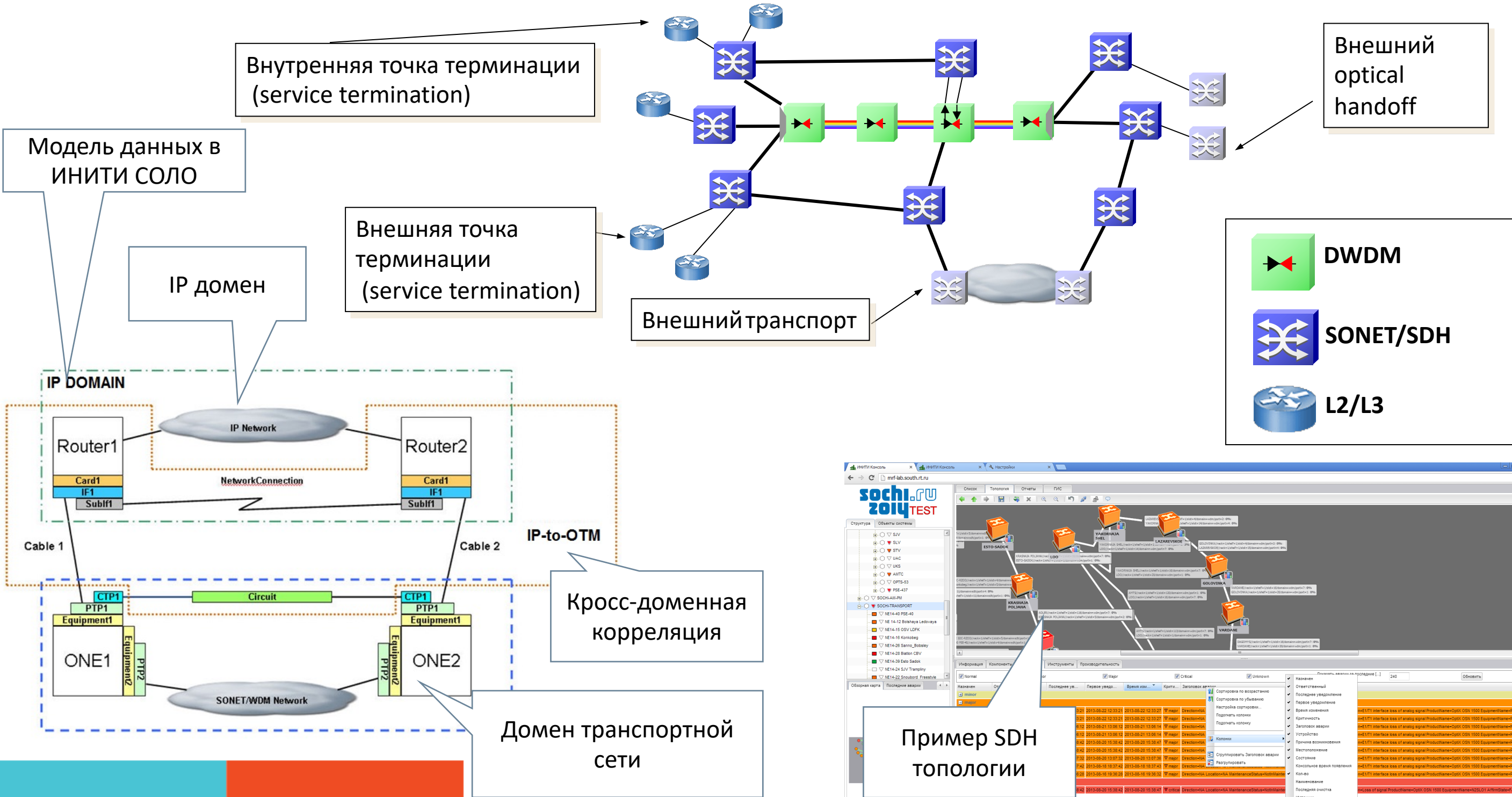
VPN
Multicast VPN
VRF
Route Target



Мониторинг сетевой инфраструктуры – SDH / WDM

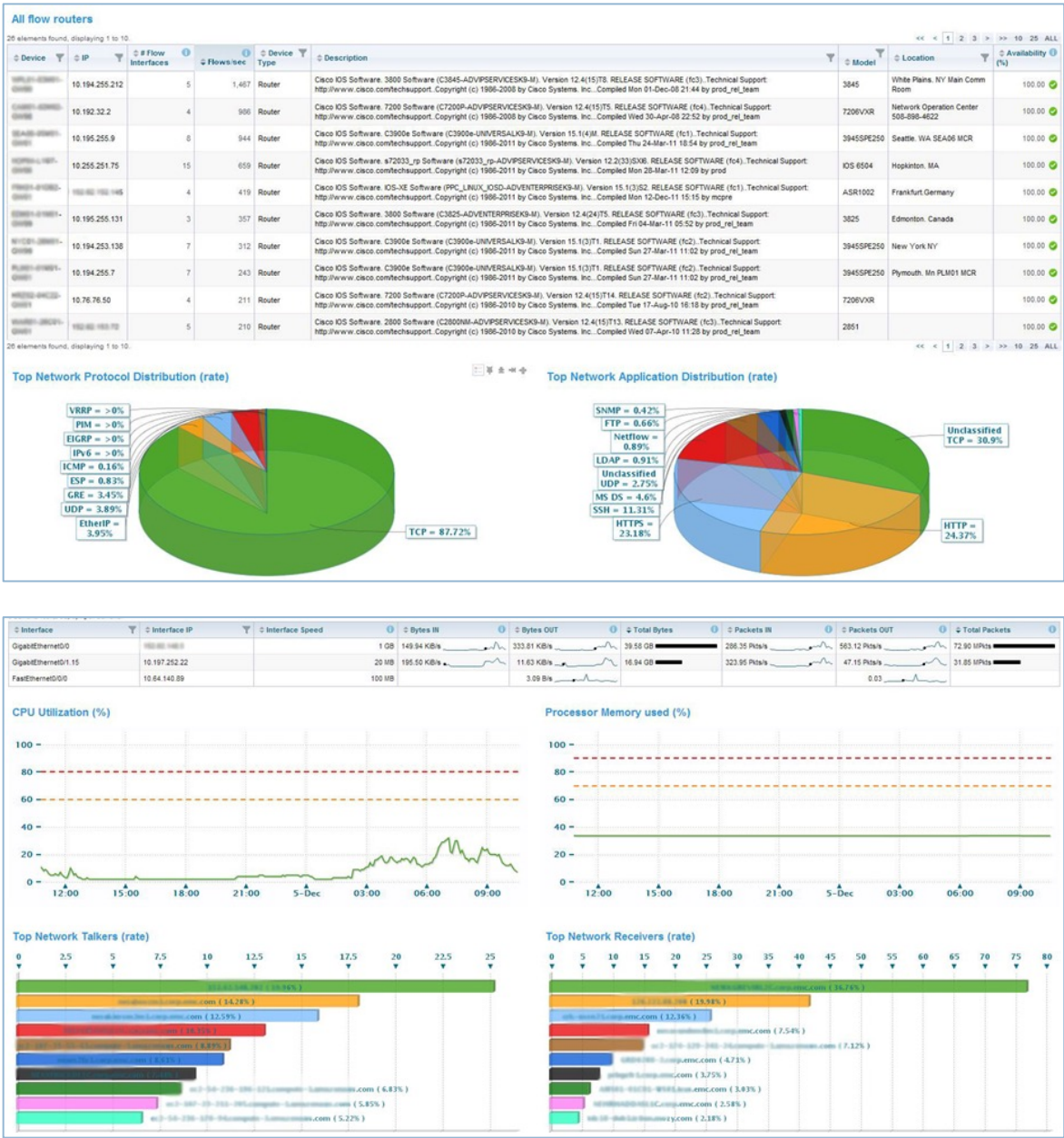
Мониторинг и поиск первопричины сбоя в различных сетевых инфраструктурах (IP/MPLS, SDH/WDM, RRL и пр..)

- **Технологии**
 - DWDM
 - SONET/SDH
 - Low Order SONET/ PDH
- Поддержка работы в мультивендорных средах
- **Модели**
 - Элементы сети, карты, физические / логические порты
 - Топологические линки, Fiber, Fiber bundle
 - Логические линки, Wavelength
 - Client circuit, Trail
 - Protection Groups
- **Анализ**
 - Поиск первопричины сбоя для SONET/SDH
 - Поиск первопричины сбоя для WDM
 - Определение воздействия WDM на SONET/SDH
 - Определение воздействия WDM на Low OrderSONET/PDH
 - IP поверх SONET/SDH
 - IP поверх WDM



Мониторинг параметров сетевой инфраструктуры

Сбор данных NetFlow, sFlow, jFlow, etc..



- Сбор данных от оборудования (Netflow, Jflow, sFlow, Cflow и IPFIX) через Инити xFlow коллекторы с поделующей нормализацией и сохранением данных о производительности по заданным метрикам. Возможность выноса коллекторов на региональные сервера.

- Установка пороговых (следящих) функций по заданным параметрам.
- Привязка полученных данных к каналам связи.
- Построение графических отчётов по типам трафика и загрузке каналов связи.

Сбор данных IP SLA, TWAMP, RPM, QoS, etc..:

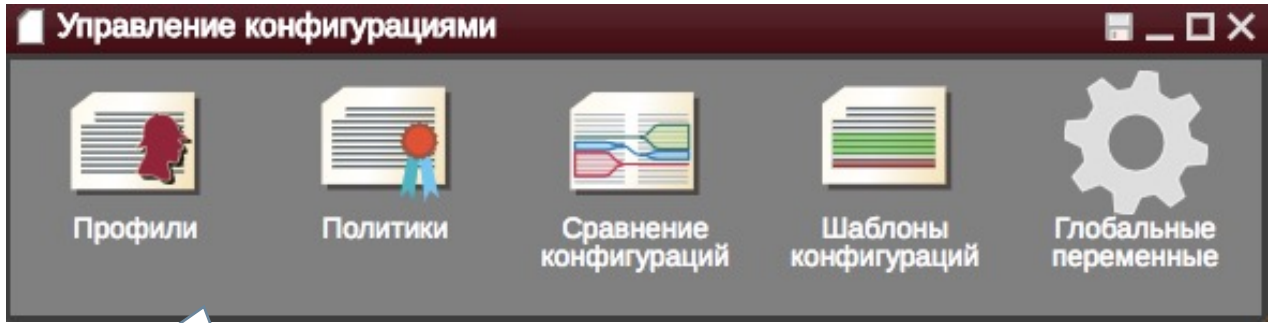
- IP/ICMP Echo (Hosts response time)
- SNA Echo (SNA response time)
- IP/ICMP Path Echo (Hop by hop response time)
- TCP Connection (Application response time)
- UDP Echo (UDP response time)
- Jitter/UDP Plus (Jitter measurements)
- HTTP (Web server response time)
- FTP (Ftp server response time)
- DHCP (DHCP server response time)
- DLSw+ (DLSw peer response time)
- DNS (DNS server response time)

При этом по умолчанию поддерживается сбор следующих метрик:

- Operation Success (%)
- Jitter Operation Completed (%)
- Jitter Operation Mean Round Trip Time (ms)
- Jitter Relative to Packet Interval (ms)
- Jitter Packet Loss (%)
- Jitter Maximum (Positive/Negative, ms)
- Operation completion time (ms)
- DNS Request completion time (ms)
- TCP Connect completion time (ms)
- Transaction completion time (ms)
- Operation Statistics

Управление конфигурациями сетевой инфраструктуры

Подсистема управления конфигурациями



Выделенный интерактивный виджет

Создание шаблонных конфигураций

ConfigurationPatterns.label	Название
Включить SNMP v 3	snmpOnv3.pl
Включить SNMP v 1, 2	snmpOn.pl
Выключить SNMP v 3	snmpOffv3.pl
Выключить SNMP v 1, 2	snmpOff.pl
Включить CDP	cdpOn.pl
Выключить CDP	cdpOff.pl

Профили

Добавить Редактировать Удалить Копировать

name	Драйвер	Логин	Пароль	Мастер-пароль	Таймаут
test1					
test					
Unix_host					
Cisco_Telnet_Tftp	Cisco: TFTP через Telnet с Enable	admin			300
Cisco_SNMP_Tftp					

Редактировать

Имя профиля: Cisco_Telnet_Tftp

Драйвер: Cisco: TFTP через Telnet с Enable

Логин: Cisco: TFTP через SNMP

Пароль: Juniper: SSH

Мастер-пароль: Unix: SSH

Таймаут: Cisco: Telnet с Enable

Cisco: TFTP через Telnet с Enable

Juniper: Telnet

Отменить Подтвердить

Возможность создавать собственные профили работы с оборудованием

Пример пользовательского профиля для сбора конфигураций Cisco

Профили могут быть скопированы или наследованы

Управление конфигурациями сетевой инфраструктуры

Подсистема управления конфигурациями

Глобальные переменные

Имя	Значение
test	test

Создание глобальный переменных или алиасов

Сравнение конфигураций

Создание и контроль политик конфигураций

Группировка и редактирование политик конфигураций

Редактор политик

Имя

passwords_encrypted

Критичность

Внимание

Способ распространения

с помощью поиска

Фильтр

Наименование м

Тип модели

IP

Выбрано

Тип модели

Политики

Добавить

Редактировать

Удалить

Копировать

Имя

Критичность

passwords_encrypted

Внимание

no_ip_http

Внимание

Редактор компаратора

Тип сравнения

Есть все

Строки

^service password-encryption
^enable secret .*

Отменить

Применить

Добавить компаратор

Добавить And блок

Добавить Or блок

Добавить Not блок

Авторасстановка

Загрузить из файла

Сохранить в файл

Подтвердить изменения

hasAll

hasNothing

AND

result

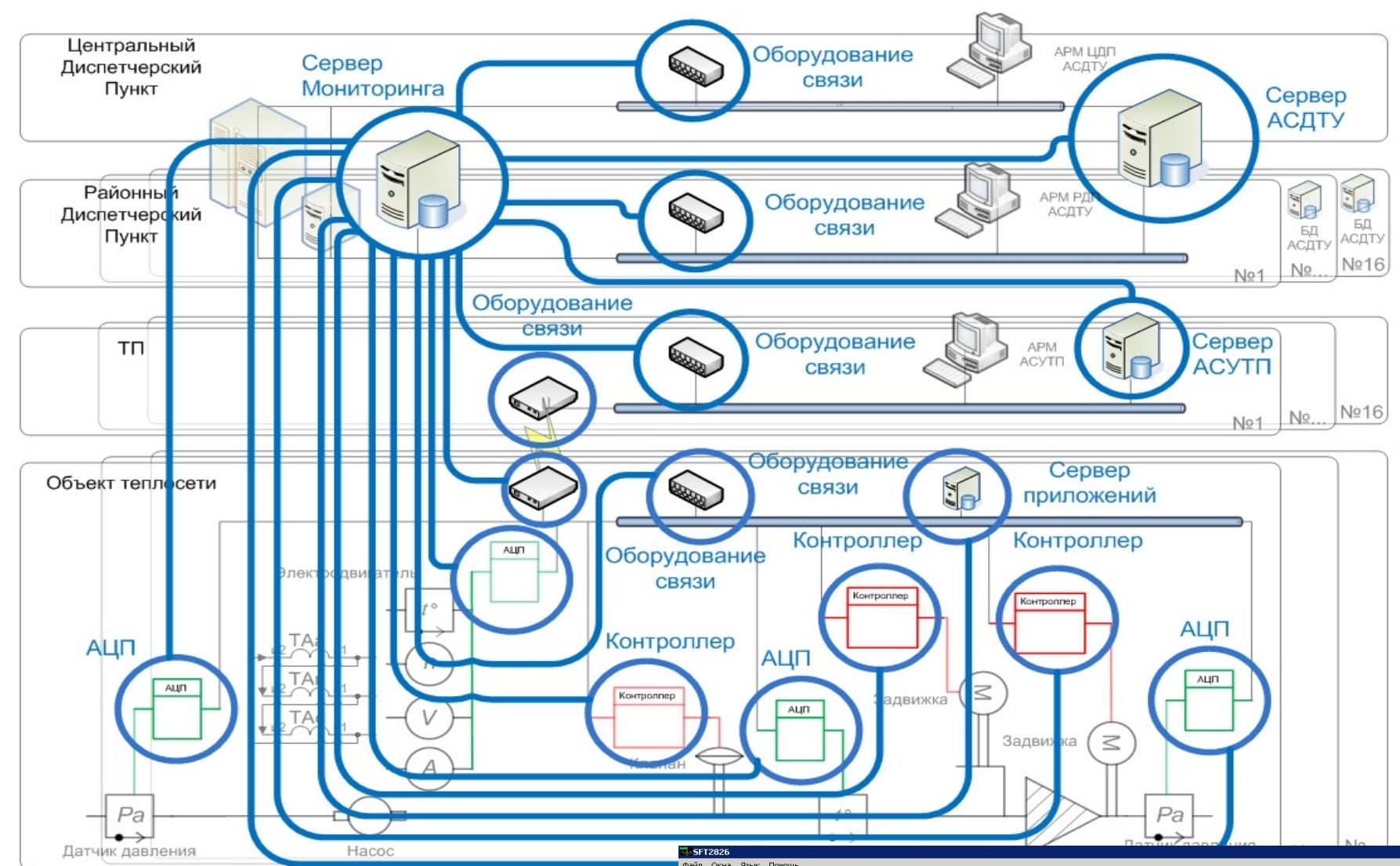
Технологическое оборудование и элементы АСУТП - проблематика

Сбор данных напрямую или от элемент-менеджеров (систем управления) компонент технологического сегмента:

- Контрольно-измерительные приборы
- Контроллеры (ПЛК)
 - Универсальные программируемые контроллеры
 - PC-совместимые контроллеры
 - Программируемые реле
- Рабочие станции пользователя (АРМ)
- Индустриальные стандарты: Modbus, DNP3, IEC 61850, TCP/IP
- Операционные Системы: стандартные плюс Tru64, WinNT, VMS и пр..
- Штатные системы управления и мониторинга: ABB 800xA, Symphony/Harmony, Infi90, Network Manager, FACTS, SYS600, MicroSCADA, Automsoft RAPID Historian, Emerson DeltaV and Emerson Ovation, Emerson/Westinghouse WDPF, GE XA/21, GE PowerOn Fusion, Foxboro I/A Series, Honeywell Experion, Itron OpenWay System, Rockwell RSView, Schneider/Telvent Oasys, Citect Momentum, Quantum, Siemens PCS7, Yokogawa Centrum CS 3000
- Повышенный жизненный цикл технологий (20 лет и более)
- Информационные системы должны работать в режиме реального времени, время отклика критично
- Наличие большого числа разнородного оборудования, разнородных (проприетарных) интерфейсов интеграции и методов съёма данных
- Большой поток сырых событий
- Информационная система должна функционировать в режиме 24x7
- Недопустимы задержки в работе сетевой инфраструктуры и оборудования
- Комбинированная сетевая инфраструктура – проводные технологии, радио доступ, спутниковая связь
- Изменения (патчи, обновления) должны быть тщательно протестированы перед установкой

Технологическое оборудование и элементы АСУТП – пример

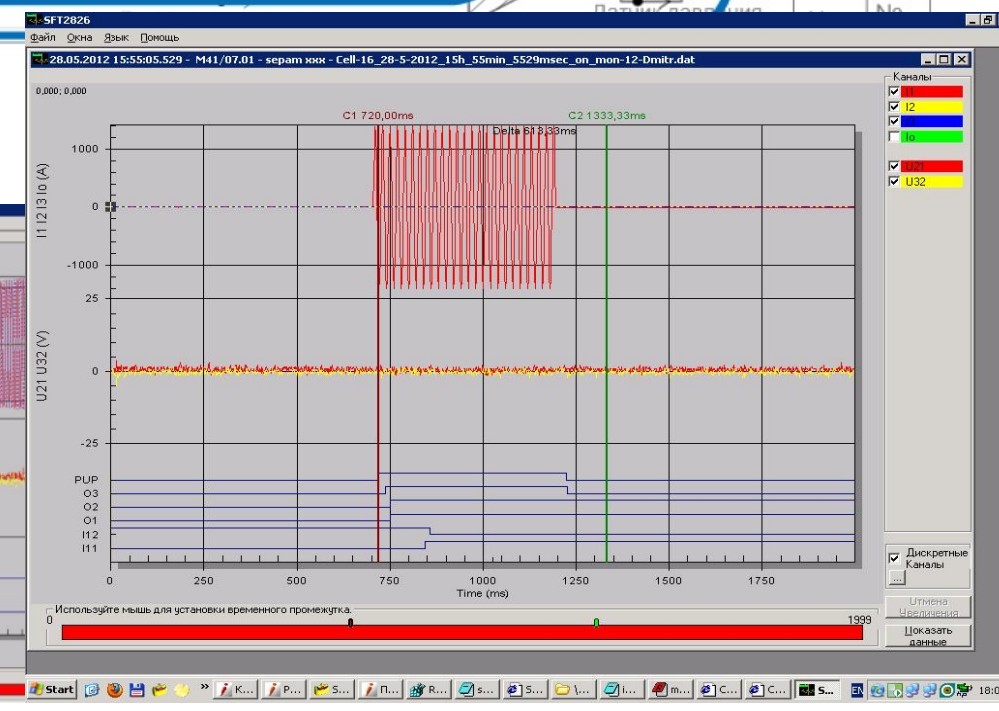
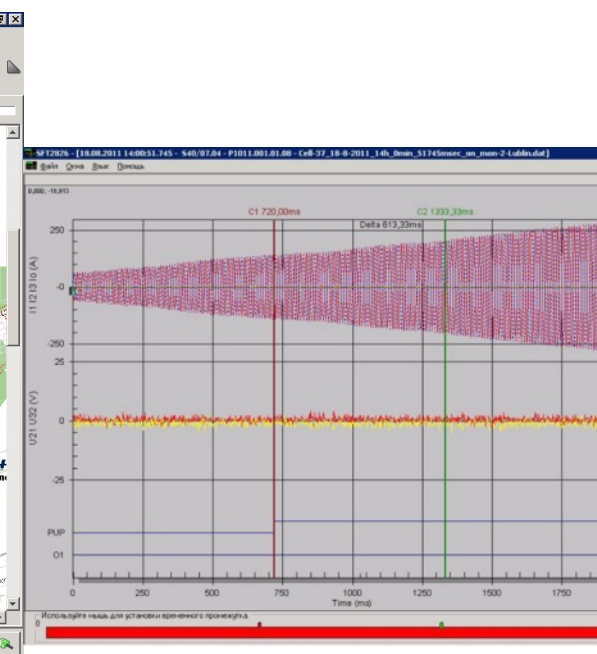
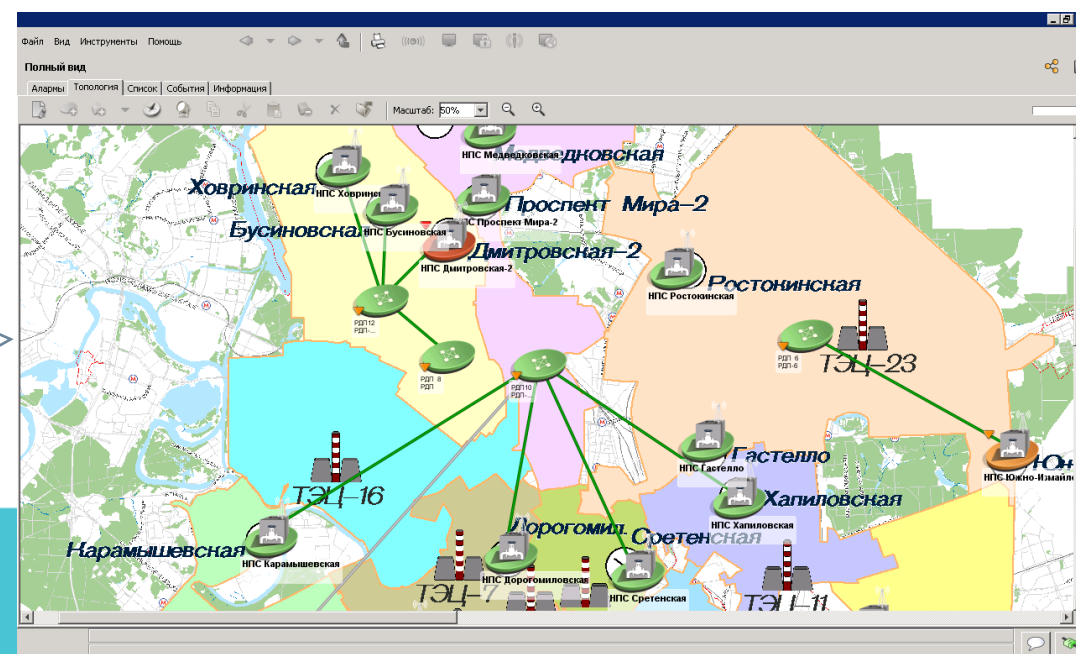
- Система мониторинга ИТ оборудования
- Штатные средства сетевой ИБ Cisco
- Сервера HP и ОС Windows, Linux, Unix
- Устройства защиты серии «Seram», производства компании «SCHNEIDER ELECTRIC». Предназначены для контроля и управления силовым электрооборудованием напряжением 6-10 кВ.
- Контроллеры серии «Freelance» производства компании «ABB». Предназначены для управления дросселирующими задвижками на магистральном трубопроводе подачи теплового носителя.
- Коммутаторы профессиональной мобильной радиосвязи «EADS TETRA» производства концерна «EADS».



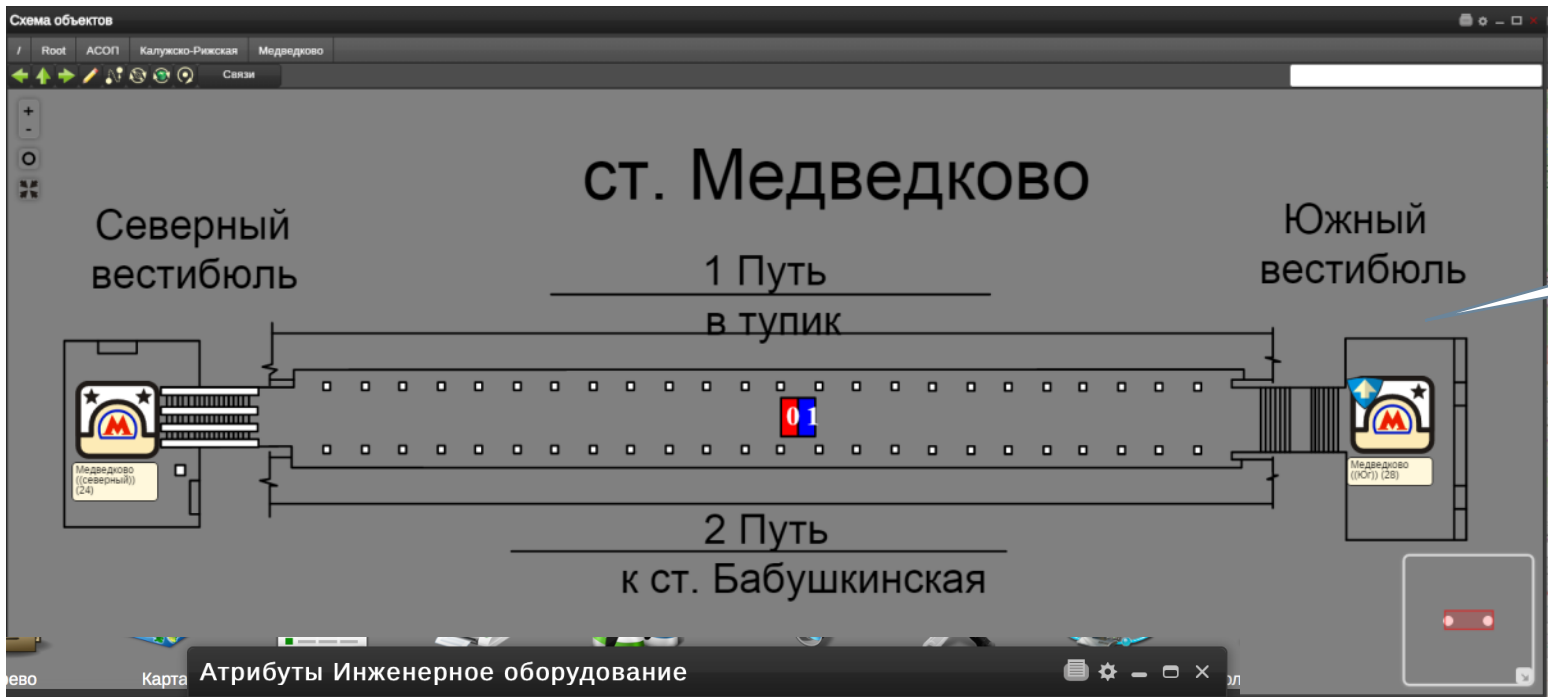
Зеленый - объект работает в штатном режиме.

Оранжевый - объект работает в предаварийном режиме, нештатная ситуация

Красный - на объекте критическая ситуация.



Технологическое оборудование и элементы АСУТП



Технологическое оборудование

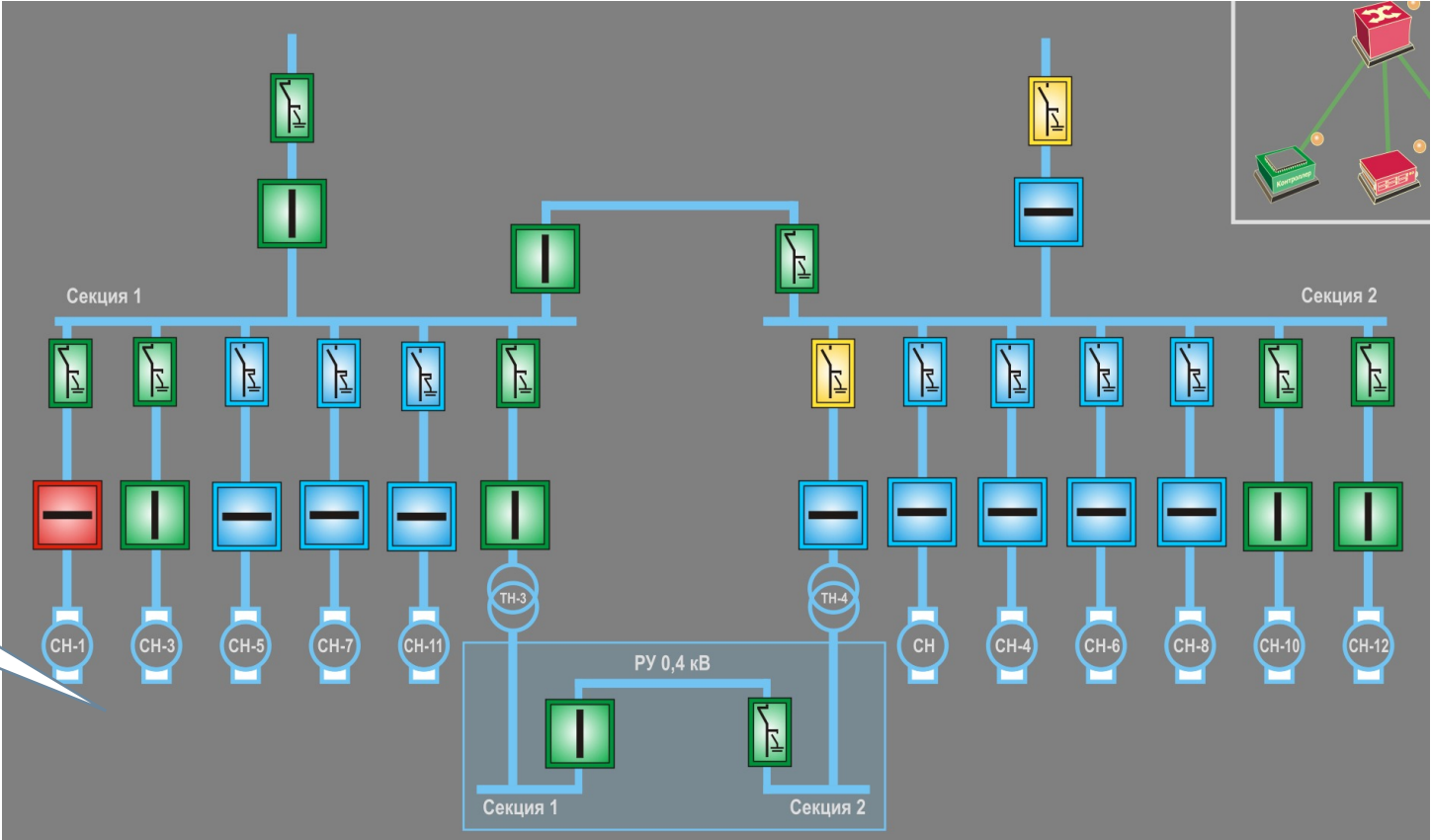
Объекты АСУТП – интерактивная мнемосхема

Атрибуты Инженерное оборудование

Имя	Значение
Установить отслеживание	
Сохранить значения	
Перетащите атрибут для отображения на графике	
Воздухообмен	0
Температура холодного коридора	0
Состояние объекта	Норма
Контакты	a.kolesnikov@initi.ru
Ток электропитания на фазе 1	0
Ток электропитания на фазе 2	0
Ток электропитания на фазе 3	0
Описание	Инженерное оборудование
Датчик открытия двери	
Воспламенение	
Температура горячего коридора	0
Влажность	0
Иконка	
Широта	55.718724
Долгота	37.629622
Имя	Инженерное оборудование
Наличие электропитания на фазе 1	
Наличие электропитания на фазе 2	
Наличие электропитания на фазе 3	
Состояние компонентов	Норма
Датчик дыма	
Напряжение электропитания на фазе 1	0
Напряжение электропитания на фазе 2	0
Напряжение электропитания на фазе 3	0
Датчик проникновения влаги	

Системы жизнеобеспечения ЦОД

Параметры работы ДГУ

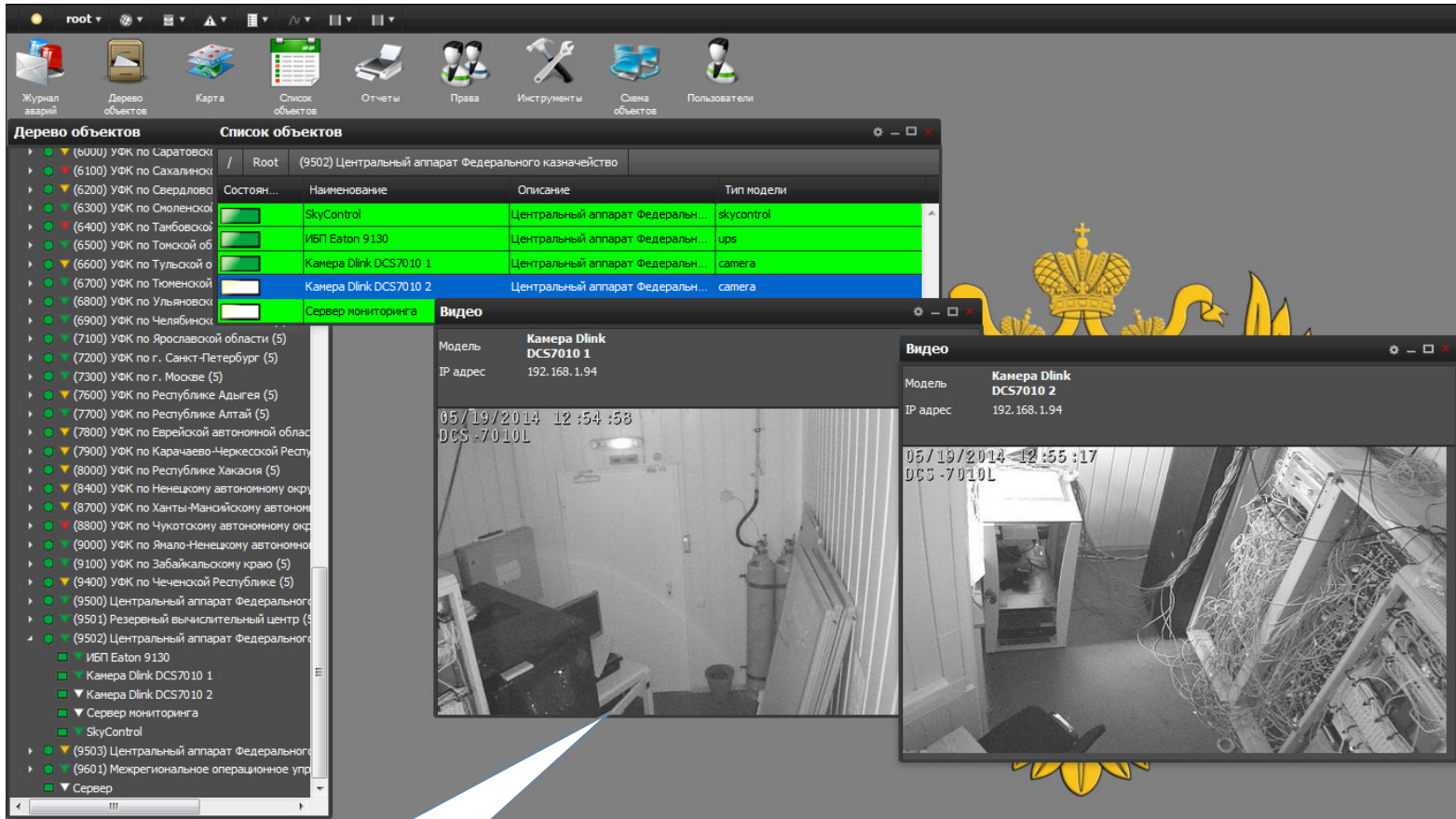


Просмотр деталей аварии

Имя	Значение
Заголовок	Генератор в работе
Имя модели	Архангельск Генератор в работе
IP-адрес	
Критичность	Внимание
Время начала	2015-11-24 14:23:32.001400 (GMT+3)
Последнее изменение	2015-11-24 14:23:32.003337 (GMT+3)
Время очистки	
Длительность	
Принято в работу	
Тип	atCustomAlarm
Причина	
Количество	1
Адрес модели	m,mm,defaultCollectorGroup-rid,2400-gen
Тип модели	powergen



Интеграция с подсистемами ИБ

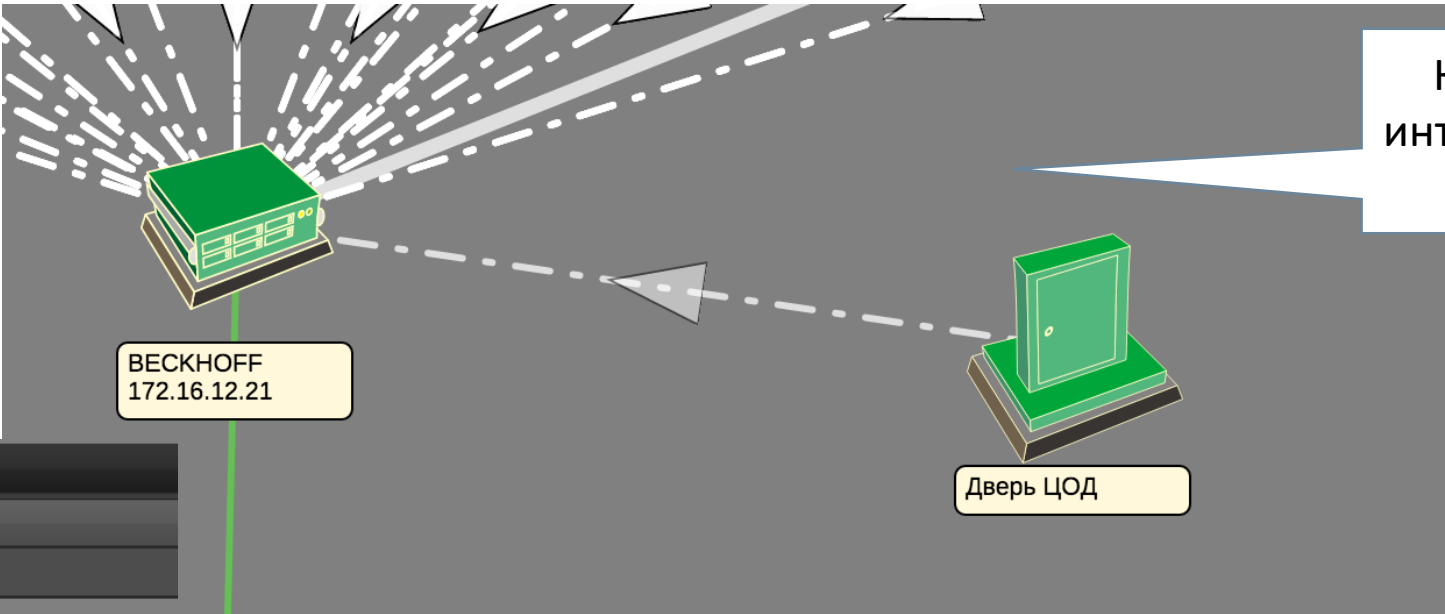


Визуальный контроль
объекта

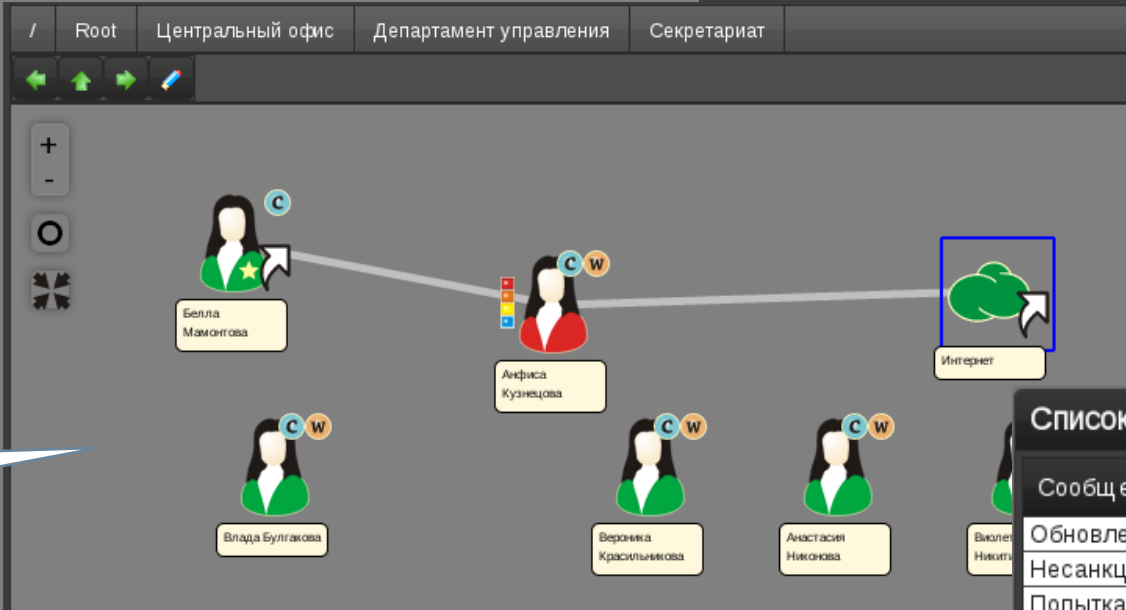
Интеграция с DLP –
трекинг email

Сообщение	Время создания
Обновление аларма типа atPossibleLeakViaEmail: Возможная утечка д...	06.02.2015 18:00:52 GMT+3
Пользователь Анфиса Кузнецова отправил конфиденциальное письмо ...	06.02.2015 18:00:52 GMT+3
Пользователь Анфиса Кузнецова отправил адресату rasteryaev@list.ru ...	06.02.2015 18:00:52 GMT+3
Создана модель Анфиса Кузнецова типа ModelType[employeeF]. Adresse...	06.02.2015 17:56:34 GMT+3

Интеграция с DLP –
контроль утечки
конфиденциальных
данных



Контроль доступа –
интеграция с системами
СКУД



Кореляция данных
событий от нескольких
внешних ИБ систем

Сообщение	Время создания
Обновление аларма типа atPossibleIntrusionARMOutside: Несанкционированное проникновение в здание! Пользователь ...	06.02.2015 17:41:06 GMT+3
Несанкционированное проникновение в здание! Пользователь Пушков Павел не в здании, но авторизован в APM	06.02.2015 17:41:06 GMT+3
Попытка пользователя Пушков Павел авторизоваться в системе APM. Успешность: true	06.02.2015 17:41:06 GMT+3
Начало нового дня	06.02.2015 17:41:05 GMT+3
Создана модель Пушков Павел типа ModelType[employee]. Address = Address["m". "mm". "g". "p.pushkov"]	06.02.2015 17:22:15 GMT+3

СПАСИБО!



ИНИТИ