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 третьестороньего коммерческого ПО
- Подтверждённая база заказчиков в РФ и за рубежом
- Наличие локальной партнёрской базы
- Решение используется рядом ведущих иностранных производителей


СИСТЕМА СЕРТИФИКАЦИИ В ОБЛАСТИ СВЯЗИ

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер: ОС-1-СУ-0434

Срок действия: с 07 июля 2015 г. до 07 июля 2018 г.


РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2015611965

Система обработки, корреляции и отображения событий «ИНИТИ СОЛО», версия 1.5.0 (INITI SOLO v 1.5.0)

Правообладатель: Общество с ограниченной ответственностью «ИНИТИ» (RU)

Авторы: Не указаны

Заявка № 2014663719

Дата поступления 25 декабря 2014 г.

Дата государственной регистрации в Реестре программ для ЭВМ 10 февраля 2015 г.


СИСТЕМА ДОБРОВОЛЬНОЙ СЕРТИФИКАЦИИ «Российский Технологический Стандарт»

Орган по сертификации ООО «РосТехСтандарт»

СЕРТИФИКАТ СООТВЕТСТВИЯ

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

СООТВЕТСТВУЕТ ТРЕБОВАНИЯМ ГОСТ ISO 9001-2011 (ISO 9001:2008)

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

Ростелеком
Газпром нефть
Bashtel
МРСК СИБИРИ
ТИС
СПУТНИКОВАЯ СВЯЗЬ
ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО СНГ СУРГУТНЕФТЕГАЗ
zain
МОЭК
БАШНЕФТЬ
TURKCELL
АЛРОСА
МГТС
РОССЕТИ
Московский Транспорт
ЦОДД
ГАЗПРОМБАНК
РОСНАНО
Российские железные дороги
EMC²
Федеральное казначейство
ZRAČNA LUKA DUBROVNIK
DUBROVNIK AIRPORT
IBM
НАЦИОНАЛЬНЫЙ БАНК РЕСПУБЛИКИ БЕЛАРУСЬ
РОСАТОМ
Т-ХЕЛПЕР
оборудование и системы радиосвязи
NAUMEN
2TEST
RID

Инити

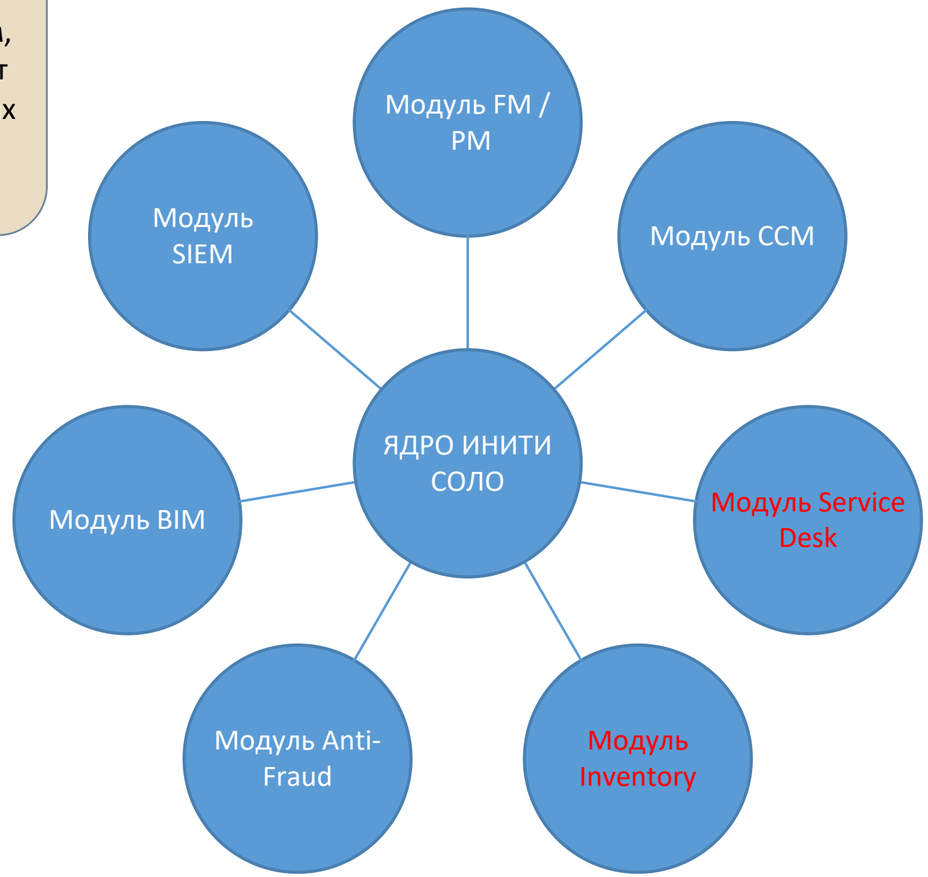
Какие процессы автоматизируем

Мониторинг

Управление событиями

Наблюдение за состоянием, данное понятие является более широким, чем управление событиями. Например, средства контроля проверяют состояние устройства на предмет его функционирования в допустимых пределах, даже если это устройство не генерирует никаких событий.

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



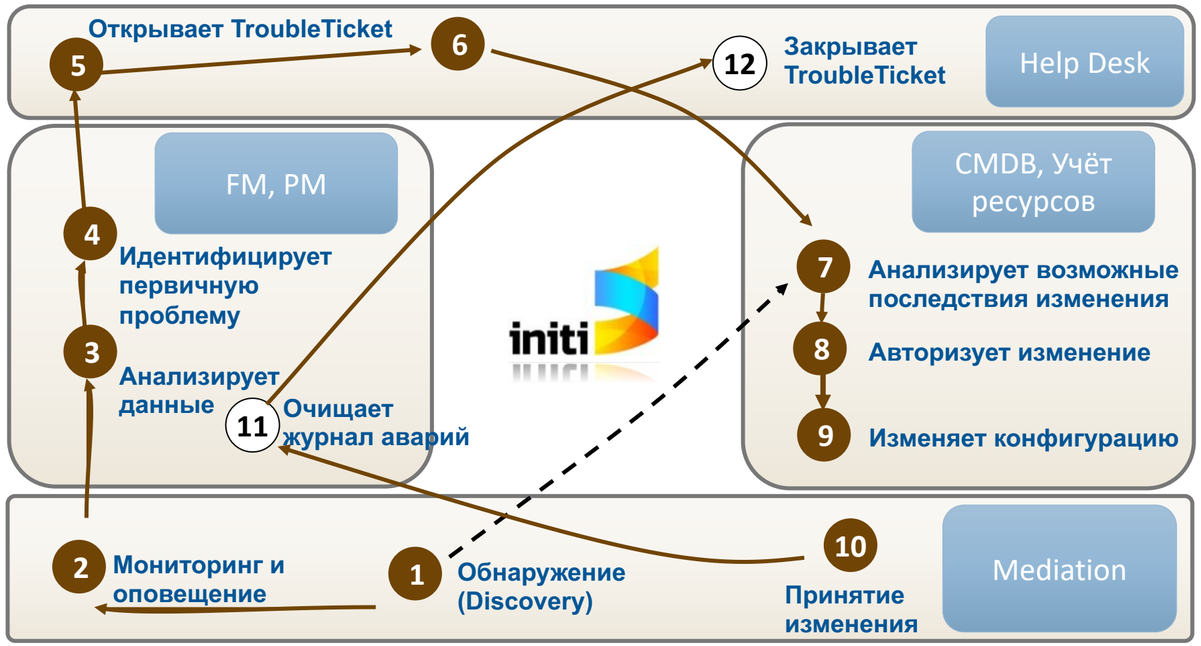
•Независимое ядро системы (зарегистрировано отдельно)
•Модуль мониторинга / сбора и анализа производительности
•Модуль контроля конфигураций оборудования
•Модуль оценки негативного влияния сбоя на бизнес-процессы
•Модуль Anti-Fraud
•Модуль SIEM

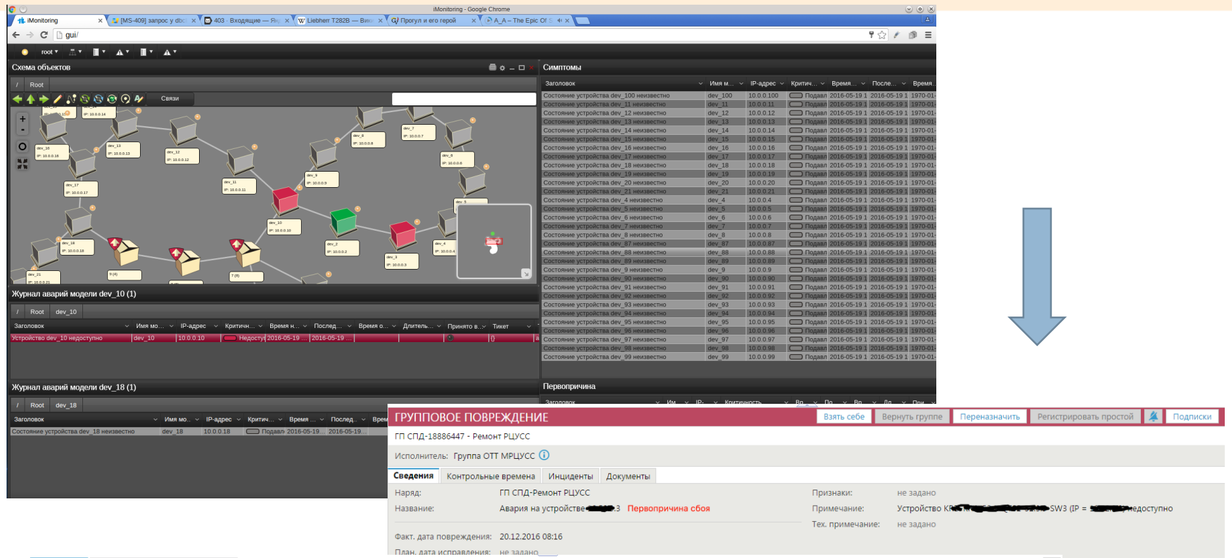
В разработке:

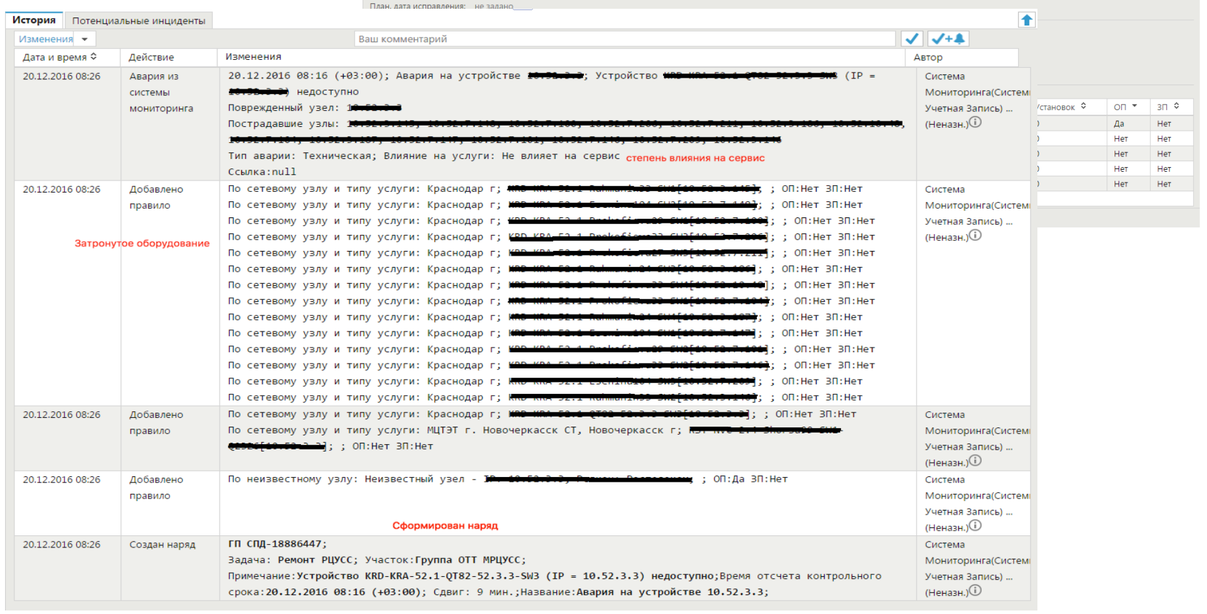
- Модуль Service-Desk (на данный момент используется ядро Naumen Service Desk)
- Модуль Inventory (на данный момент используется ядро Naumen Inventory)

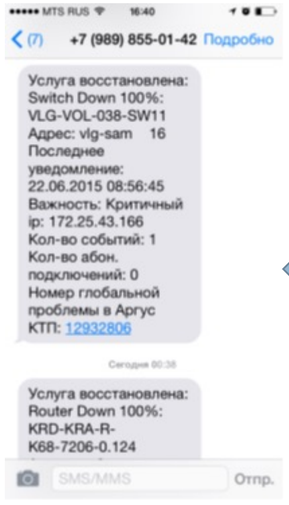
Инити

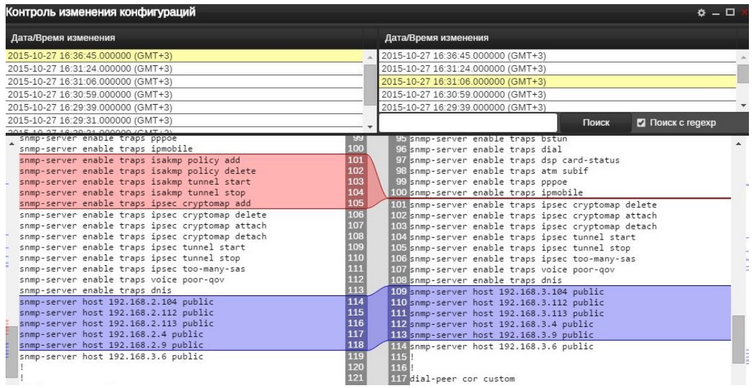
Цель – замкнутый цикл автоматизации











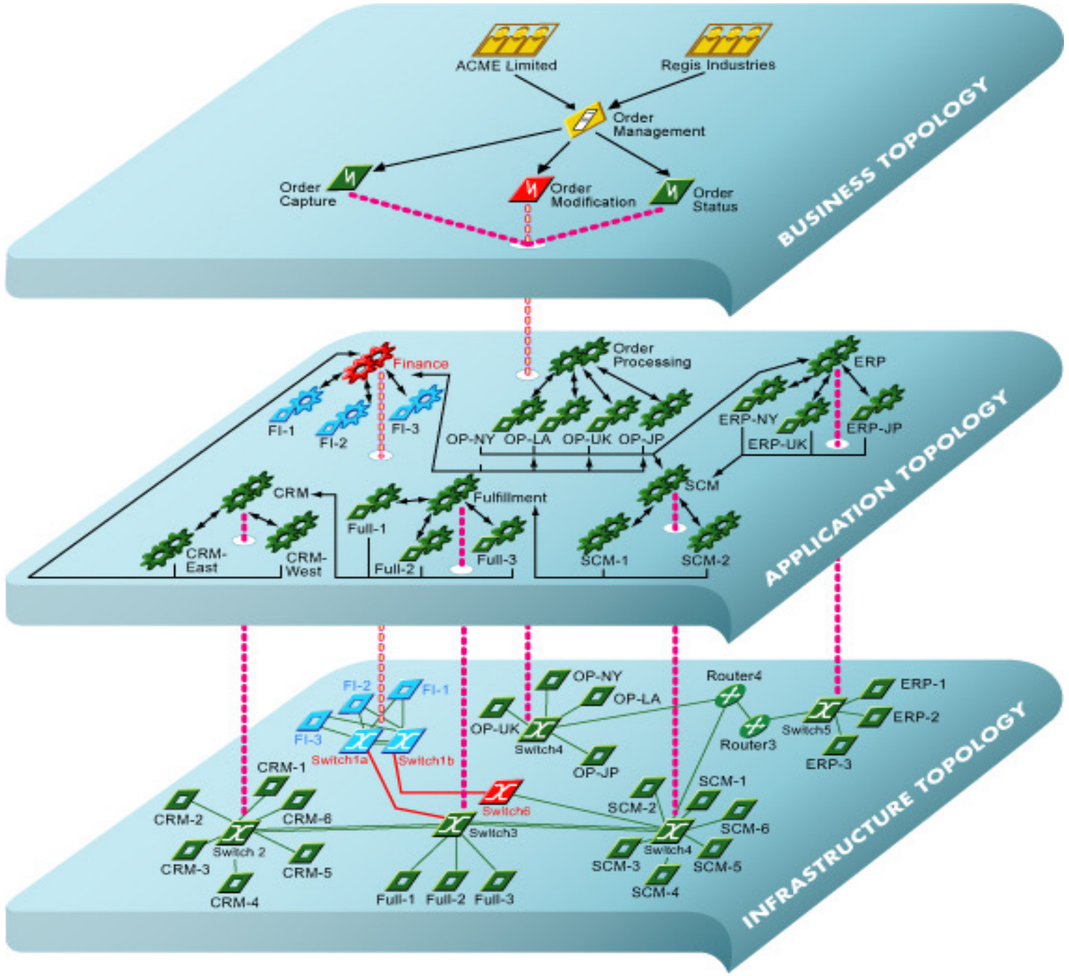
Сквозной мониторинг недоступности сервиса

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



Инити

От проблемы в инфраструктуре к сервису

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

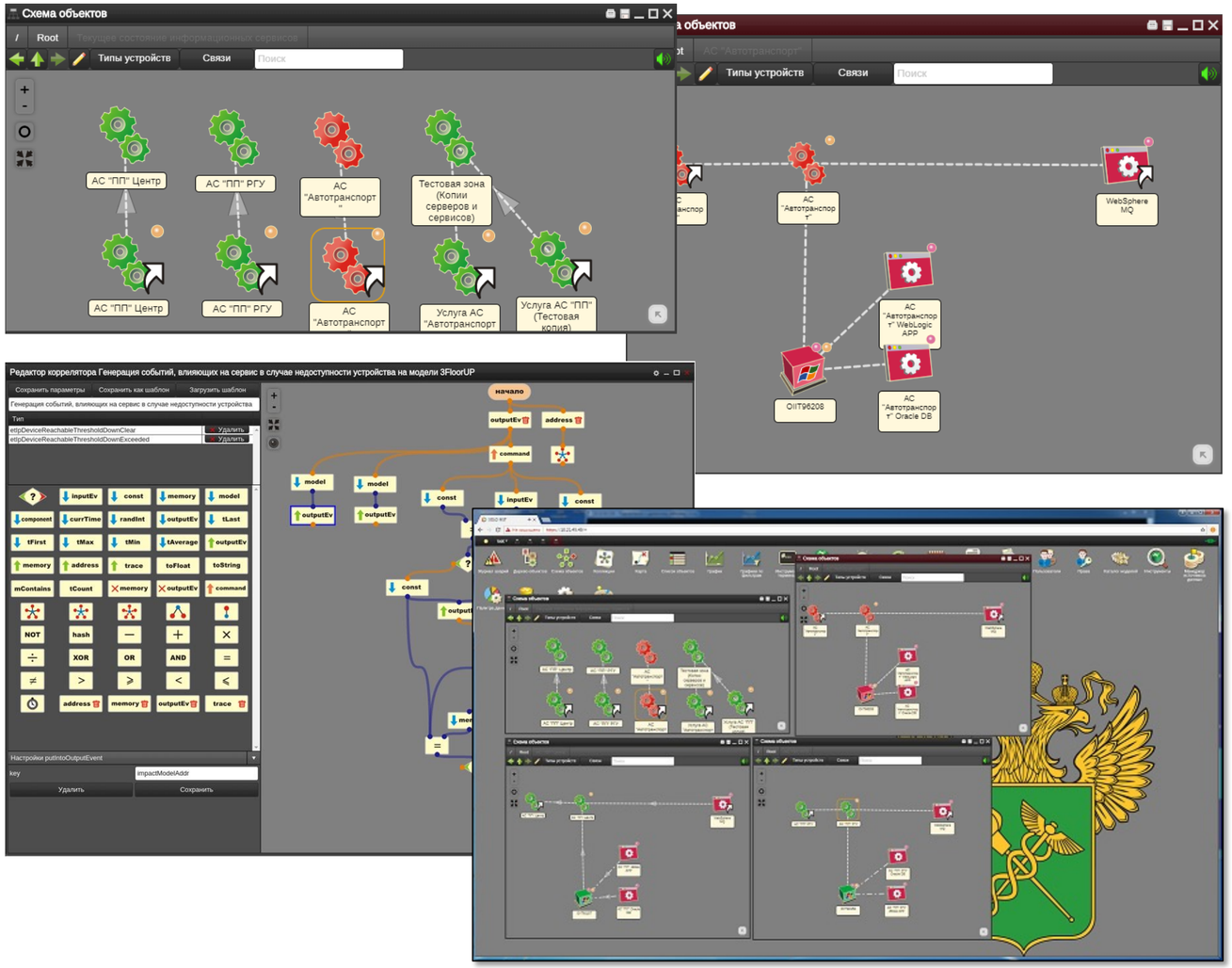
- Сокращение времени на выявление затронутых аварией сервисов
- Оперативное уведомление ответственных за эксплуатацию аварийных объектов лиц, при аварии на сервисе или при приближении к пороговым значениям прогноза аварийных ситуаций

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

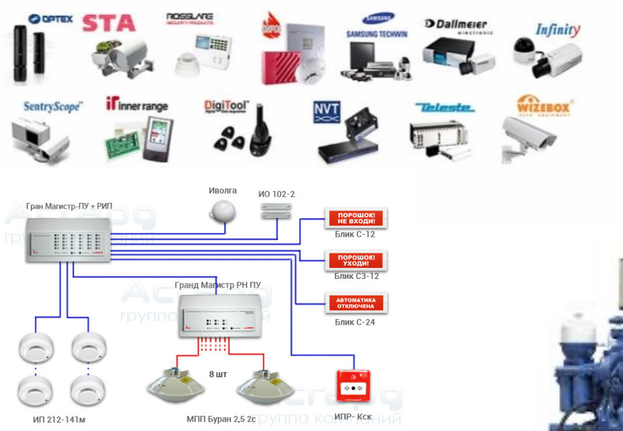


Инити

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..



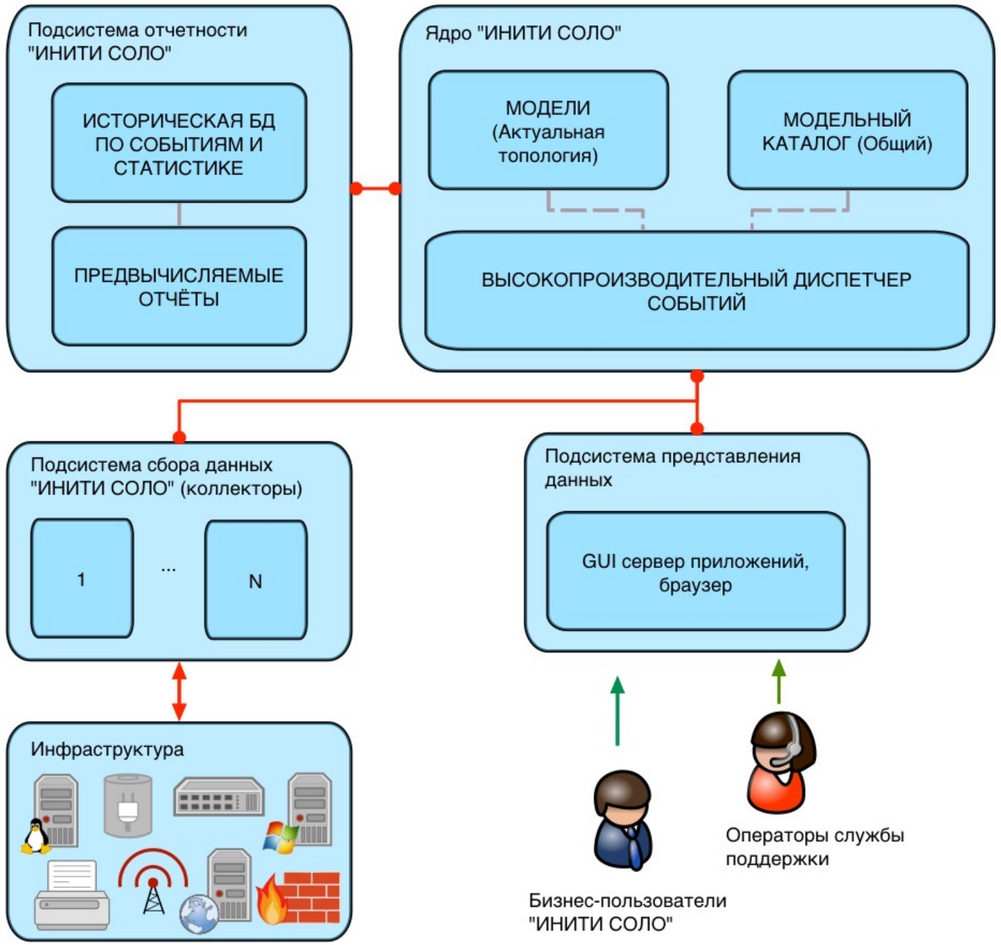
Консолидация данных:

- 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?

Инити

Техническая информация

Структура “ИНИТИ СОЛО”

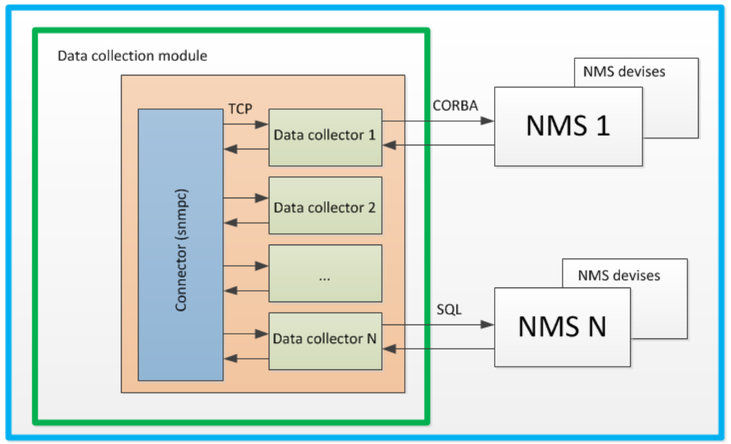


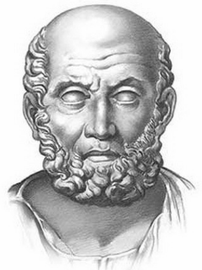
- Уровень сбора данных (Коллекторы)
- Уровень нормализации данных (Диспечер событий)
- Ядро системы (Core):
  - Модельный каталог
  - Модель инфраструктуры
  - Обработка событий
- Уровень представления (GUI)
- Высокая производительность ядра (10000+ EPS)
- Реализация отказоустойчивой и распределённой “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
- Перифирийное 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

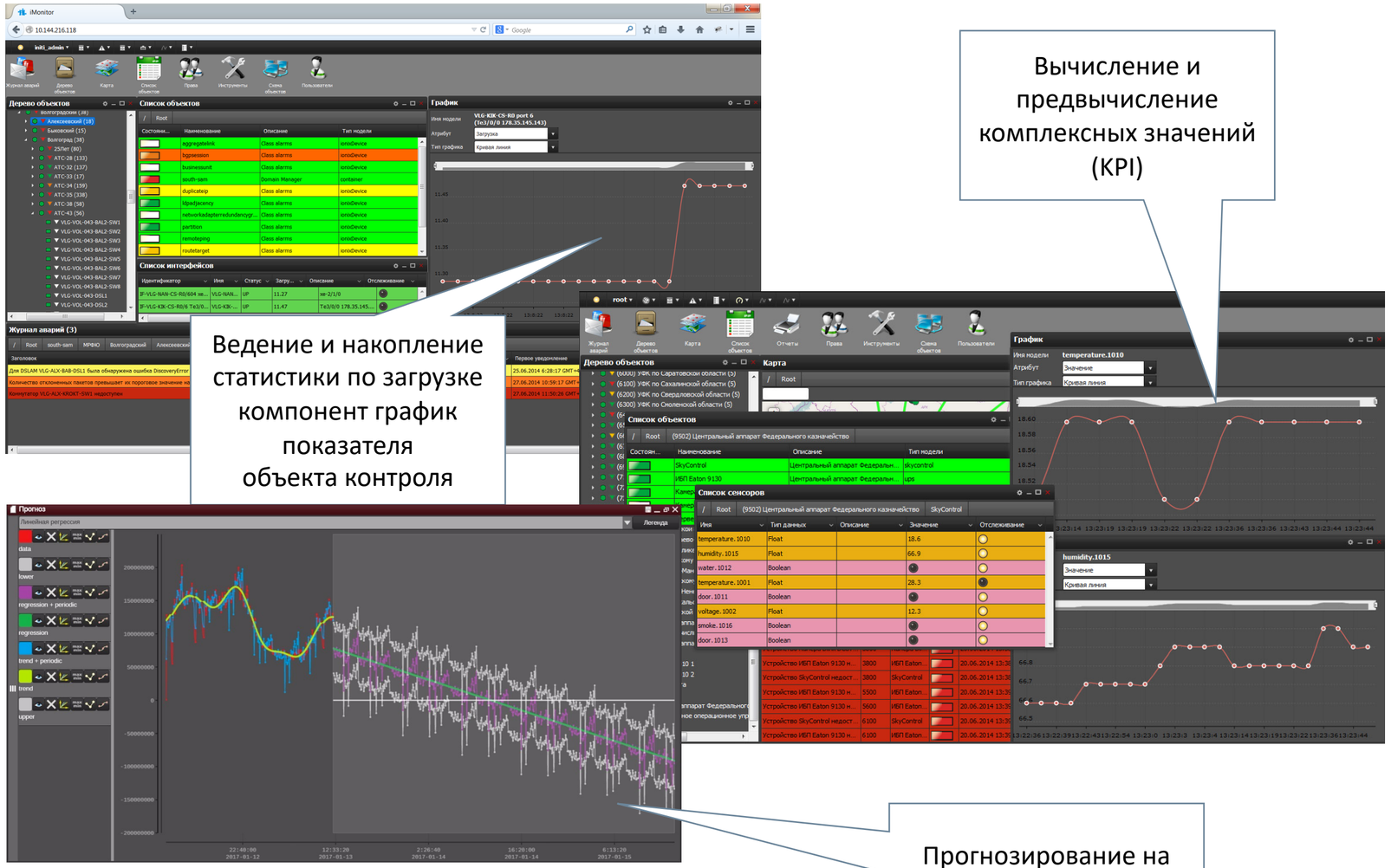
Инити

Мониторинг и сбор данных

Система работает в двух режимах:

- Активный опрос
- Сбор и анализ “сырых” событий

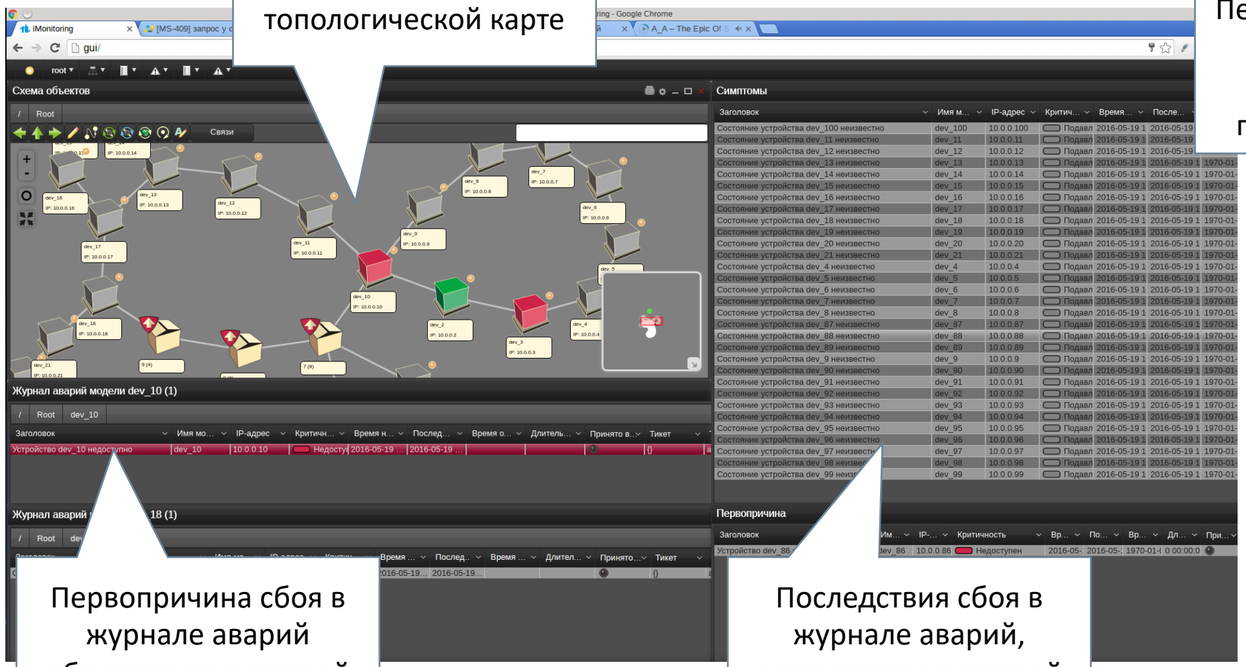
НЕКОТОРЫЕ ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ	
CORBA	**SNMP**
DB Link	**TELNET**
FTP	**TMF**
HTTP-HTTPS	**Vendor API (Java, Perl, …)**
LOG	**WebServices**
OPC	**WMI**
SMB	**XML**
Modbus	**Netbus**
***Flow**	**TS 32.432**
TS 32.435	**И многое другое…**



Инити

Интеллектуальный поиск первопричины сбоя (RCA)

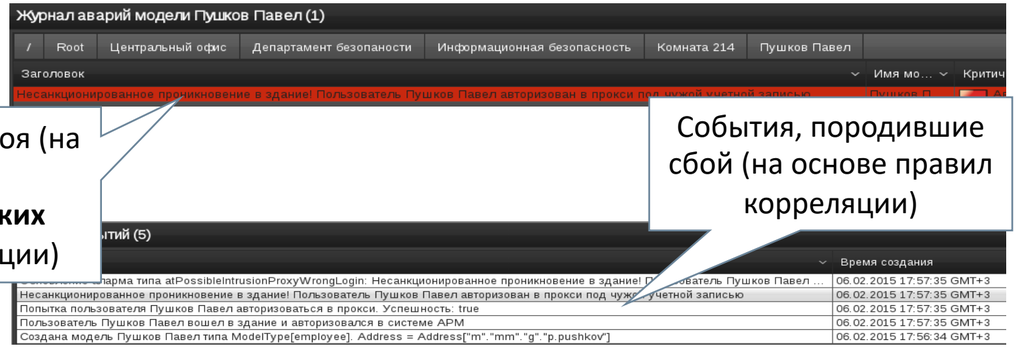
- **Автоматическая корреляция** (на основе встроенных математических методов)
- Возможность создания **собственных правил** корреляции.



Первопричина сбоя на топологической карте

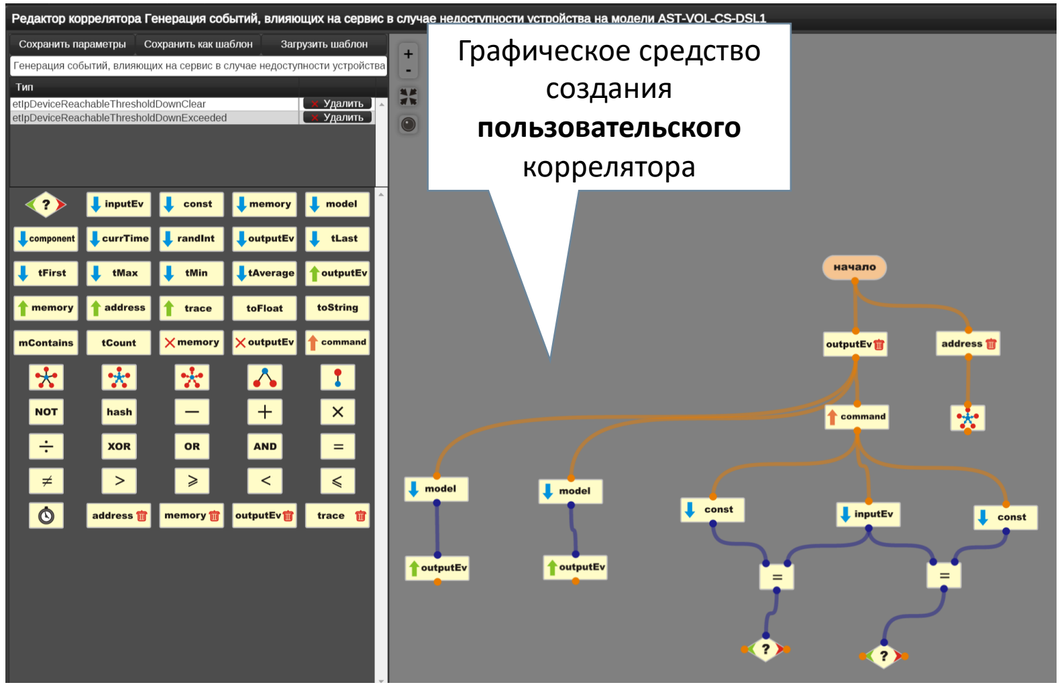
Первопричина сбоя в журнале аварий обнаружена системой **автоматически**

Последствия сбоя в журнале аварий, определены системой **автоматически**



Первопричина сбоя (на основе **пользовательских** правил корреляции)

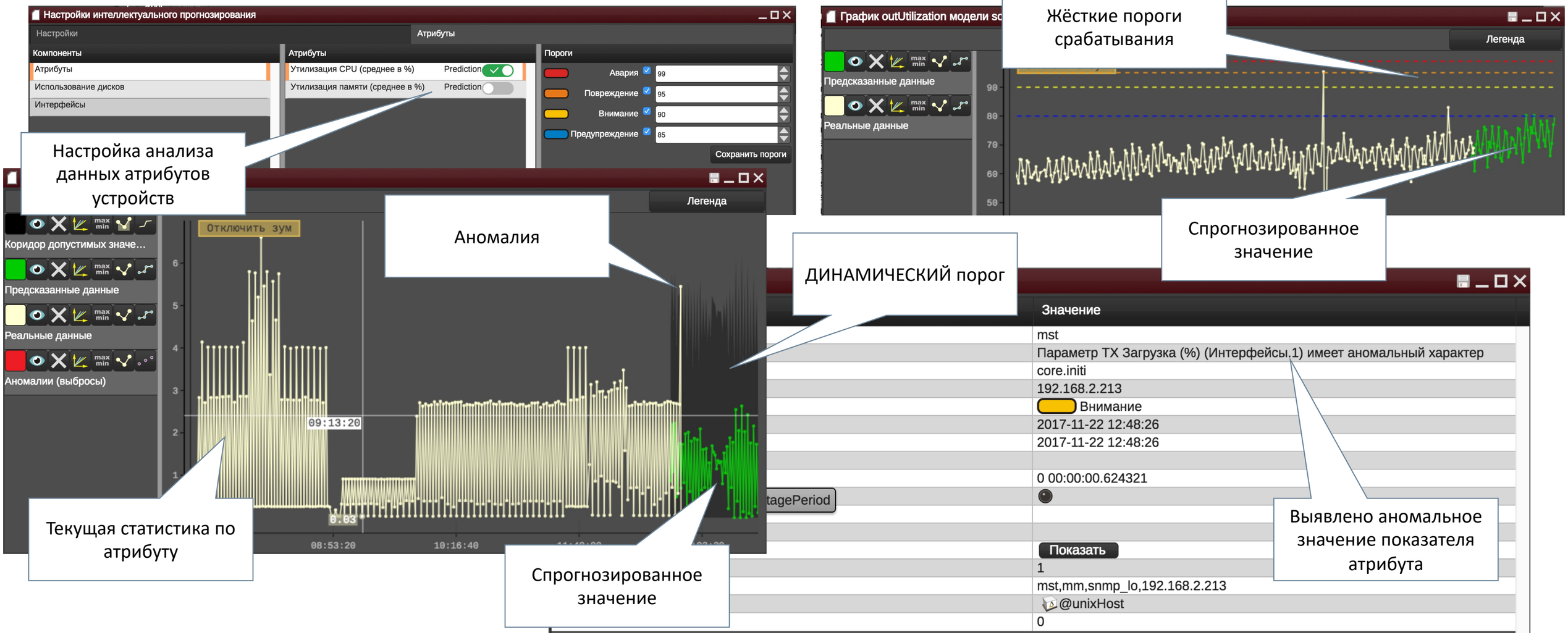
События, породившие сбой (на основе правил корреляции)



Графическое средство создания **пользовательского** коррелятора

Инити

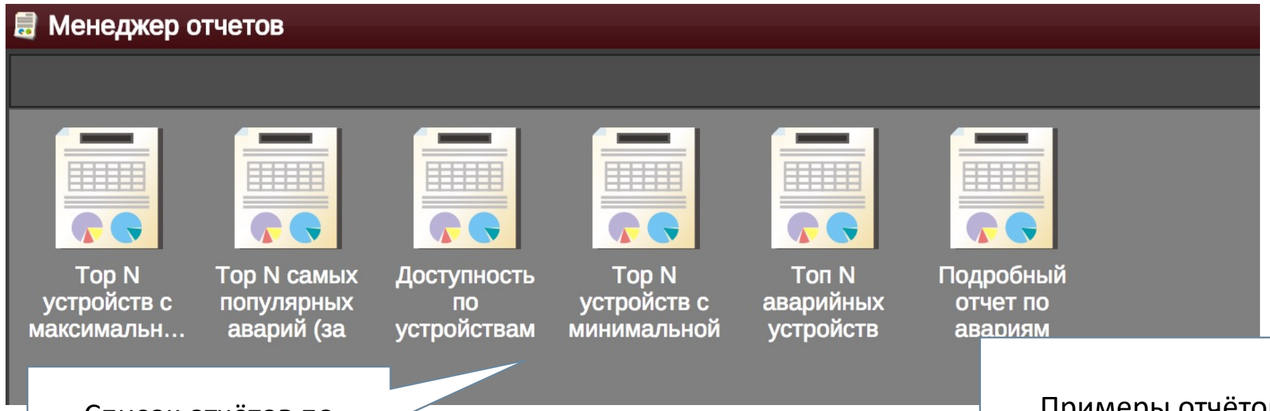
Интеллектуальный анализ данных, выявление **аномалий**



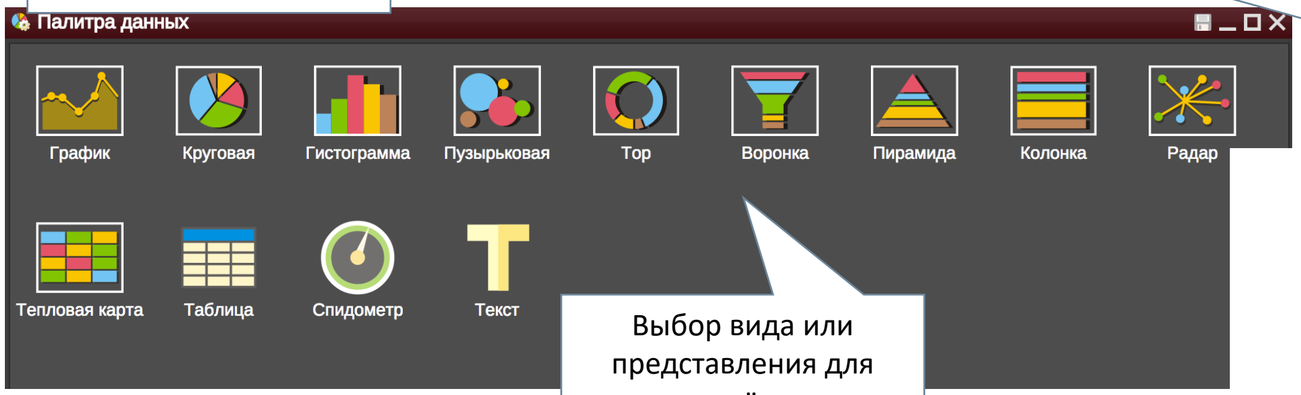
Инити

Конструктор отчётов, подсистема отчётности

Система имеет гибкий графический конструктор отчётов

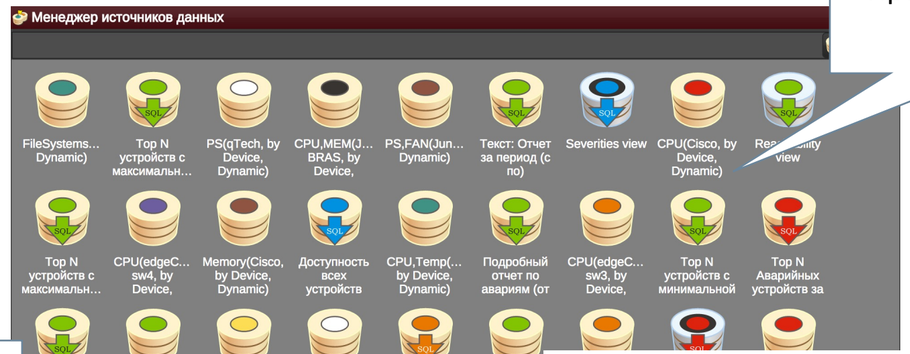


Список отчётов по запросу



Выбор вида или представления для отчёта

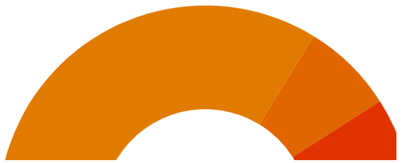
Примеры отчётов



Предрасчитываемые данные

Top N используемых интерфейсов

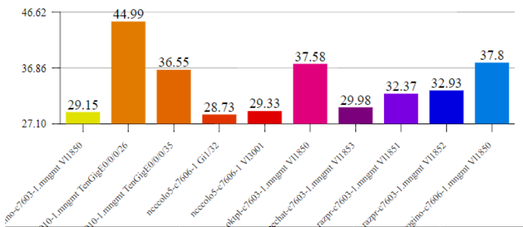
Инвентарный состав



Аварии по критичности за ден

Отчет по устройству(ам) за период с 2017-11-05 17:40:14 по 2017-1

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

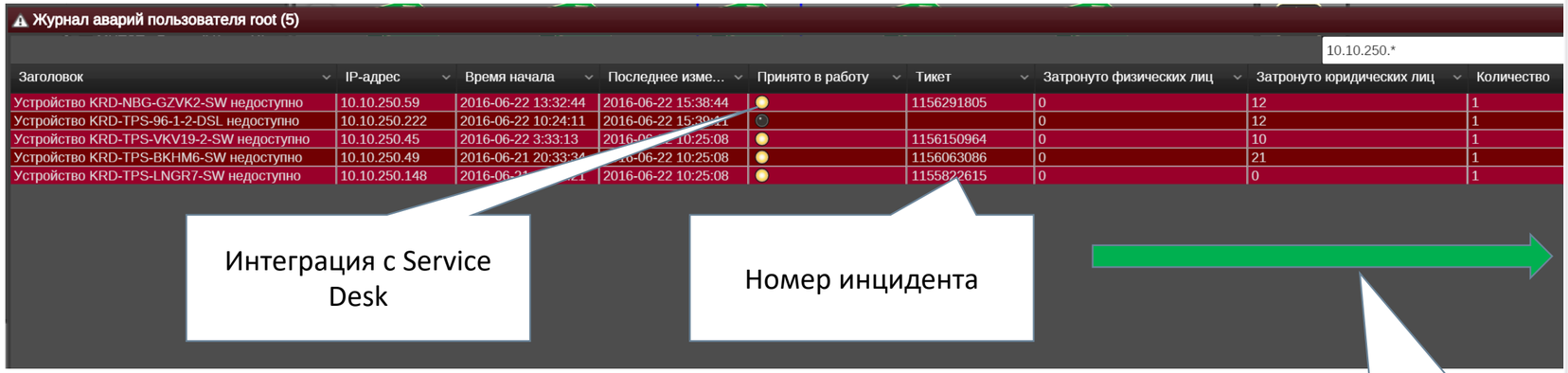


Устройство	Имя интерфейса	Alias	Тип интерфейса	Скорость интерфейса	Используемость (%)
lubyan-c7603-1.mngmt	Te1/1	Sncc-asr9010-1:TenGigE0/0/0/26$		10000000000	47.77
ncc-asr9010-1.mngmt	TenGigE0/0/0/26	$lubyan-c7603-1:TenGigabitEthernet1/1$		10000000000	44.99
strogino-c7606-1.mngmt	Vl1850	17/1592, ISVN MosMetro, 300M, VRF		1000000	37.8

Инити

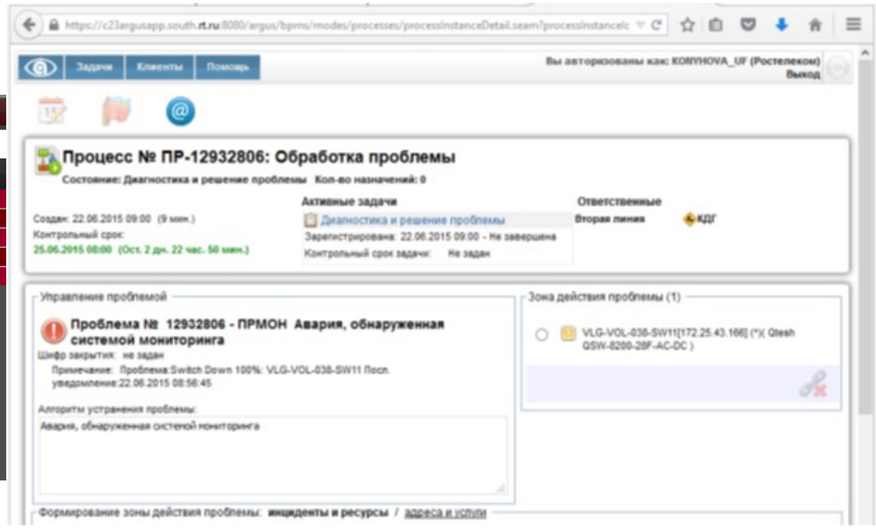
Интеграция с внешними OSS/BSS системами

Система обладает документированным открытым API



Интеграция с Service Desk

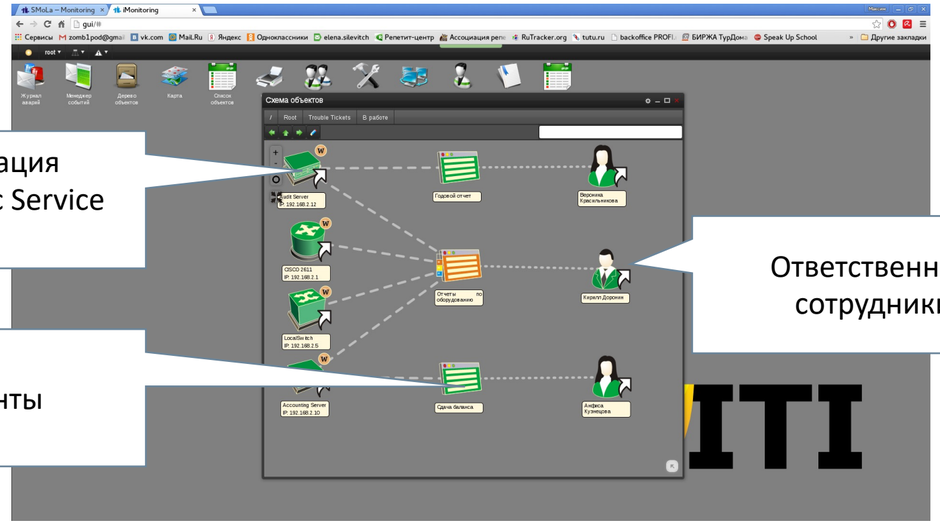
Номер инцидента



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

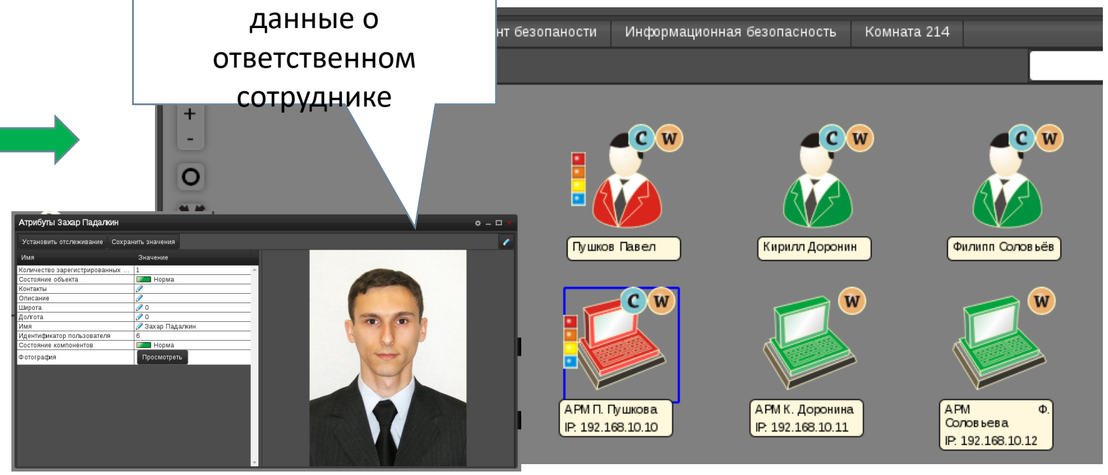
Визуализация интеграции с Service Desk

Инциденты



Ответственные сотрудники

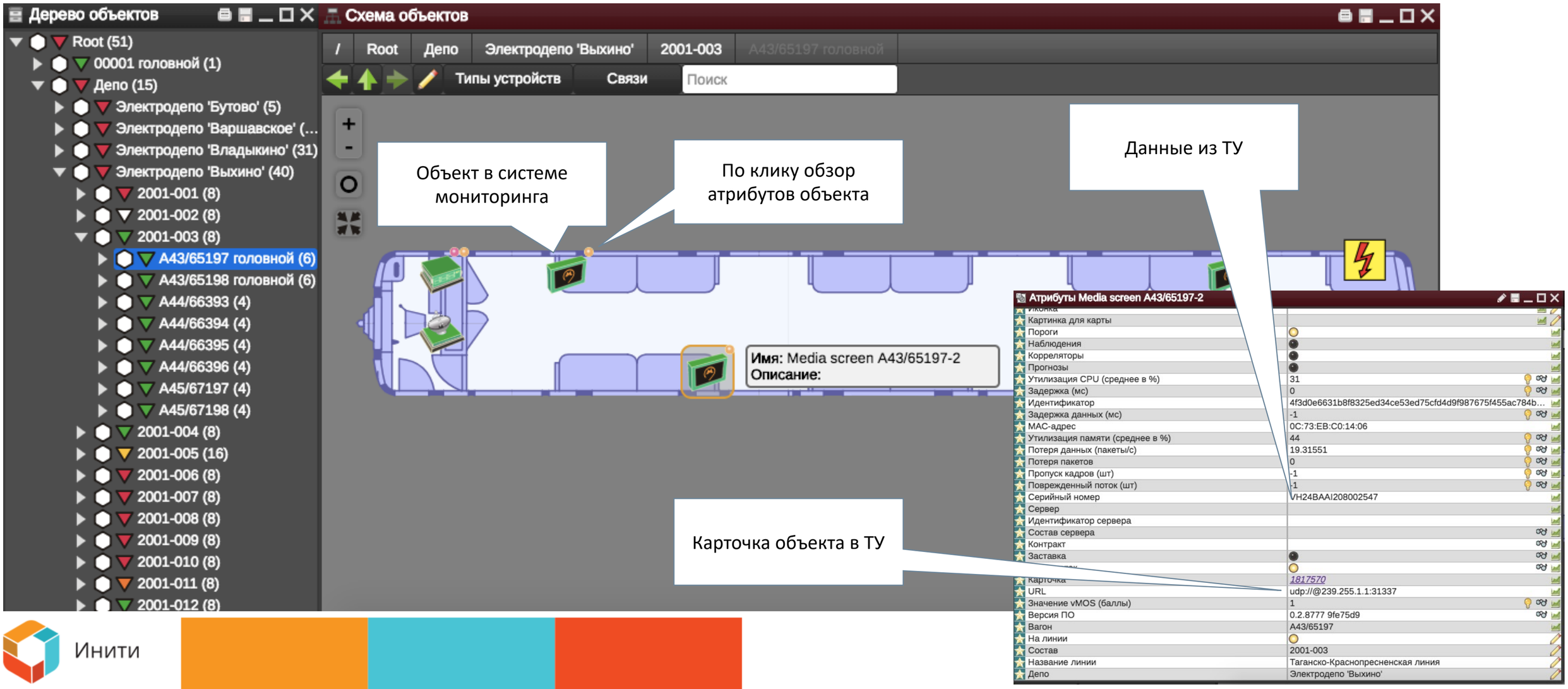
По клику переход – данные о ответственном сотруднике



Инити

Интеграция с внешними OSS/BSS системами – пример Naumen

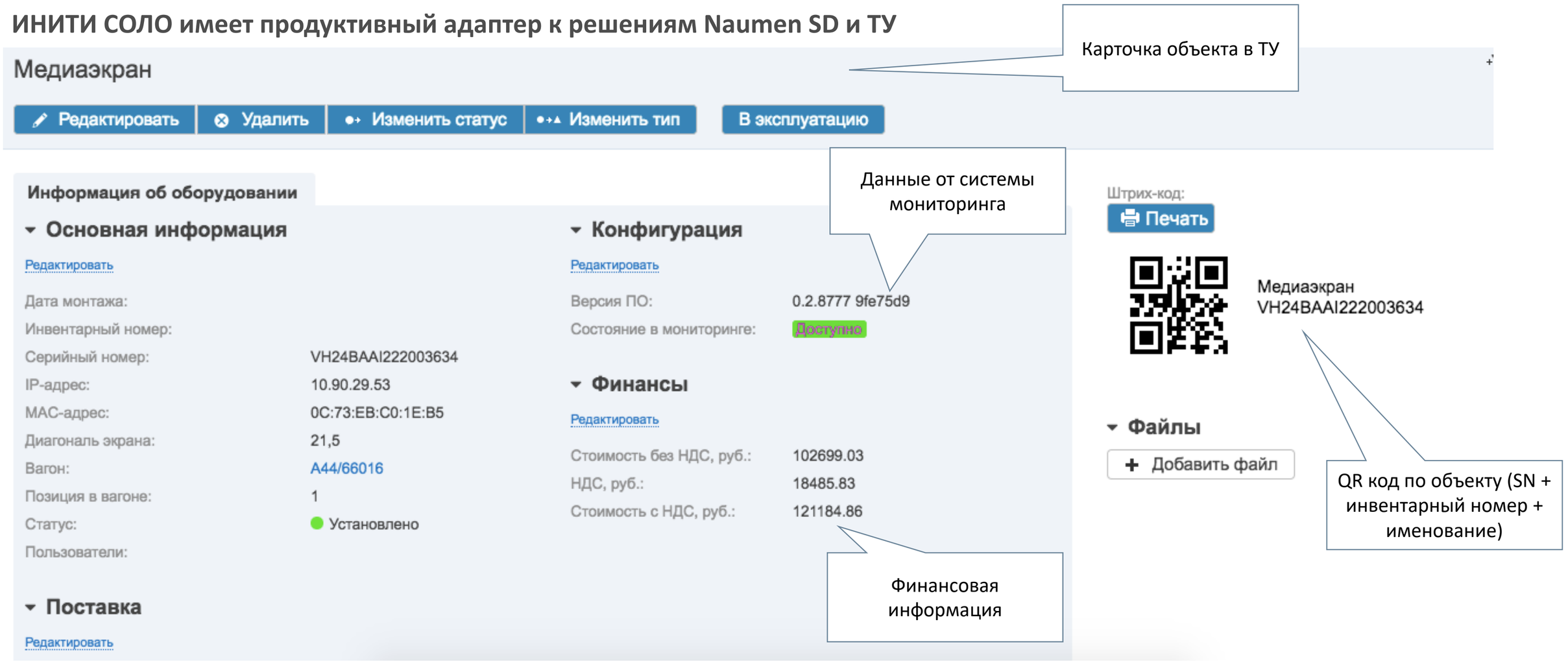
ИНИТИ СОЛО имеет продуктивный адаптер к решениям Naumen SD и ТУ



Инити

Интеграция с внешними OSS/BSS системами – пример Naumen

ИНИТИ СОЛО имеет продуктивный адаптер к решениям Naumen SD и ТУ



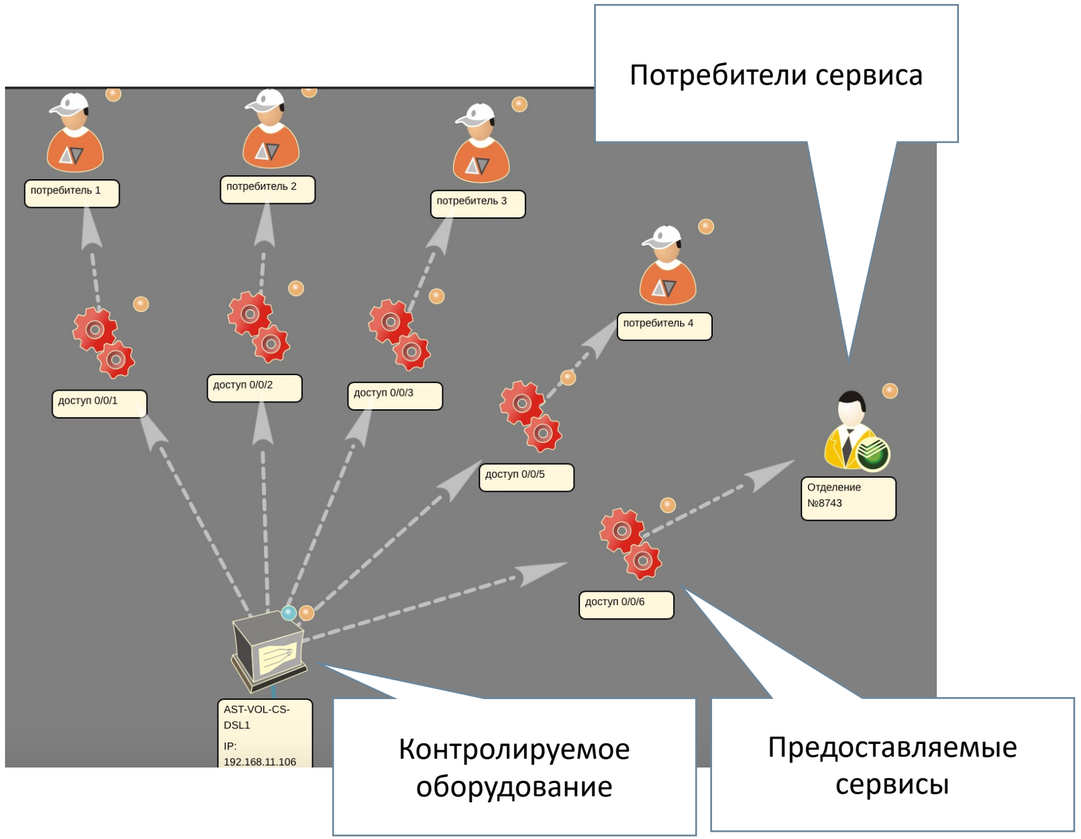
Инити

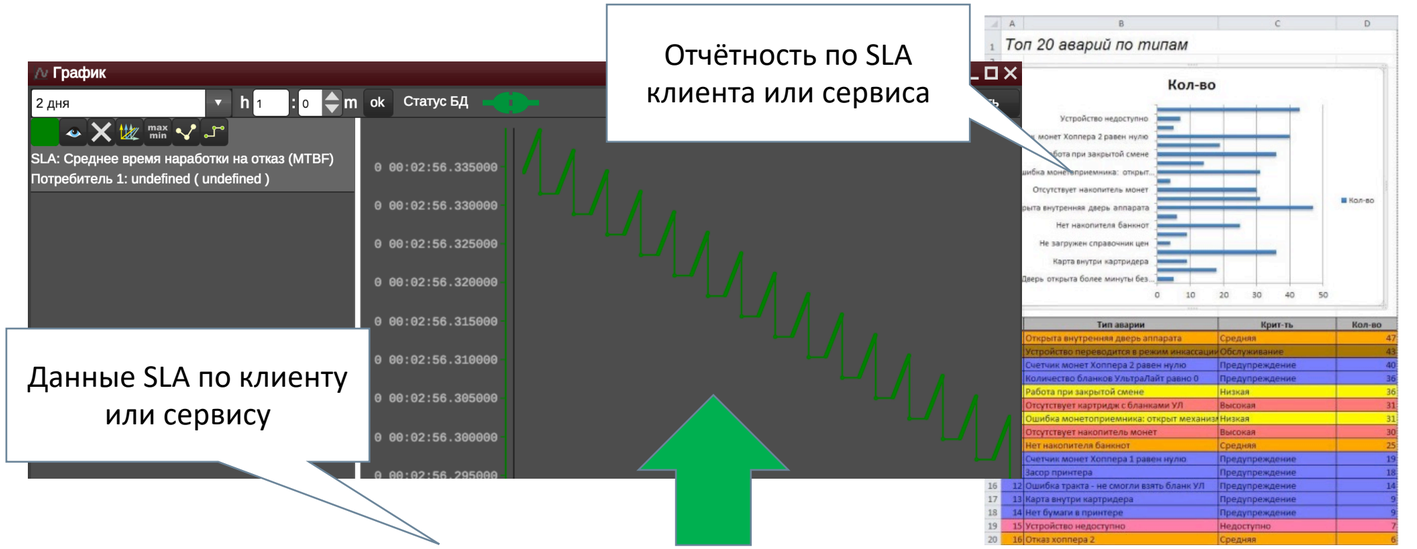
Интеграция с внешними OSS/BSS системами – пример Naumen

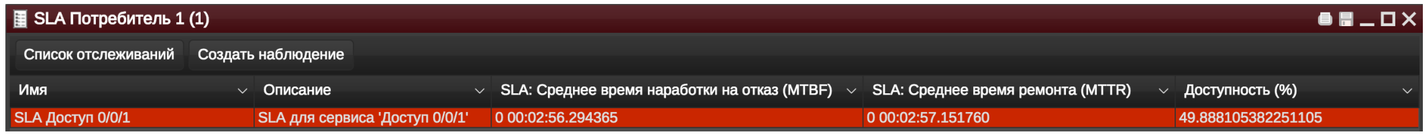
ИНИТИ СОЛО имеет продуктивный адаптер к решениям Naumen SD и ТУ

Сервисно-ресурсная модель

Контроль сервисов, предоставляемых внешним или внутренним пользователям, Контроль подрядчиков



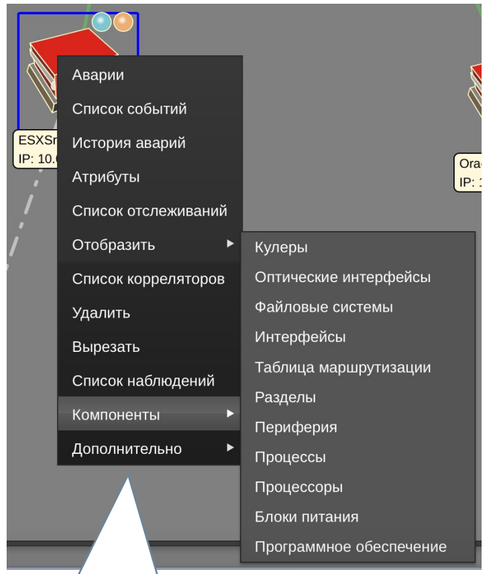




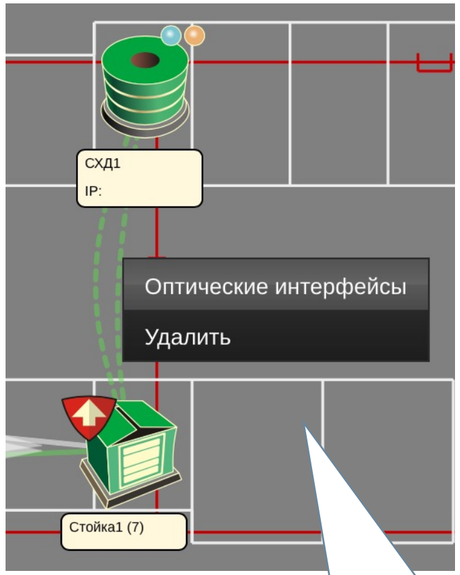
Инити

Мониторинг ИТ оборудования и сервисы

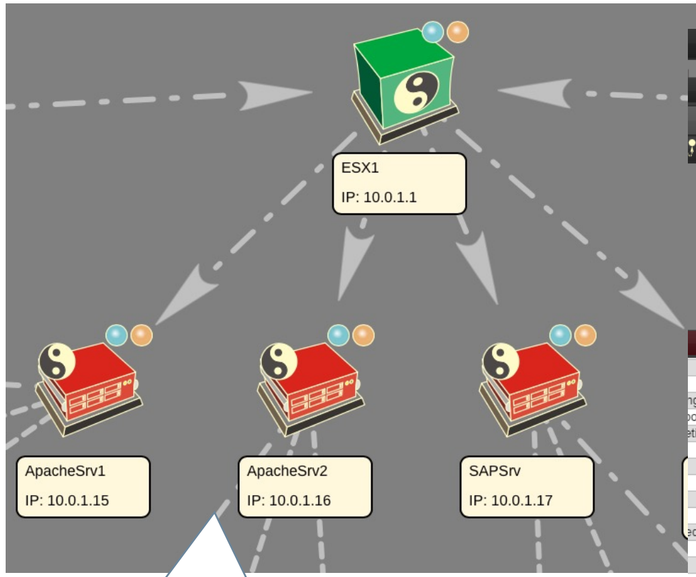
Сервера, системы виртуализации, СХД, приложения, перифирийные устройства



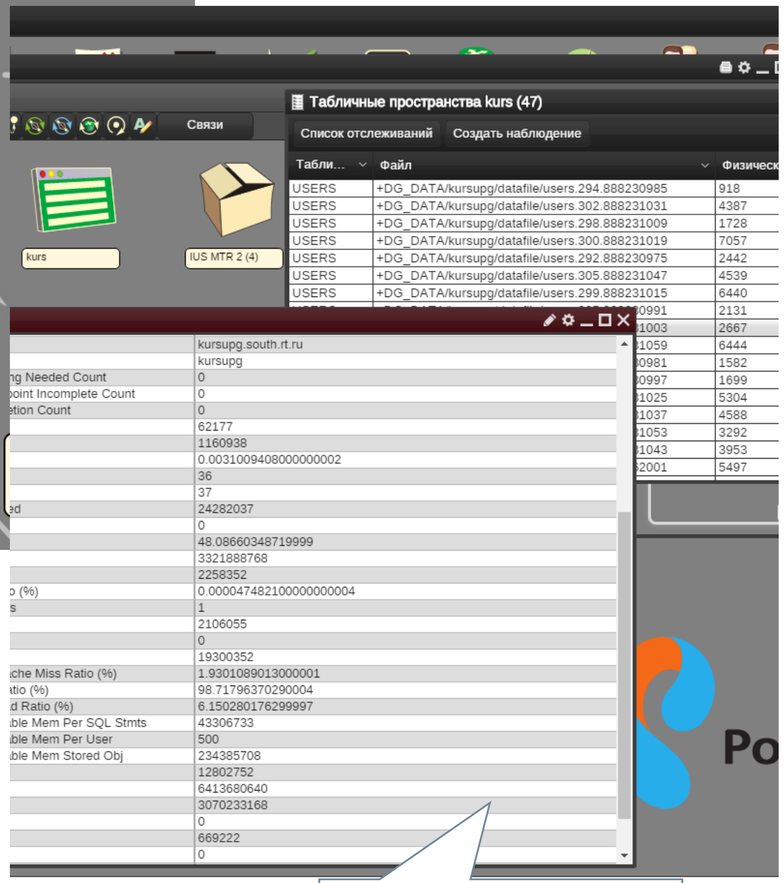
Серверное оборудование



СХД и компоненты SAN



Средства виртуализации



Детальный мониторинг ПО

Разделы ApacheSrv1 (4)

Список отслеживаний | Создать наблюдение

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

Компоненты ОС

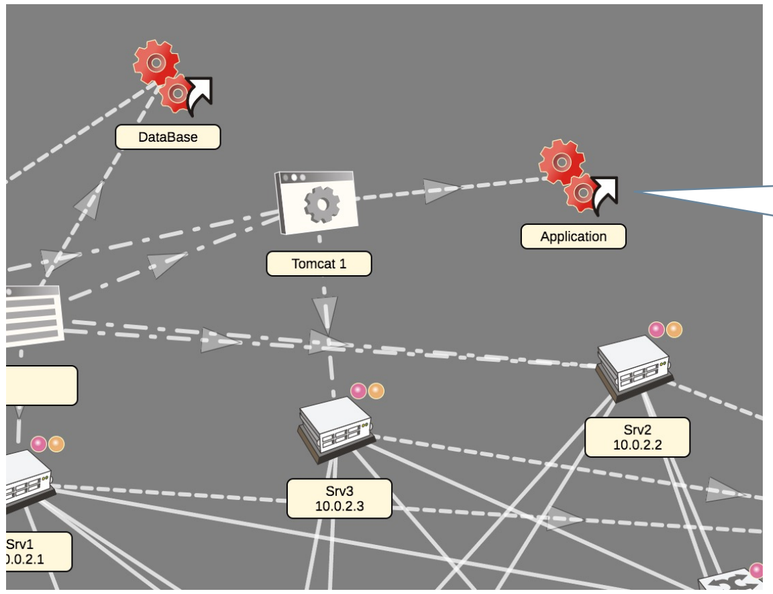
Инити

Мониторинг пользовательских действий

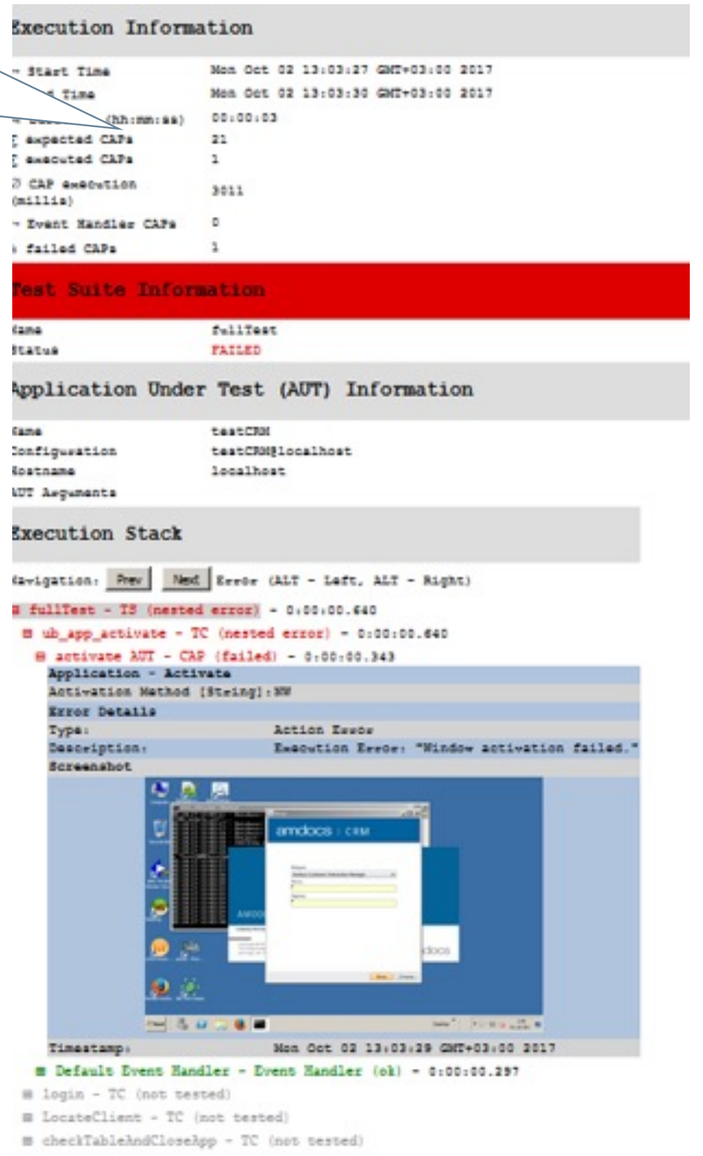
Setp No.	Command	URL	Value	Step status	Message	Description	Time
1	newSession			1	ok		
2	implicitlyWait			1	Message: POST /session/0cc266f6-3435-43c5-a93a-0c93f3c39001/timeouts/implicit_wait did not match a known command		
3	get	http://10.29.6.40:8080/RostelPoints/login.jsf		1	Message: Reached error page: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



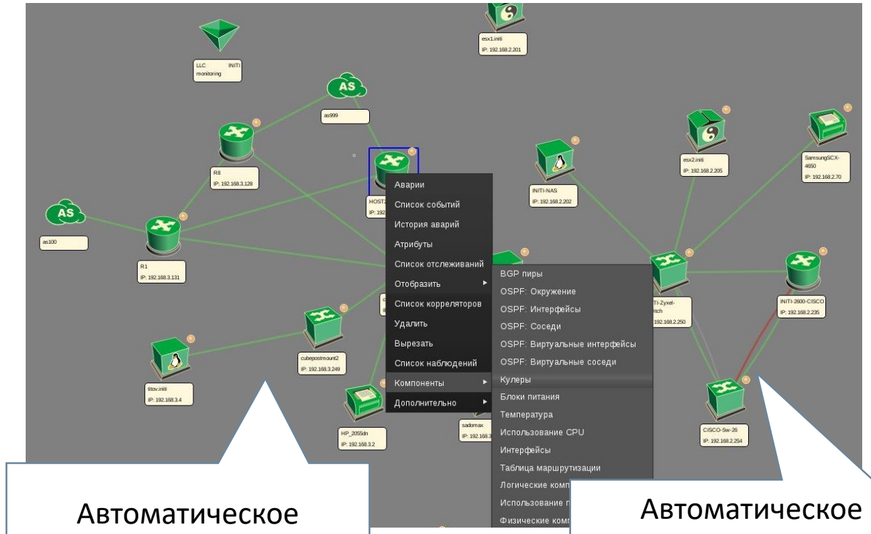
Маппирование сбоя на сервисную модель ИТ сервиса



Инити

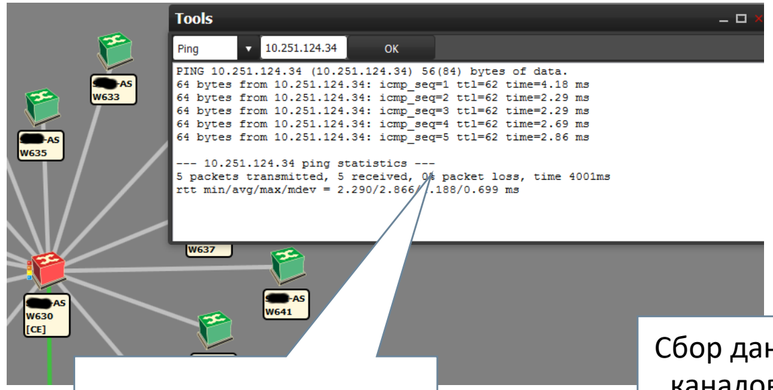
Мониторинг сетевой инфраструктуры

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

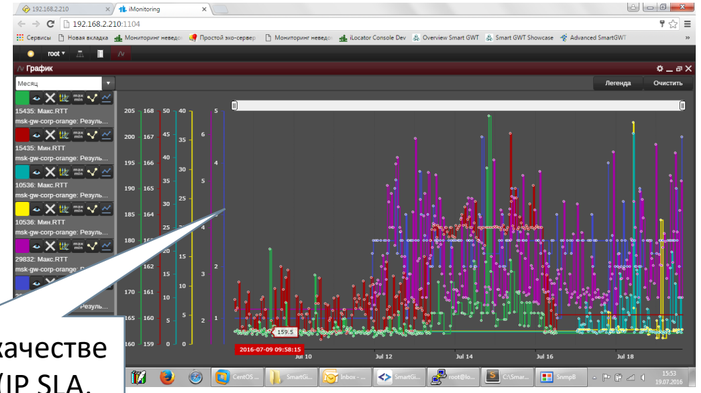


Автоматическое построение топологии

Автоматическое построение топологии маршрутизации

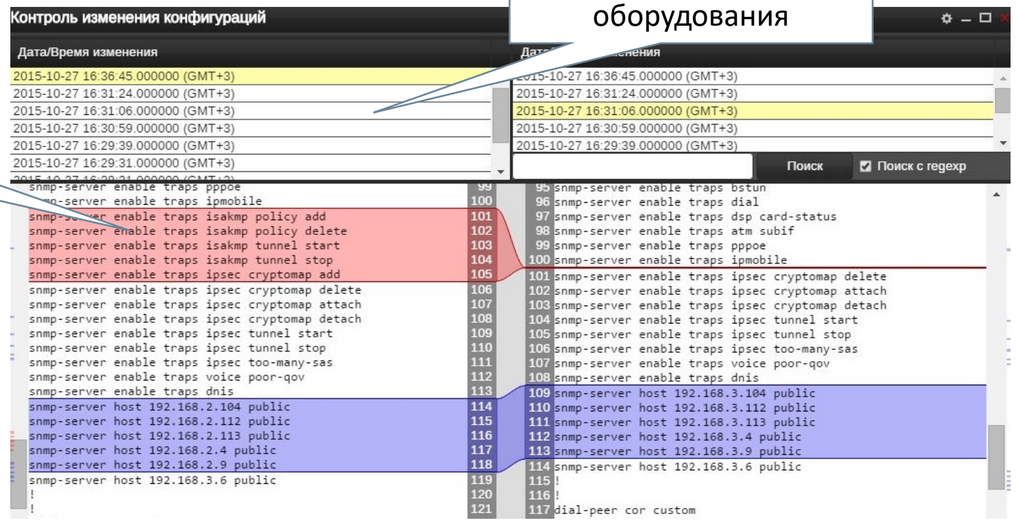


Контекстный запуск утилит по диагностике

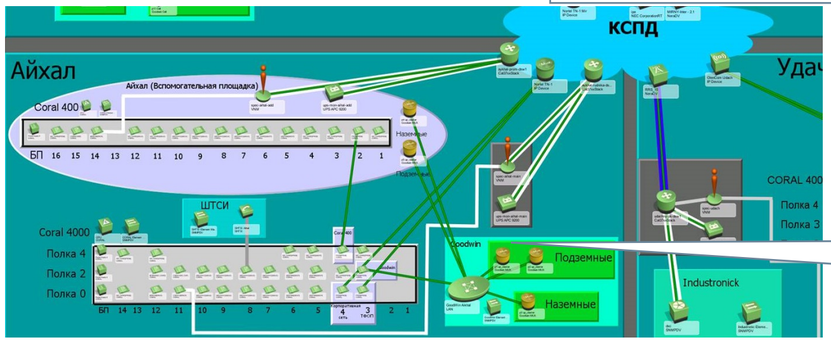


Сбор данных о качестве каналов связи (IP SLA, QoS, TWAMP и пр..)

Сбор и ведение конфигураций оборудования



Отслеживание изменений конфигураций



Мониторинг телефонных станций

Инити

Мониторинг сетевой инфраструктуры – IP/MPLS

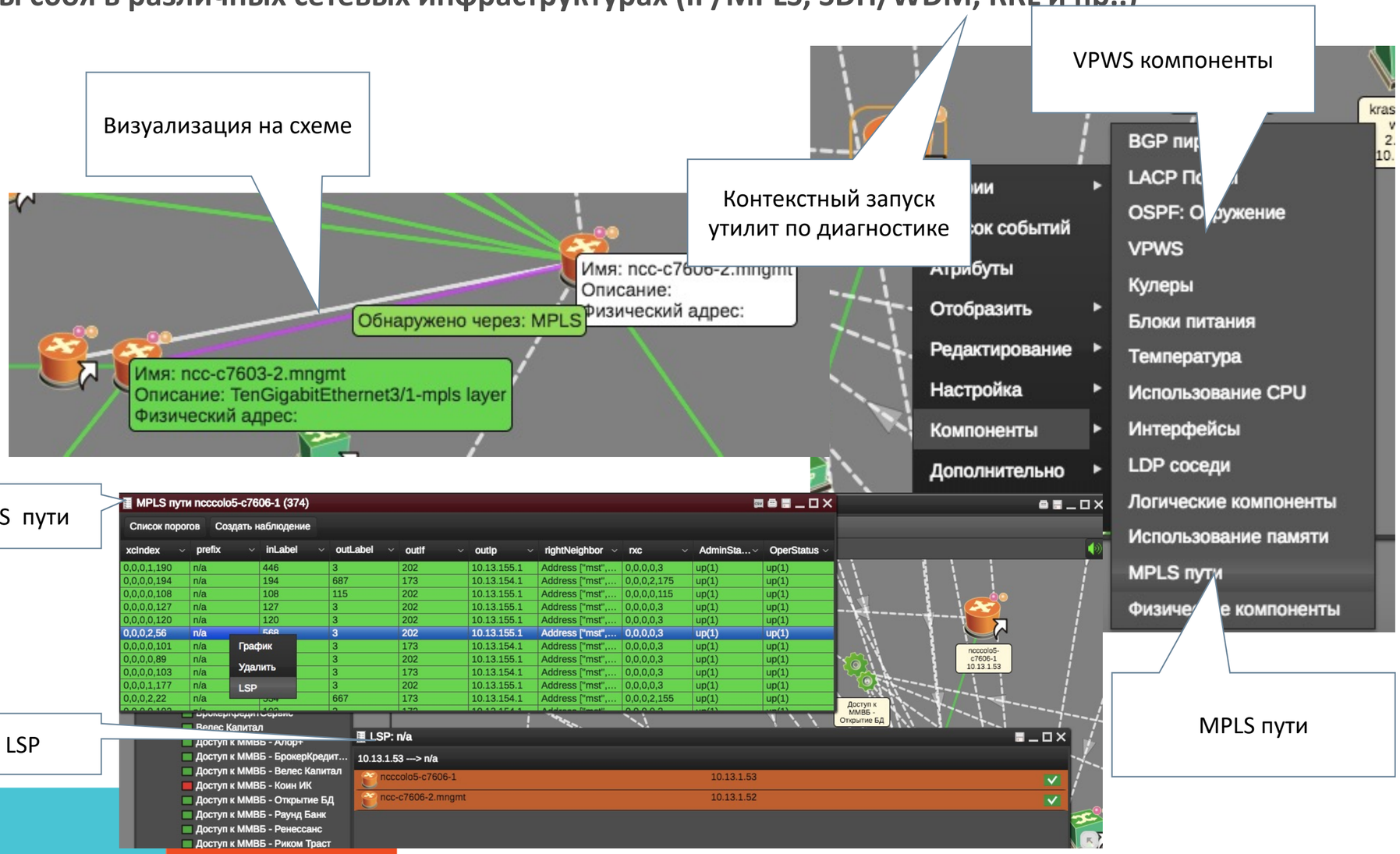
Мониторинг и поиск первопричины сбоя в различных сетевых инфраструктурах (IP/MPLS, SDH/WDM, RRL и пр..)

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



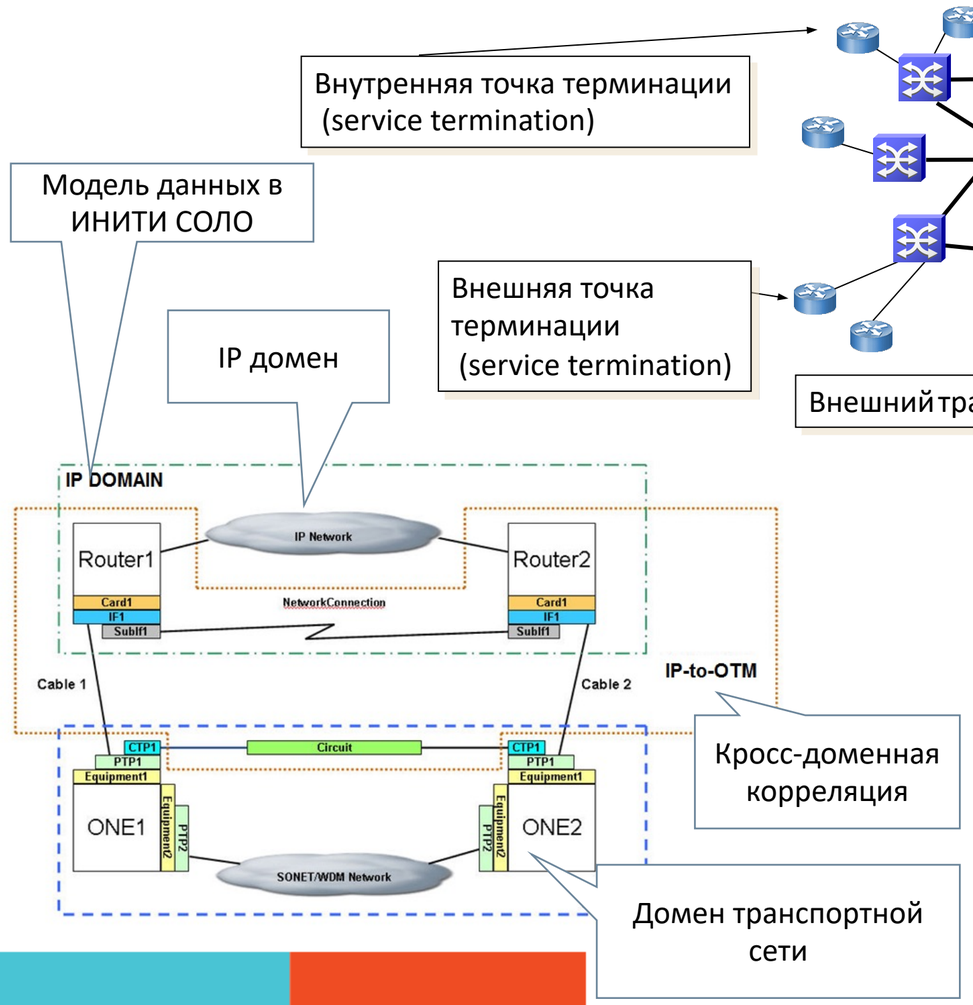
Инити

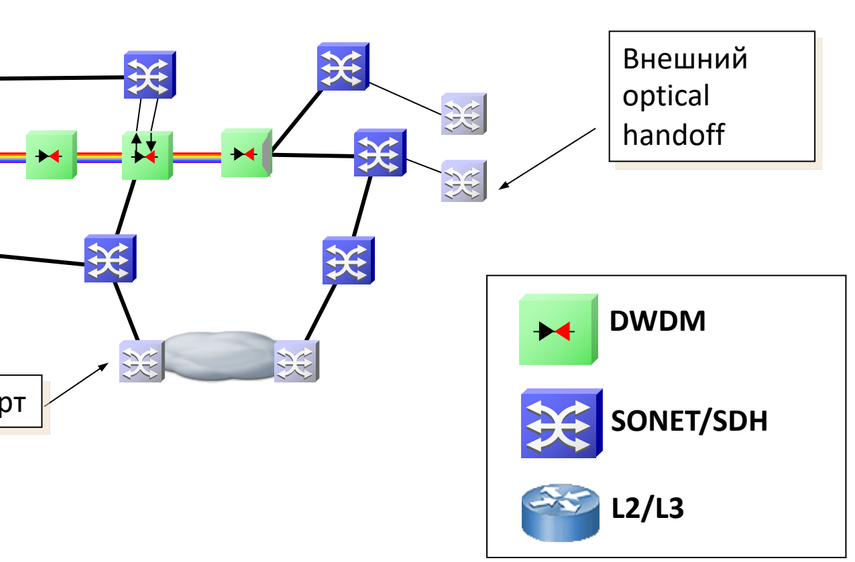
Мониторинг сетевой инфраструктуры – SDH / WDM

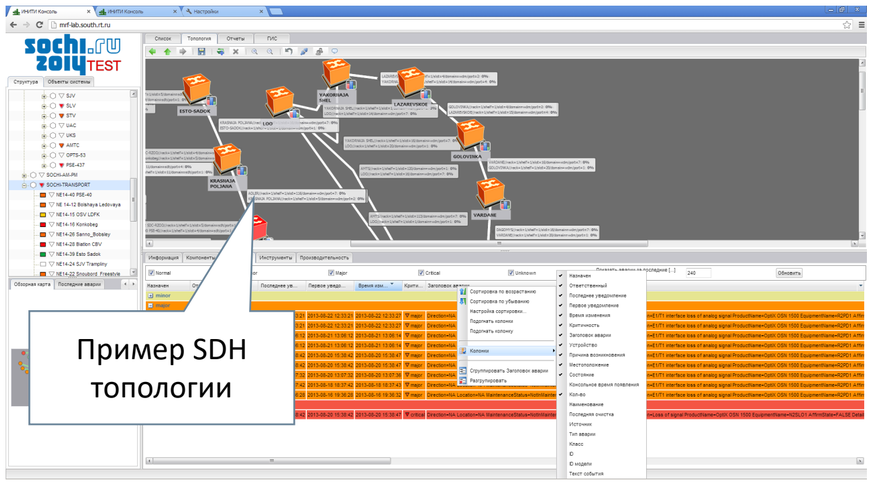
Мониторинг и поиск первопричины сбоя в различных сетевых инфраструктурах (IP/MPLS, SDH/WDM, RRL и пр..)

- **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



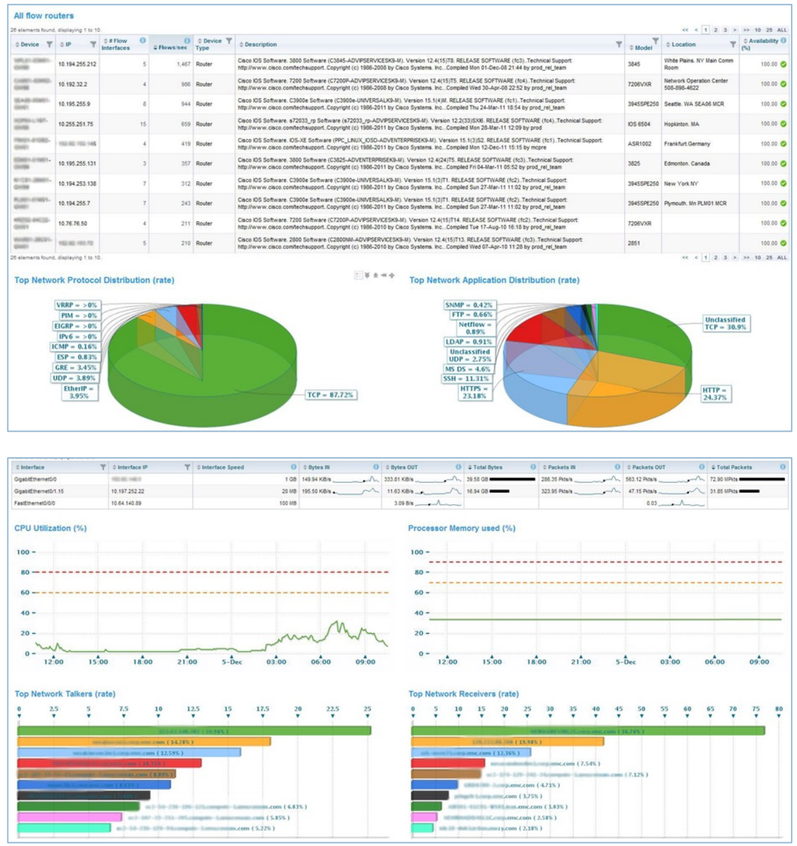




Инити

Мониторинг параметров сетевой инфраструктуры

Сбор данных NetFlow, cFlow, jFlow, etc..



- Сбор данных от оборудования (Netflow, Jflow, sFlow, Cflow и IPFIX) через Инити xFlow коллекторы с посделующей 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)

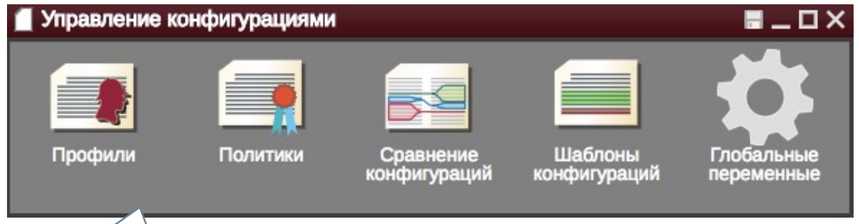
При этом по умолчанию поддерживается сбор следующих метрик:

- 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

Инити

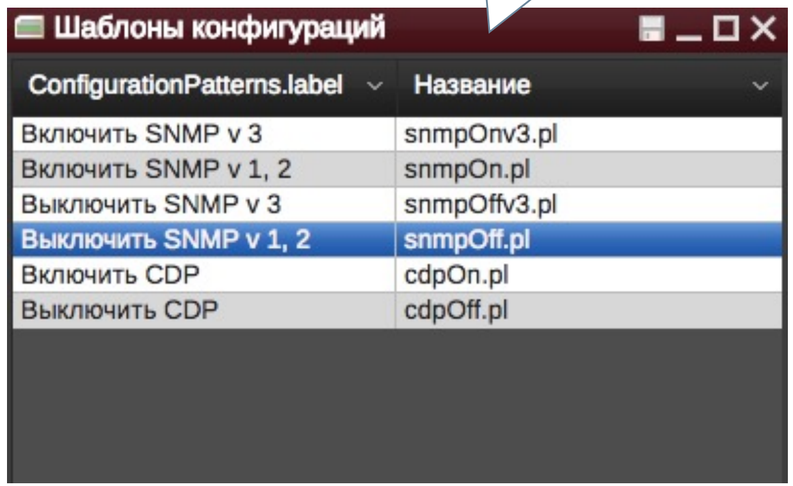
Управление конфигурациями сетевой инфраструктуры

Подсистема управления конфигурациями

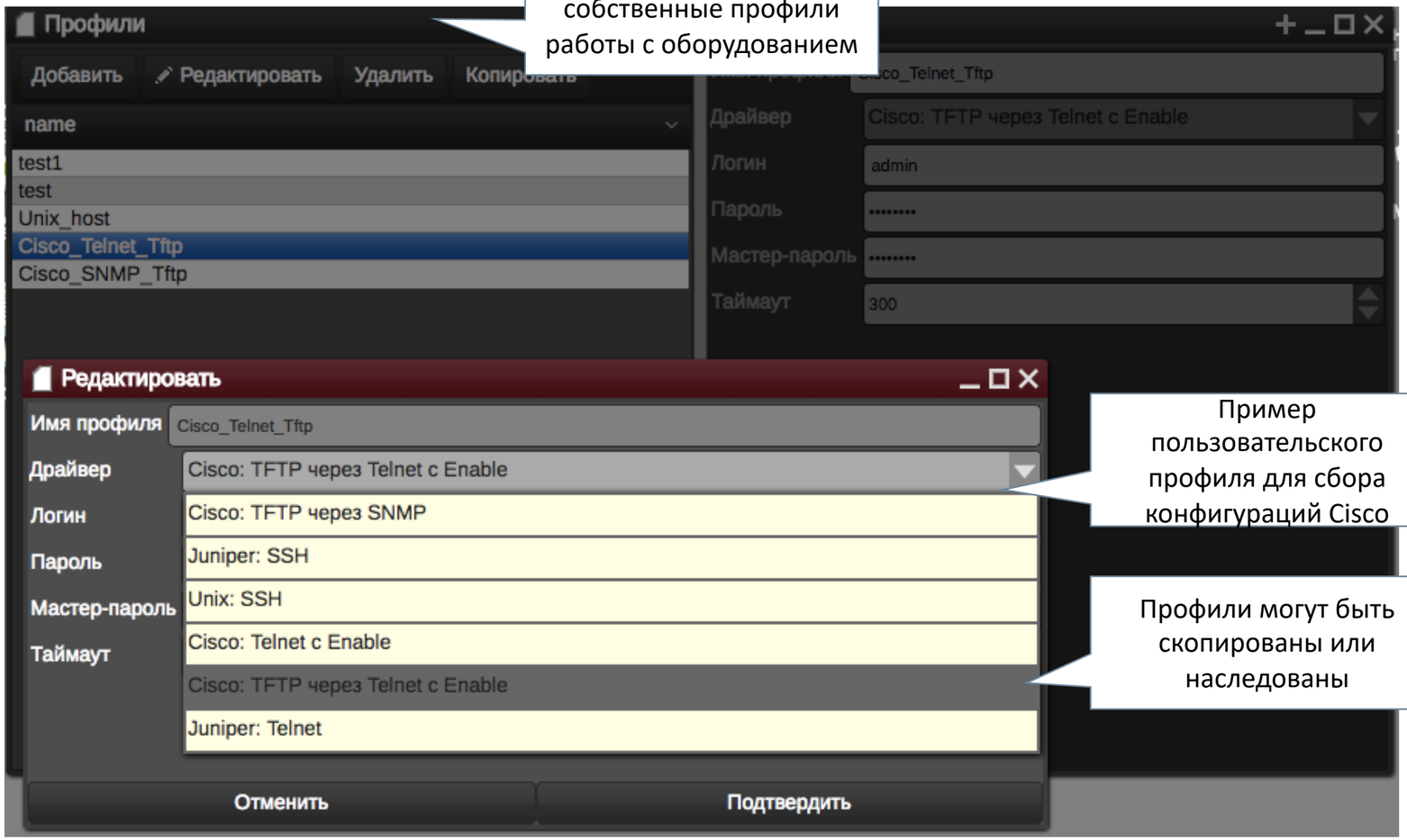


Выделенный интерактивный виджет

Создание шаблонных конфигураций



Возможность создавать собственные профили работы с оборудованием



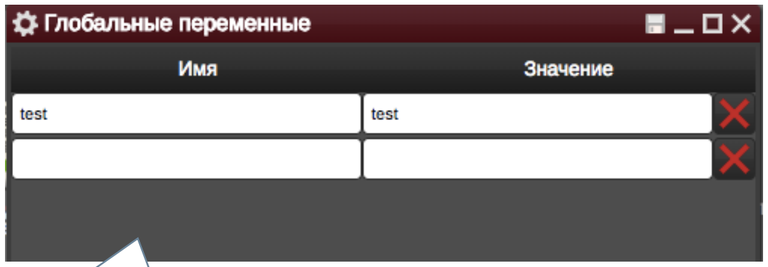
Пример пользовательского профиля для сбора конфигураций Cisco

Профили могут быть скопированы или наследованы

Инити

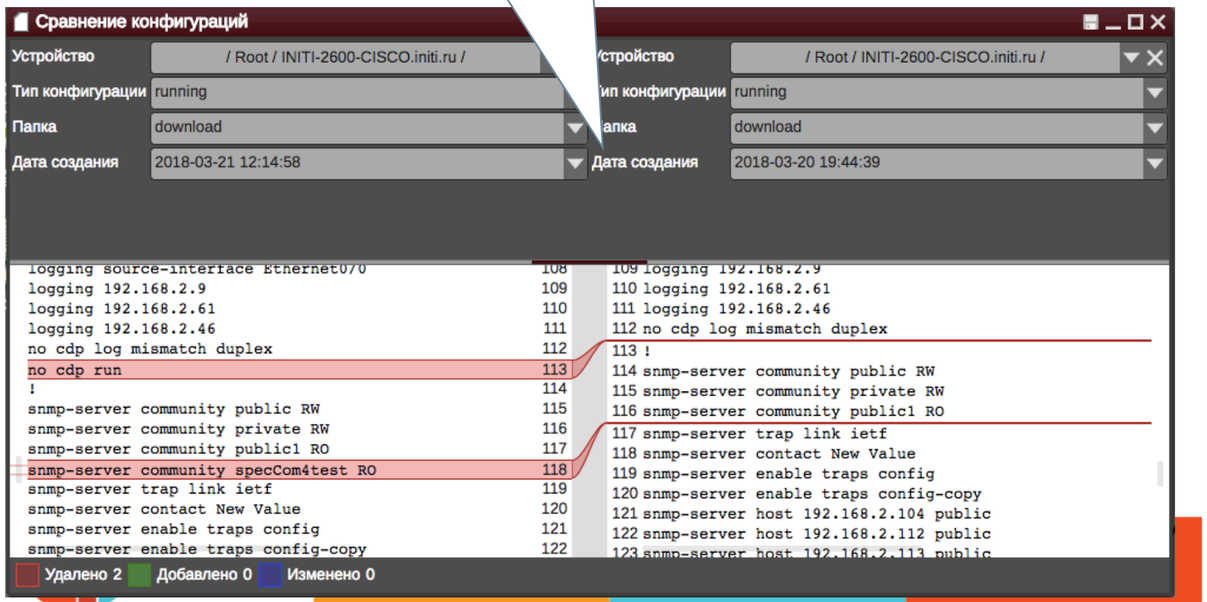
Управление конфигурациями сетевой инфраструктуры

Подсистема управления конфигурациями



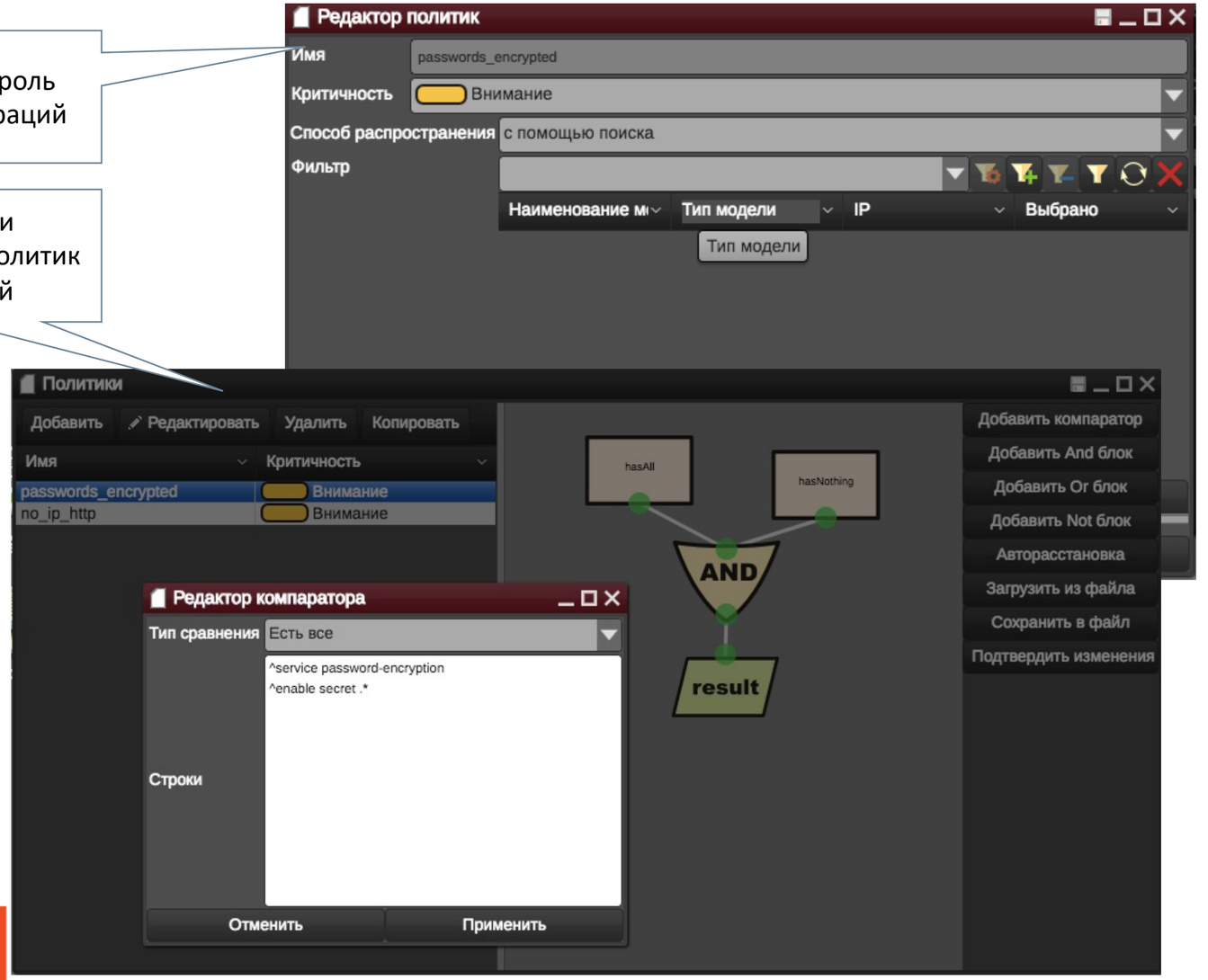
Создание глобальный переменных или алиасов

Сравнение конфигураций



Создание и контроль политик конфигураций

Группировка и редактирование политик конфигураций



Технологическое оборудование и элементы АСУТП - проблематика

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

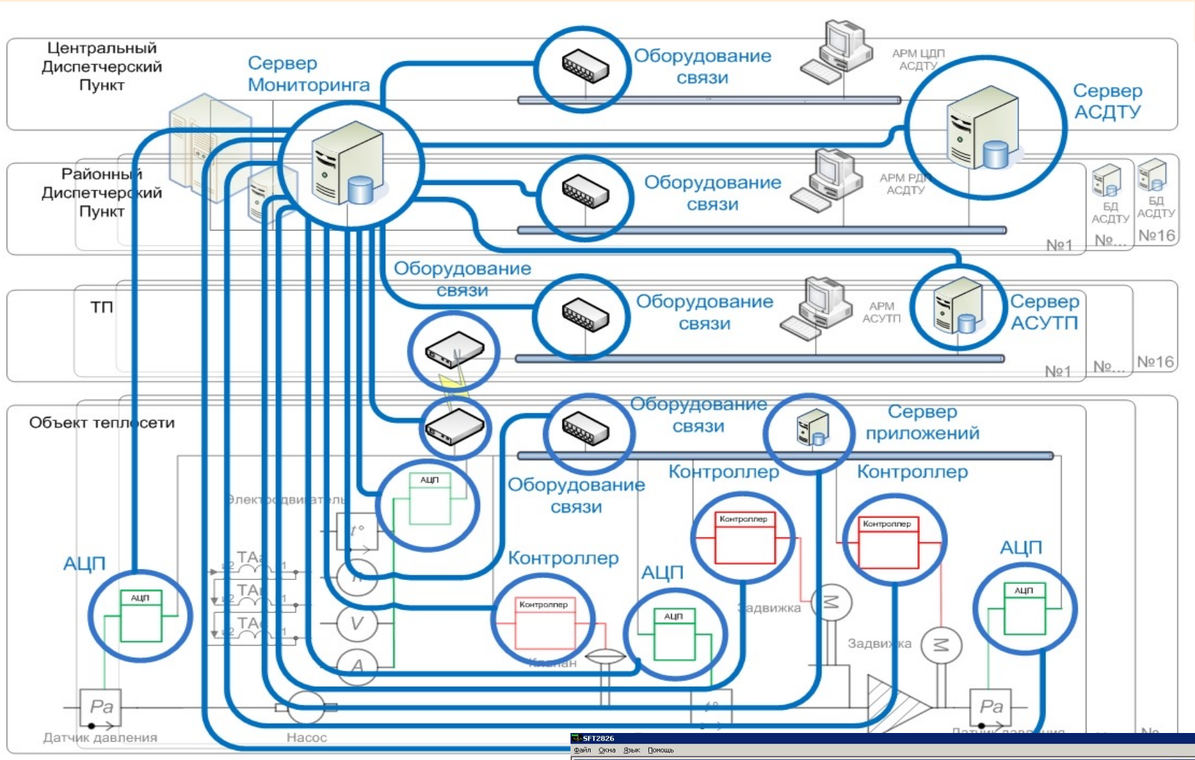
- Контрольно-измерительные приборы
- Контроллеры (ПЛК)
  - Универсальные программируемые контроллеры
  - PC-совместимые контроллеры
  - Программируемые реле
- Рабочие станции пользователя (АРМ)

- Индустриальные стандарты: Modbus, DNP3, ICCP, 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

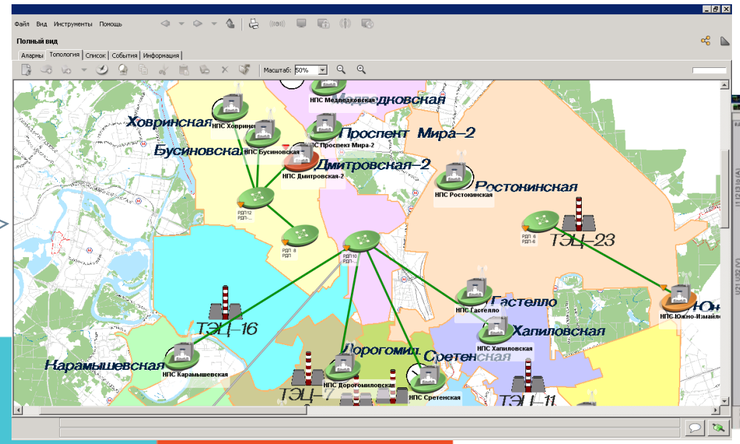
- Система мониторинга ИТ оборудования
- Штатные средства сетевой ИБ Cisco
- Сервера HP и ОС Windows, Linux, Unix
- Устройства защиты серии «Sepam», производства компании «SCHNEIDER ELECTRIC». Предназначены для контроля и управления силовым электрооборудованием напряжением 6-10 кВ.
- Контроллеры серии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

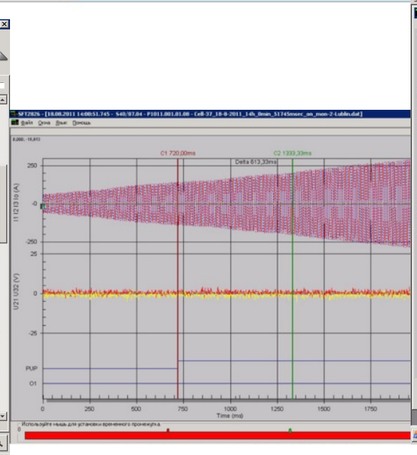


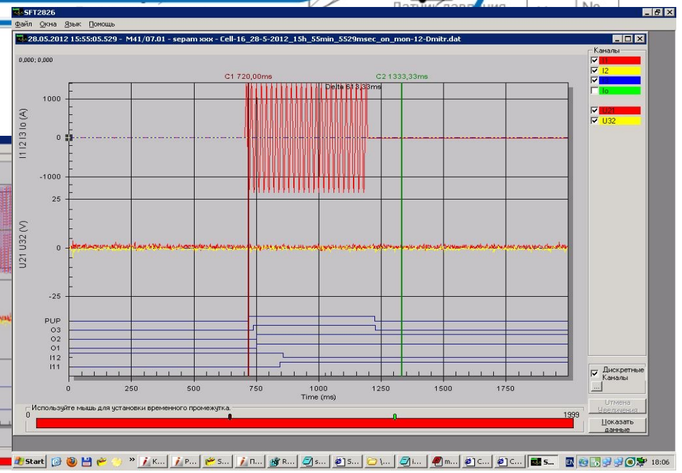
Зеленый - объект работает в штатном режиме.

Оранжевый - объект работает в предаварийном режиме, нештатная ситуация

Красный - на объекте критическая ситуация.

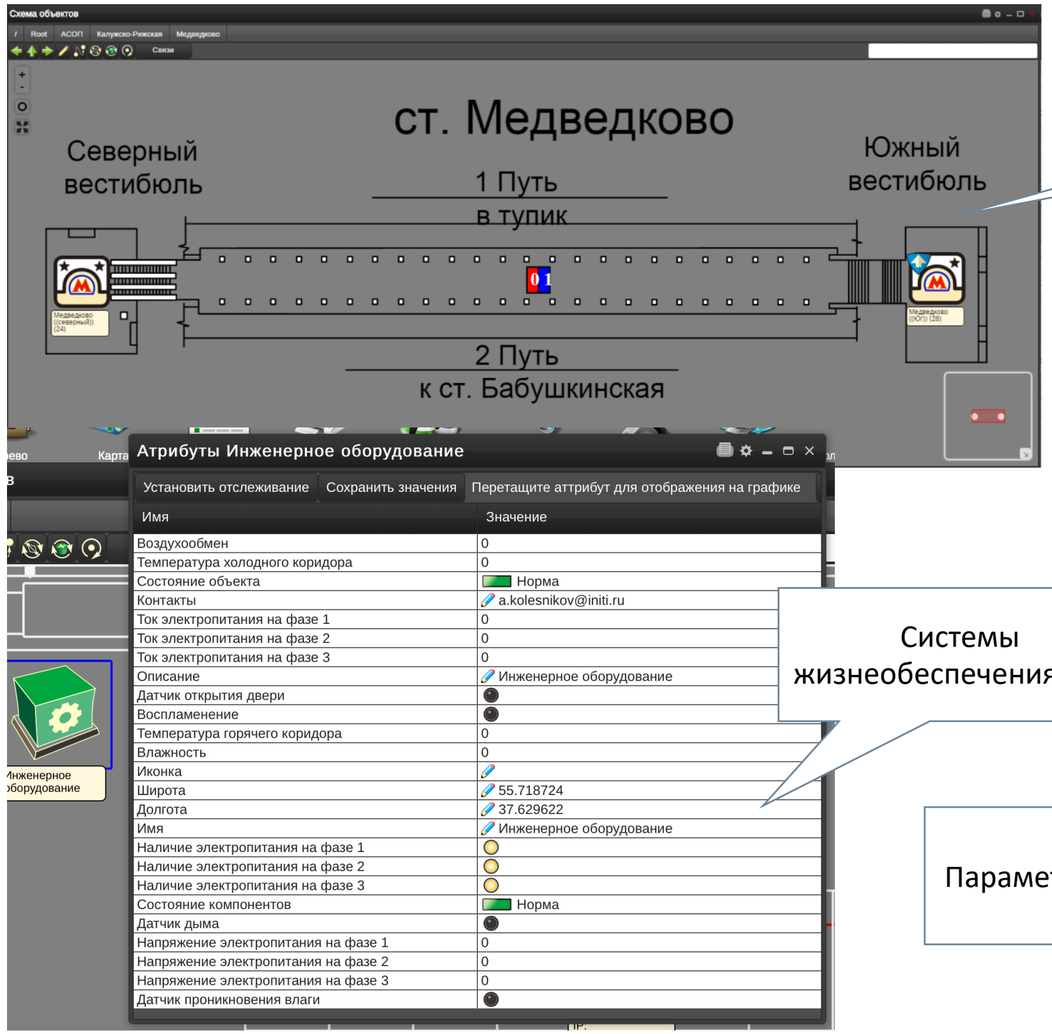




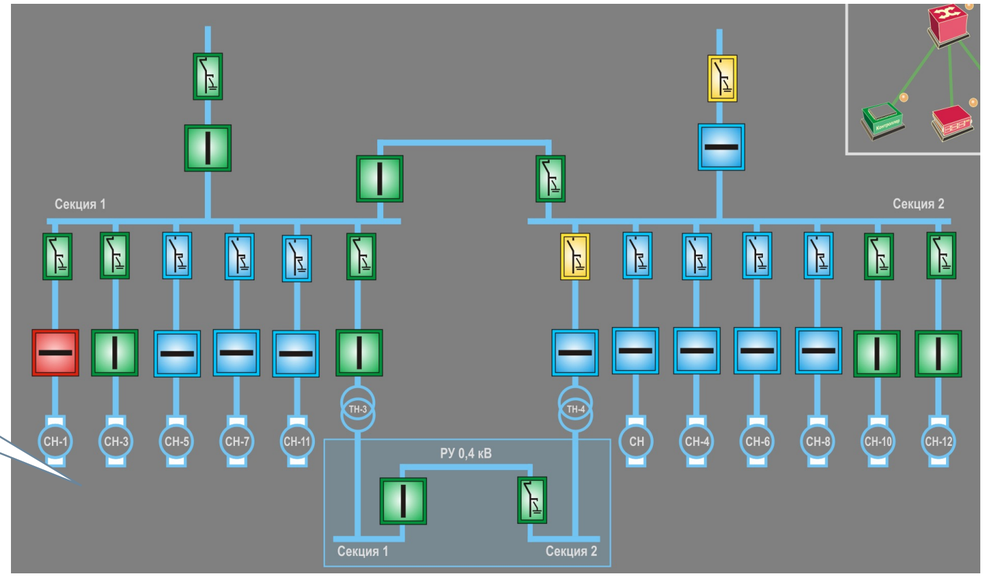


Инити

Технологическое оборудование и элементы АСУТП



Технологическое оборудование



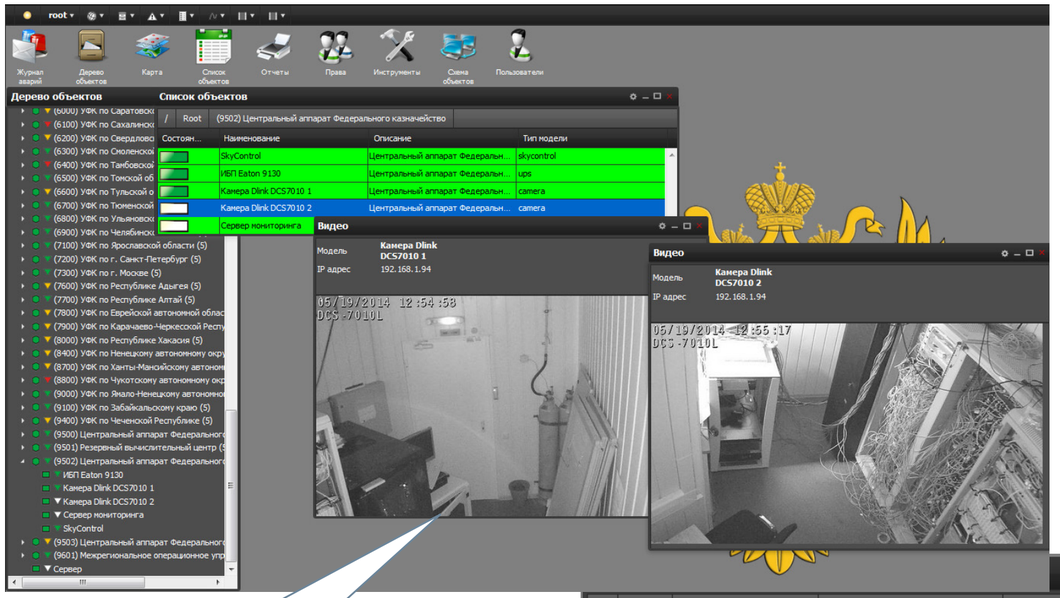
Объекты АСУТП – интерактивная мнемосхема

Системы жизнеобеспечения ЦОД

Параметры работы ДГУ

Инити

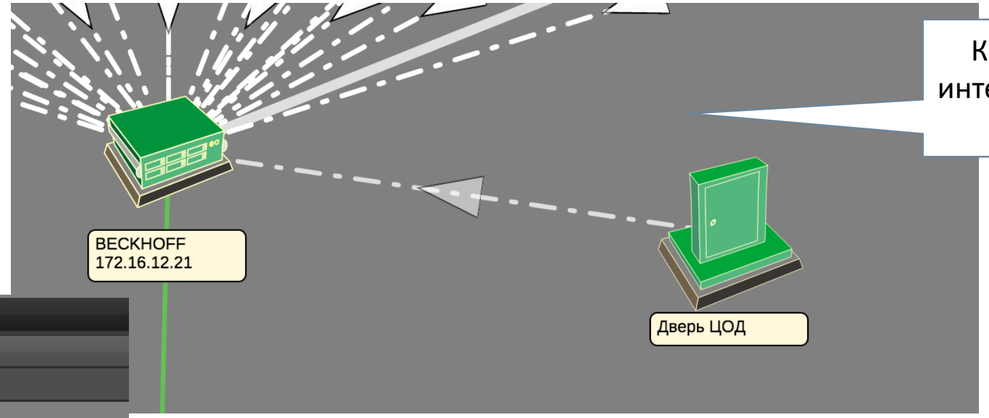
Интеграция с подсистемами ИБ



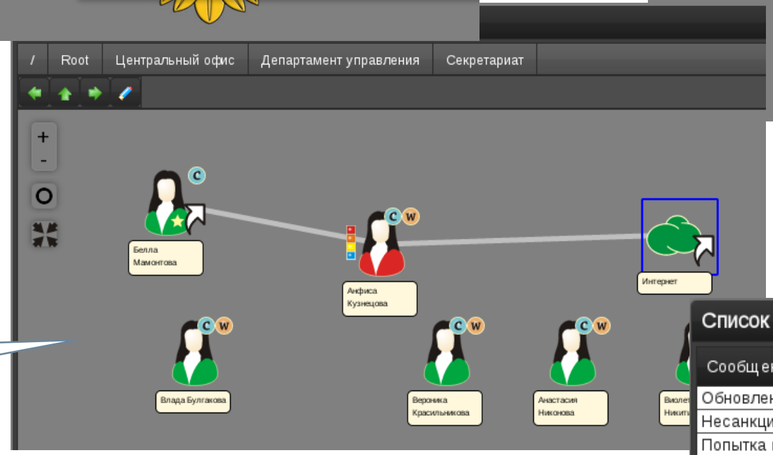
Визуальный контроль объекта

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]. Addre…	06.02.2015 17:56:34 GMT+3

Интеграция с DLP – контроль утечки конфиденциальных данных



Контроль доступа – интеграция с системами СКУД



Интеграция с DLP – трекинг email

Кореляция данных событий от нескольких внешних ИБ систем

Список событий (5)

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 АРМ	06.02.2015 17:41:06 GMT+3
Попытка пользователя Пушков Павел авторизоваться в системе АРМ. 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

Инити

СПАСИБО!

Инити