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

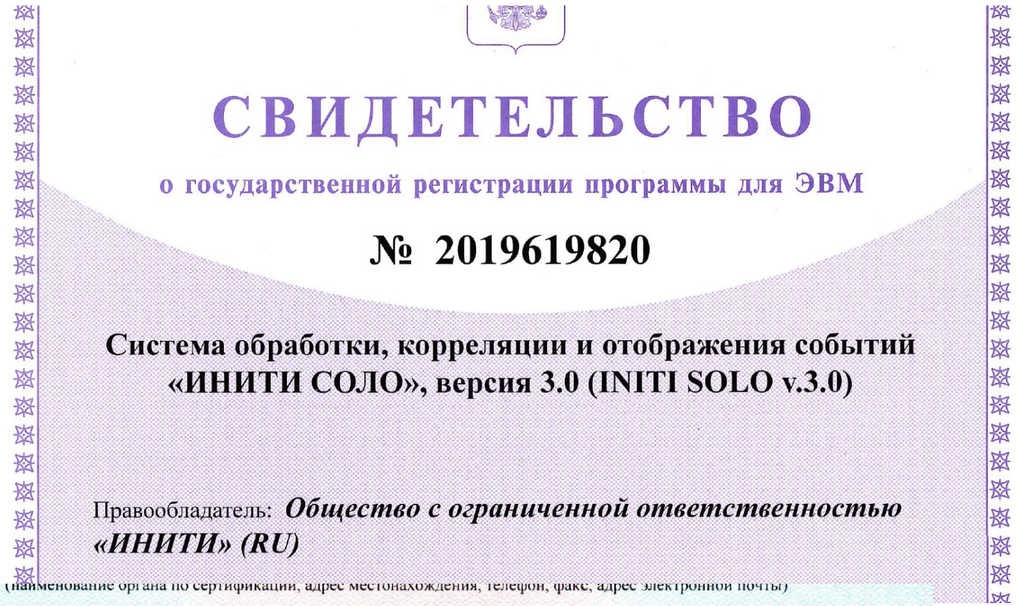
- создание единого центра мониторинга, управления и диспетчеризации для контроля всех технологический доменов ИКТ инфраструктуры
- повышение эффективности работы инженеров за счет унификации рабочих мест
- построение вертикали управления на основе введенных регламентов и прав доступа
- ведение единой 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 30+
- Решение включено в Реестр Российского ПО
- 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



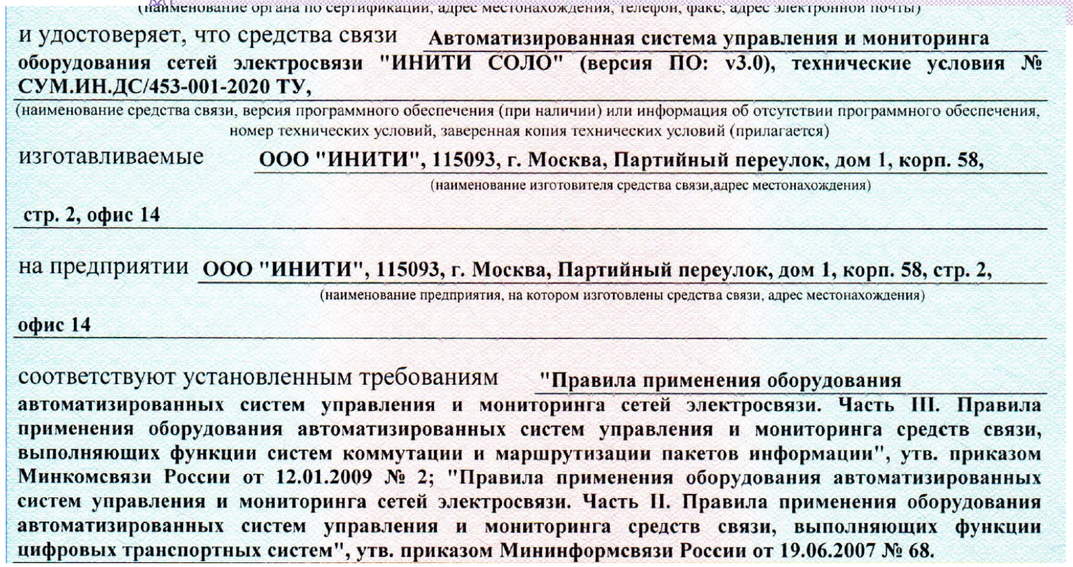
СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019619820

Система обработки, корреляции и отображения событий «ИНИТИ СОЛО», версия 3.0 (INITI SOLO v.3.0)

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



(наименование органа по сертификации, адрес местонахождения, телефон, факс, адрес электронной почты)

и удостоверяет, что средства связи **Автоматизированная система управления и мониторинга оборудования сетей электросвязи "ИНИТИ СОЛО" (версия ПО: v3.0), технические условия № СУМ.ИН.ДС/453-001-2020 ТУ,**

(наименование средства связи, версия программного обеспечения (при наличии) или информация об отсутствии программного обеспечения, номер технических условий, заверенная копия технических условий (прилагается)

изготавливаемые **ООО "ИНИТИ", 115093, г. Москва, Партийный переулок, дом 1, корп. 58, стр. 2, офис 14**

(наименование изготовителя средства связи,адрес местонахождения)

на предприятии **ООО "ИНИТИ", 115093, г. Москва, Партийный переулок, дом 1, корп. 58, стр. 2, офис 14**

(наименование предприятия, на котором изготовлены средства связи, адрес местонахождения)

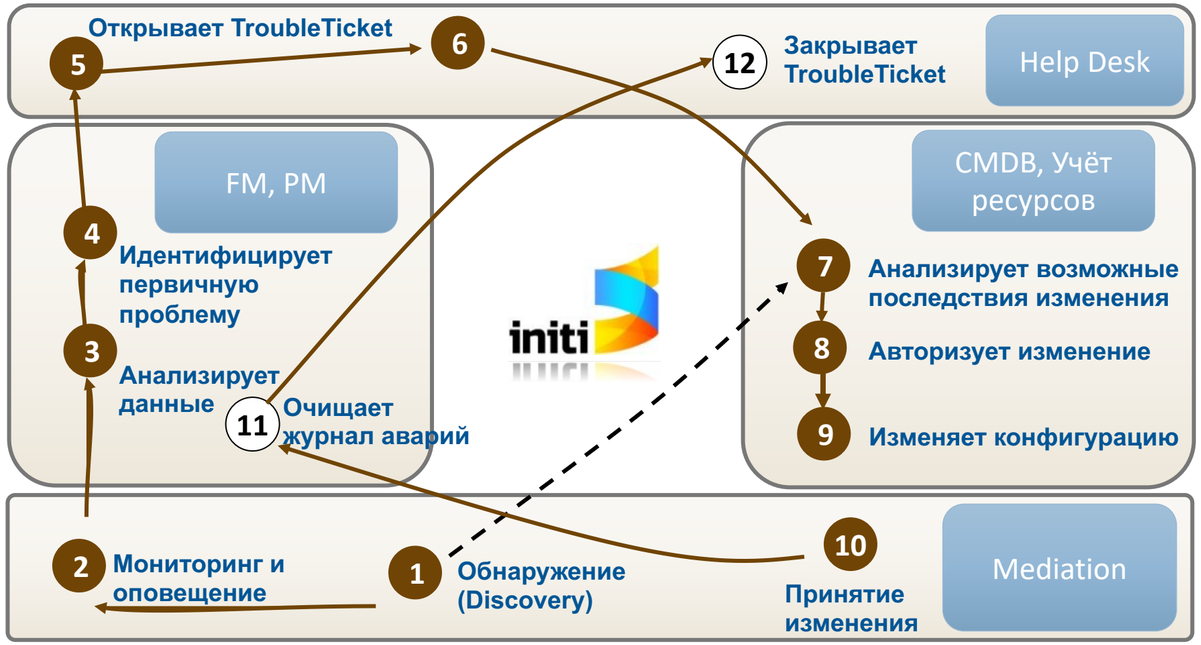
соответствуют установленным требованиям **"Правила применения оборудования автоматизированных систем управления и мониторинга сетей электросвязи. Часть III. Правила применения оборудования автоматизированных систем управления и мониторинга средств связи, выполняющих функции систем коммутации и маршрутизации пакетов информации", утв. приказом Минкомсвязи России от 12.01.2009 № 2; "Правила применения оборудования автоматизированных систем управления и мониторинга сетей электросвязи. Часть II. Правила применения оборудования автоматизированных систем управления и мониторинга средств связи, выполняющих функции цифровых транспортных систем", утв. приказом Мининформсвязи России от 19.06.2007 № 68.**

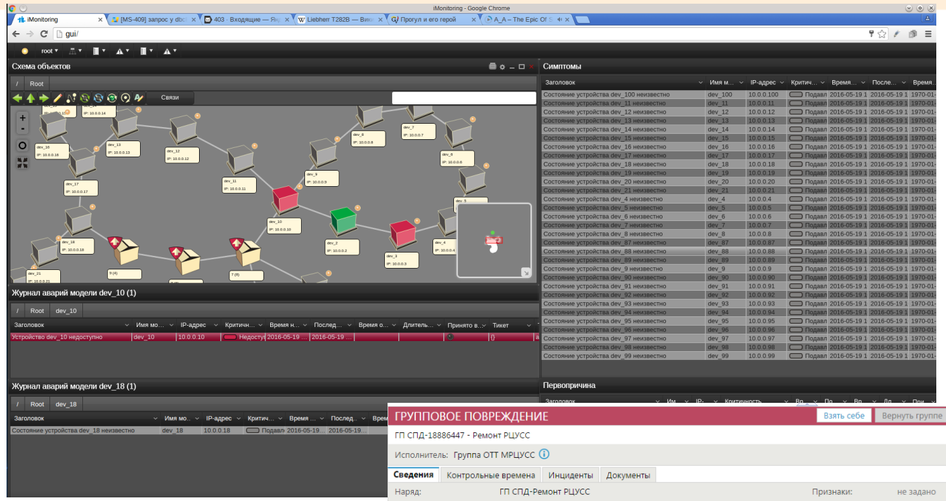
Инити

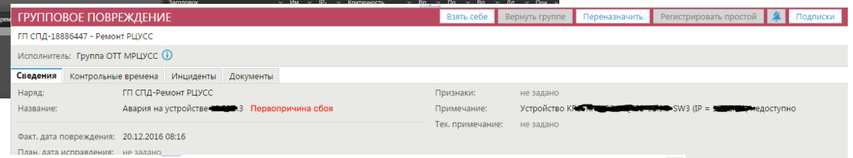
Почему “ИНИТИ СОЛО” – особенности решения

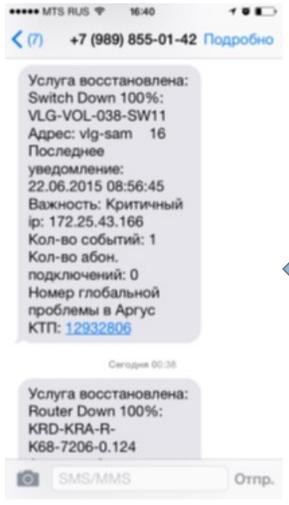
- Независимое ядро системы (зарегистрировано отдельно)
- Работа в высоконагруженных системах с большим количеством событий
- Использование технологий параллельных вычислений и EEDA
- Работа на x86 архитектуре и открытых ОС (Linux)
- Поддержка работы на защищённых ОС (Astra Linux, RedOS, ALT)
- Русифицированный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

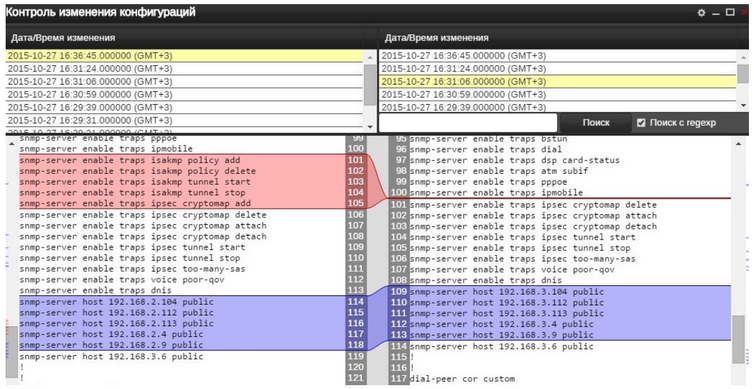
Цель – замкнутый цикл автоматизации

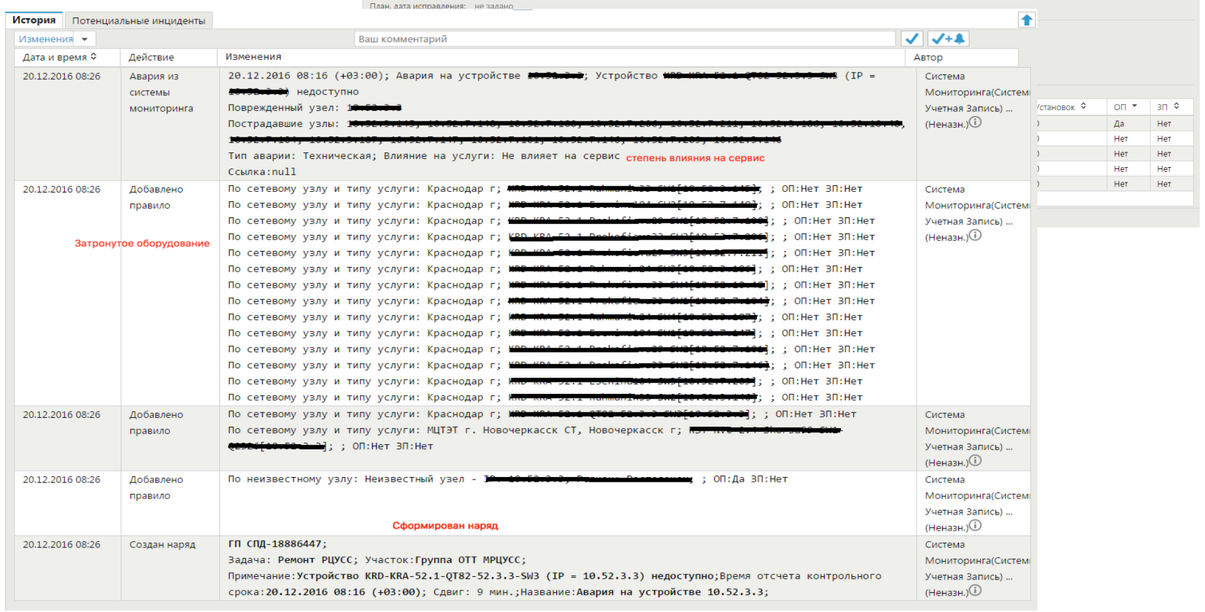












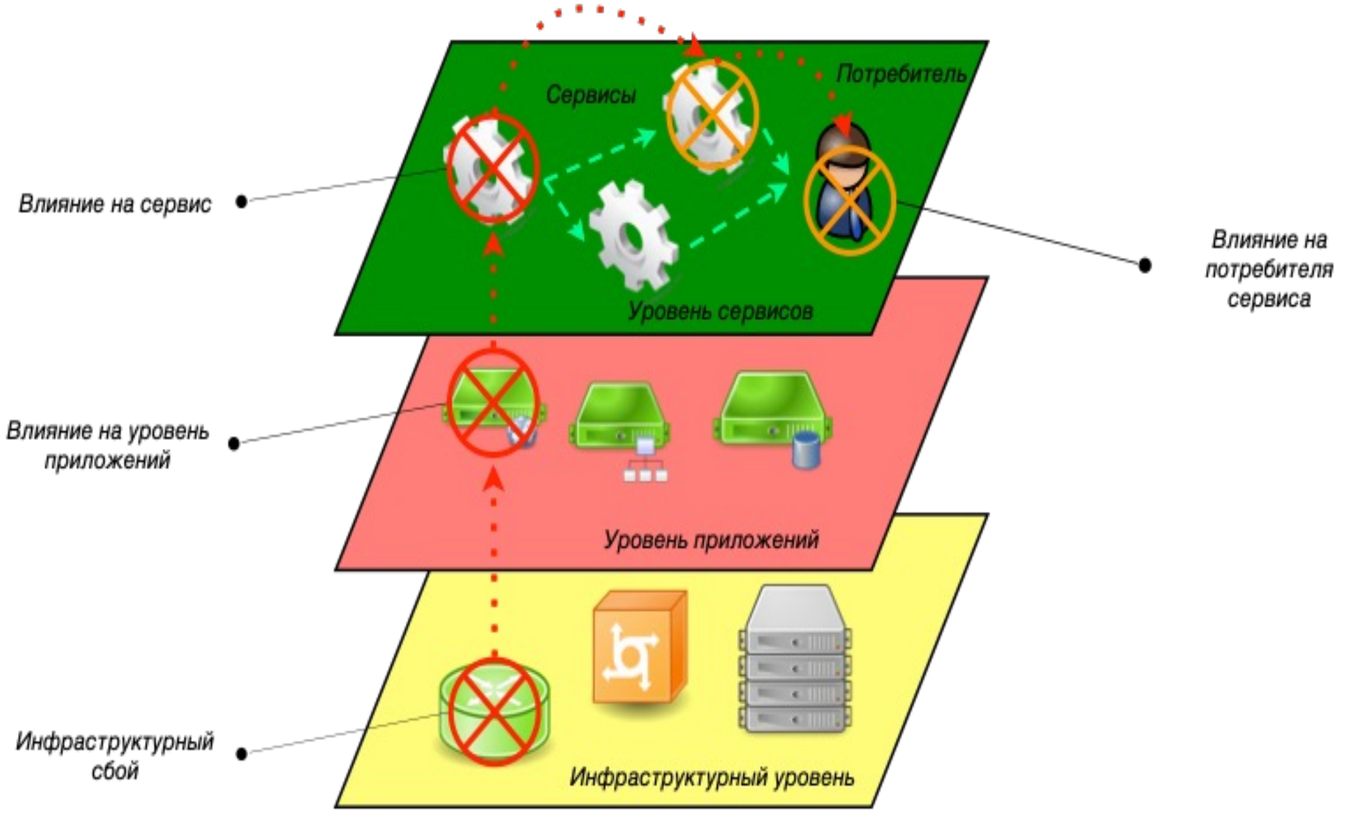
Сквозной мониторинг недоступности сервиса

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:

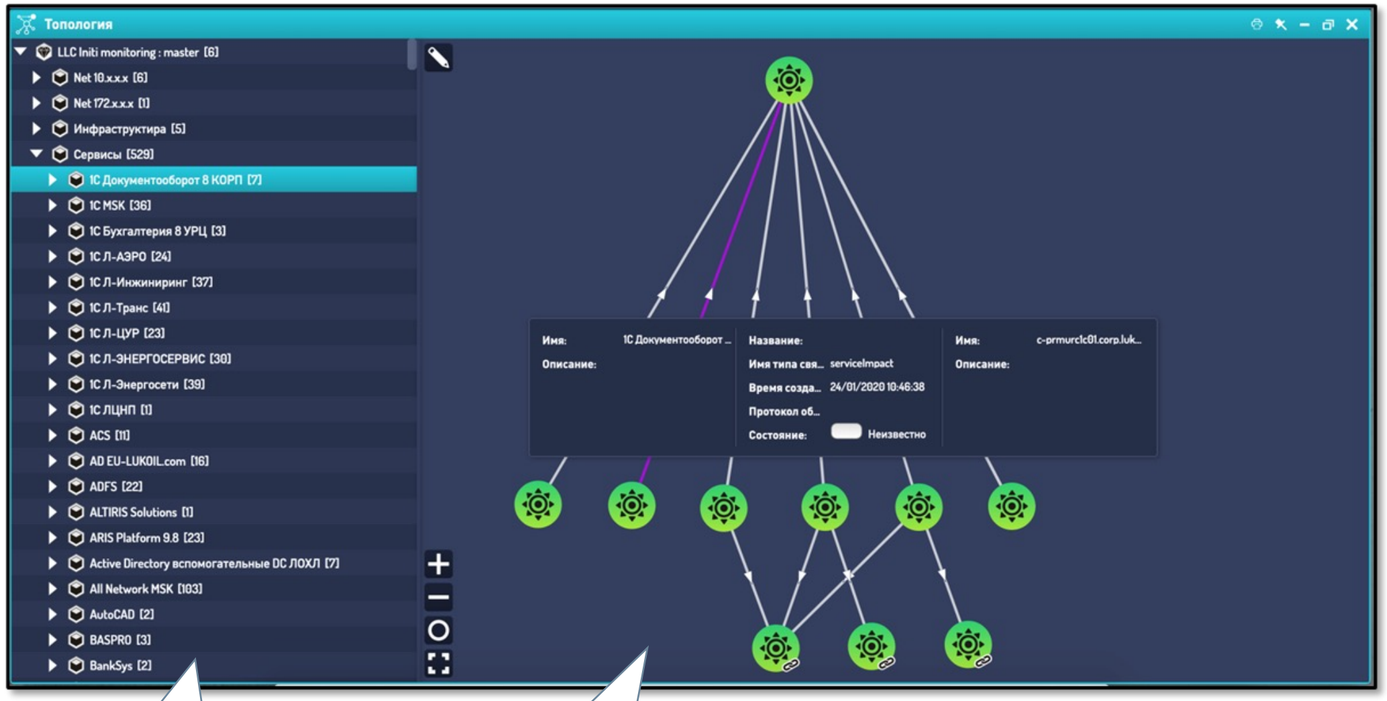
- Сокращение времени на выявление затронутых аварией сервисов
- Оперативное уведомление ответственных за эксплуатацию аварийных объектов лиц, при аварии на сервисе или при приближении к пороговым значениям прогноза аварийных ситуаций

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



Каталог сервисов

Визуальное представление сервисной модели

Инити

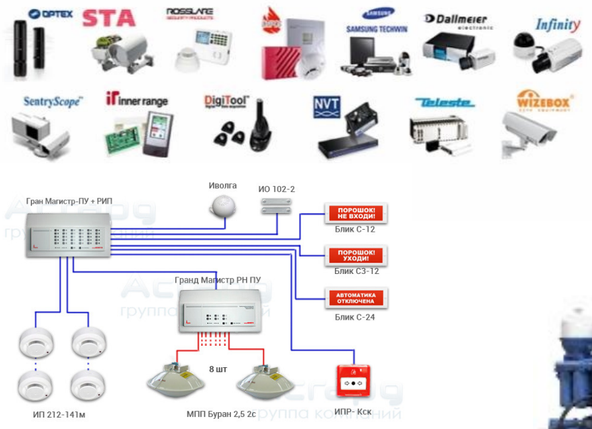
Первоочередные эффекты от внедрения

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?

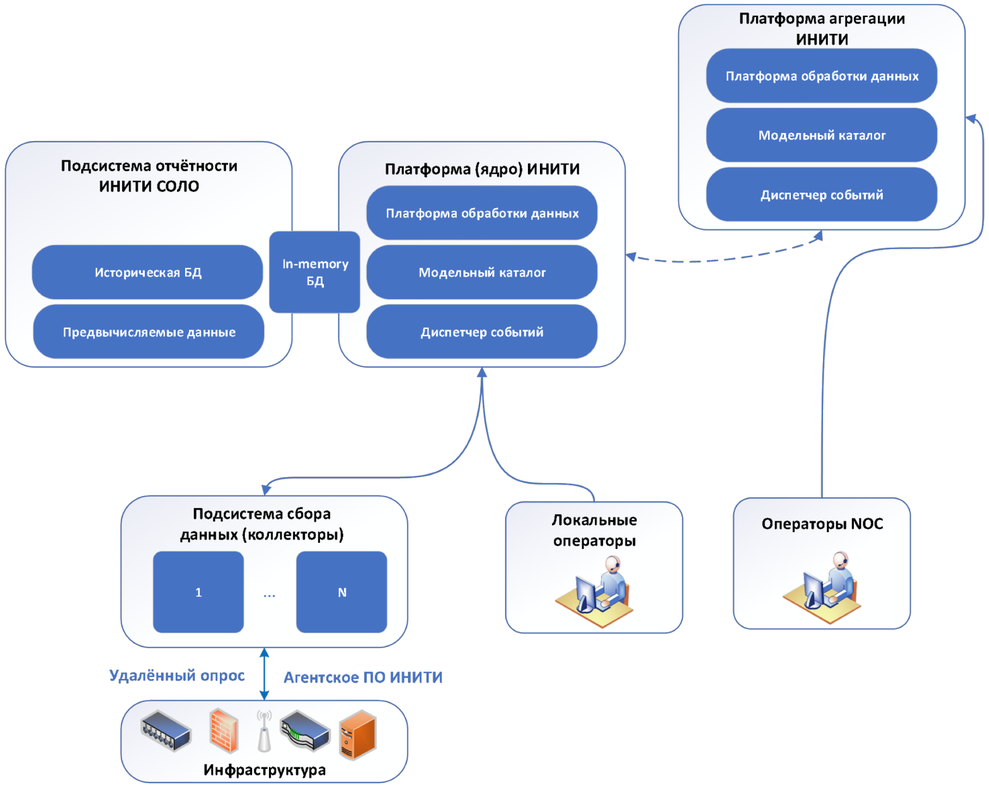


Инити

Техническая информация

Инити

Структура “ИНИТИ СОЛО”



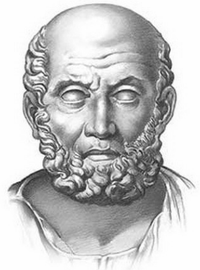
- Уровень сбора данных (Коллекторы)
- Уровень нормализации данных (Диспечер событий)
- Ядро системы (Core):
  - Модельный каталог
  - Модель инфраструктуры
  - Обработка событий
- Уровень представления (GUI)
- Высокая производительность ядра (10000+ EPS)
- Реализация отказоустойчивой и распределённой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

Инити

Уровень сбора данных – любой цифровой протокол

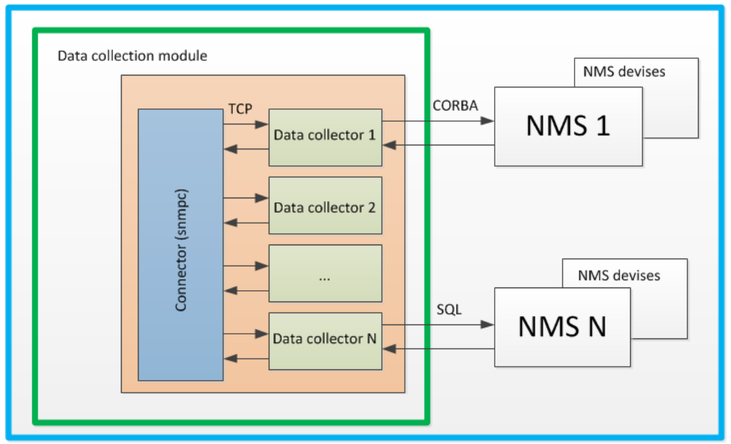
Единая платформа для сбора и нормализации данных с большого количества разнородных источников

- 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

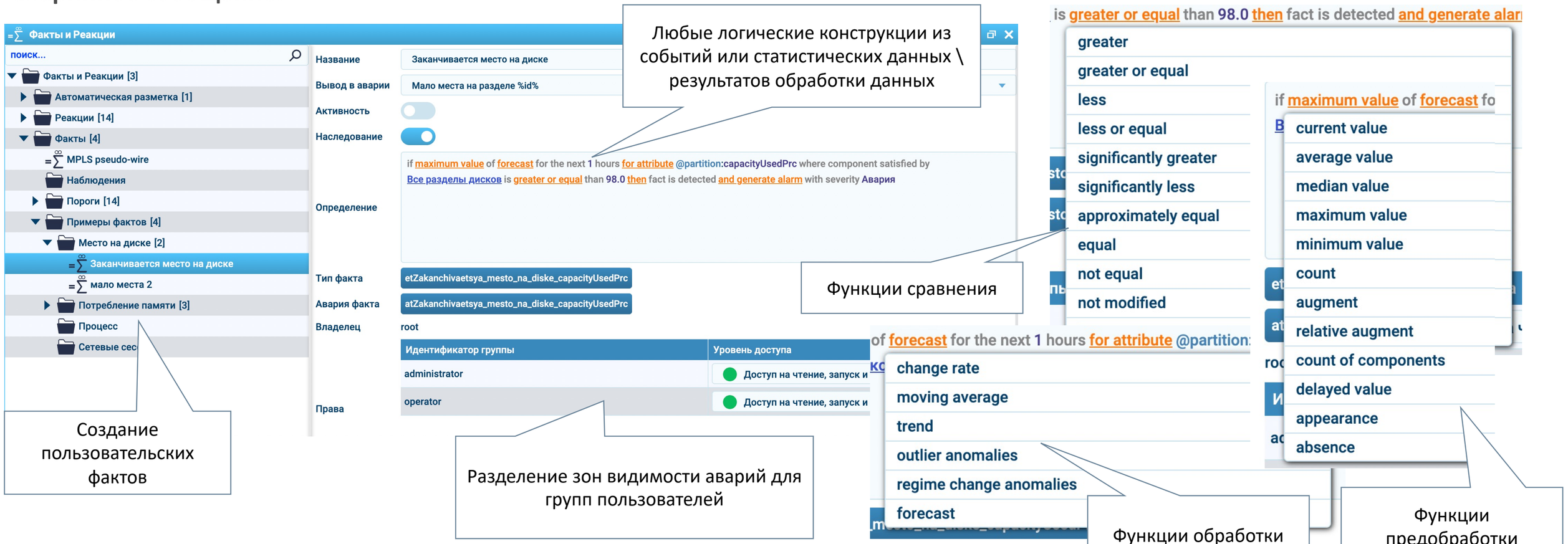
НЕКОТОРЫЕ ПОДДЕРЖИВАЕМЫЕ ПРОТОКОЛЫ	
CORBA	SNMP
DB Link	TELNET
FTP	TMF
HTTP-HTTPS	Vendor API (Java, Perl, …)
LOG	WebServices
OPC	WMI
SMB	XML
Modbus	Netbus
*Flow	TS 32.432
TS 32.435	И многое другое…

Ведение и накопление статистики по загрузке компонент график показателя объектов контроля

Инити

От системы мониторинга к **экспертной** системе

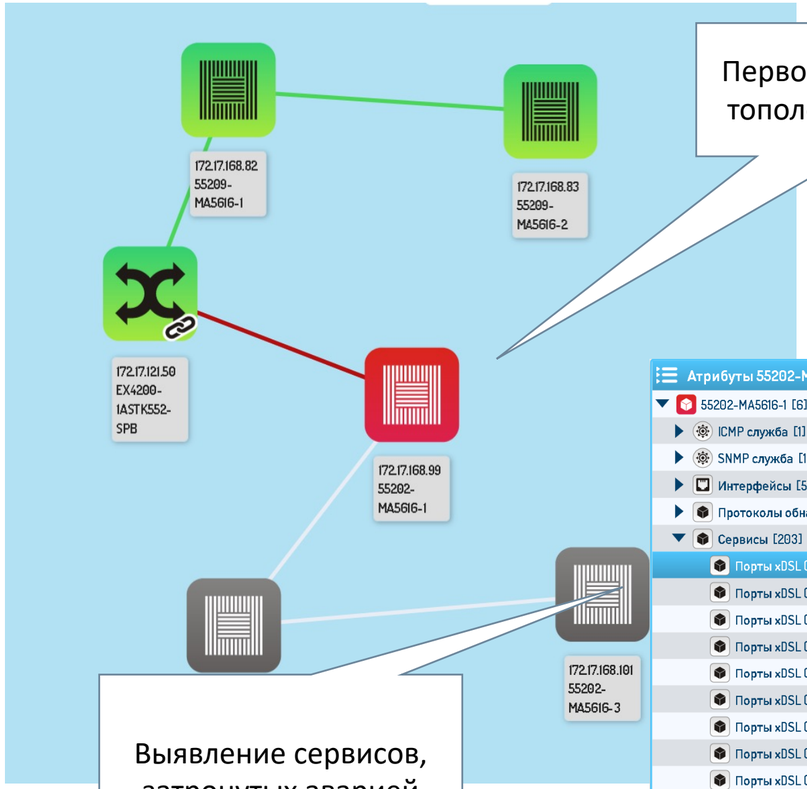
Факты – любая комбинация последовательности событий, данных о производительности, их комбинаций, а также результатов работы производных функций во времени. Факт может быть использован в логической цепочке фактов или формировать аварийное сообщение.



Инити

Интеллектуальный поиск первопричины сбоя (RCA)

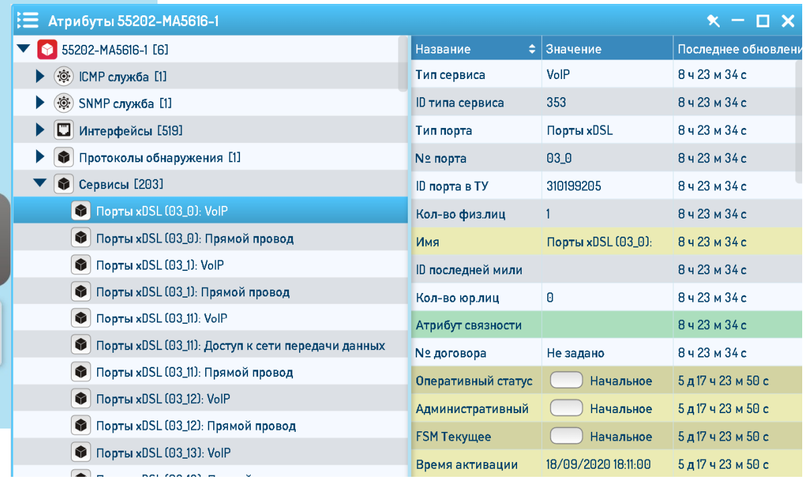
- **Автоматическая корреляция** (на основе встроенных математических методов)
- Возможность создания **собственных правил** корреляции.

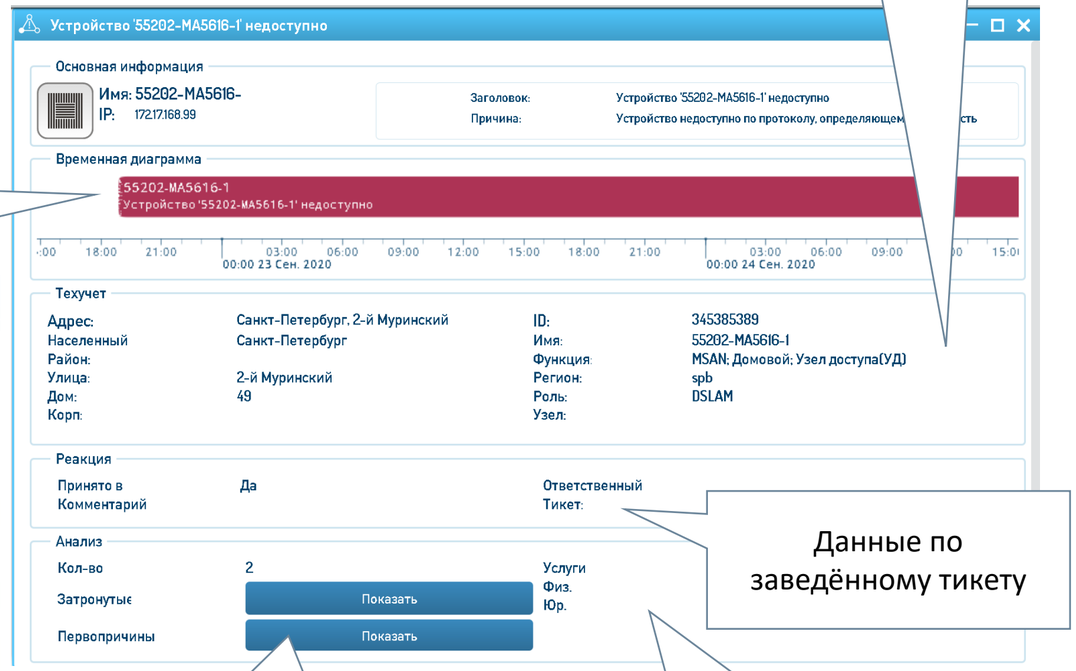


Первопричина сбоя на топологической карте

Временная диаграмма аварии

Инвентарные данные по аварийному устройству





Данные по заведённому тикету

Выявление сервисов, затронутых аварией

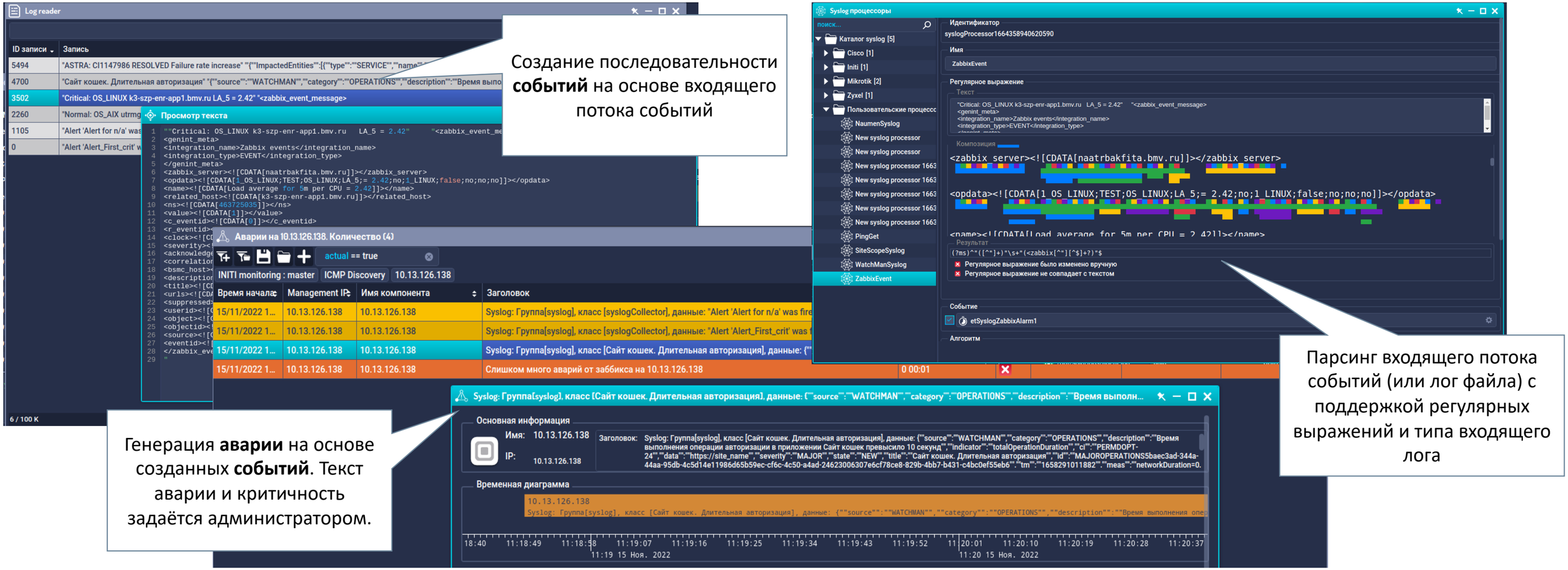
События, породившие сбой (на основе правил корреляции)

Услуги, затронутые аварией

Инити

Работа с «сырыми» событиями и анализ логов

- Возможность создания **собственных правил** обработки и корреляции для syslog, trap, данных лог-файлов или внешних API от сторонних систем.



Инити

Конструктор отчётов, подсистема отчётности

Система имеет гибкий графический конструктор отчётов. Дашборд = отчёт.

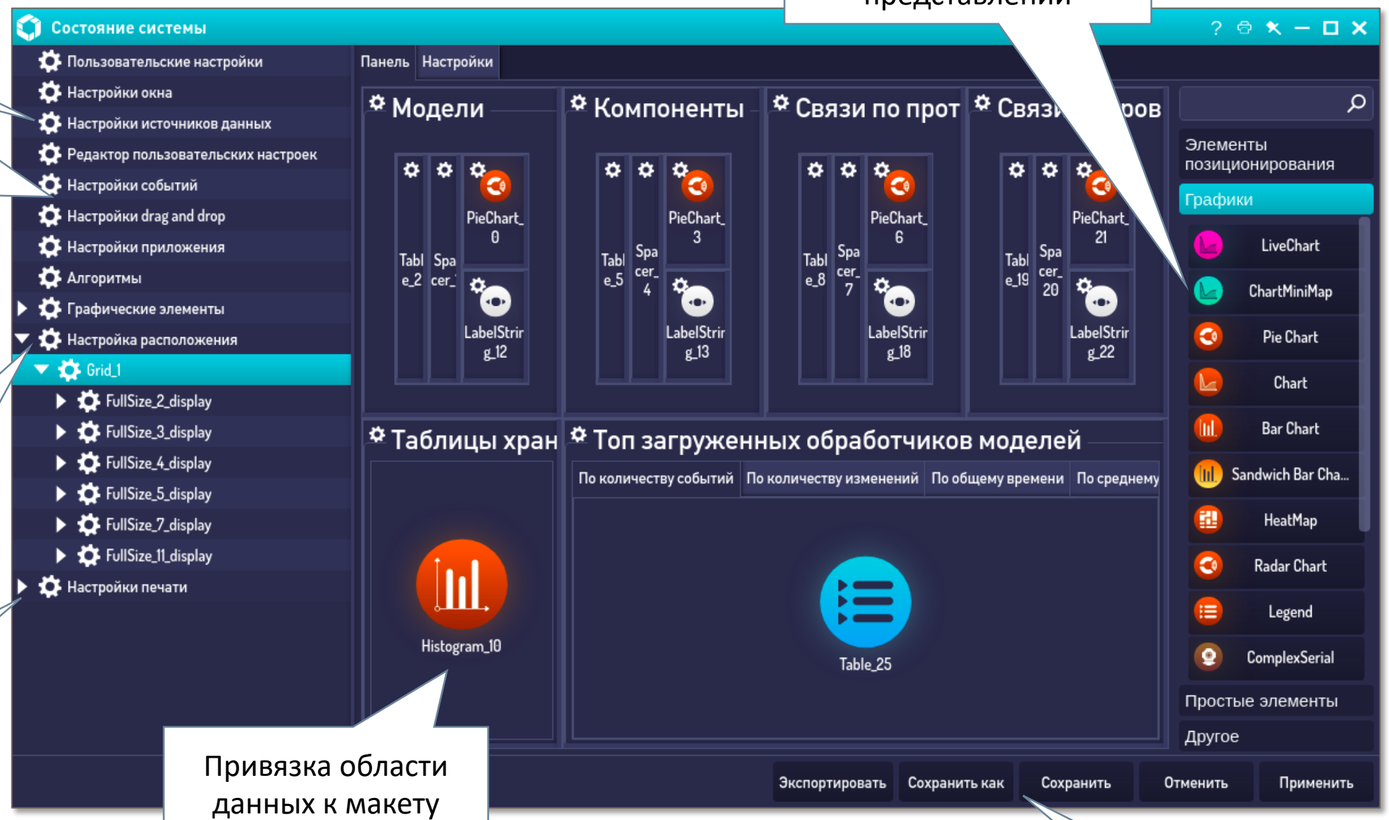
Настройка области данных (dataset)

Настройки взаимодействия между областями данных

Настройка макета дашборда / отчёта

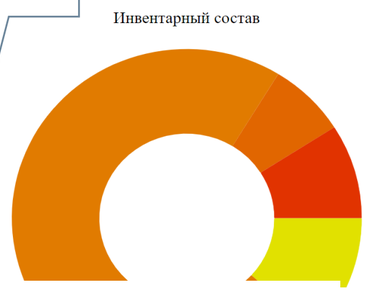
Настройка печатной формы

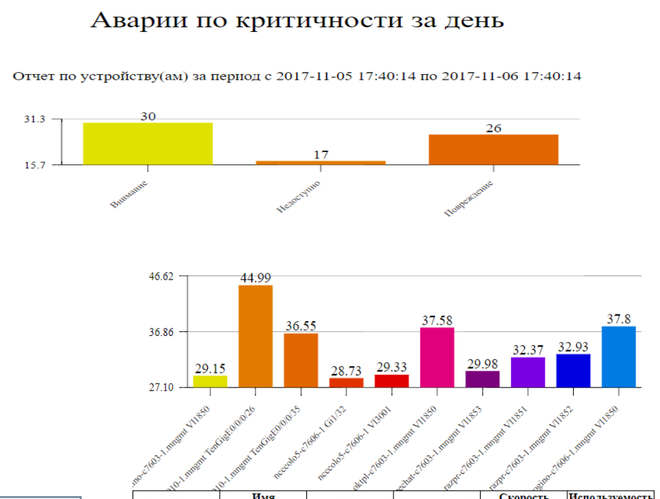
Настройка визуальных представлений



Привязка области данных к макету дашборда / отчёта

Примеры печатных форм отчётов





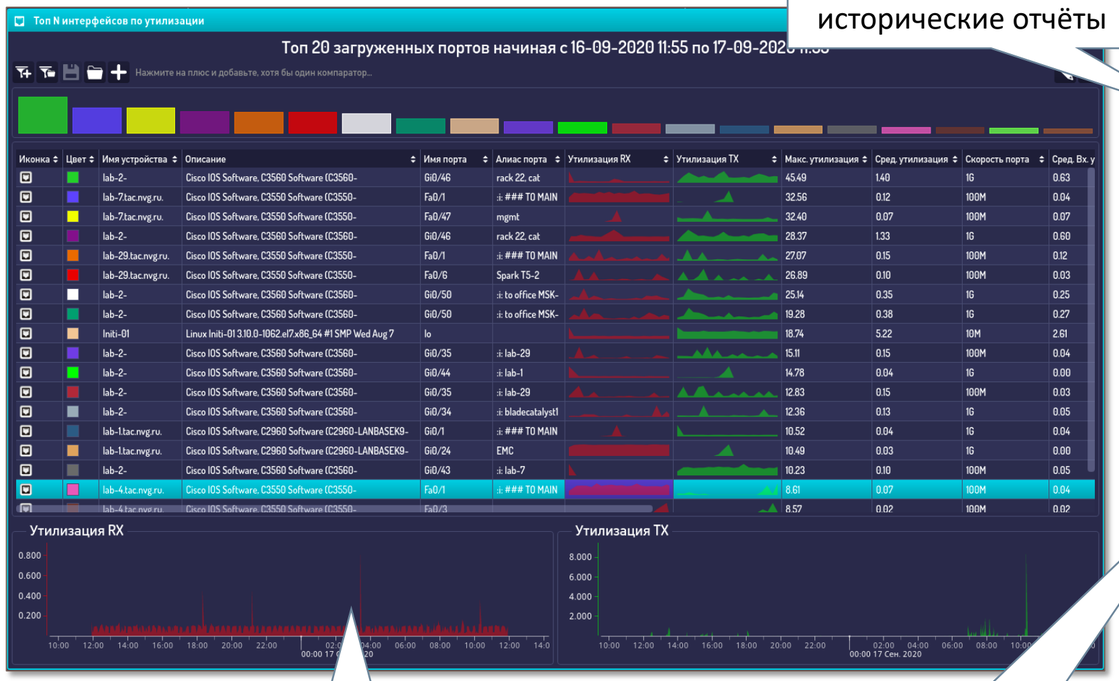
Устройство	Имя интерфейса	Alias	Тип интерфейса	Скорость интерфейса	Используемость (%)
lubyan-c7603-1.mngmt	Te1/1	Sncc-asr9010-1:TenGigE0/0/0/26$		10000000000	47.77
ncc-asr9010-1.mngmt	TenGigE0/0/0/26	Slubyan-c7603-1:TenGigabitEthernet1/1$		10000000000	44.99
strogino-c7606-1.mngmt	Vl1850	17/1592, ISVN MosMetro, 300M, b2B		1000000	37.8

Возможность наследования дашбордов и сохранения

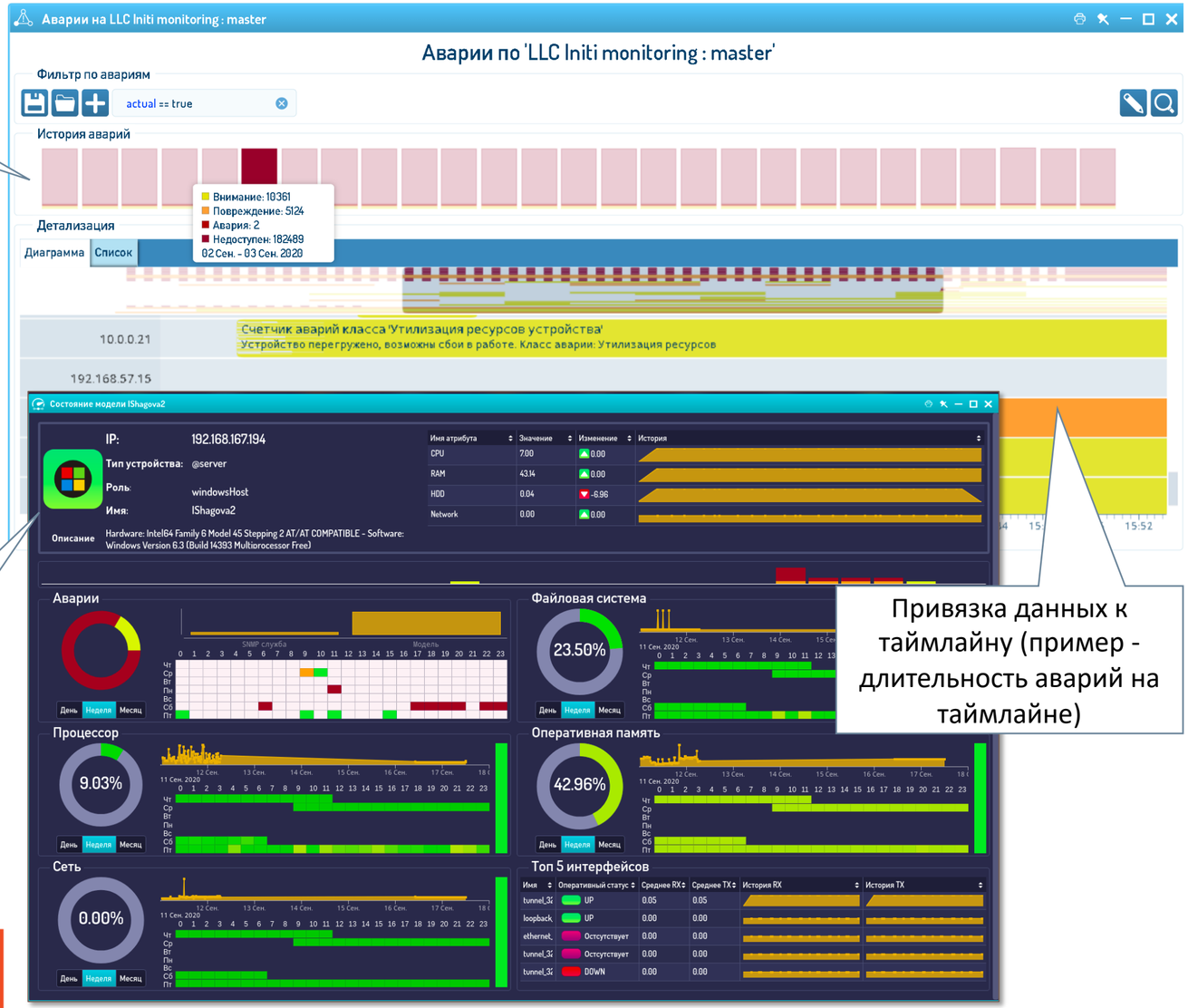
Инити

Сводные дашборды - отчётность

Примеры специализированных представлений (дашбордов)



Различного вида исторические отчёты



Привязка данных к таймлайну (пример - длительность аварий на таймлайне)

Различные TOP-N отчёты и дашборды

Специализированные дашборды для различных типов оборудования

Инити

Интеграция с внешними OSS/BSS системами

actual == true

Время начала	Имя компонента	Заголовок	Принято	Ответственный	Кол-во затронутых	Тикет	Критичность	И
24/09/2020	10.173.20.1	Устройство '10.173.20.1' недоступно	✅		0	АВР_Соло-15861360	Недоступен	10
23/09/2020	81365768K0001-MES3324F-1	Устройство '81365768K0001-MES3324F-1' недоступно	✅		0	АВР_Соло-15856423	Недоступен	81
18/09/2020	GATCHINA-PTS-Z8-HIX5630-2	Устройство 'GATCHINA-PTS-Z8-HIX5630-2' недоступно	✅		0	АВР_Соло-15828726	Недоступен	GA
24/09/2020	Voiskovitsy-C3750	Устройство 'Voiskovitsy-C3750' недоступно	✅		0	03-15851361	Недоступен	Vo
24/09/2020	Gi3/26	RX утилизация, % >= 80.0. Компонент: 'Gi3/26' (interf... Атрибут:	❌		0		Внимание	pu

Устройство

Журнал аварий: мониторинг

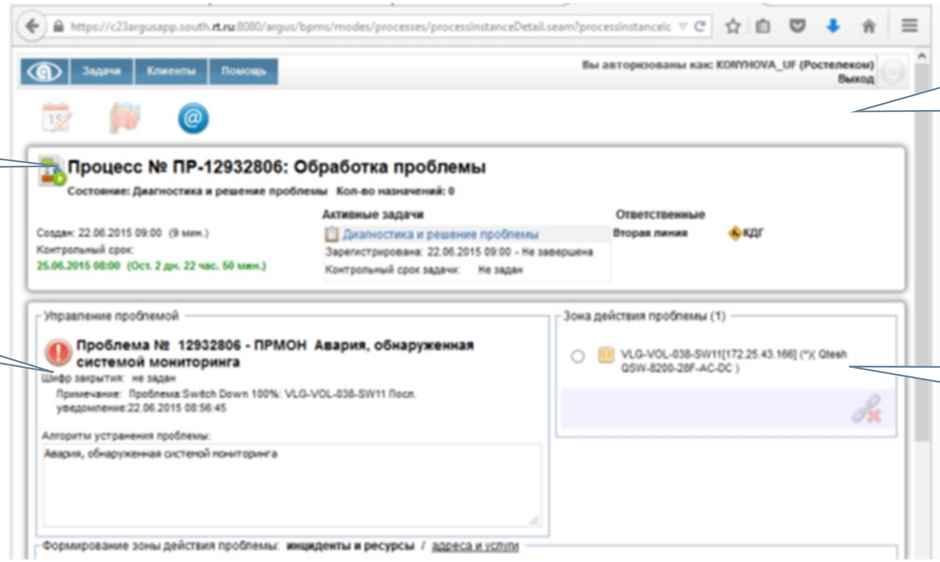
Текст события

Принято или нет в работу в Service Desk

Открытый API

Кем принято (при наличии) из Service Desk

Уникальный номер тикета



Идентификатор тикета

Автоматически сформированный тикет в Service Desk

Текст аварии

Зона действия проблемы

Инити

Результаты Discovery – наполнение и синхронизация с CMDB

Карточка сетевого оборудования в системе мониторинга

Атрибуты core1.sz.rt.su

- Атрибуты
- Платы
- Шасси
- Протоколы обнаружения
- Вентиляторы
- ICMP служба
- Интерфейсы
- Порты
- Блоки питания
- Сенсоры
- Слоты
  - Port Container 1/1
  - Port Container 1/2
  - Fan Tray Bay
  - Container of Power Supply Bay
  - Power Supply Bay 1
  - Power Supply Bay 2
  - Slot 1
  - Clock Module
  - Port Container 2/1
  - Port Container 2/2

Название	Значение		Последнее обновление
Инвентарный номер		String	Не обновлялся
Время активации	26/11/2019 11:54:50	Time	4 д 2 ч 25 м 50 с
Административный	Начальное	Integer	Не обновлялся
Адрес в ТУ	Тервеничи, Народная	String	1 д 7 м
Населенный пункт в	Тервеничи	String	1 д 7 м
Корпус в ТУ		String	1 д 7 м
Район в ТУ	Лодейнопольский	String	1 д 7 м
Функция в ТУ	IP-DSLAM; Узел	String	1 д 7 м
Дом в ТУ	21	String	1 д 7 м
ID в ТУ	79389615	Integer	1 д 7 м
Модель в ТУ	IskraTel UTA6044DD	String	1 д 7 м
Имя в ТУ	6437-1-UTA6044DD-	String	1 д 7 м
Регион в ТУ	spb	String	1 д 7 м
Роль в ТУ	DSLAM	String	1 д 7 м
Улица в ТУ	Народная	String	1 д 7 м
Узел в ТУ	Ленинградская	String	1 д 7 м
Загрузка ЦПУ %	0.0	Float	
Загрузка накопителя	0.0	Float	
Загрузка ОЗУ %	0.0	Float	

Атрибуты W2K8

- Атрибуты
- Физические процессоры
- ПО Управления Базами данных
- Экземпляры базы данных
- Диски
- Файловые системы
- Интерфейсы
- Операционная система - Windows
- Процессы
- Windows. Сервисы операционной системы
- WMI служба

Карточка серверного оборудования в системе мониторинга

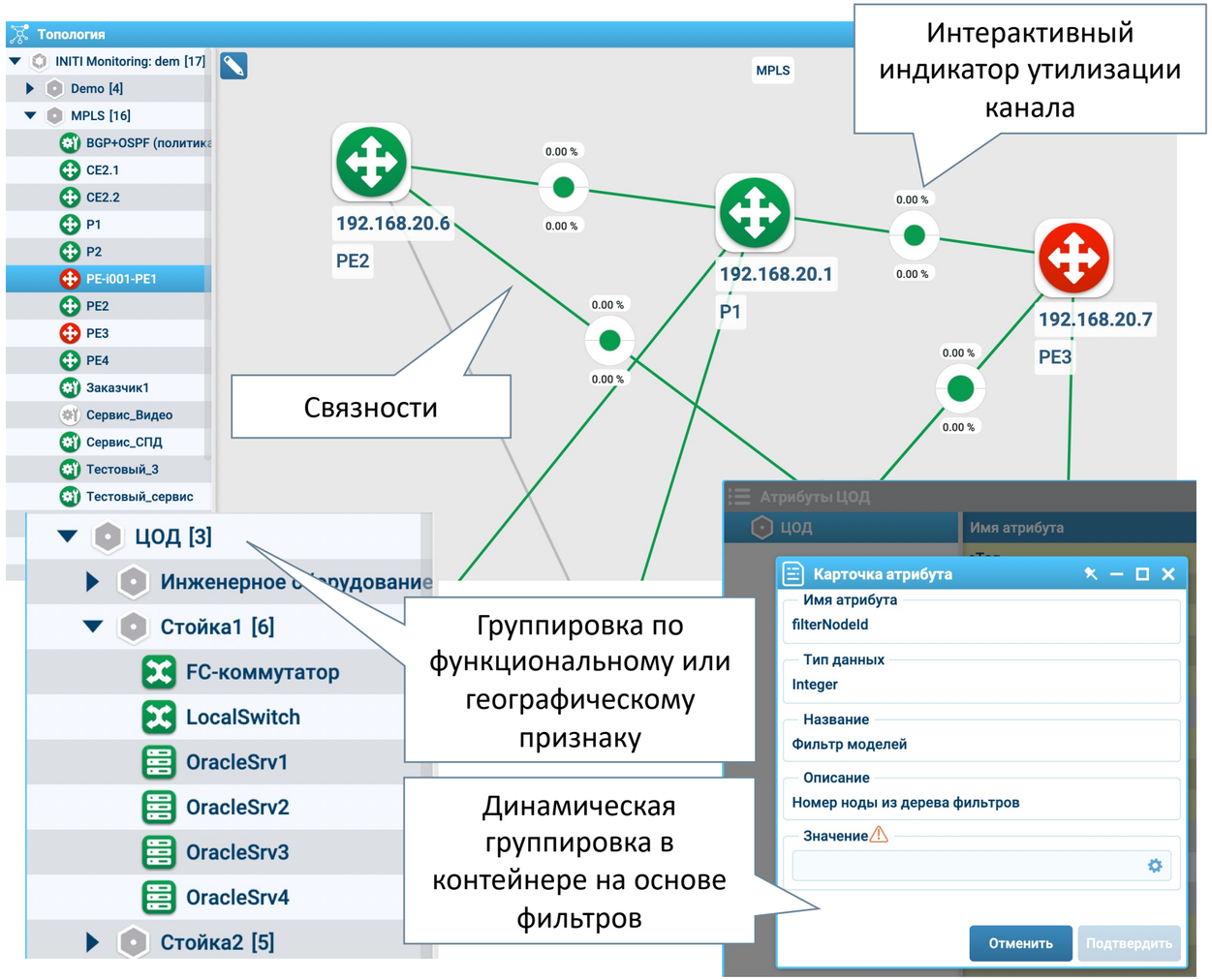
Атрибуты W2K8

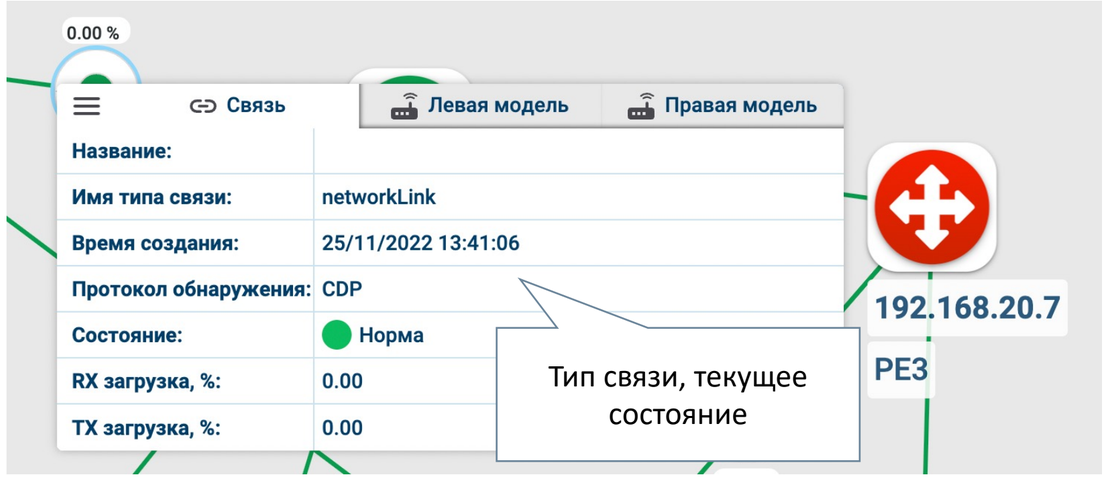
- Атрибуты
- Физические процессоры
- ПО Управления Базами данных
  - Microsoft SQL Server 2012
- Экземпляры базы данных
  - MASTER
  - MODEL
  - MSDB
  - TEMPDB
  - TESTDB
- Диски
  - \\.\PHYSICALDRIVE0
- Файловые системы
- Интерфейсы
- Операционная система - Windows
  - Microsoft Windows Server 2008 R2 Enterprise IC:\Windows\Device\Harddisk0\Partiti
- Процессы
- Windows. Сервисы операционной системы
- WMI служба

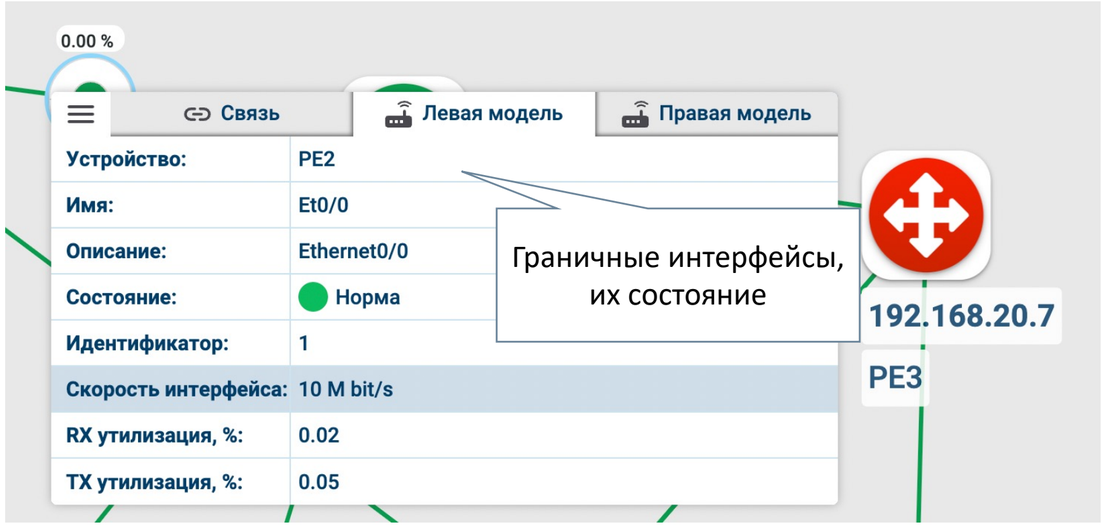
Не мониторится	false	Boolean	Не обновлялся
Объем памяти, Б	0	Integer	Не обновлялся
Объем диска, Б	0	Integer	Не обновлялся

Инити

Результаты Discovery - CMDB



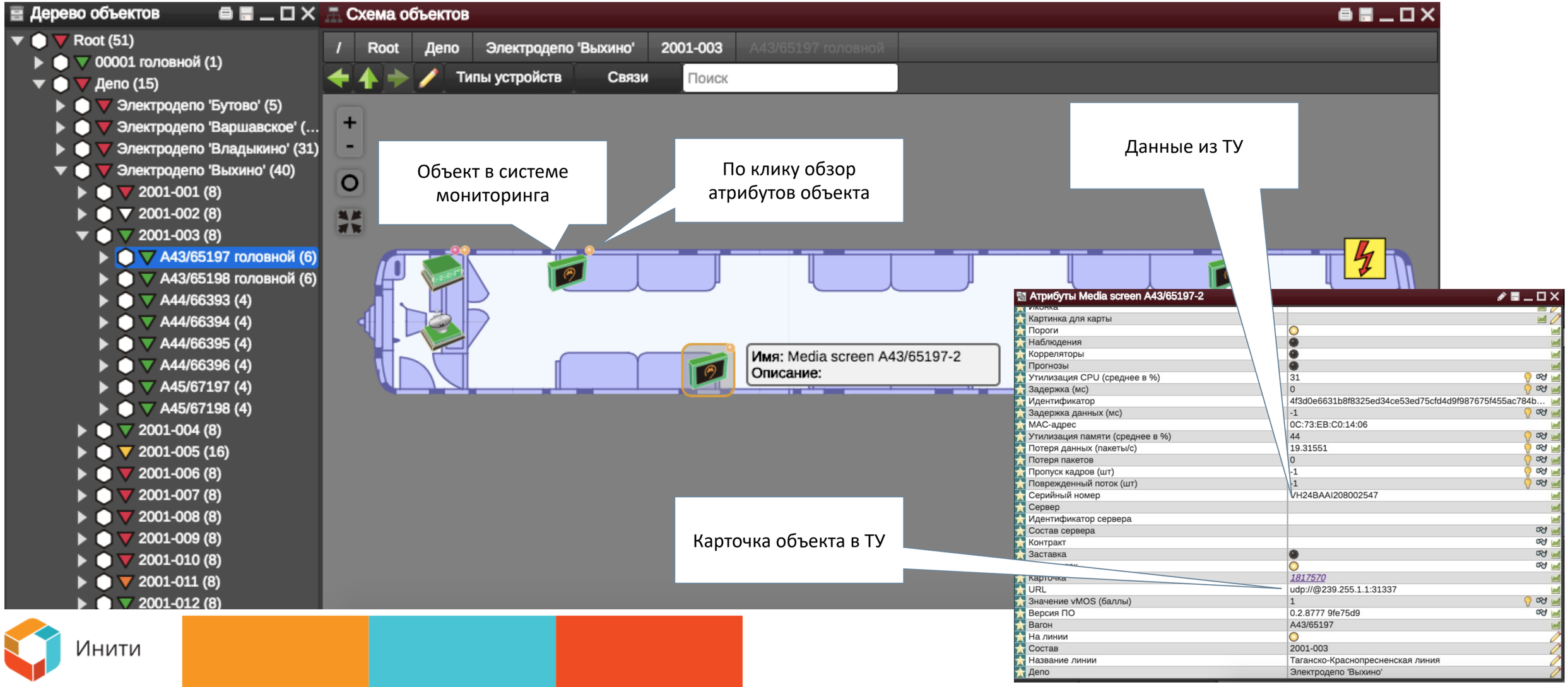




Инити

Интеграция с внешними OSS/BSS системами – пример

ИНИТИ СОЛО имеет продуктивный адаптер к решениям SD и ТУ



Инити

Интеграция с внешними OSS/BSS системами – пример

ИНИТИ СОЛО имеет продуктивный адаптер к решениям SD и ТУ

Карточка объекта в ТУ

Медиаэкран

Редактировать | Удалить | Изменить статус | Изменить тип | В эксплуатацию

Данные от системы мониторинга

Информация об оборудовании

Основная информация

Редактировать

Дата монтажа:	
Инвентарный номер:	
Серийный номер:	VH24BAAI222003634
IP-адрес:	10.90.29.53
MAC-адрес:	0C:73:EB:C0:1E:B5
Диагональ экрана:	21,5
Вагон:	A44/66016
Позиция в вагоне:	1
Статус:	Установлено
Пользователи:	

Конфигурация

Редактировать

Версия ПО:	0.2.8777 9fe75d9
Состояние в мониторинге:	Доступно

Финансы

Редактировать

Стоимость без НДС, руб.:	[redacted].03
НДС, руб.:	[redacted].83
Стоимость с НДС, руб.:	[redacted].86

Поставка

Редактировать

Штрих-код:

Печать

Медиаэкран
VH24BAAI222003634

Файлы

+ Добавить файл

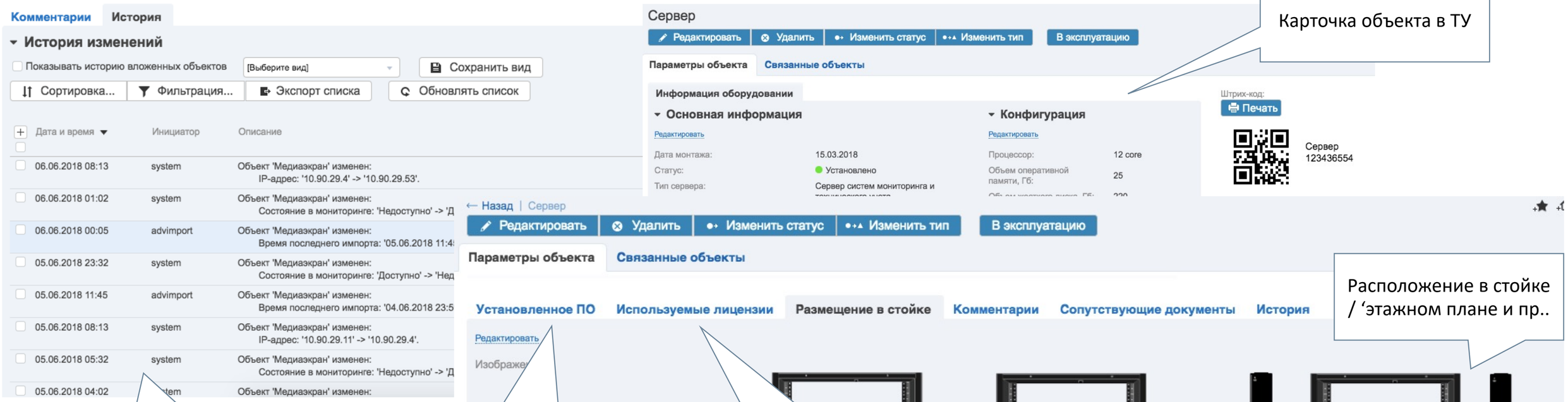
QR код по объекту (SN + инвентарный номер + именование)

Финансовая информация

Инити

Интеграция с внешними OSS/BSS системами – пример

ИНИТИ СОЛО имеет продуктивный адаптер к решениям SD и ТУ



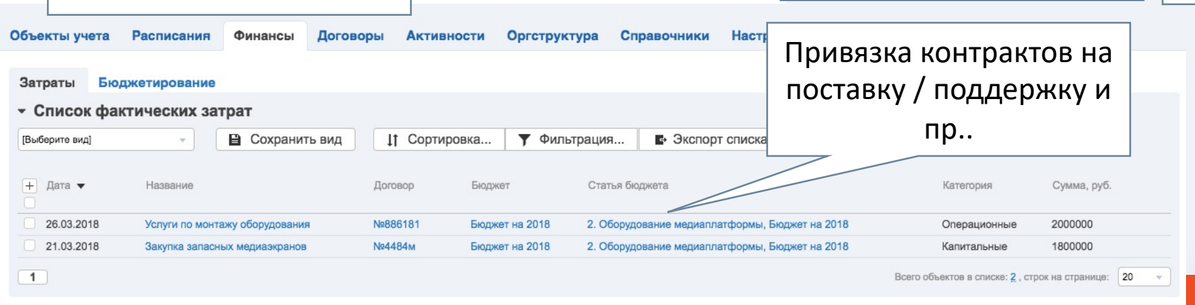
Карточка объекта в ТУ

Логирование истории изменений по объекту

Данные от системы мониторинга – установленное ПО

Используемые лицензии

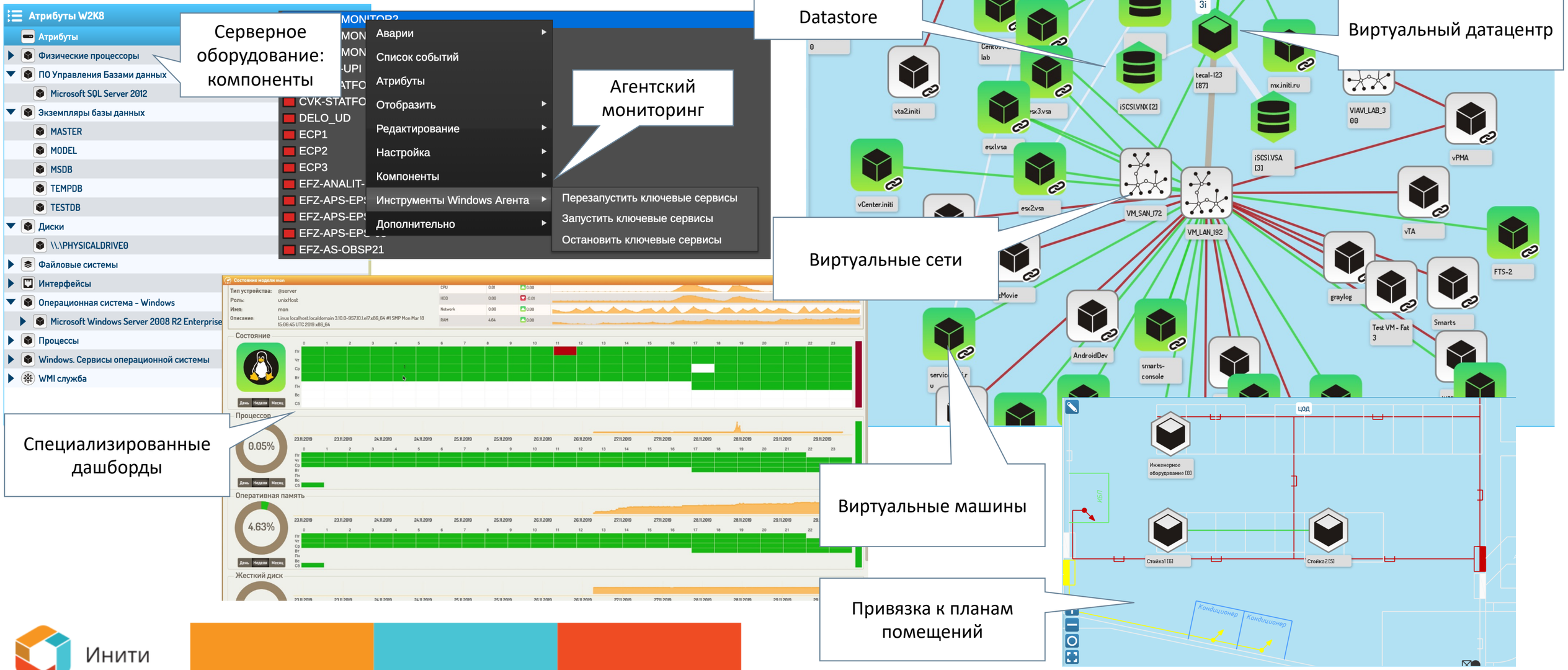
Расположение в стойке / ‘этажном плане и пр..



Привязка контрактов на поставку / поддержку и пр..

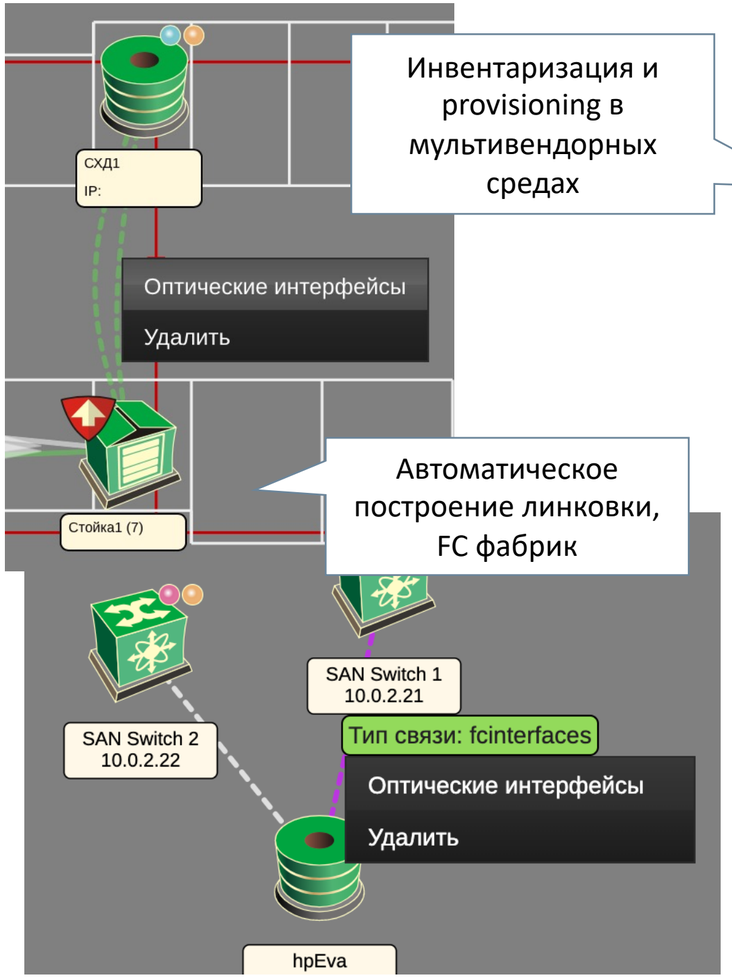
Мониторинг ИТ оборудования – сервера и ОС

Сервера, системы виртуализации, перифирийные устройства



Инити

Мониторинг ИТ оборудования – СХД и SAN



Инвентаризация и provisioning в мультивендорных средах

Автоматическое построение линковки, FC фабрик

LUNs EVA-6500-5 (7)

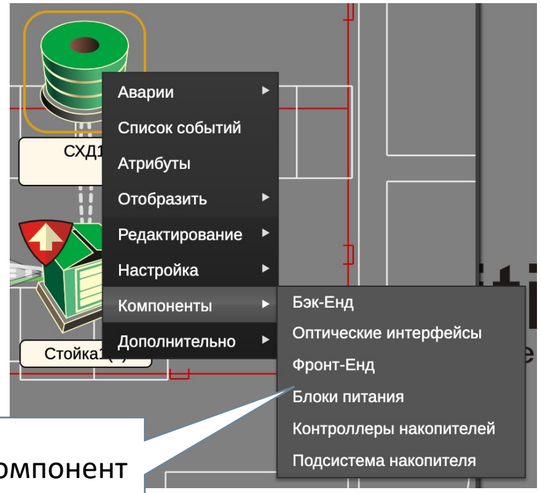
Список порогов | Создать наблюдение

Имя	core:Attributes.titles.virtualdiskname	Имя хоста	Номер LUN
/Hosts/Itanium_VMS_Cluster/92	/Virtual Disks/AUD/Copy of 1dga5820	/Hosts/Itanium_VMS_Cluster	92
/Hosts/Itanium_VMS_Cluster/4	/Virtual Disks/SYSTEM/1dga5005_ora	/Hosts/Itanium_VMS_Cluster	4
/Hosts/Itanium_VMS_Cluster/3	/Virtual Disks/SYSTEM/1dga5000_vm	/Hosts/Itanium_VMS_Cluster	3
/Hosts/B4_890/92	/Virtual Disks/AUD/Copy of 1dga5820	/Hosts/B4_890	92
/Hosts/B4_890/91	/Virtual Disks/AUD/Copy of 1dga5810	/Hosts/B4_890	91
/Hosts/B4_890/4	/Virtual Disks/SYSTEM/1dga5005_ora	/Hosts/B4_890	4
/Hosts/B4_890/3	/Virtual Disks/SYSTEM/1dga5000_vm	/Hosts/B4_890	3

Диски EVA-6500-5 (248)

Список порогов | Создать наблюдение

Диск	Модель	Статус	Описание	Дисковы	WWID	Дискова	Номер с	Номер г	core:Attrib	Форматир	Серийный	Использу
Disk 248	HSV360			EVA-6500-!	5001-E820·	SSD	2	10	sas	0	40358412	0
Disk 247	HSV360			EVA-6500-!	5001-E820·	SSD	3	5	sas	0		
Disk 246	HSV360			EVA-6500-!	5001-E820·	SSD	1	7	sas	0		
Disk 245	HSV360			EVA-6500-!	5001-E820·	SSD	2	7	sas	0		
Disk 244	HSV360			EVA-6500-!	5001-E820·	SSD	2	9	sas	0		
Disk 243	HSV360			EVA-6500-!	5001-E820·	SSD	2	3	sas	0		
Disk 242	HSV360			EVA-6500-!	5001-E820·	SSD	2	5	sas	0		
Disk 241	HSV360			EVA-6500-!	5001-E820·	SSD	1	5	sas	0	40119800	0
Disk 240	HSV360			EVA-6500-!	5001-E820							
Disk 239	HSV360			EVA-6500-!	5001-E820							
Disk 238	HSV360			EVA-6500-!	5001-E820							
Disk 237	HSV360			EVA-6500-!	5001-E820							



Мониторинг компонент СХД

Подсистема накопителя СХД1 (4)

Список порогов | Создать наблюдение

Серийный но	Массив	Дата	Перис	IOPS	Чтение	Запись	Хит (%
000290101870	SYMM 000290101870 Array		0	24081.1	0.0	0.0	0.0
000290101869	SYMM 000290101869 Array		0	23076.1	0.0	0.0	0.0
000290101868	SYMM 000290101868 Array		0	22138.0	0.0	0.0	0.0
000290101867	SYMM 000290101867 Array		0	23724.7	0.0	0.0	0.0

График

Реальное время | h 1 : 0 m | ok

IOPS
СХД1: Подсистема н…
IOPS: 24081.1

24500 24000 23500 23000 22500 22000

11:50:00 2019-04-07 | 11:58:20 2019-04-07 | 12:06:40 2019-04-07 | 12:15:0 2019-04-

Просмотр деталей (Подсисте…

Имя	Значение
Серийный номер	000290101870
Массив	SYMM 000290101870 Array
Дата	
Период	0
IOPS	24081.1
Чтение (%)	0.0
Запись (%)	0.0
Хит (%)	0.0
Скорость (Мб/с)	876.1
Загрузка	45.4
Емкость (Гб)	0
Использовано (Гб)	0
Использовано (%)	0.0

Отслеживание утилизации компонент в мультивендорных SAN средах

Инити

Мониторинг ИТ оборудования – приложения

Процессы OracleSrv1 (6)

Список порогов | Создать наблюдение

ID проце	Имя	Память	Память	CPU	Пользова	Время р	Команда	Время за	Путь	Параметр	Тип	Идентифи
32434	Oracle	8.85Gb	0.00	10.2		1630 20:57	/usr/bin/ora	2014-10-19				
13718	nm-dispatc	14.78Gb	0.00	95.4		1630 20:56	/usr/libexec	2014-10-19				
6026	httpd	9.78Gb	0.00	94.8		1630 20:57	/usr/sbin/htt	2014-10-19				
577	python	13.99Gb	0.00	99.5		1630 20:57	/usr/bin/pytl	2014-10-19				
452	systemd-jo	10.10Gb	0.00	98.7		1630 20:57	/usr/lib/syst	2014-10-19				
1	systemd	15.25Gb	0.00	98.9		1630 20:57	/usr/lib/syst	2014-10-19				

Просмотр деталей (Процессы OracleSrv1)

Имя	Значение
ID процесса	13718
Имя	nm-dispatcher
Память	8.44Gb
Память (%)	0.00
CPU	95.5
Пользователь	
Время работы	1630 20:55:05.928518
Команда	/usr/libexec/nm-dispatcher.action
Время запуска	2014-10-19 16:55:03
Путь	
Параметр	
Тип	
Идентификатор статуса	

График

Реальное время h 1 : 0 m ok

100 98 96 94

12:15:00 2019-04-07 | 12:31:40 2019-04-07 | 12:48:20 2019-04-07

Процессы приложений

Специализированные приложения и сервисы: Параметры AD

Базы данных

GREEN

Очереди

IBM MQ

Очереди MQ

Атрибуты Active Directory

Установить отслеживание | Сохранить значения | Перетащите аттрибут для отображения на графике

Имя	Значение
Состояние объекта	Норма
Контакты	Администратор. Подопрелов М.Г.
Описание	Служба Active Directory
Иконка	
Широта	55.718699
Долгота	37.629622
Имя	Active Directory
Состояние компонентов	Норма
Загрузка процессора (суммарно)	0
Использовано ОЗУ (суммарно)	0
Пользовательский атрибут 4	false
Пользовательский атрибут 3	0
Пользовательский атрибут 2	0

Тесты (vHmrun) Oracle DB (28)

Список порогов | Создать наблюдение

Идентифика	Идентификат	Имя	Числ	Имя теста	Число инциде	Время начала	Время заверш	Источник инци	Режим запуска
7601	COMPLETED	HM_RUN_7601	0	DB Structure Int	0	2017-02-20 17:(	2017-02-20 17:(	0	REACTIVE
7581	COMPLETED	HM_RUN_7581	0	DB Structure Int	0	2017-02-20 17:(	2017-02-20 17:(	0	REACTIVE
7561	COMPLETED	HM_RUN_7561	0	DB Structure Int	0	2017-02-20 17:(	2017-02-20 17:(	0	REACTIVE
7541	COMPLETED	HM_RUN_7541	0	DB Structure Int	0	2017-02-20 16:5	2017-02-20 16:5	0	REACTIVE
7521	COMPLETED	HM_RUN_7521	0	DB Structure Int	0	2017-02-20 16:5	2017-02-20 16:5	0	REACTIVE
7501	COMPLETED	HM_RUN_7501	0	DB Structure Int	0	2017-02-20 16:5	2017-02-20 16:5	0	REACTIVE
7481	COMPLETED	HM_RUN_7481	0	DB Structure Int	0	2017-02-20 16:5	2017-02-20 16:5	0	REACTIVE
7461	COMPLETED	HM_RUN_7461	0	DB Structure Int	0	2017-02-20 16:5	2017-02-20 16:5	0	REACTIVE
7441	COMPLETED	HM_RUN_7441	0	DB Structure Int	0	2017-02-20 16:5	2017-02-20 16:5	0	REACTIVE

Атрибуты Веб-интерфейс АС Обеспечение

Описание	
Выборы: Тип устройства	
Площадка	
Иконка	urlcheck
Картинка для карты	
IP	10.21.42.95
Последний ответ	1970-01-01 03:00:00
Время старта таймера недоступности	2019-04-07 12:56:47
Широта	0
Расположение	
Долгота	0
Прокси для инструментов	
Состояние	Начальное
Имя	Веб-интерфейс АС Обеспечение
Порт	0
Имя БД	
ФТС - Имя объекта	
ФТС - Тип объекта	
ФТС - Имя сервера	
Загрузка процессора (суммарно)	0
Использовано ОЗУ (суммарно)	0
Web-server - Строка запроса	http://10.21.42.95:7003/Asg.html
Web-server - Время ответа (сек.)	0
Web-server - Код ответа	200
core:Attributes.titles.webResponseStatus	
Web-server - Ответ сервера	OK
Web-server - Тип сервера	UNKNOWN
Таймаут недоступности	60
(Вспом.) Влияет на сервисы	АС «Обеспечение»
(Вспом.) ФТС - Имя объек	
(Вспом.) ФТС - Тип объек	Web сервер

WEB сервис

Аварии
Список событий
Атрибуты
Отобразить
Редактирование
Настройка
Компоненты
Дополнительно

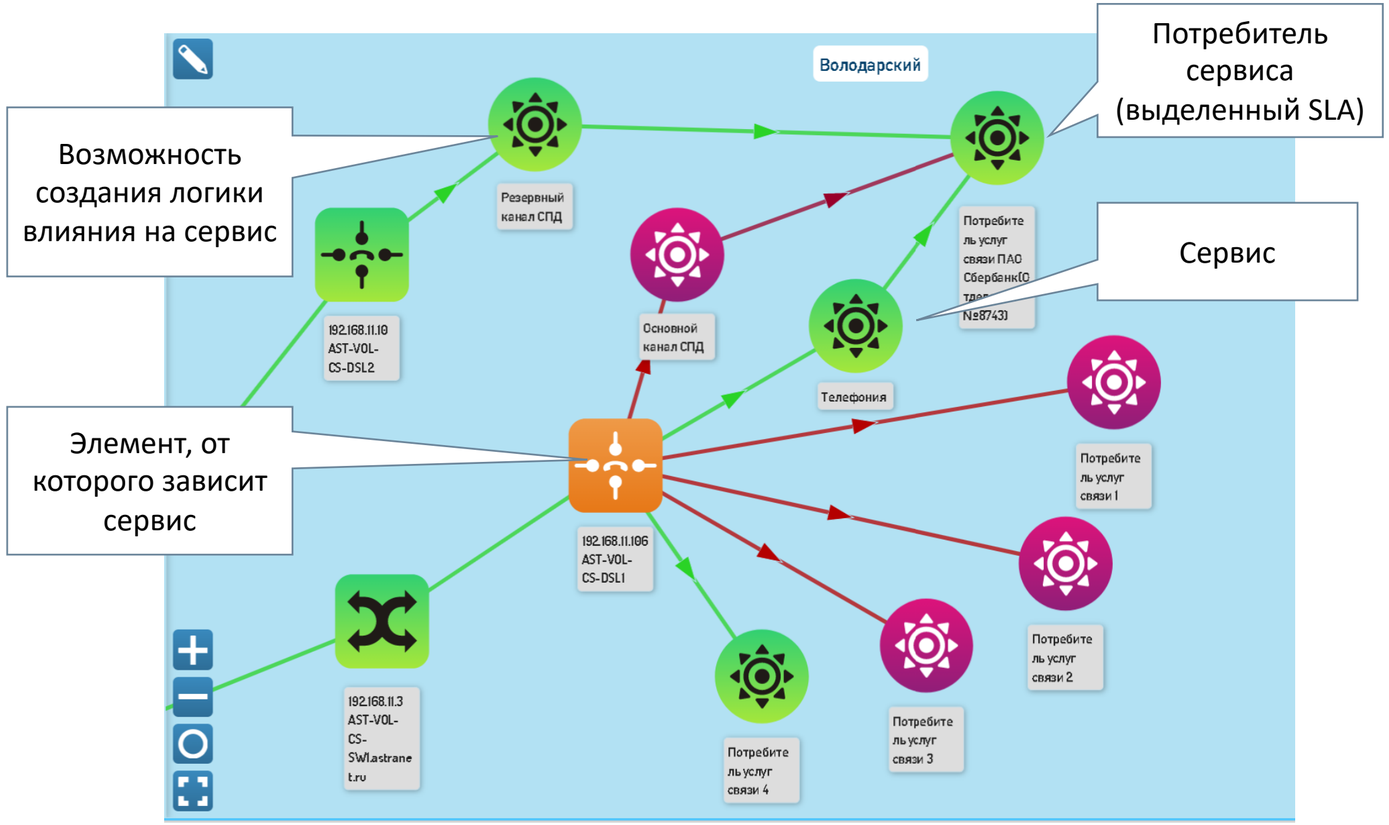
Результаты тестов (vHmfinding)
Тесты (vHmrun)
Процессы (vProcess)
Сессии пользователей (vSession)
Ожидающие сессии (vSessionwait)
SGA информация (vSgainfo)
Показатели производительности (vSysstat)
Табличные пространства (vTablespace)

Детальный мониторинг ПО: СУБД

Инити

Сервисно-ресурсная модель

Контроль сервисов, предоставляемых внешним или внутренним пользователям, Контроль подрядчиков



Каталог ИКТ сервисов — реестр предоставляемых сервисов, включает в себя описание сервисов, SLA, элементы финансовой оценки. Каталог услуг в разрезе системы мониторинга (сервисная модель) может быть:

- Импортирован из внешнего каталога услуг, доступных к заказу конечным пользователем;
- Импортирован из структурированного документа, описывающий предоставляемые ИКТ услуги (сервис-каталог);
- Синхронизирован с сервисами и SLA в системе Сервис Деск для привязки обращений к ИКТ услугами и последующей обработки запросов в соответствии с ассоциированными SLA;
- Описан сервисов и SLA в системе мониторинга ИНИТИ для обеспечения оперативного мониторинга предоставляемых ИКТ услуг на предмет качества (встроенный конструктор).

Сервисно-ресурсная модель

Сводные показатели сервиса (сервисный дашборд)

Сводные данные на timeline

Настройки сервиса: Цифровое ТВ (IPTV)

Ресурсы

Имя	Состояние
Порт IPTV	Авария
Порт IPTV	Авария
Порт IPTV	Норма
Порт IPTV	Авария
Порт IPTV	Авария

Возможность привязки состояния сервиса к конкретным компонентам оборудования или ПО

Показатели с... Потребитель услуг связи ПАО Сбербанк(Отделение №8743)

Сервис

Имя: Потребитель услуг связи

Описание: ПАО Сбербанк России

Доступность: Активен

Доступность: Активен, Активен

18:00 20:00 22:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00

00:00 24 Сен. 2020

SLA

SLA [1]

Ежедневный SLA

Показатели SLA

02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00

00:00 25 Сен. 2020

Название	Значение	Последнее обновление
Уровень доступности, %	98.68	5 ч 2 м 42 с
Отказы	4	5 ч 2 м 42 с
Время простоя	00 дней 00:10:17	5 ч 2 м 42 с

Возможность создания различных SLA (привязка ко времени, дням недели и пр..)

Настройки сервиса: Аппаратные сервера

Ресурсы

Имя	Состояние
Состояние MSK-ESOTSTSRV06	Норма
Состояние MSK-ESOTSTSRV04	Норма
Состояние MSK-ESOTSTSRV03	Норма
Состояние MSK-ESOTSTSRV02	Норма
Состояние MSK-ESOTSTSRV01	
Состояние MSK-ESO-DEP01	
Состояние MSK-DV-TEST	

Возможность привязки состояния сервиса к конкретному оборудованию целиком

Ресурсы

24/09/2020

Сервис Основной канал СПД : Ежедневный SLA0 49.72

03:00 06:00 09:00 12:00 18:00 21:00

00:00 24 Сен. 2020 00:00 25 Сен. 2020

Имя	Состояние
Сервис Телефония	Норма
Сервис Основной канал СПД	Недоступен
...л СПД	Норма

3 / 100 000

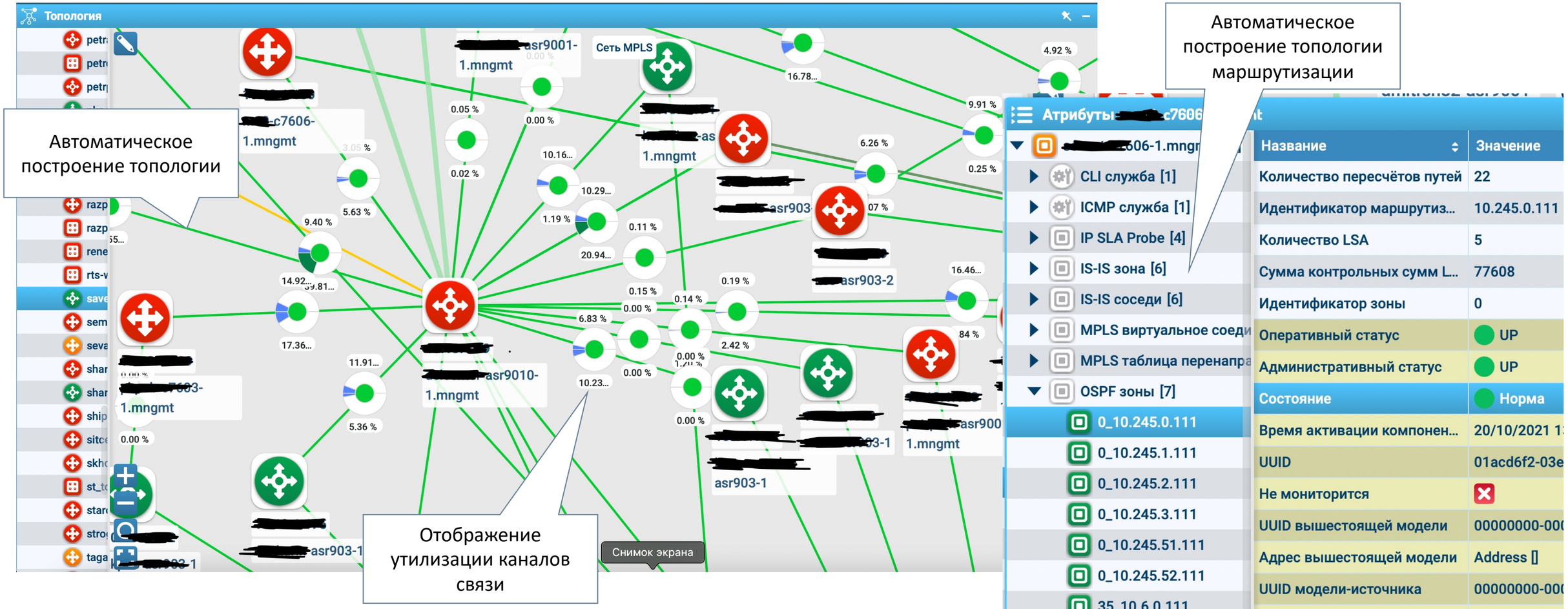
Статус подсервисов

Состояние сервисов на диаграмме в зависимости от выполнения SLA, просмотр изменений на временной шкале

Инити

Мониторинг сетевой инфраструктуры

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



Инити

Мониторинг сетевой инфраструктуры – IP/MPLS

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

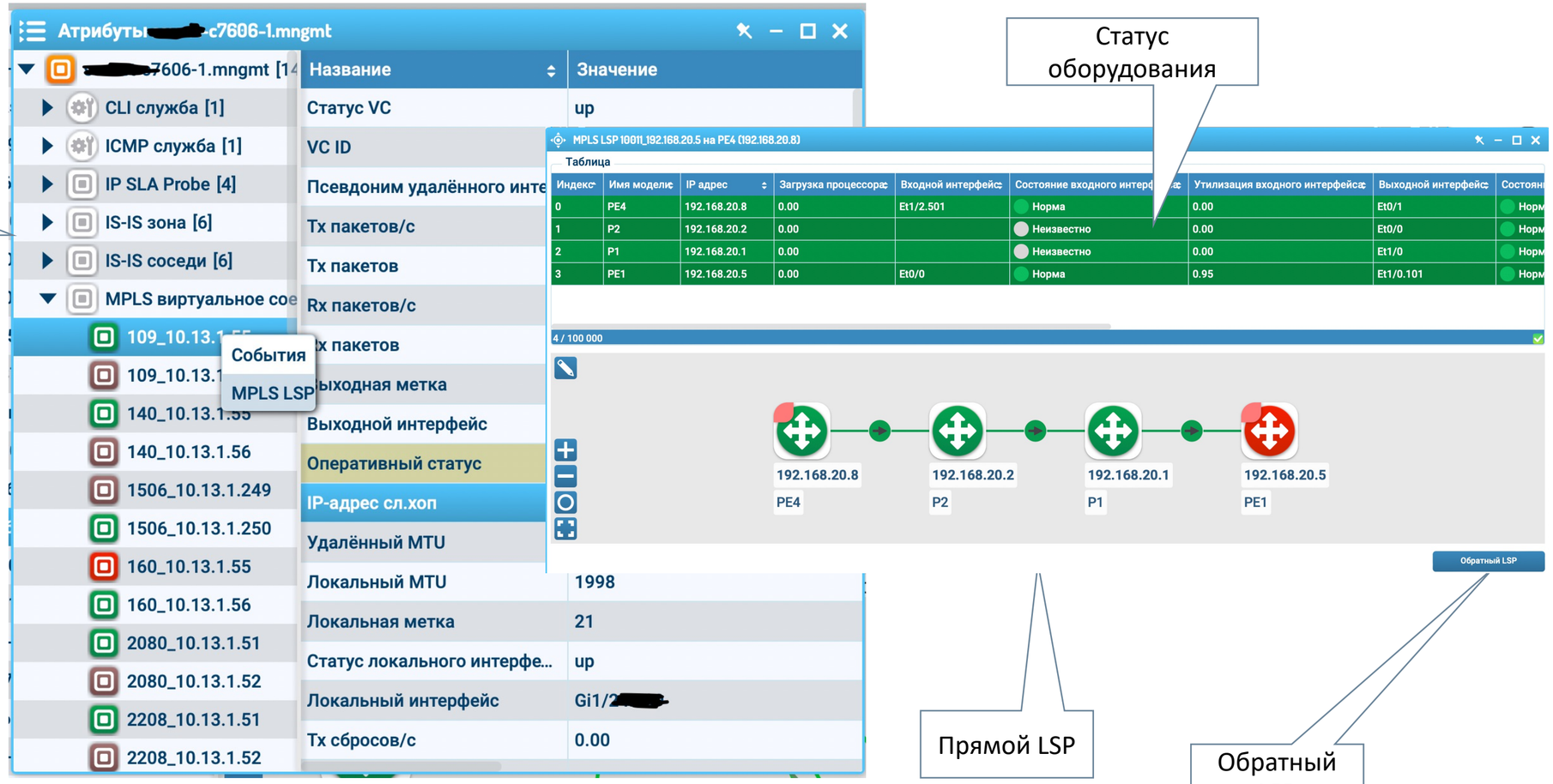
Общие объекты и компоненты MPLS сети:

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

MPLS пути

Объекты L2VPN:
Forwarder
Forwarder Endpoint
PseudoWire
VPN
VLAN
LdpAdjacency
LdpProtocol Endpoint
EVC
VRF
Route target

Объекты L3VPN:
VPN
Multicast VPN
VRF
Route Target



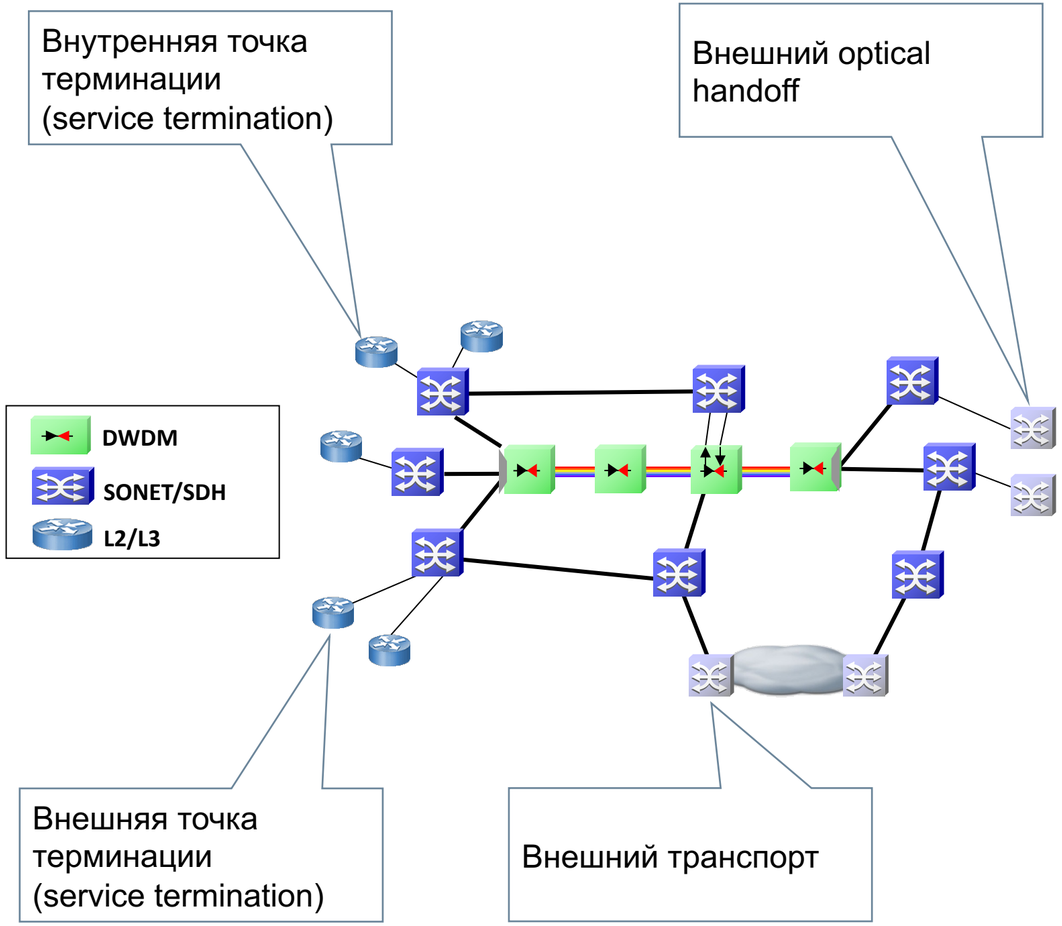
Статус оборудования

Прямой LSP

Обратный LSP

Инити

Мониторинг транспортных сетей



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

Технологии

- DWDM
- SONET/SDH
- Low Order SONET/ PDH

Модели

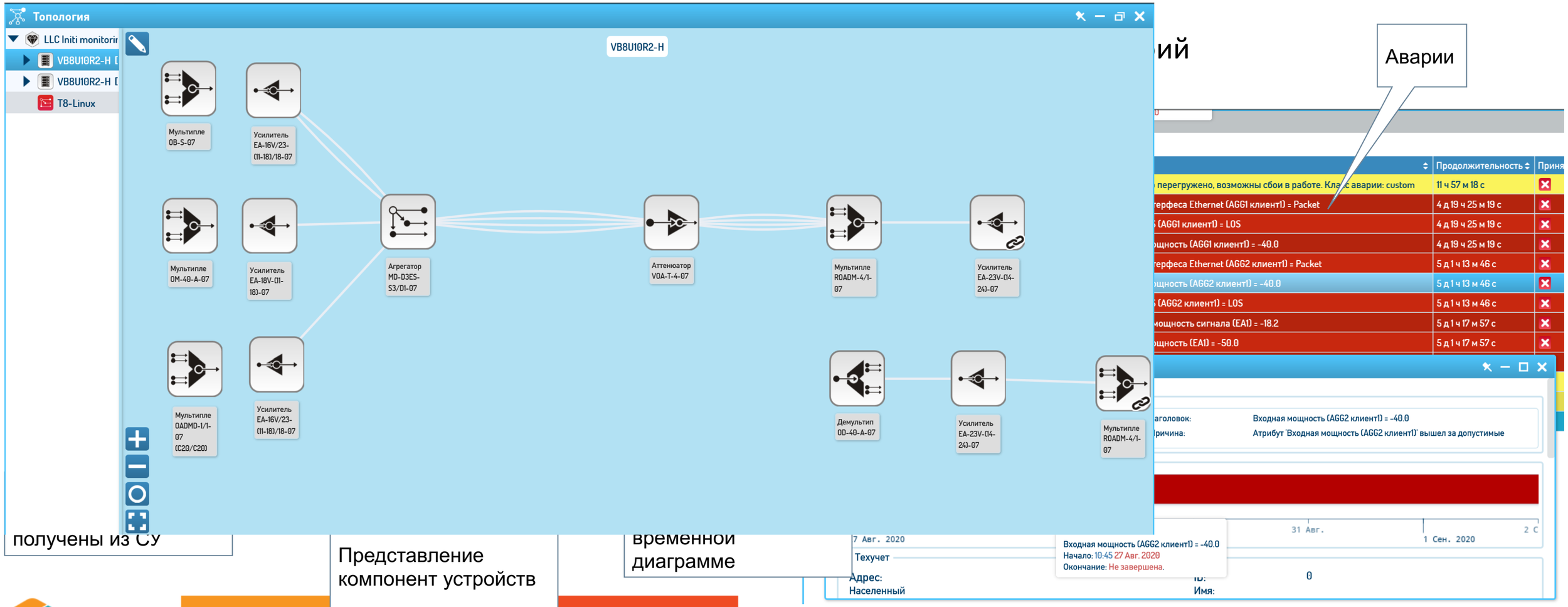
- Элементы сети, карты, физические / логические порты
- Топологические линки, Fiber, Fiber bundle
- Логические линки, Wavelength
- Client circuit, Trail
- Protection Groups

Поддержка работы в мультивендорных средах

Инити

Мониторинг транспортных сетей – примеры

Топология SDH, WDM



получены из СУ

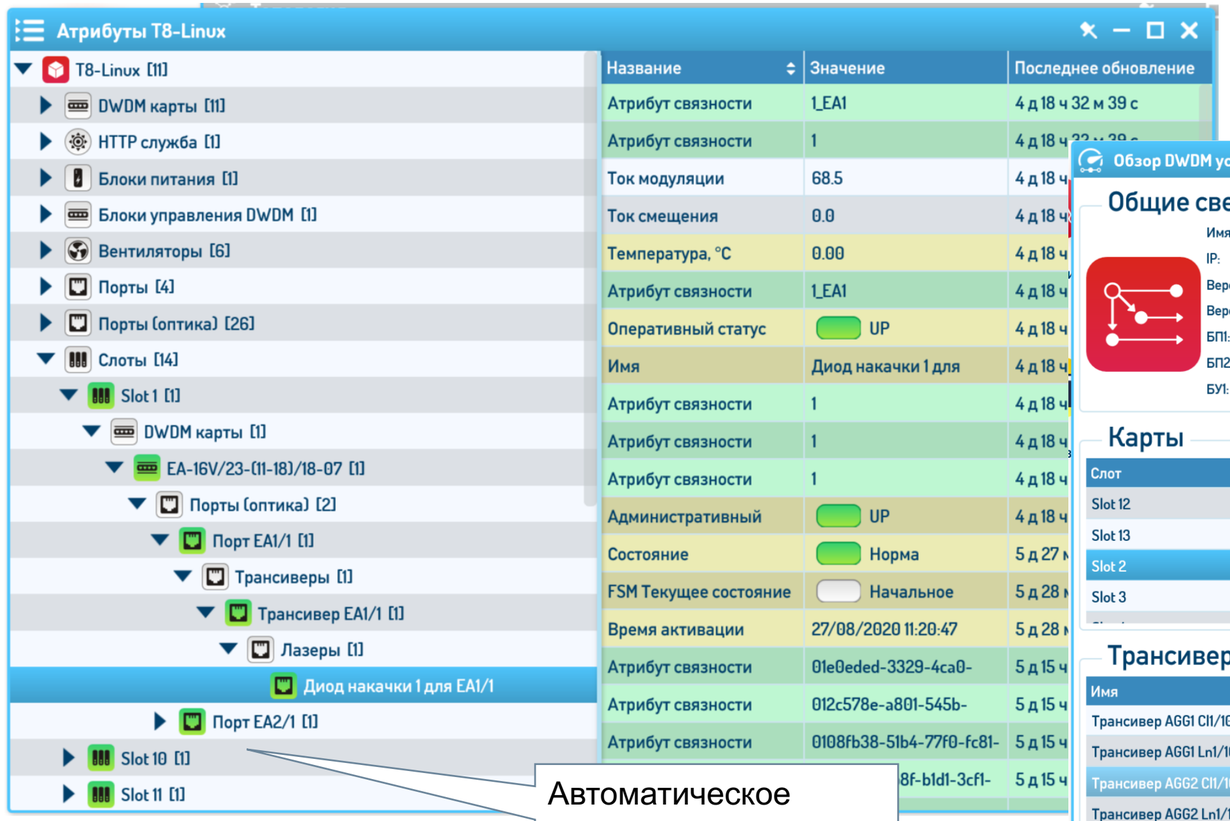
Представление компонент устройств

временной диаграмме

Инити

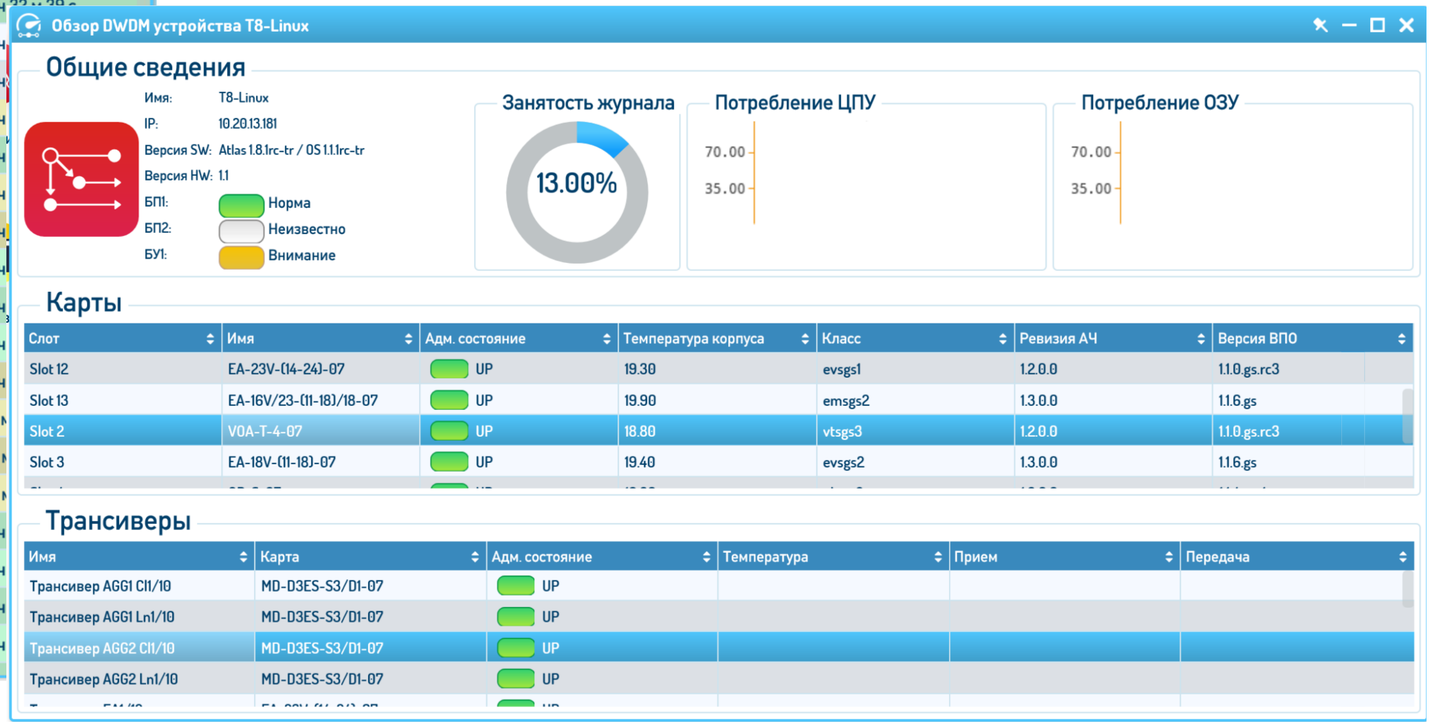
Мониторинг транспортных сетей – примеры

Иерархия объектов:



Автоматическое наполнение модели данных

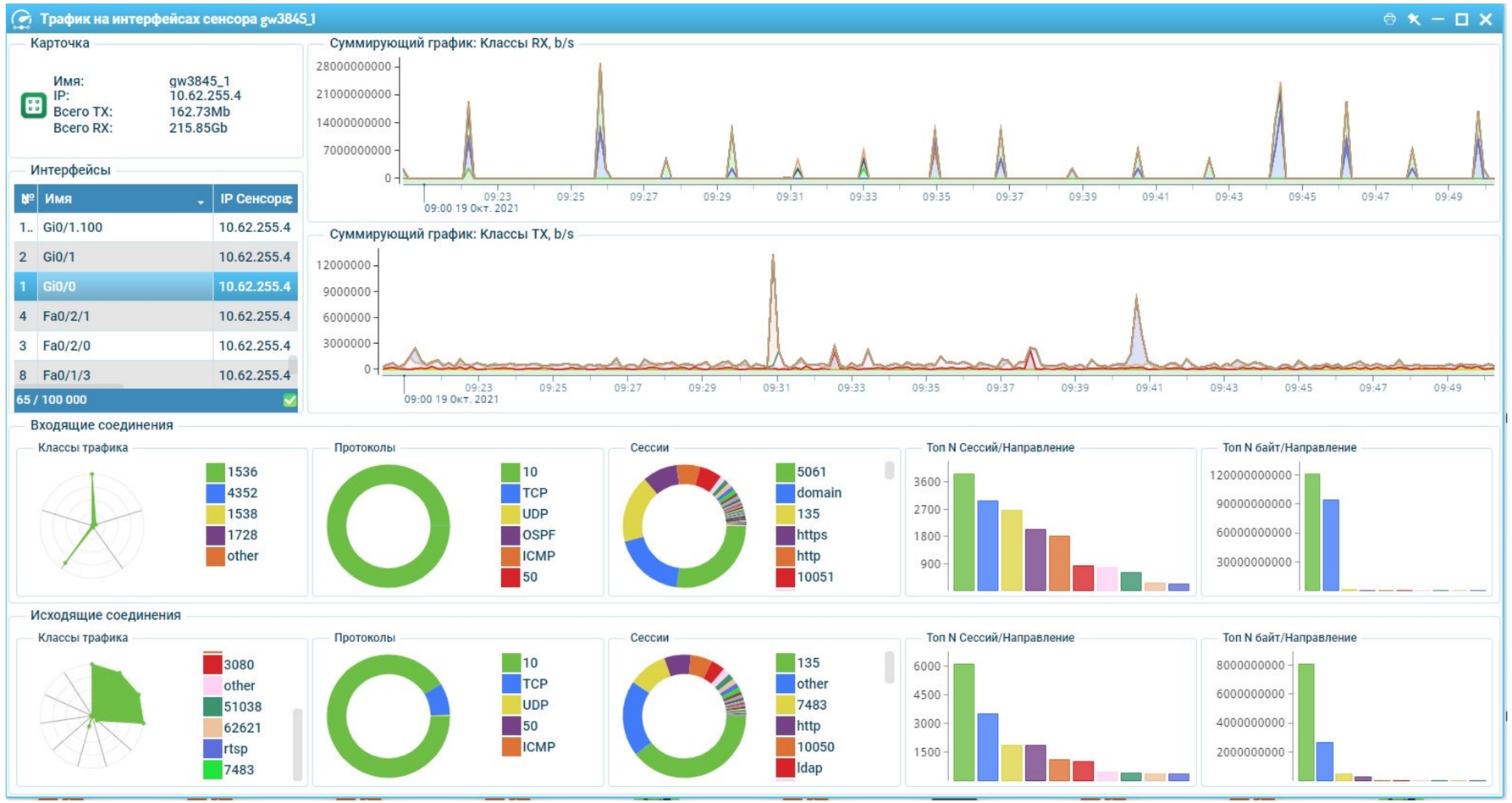
Специализированные дашборды



Инити

Мониторинг параметров сетевой инфраструктуры

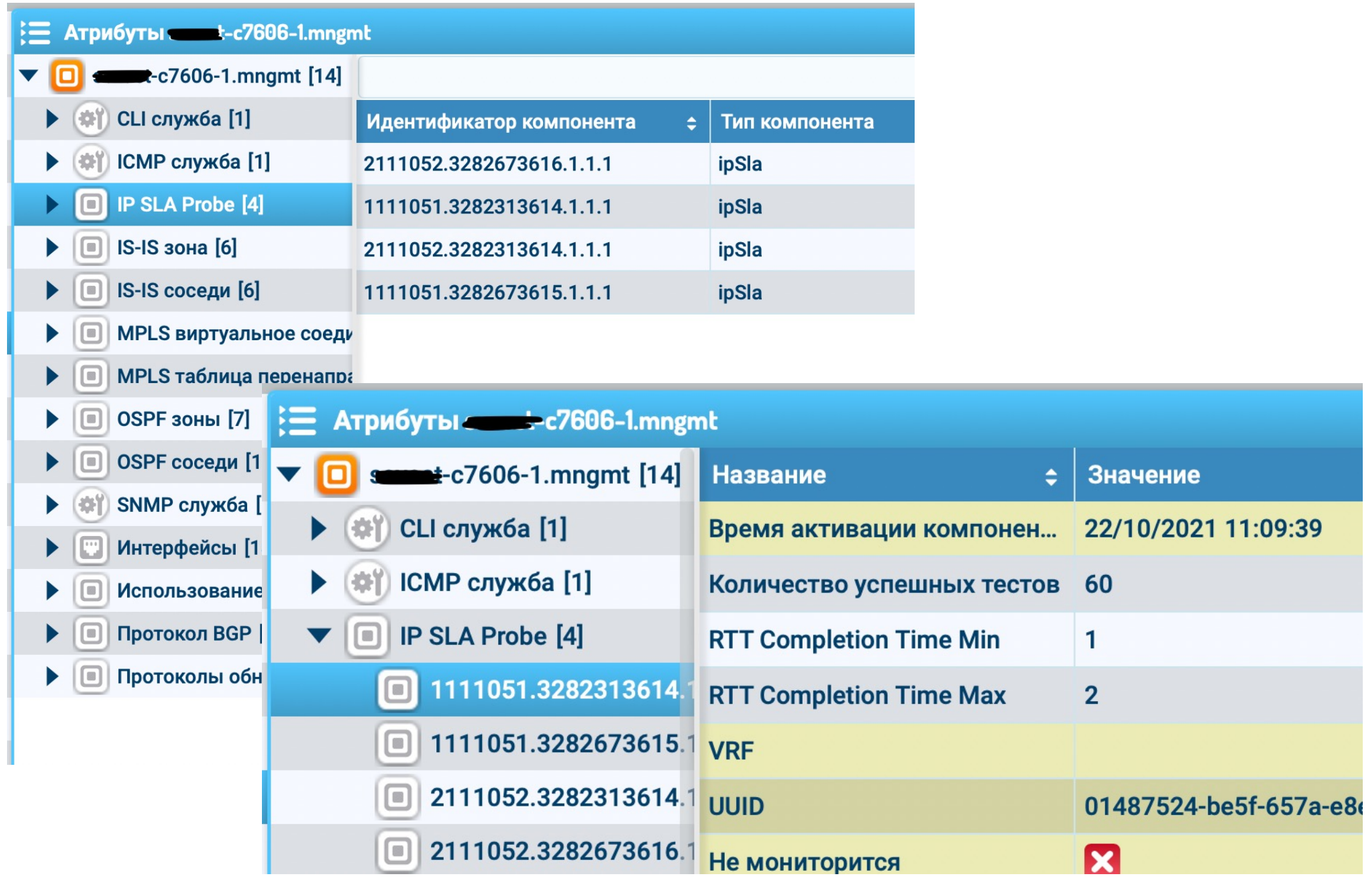
Сбор данных NetFlow, cFlow, jFlow, etc..



- 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.

Инити

Мониторинг параметров сетевой инфраструктуры



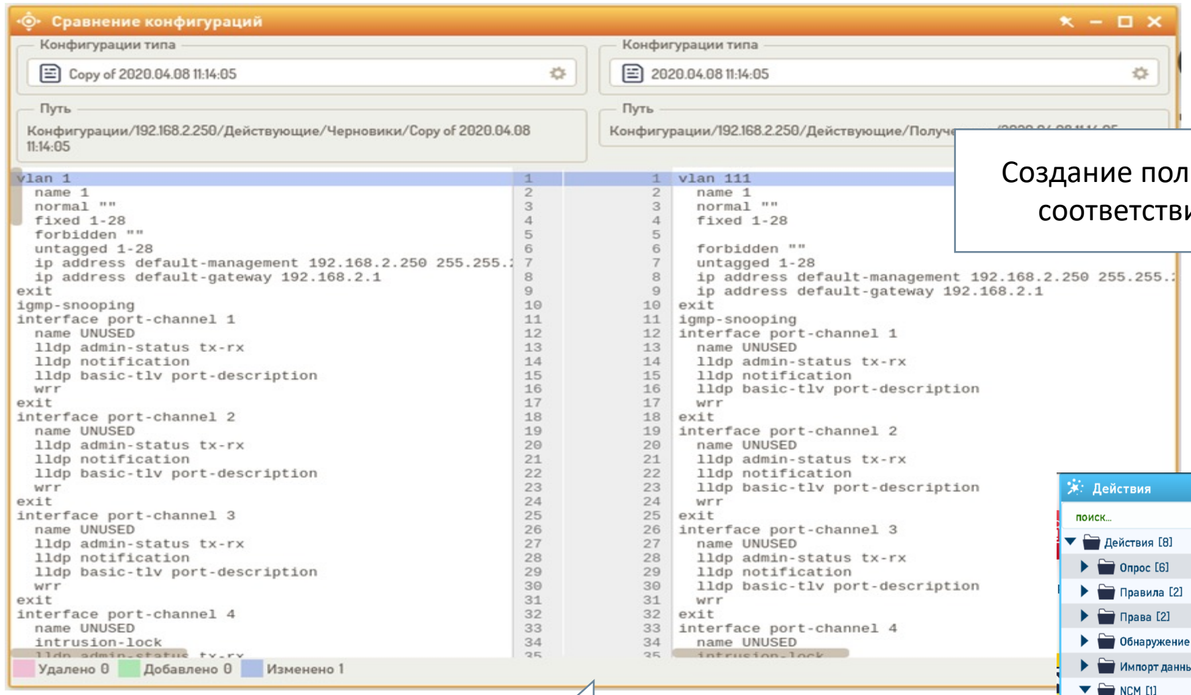
Сбор данных IP SLA, TWAMP, RPM, QoS, etc..:

- 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:

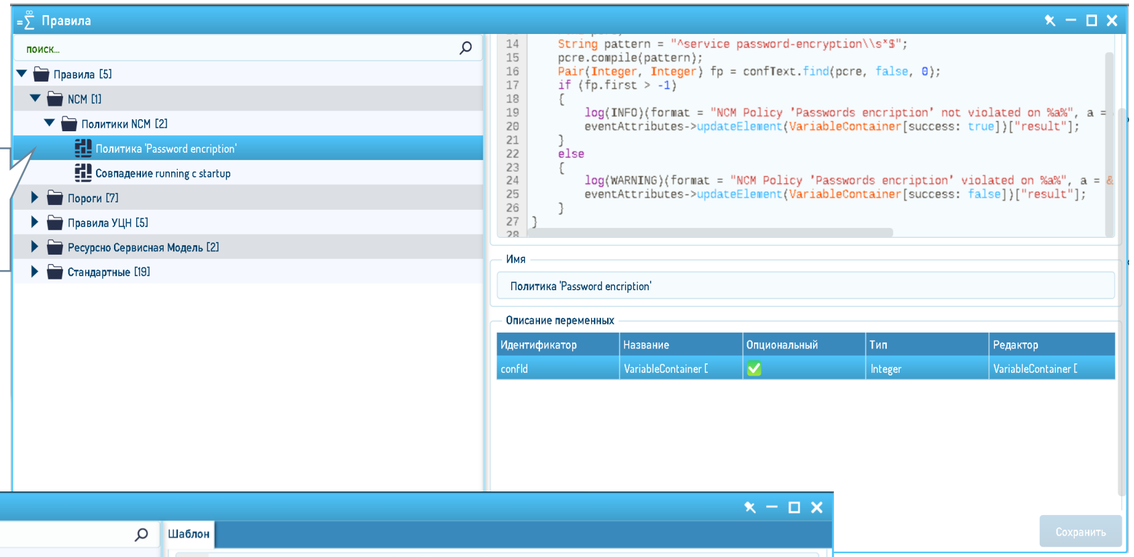
- Operation Success (%)
- Jitter Operation Completed (%)
- Jitter Operation Mean Round Trip Time (ms)
- Jitter Relative to Packet Interval (ms)
- Jitter Packet Loss (%)
- Jitter Maximum (Positive/Negative, ms)
- Operation completion time (ms)
- DNS Request completion time (ms)
- TCP Connect completion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

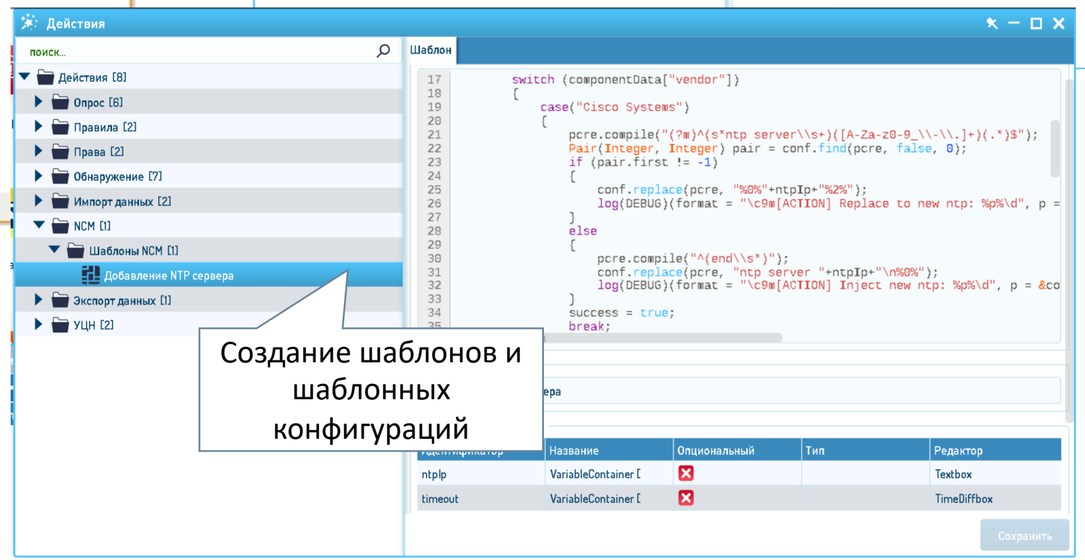
Управление конфигурациями сетевой инфраструктуры



Сравнение конфигураций

Создание политик соответствия



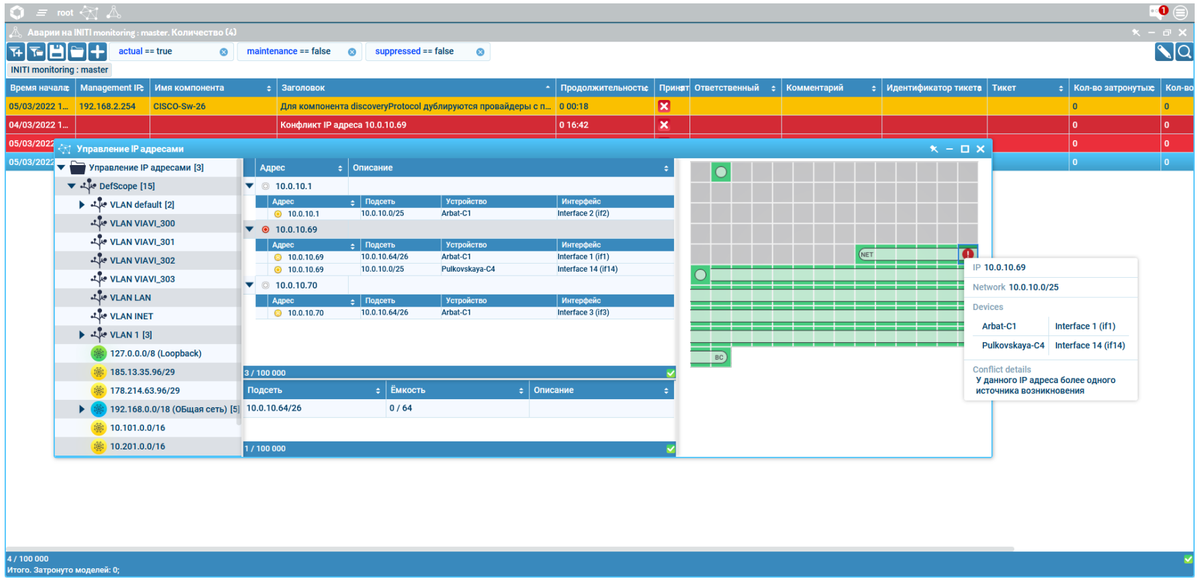


Создание шаблонов и шаблонных конфигураций

Инити

Управление адресным пространством

- Ведение учёта сетей и IP адресов
- Автоматизированное составление иерархии подсетей при обнаружении устройств
- Автоматическое создание областей видимости по принадлежности коллекторов, VRF и VLAN
- Сканирование сетей без создания моделей устройств
- Выявление и аварийное оповещение о конфликтах IP адресов на сети
- Автоматическое и ручное распределение сетей по областям видимости
- Контекстное отображение карты сетей моделей и их контейнеров в IPAM
- Визуализация занятых ресурсов сети
- Быстрый переход в устройство и интерфейс с карты сети
- Предвалидация сетевых реквизитов (контроль и исключение ошибок оператора)



Инити

Технологическое оборудование и элементы АСУТП - проблематика

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

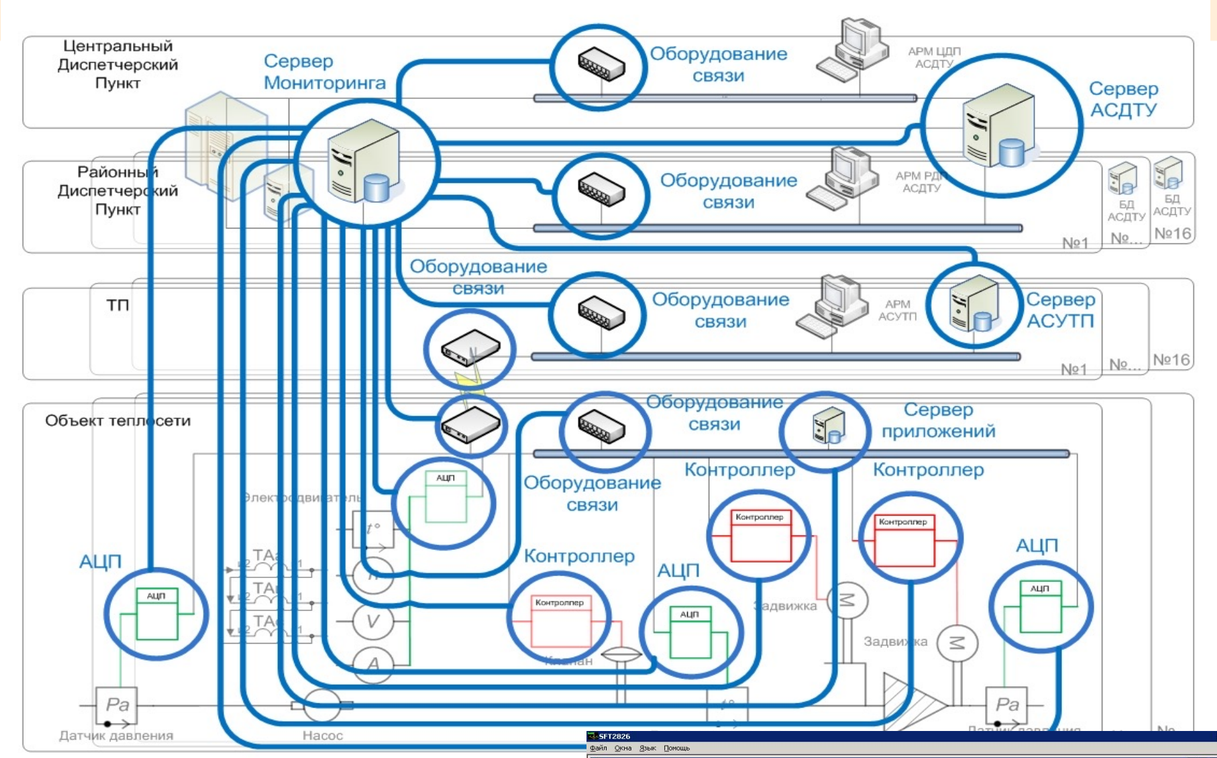
- Контрольно-измерительные приборы
- Контроллеры (ПЛК)
    - Универсальные программируемые контроллеры
    - PC-совместимые контроллеры
    - Программируемые реле
- Рабочие станции пользователя (АРМ)

- 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

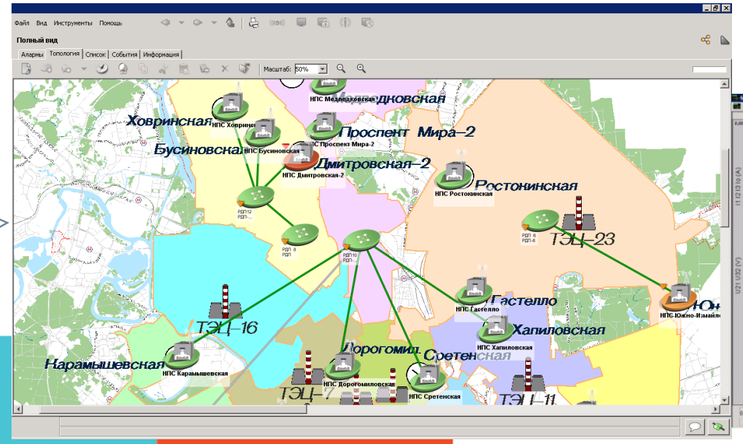
- Система мониторинга ИТ оборудования
- Штатные средства сетевой ИБ Cisco
- Сервера HP и ОС Windows, Linux, Unix
- Устройства защиты серии «Sepam», производства компании «SCHNEIDER ELECTRIC». Предназначены для контроля и управления силовым электрооборудованием напряжением 6-10 кВ.
- Контроллеры серии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

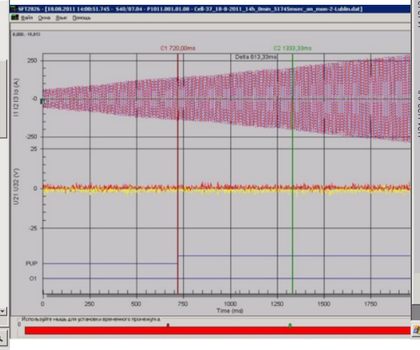


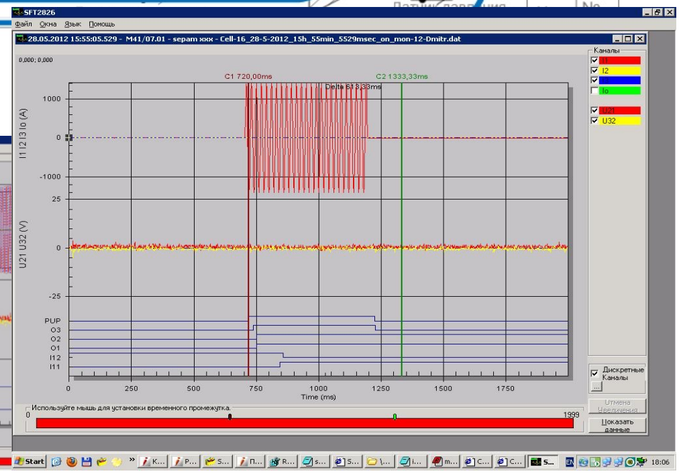
Зеленый - объект работает в штатном режиме.

Оранжевый - объект работает в предаварийном режиме, нештатная ситуация

Красный - на объекте критическая ситуация.

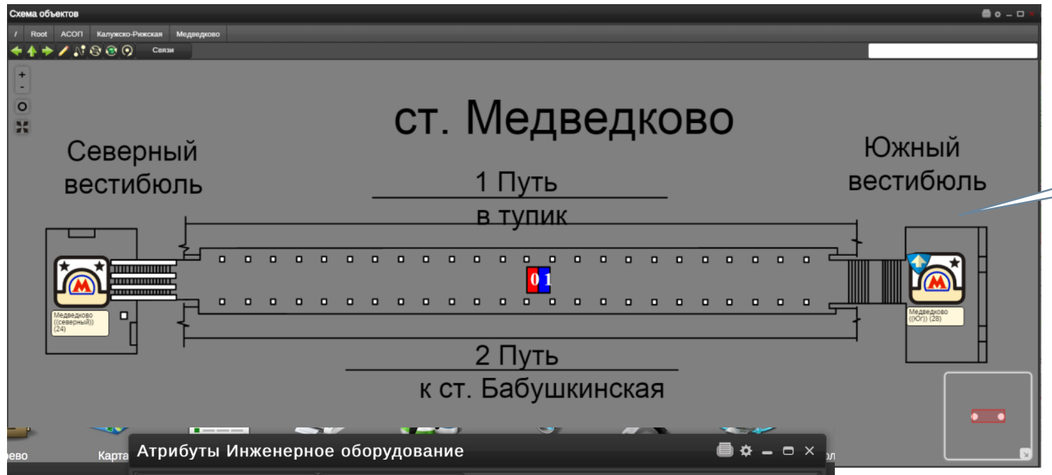






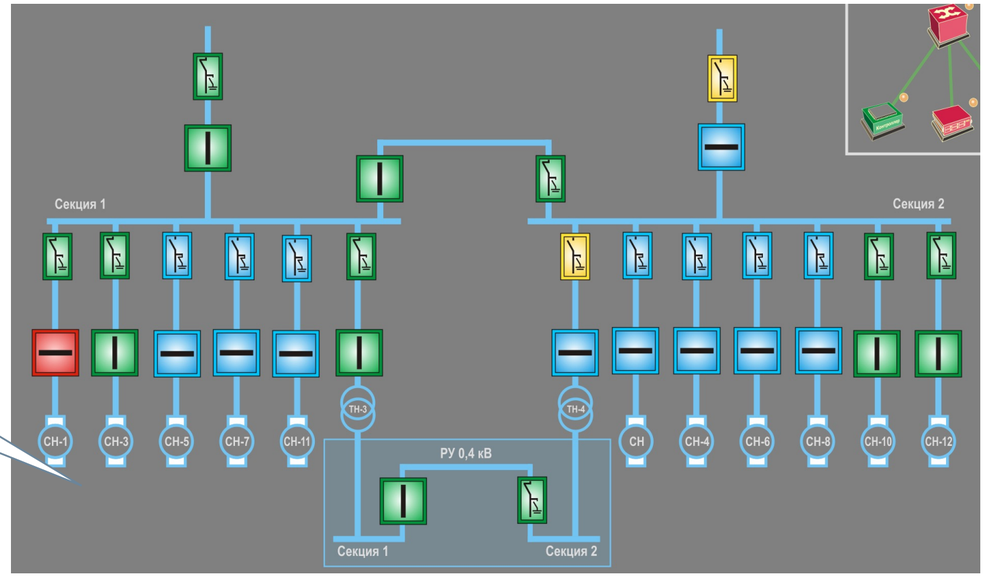
Инити

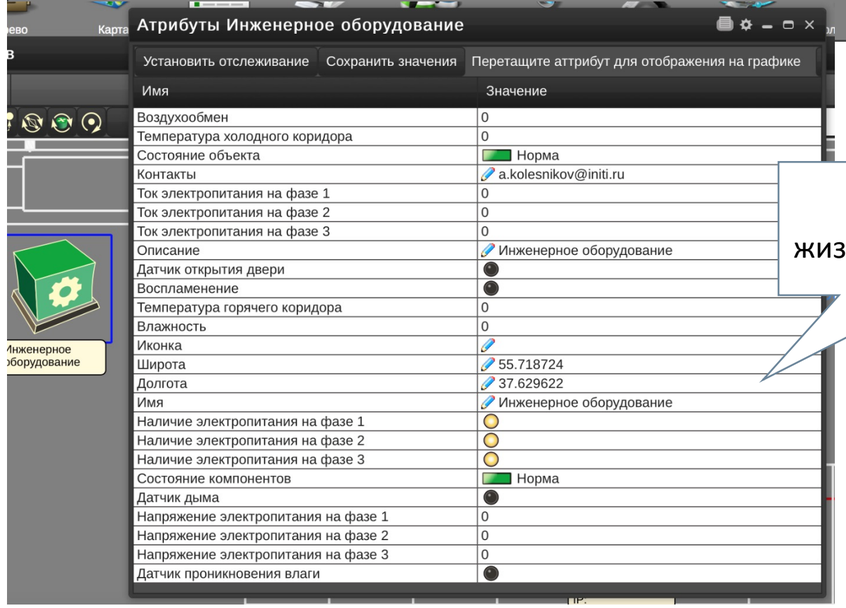
Технологическое оборудование и элементы АСУТП



Технологическое оборудование

Объекты АСУТП – интерактивная мнемосхема





Системы жизнеобеспечения ЦОД

Параметры работы ДГУ

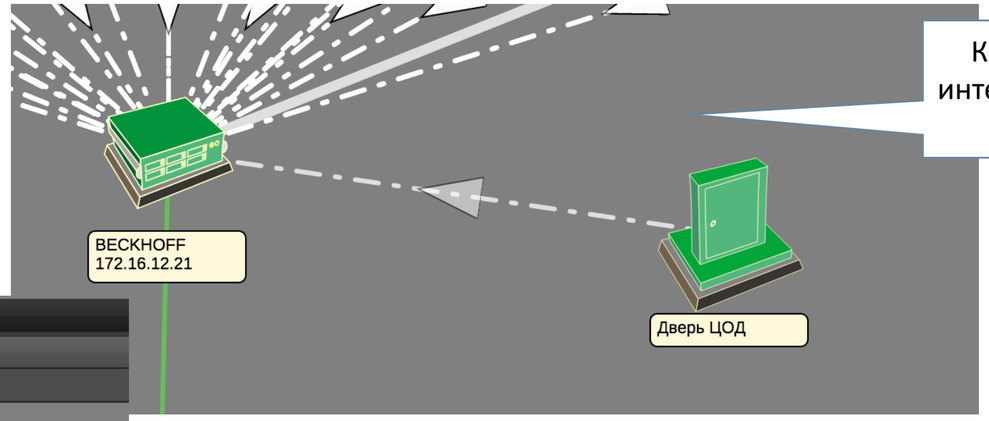
Инити

Интеграция с подсистемами ИБ

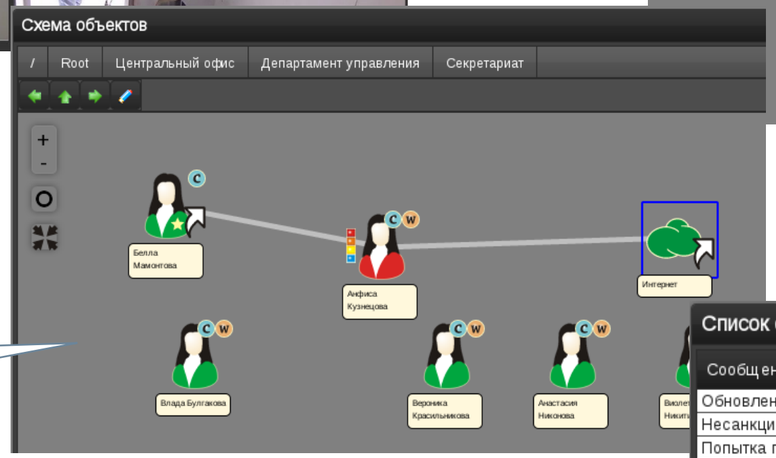
Визуальный контроль объекта

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

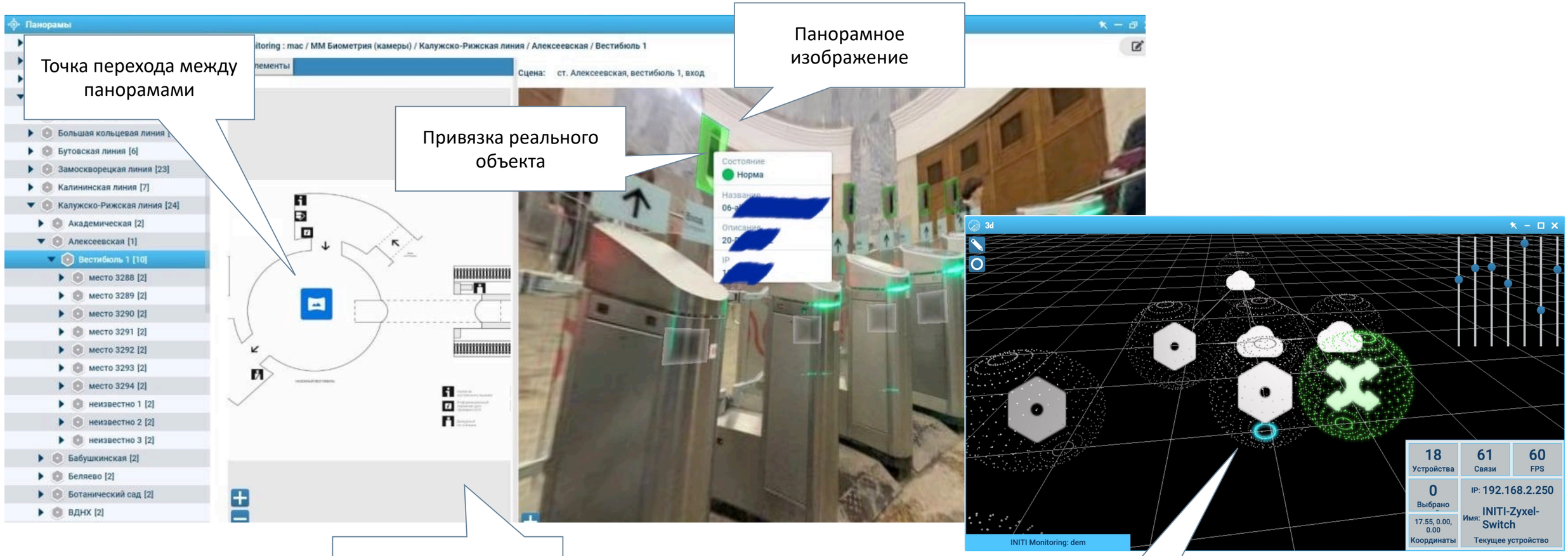
Кореляция данных событий от нескольких внешних ИБ систем

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

Интерфейс панорамного представления



Точка перехода между панорамами

Привязка реального объекта

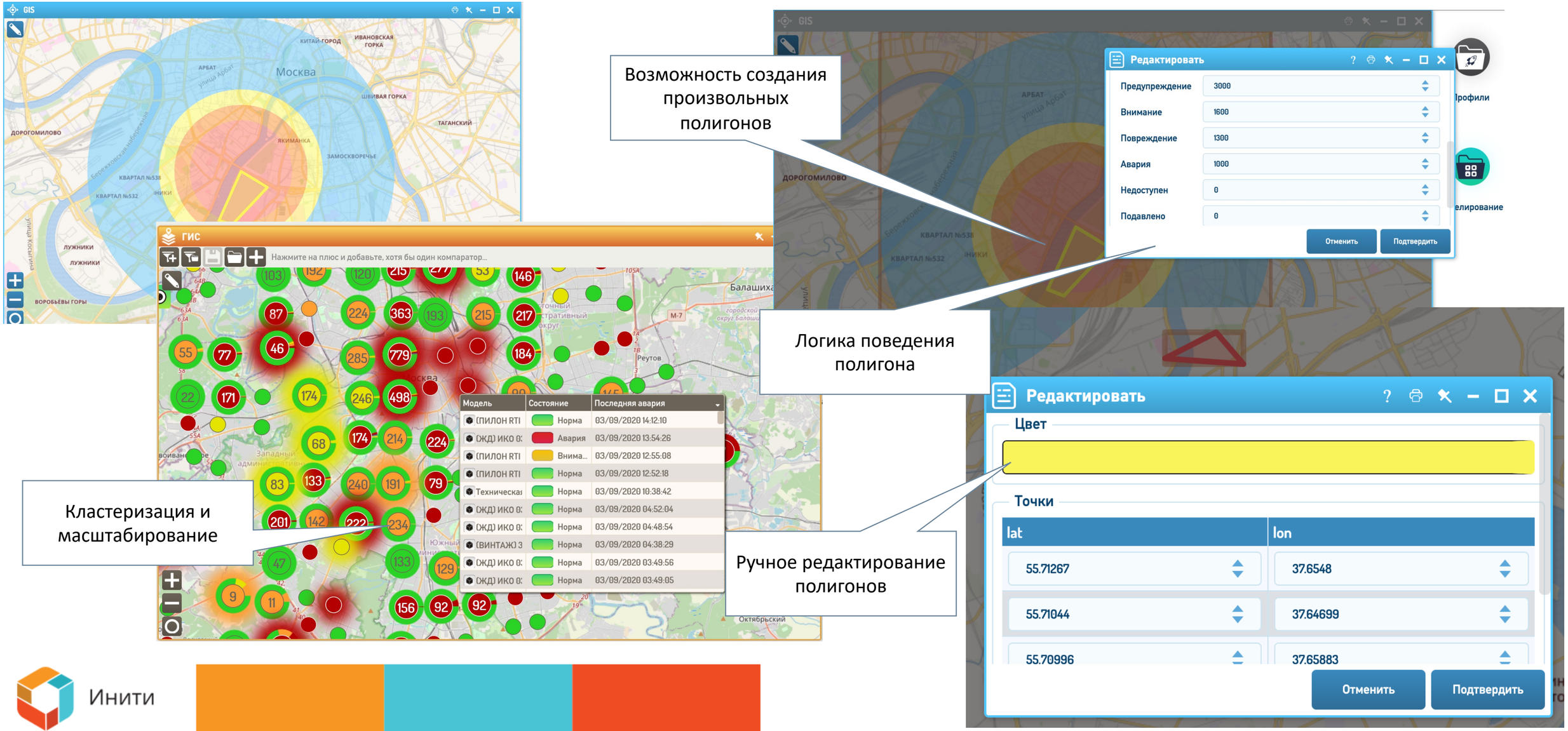
Панорамное изображение

Масштабируемая схема помещения

Трёхмерная визуализация топологии

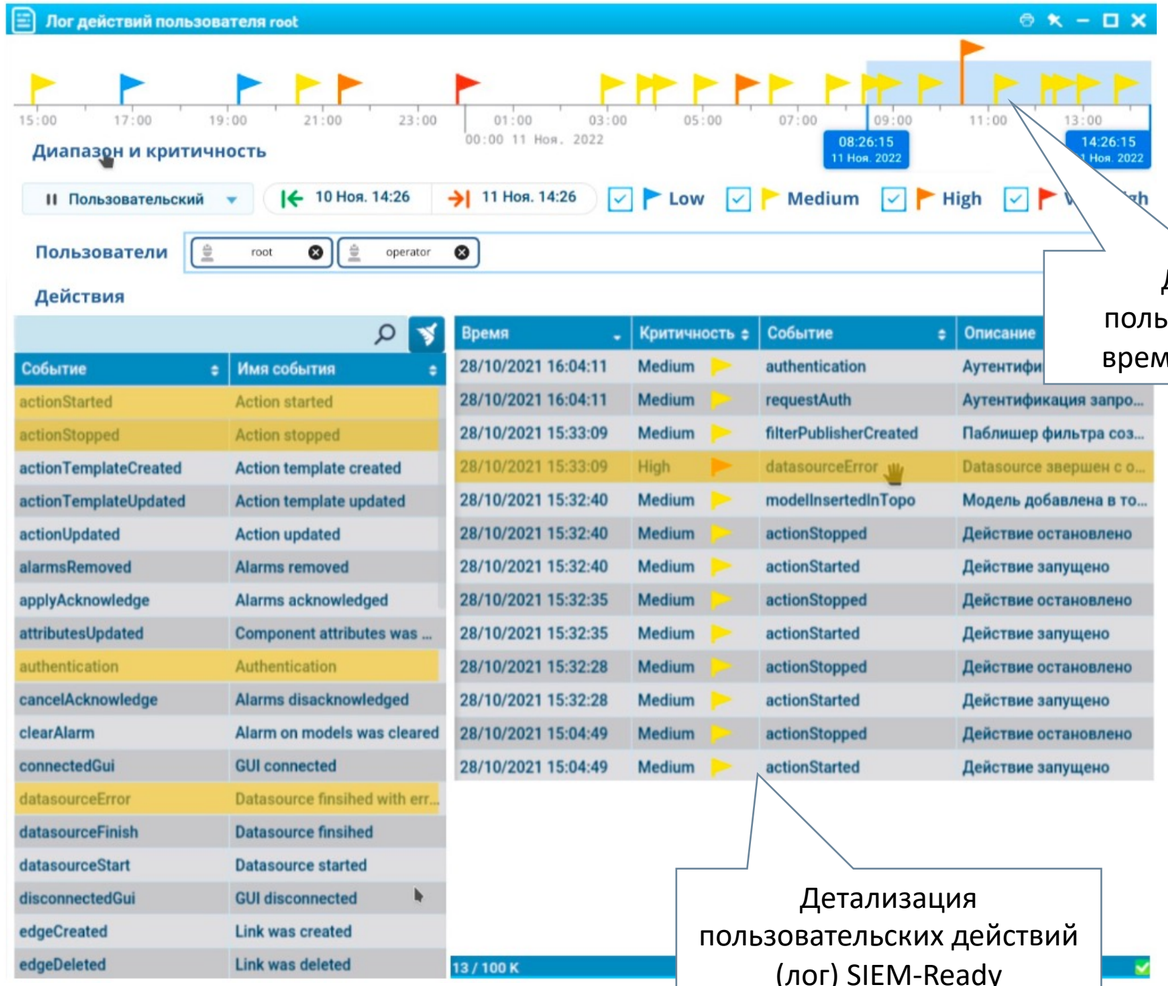
Инити

Гео-информационный интерфейс



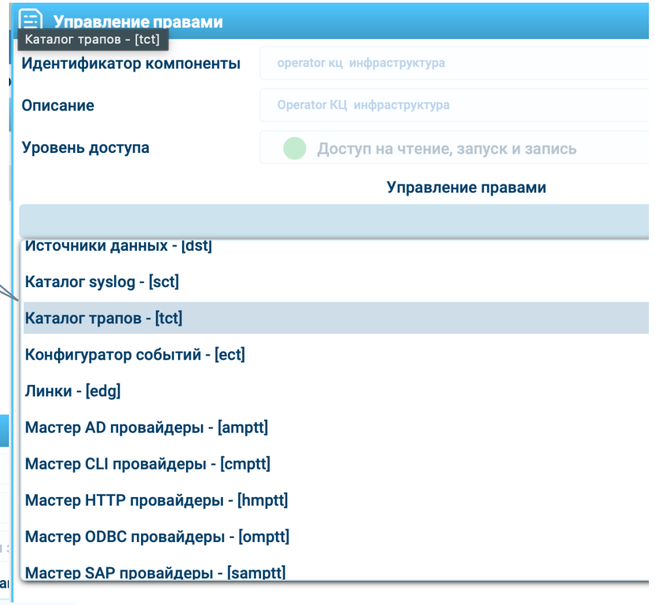
Инити

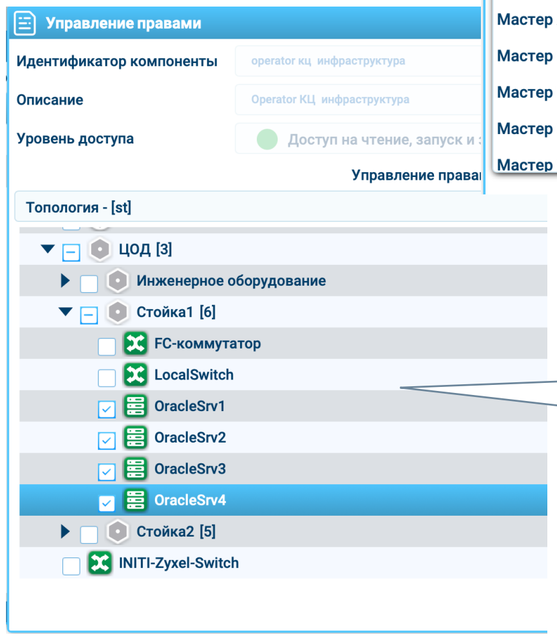
Разделение пользовательских прав



Действия пользователей на временной шкале

Настройка действий, зон видимости, областей данный и пр..





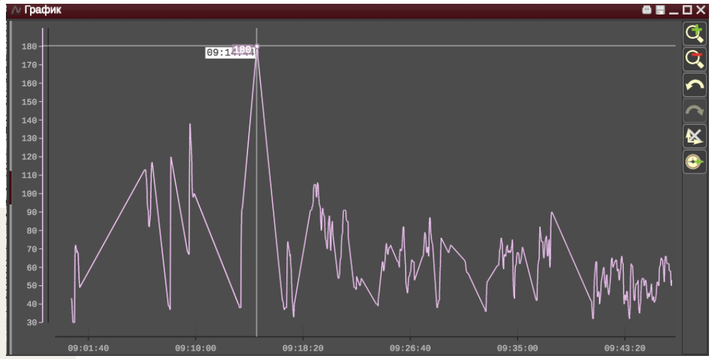
Пример настройки зоны видимости для топологии

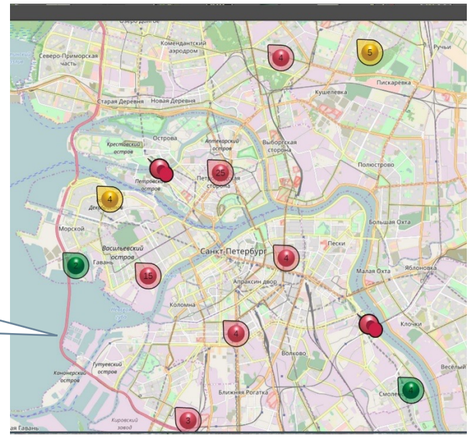
Детализация пользовательских действий (лог) SIEM-Ready

Инити

Контроль персонала и мобильных средств

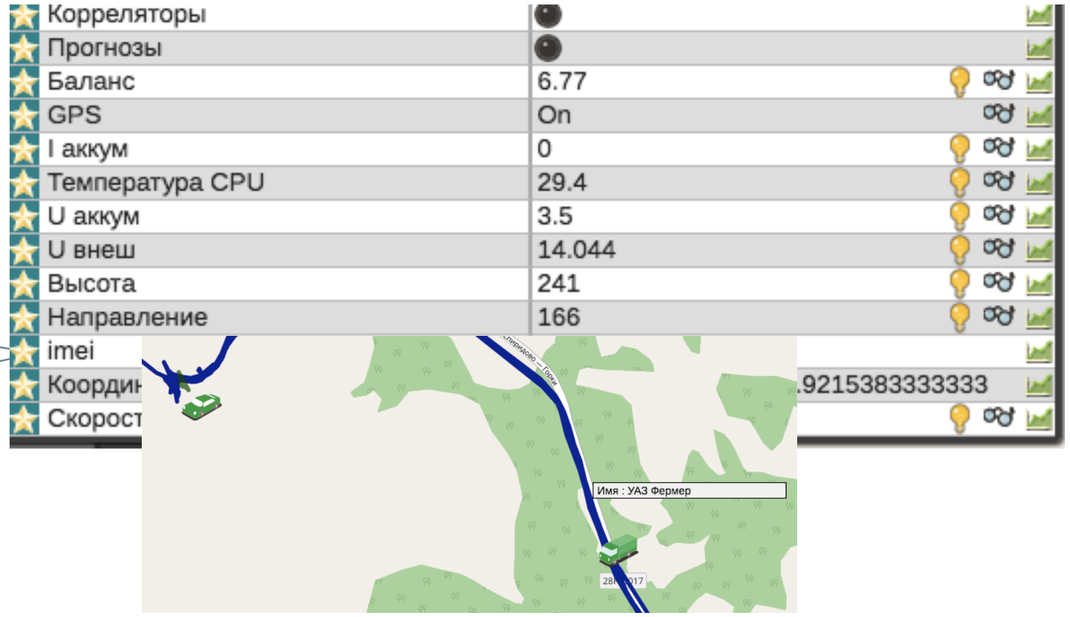
- Актуальные данные – параметры жизнедеятельности
- Актуальные данные – телеметрия состояния АМ
- Вычисляемая поведенческая модель
- Гео-позиционирование и трекинг
- Контроль внутреннего фрода





Состояние удалённых объектов

Отслеживание местоположения сотрудника, трекинг, сбор телеметрии

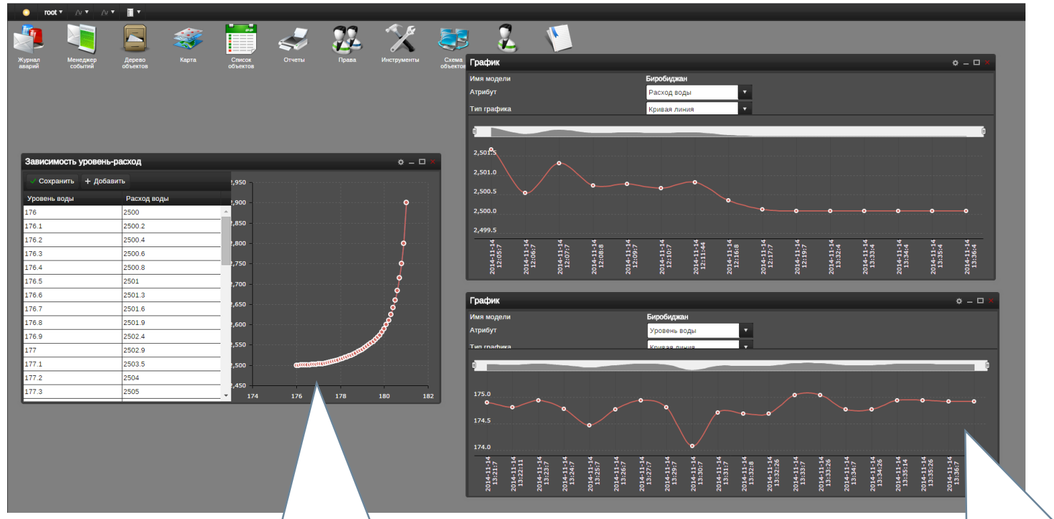


Контроль и трекинг состояния автотранспортных средств

Инити

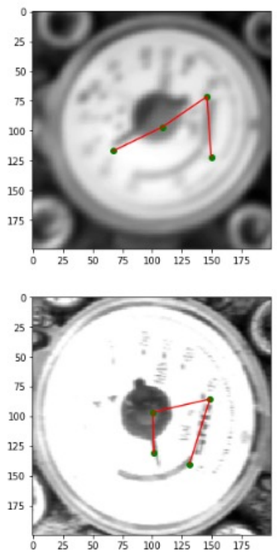
Сбор и анализ данных от аналогового оборудования

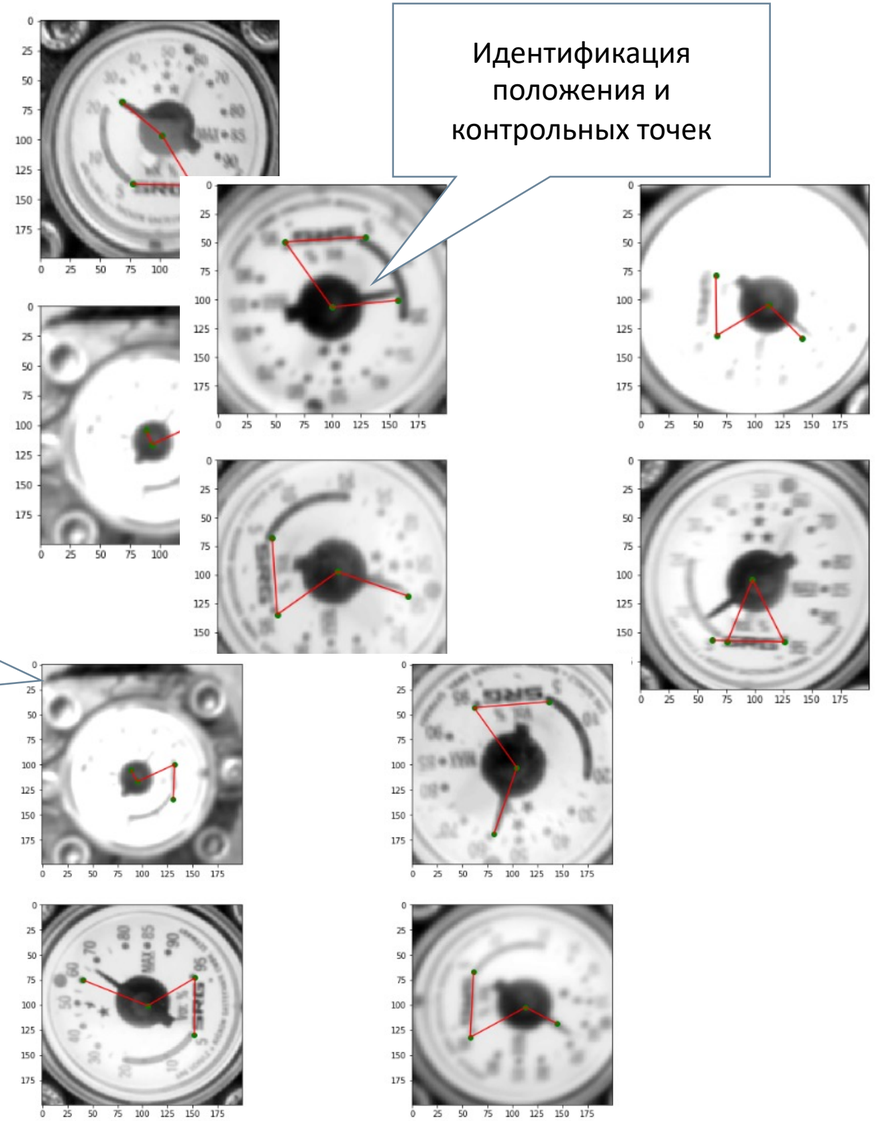
- Обучаемая нейронная сеть
- Анализ фото-материала
- Анализ видео-данных
- Накопление статистики (+дальнейшая отчётность)
- Использование в сервисно-ресурсной модели



Построение зависимостей

Накопление статистики и дальнейшая отчётность





Идентификация положения и контрольных точек

Возможность работы с изображениями низкого качества

Инити

СПАСИБО!

Инити