

# Система мониторинга на базе программного продукта PRTG Network Monitor



# О авторе

Василий Артемьев

Менеджер ИТ-инфраструктуры

Группа телекоммуникаций и сетевых решений, отдел развития информационных систем

АО Фирма «Август»

- <https://www.avgust.com>

# О компании

- АО Фирма «Август»
- Год основания: 1990.
- Основное направление деятельности: с 1992 года компания работает на отечественном рынке химических средств защиты растений (ХСЗР), или пестицидов. В 1994 году рынок ХСЗР был признан приоритетным для развития компании.
- «Август» сегодня: компания имеет собственный научно-исследовательский центр и три собственных завода, два на территории России (Чувашия, Алабуга) и один в республике Беларусь, и порядка 60 точек присутствия по всей территории России. На данный момент компании принадлежит крупнейшая в России сбытовая сеть. Препараты поставляются более чем 3,5 тысячам клиентов в 76 регионов России, а также в республику Беларусь, Украину, Молдавию, Азербайджан, Казахстан, Узбекистан. Компания работает также в странах Дальнего зарубежья – Южная Америка, Азия. Ассортимент ХСЗР насчитывает более 100 наименований гербицидов, инсектицидов, фунгицидов и протравителей семян, предназначенных для крупных сельхозпроизводителей и владельцев личных подсобных хозяйств и дачников.
- Штат сотрудников организации составляет более 2500 человек.

# Центральный офис

- Расположение: г. Москва
- Сотрудников: ~400

# Центральный офис



# «Август-Алабуга»

- Расположение: Республика Татарстан, территория ОЭЗ «Алабуга»
- «Август-Алабуга» — самое молодое и самое современное предприятие «Августа» по производству жидких препаративных форм пестицидов крупнотоннажного выпуска. Это высокотехнологичное предприятие способно обеспечить продукцией треть российского рынка ХСЗР.
- Официальное открытие состоялось 28 июня 2019 года.
- Сотрудников: 200 (+ 300 в перспективе)

# «Август-Алабуга»



# Вурнарский завод смесевых препаратов

- Расположение: Чувашская Республика
- Основная производственная площадка компании «Август». Крупнейшее в России и наиболее специализированное предприятие по выпуску ХСЗР.
- В 2015 году заводу исполнилось 85 лет.
- Сотрудников: 750



# Вурнарский завод смесевых препаратов



# «Август-Бел»

- Расположение: Республика Беларусь, Минская область
- Передовое предприятие по выпуску химических средств защиты растений в Республике Беларусь, одно из самых мощных на территории СНГ.
- Первая очередь завода была запущена компанией «Август» в 2009 году.
- Сотрудников: ~300

# «Август-Бел»



# Региональные представительства

- Расположения: Россия, Беларусь, Украина, Казахстан
- Общее количество 60+
- Офисы от 2 до 25 человек

# Региональные представительства



# Проект: Внедрение системы мониторинга

- Локализация: для внутреннего ИТ-отдела
- Дата начала: Май 2018
- Дата окончания: Март 2019
- Общая длительность: 9 месяцев (6+3) + подготовительный и завершающие этапы (+2)

# Причины инициации проекта (очевидные)

- Необходимость контролировать работоспособность (доступность) большого количества точек (устройств) одновременно (не только на локальных площадках и не только в зоне своей ответственности)
- Информирование о нештатных ситуациях
- Медленное развитие и недостаточный функционал уже используемых продуктов для мониторинга



# Причины инициации проекта (не очевидные)

- Получение инструмента проактивной работы с ИТ-инфраструктурой
- Поддержка необходимого уровня качества ИТ-услуг для потребителей
- Повышение информированности ответственных лиц о состоянии отдельных элементов ИТ-инфраструктуры (ОС, оборудования, приложений, каналов связи, процессов)
- Исключение (уменьшения времени) простоя оборудования
- Сокращение времени реагирования на инциденты (нештатные ситуации)
- Повышение эффективности обслуживания и планирования компонентов ИТ-инфраструктуры
- Повышение качества и количества статистики и отчетности по работе ИТ-инфраструктуры



# Причины инициации проекта (основные)

- Необходимость расширить масштаб и глубину контроля ИТ-инфраструктуры
- Централизация контроля ИТ-инфраструктуры

# Цель проекта

- Получение единой, централизованной системы (продукта), способной отслеживать состояние (доступность, загрузка) различных элементов существующей инфраструктуры (АО, ПО, каналы связи), имеющей функционал оповещений, автоматических корректирующих действий, сбора статистики, формирования отчетности, взаимодействия с внешними системами (почта, ServiceDesk, SMS). Так же система должна быть интегрирована в существующие ИТ-процессы (и не должна игнорировать их наличие).

# Выбор системы (критерии) Часть 1.

- Наличие подробной документации (в т.ч. язык)
- Перспективы развития и добавления новых функций (в ногу с ИТ)
- Основная ОС и БД (интеграция с Microsoft AD)
- Тип поддержки и время реакции (в т.ч. язык)
- Представители\интеграторы в РФ
- Возможность обучения (курсы)
- Наличие и активность сообщества
- Возможность быстрого развертывания (в т.ч. внутренними специалистами)
- Возможность вести траблшутинг своими силами
- Наличие\отсутствие агентского мониторинга
- Интеграция с другими системами
- Механизмы отказоустойчивости

# Выбор системы (критерии) Часть 2.

- Визуализация (карты)
- Мобильное приложение
- Возможность кастомизации
- Функции AutoDiscovery
- Система отчетов
- Поддержка NetFlow
- Технологии мониторинга (чем больше, тем лучше)
- Наличие готовых шаблонов (чем больше, тем лучше)
- Наличие дополнительных функций (API, управление конфигурациями и т.д.)
- Другие плюсы\минусы
- Цена

# Выбор системы (продукты)

- WhatsUp Gold
- PRTG Network Monitor
- Zabbix
- Nagios XI
- SCOM
- SolarWinds
- ManageEngine OpManager

# PRTG Network Monitor (Преимущества)

## Часть 1.

- Система лицензирования, включающая большое количество встроенных модулей (отчеты, оповещения, карты, готовые шаблоны и пр.) и мобильное приложение. Система поставляется как единый продукт.
- Быстрота освоения и удобство использования системы для не профильных ИТ-специалистов (что позволяет использовать продукт как платформу для специалистов всех уровней).
- Возможность на базе бесплатной версии развернуть пилотный проект любых масштабов.
- Форум со специалистами технической поддержки.
- Доступная база знаний.
- Система работа с ID.

# PRTG Network Monitor (Преимущества)

## Часть 2.

- Возможность доработки встроенных решений и подключения своих.
- Техническая поддержка без ограничений количества запросов (с 10:00 до 18:00 МСК).
- Простая реализация отказоустойчивости включенная в лицензию.
- Нет необходимости устанавливать локальных агентов.
- Удобная система API.
- Наличие публичной RoadMap для продукта.
- Огромное количество готовых решений в свободном доступе.
- Ежеквартальные обновления (новые функции и фиксы)
- Очень подробная документация

# PRTG Network Monitor (Особенности)

- Проприетарная БД
- Недостаточная гибкость работы с NetFlow
- Усреднение больших отчетов
- Работа с элементами карт в MapDesigner
- Работа кластера ограничена количеством сенсоров
- Использование шаблонов и клонирование не являются универсальными инструментами автоматизации
- Не все браузеры корректно работают с системой (Java)
- Система поддерживает только один домен Active Directory
- Нет 2FA (на 09.2019)
- Одно устройство – один IP
- Нет клавиши «Отмена изменений»



# Состав проекта и роли

- Заказчик проекта
- Руководитель проекта
- Куратор проекта
- Специалист по качеству
- Внутренние специалисты различных направлений

# Этапы проекта

- Подготовительный этап
- Планирование архитектуры
- Развертывание системы
- Инвентаризация и выделение элементов
- Подключение устройств
- Доработка системы

## Этапы проекта. Подготовительный этап.

- Составление планов
- Выделение ресурсов
- Тесты продукта
- Корректировка планов и ресурсов

# Этапы проекта. Планирование архитектуры.

- Оценка нагрузки на систему
- Стандартизация элементов (состава и наименований)
- Выбор точки размещения объектов в иерархии
- Планирование системы оповещений (Email, Push, NetPing)

# Этапы проекта. Развертывание системы.

- Подготовка оборудования
- Развертывание ядра системы
- Подключение аппаратных решений для оповещений (NetPing)

## Этапы проекта. Инвентаризация и выделение элементов.

- Сбор информации о конкретных типах объектов
- Выделение того, что необходимо контролировать на типе объекта

# Этапы проекта. Подключение устройств.

- Добавление устройств в систему
  - Настройка стандартных элементов
  - Настройка оповещений
- 
- Лицензирование системы

# Этапы проекта. Доработка системы.

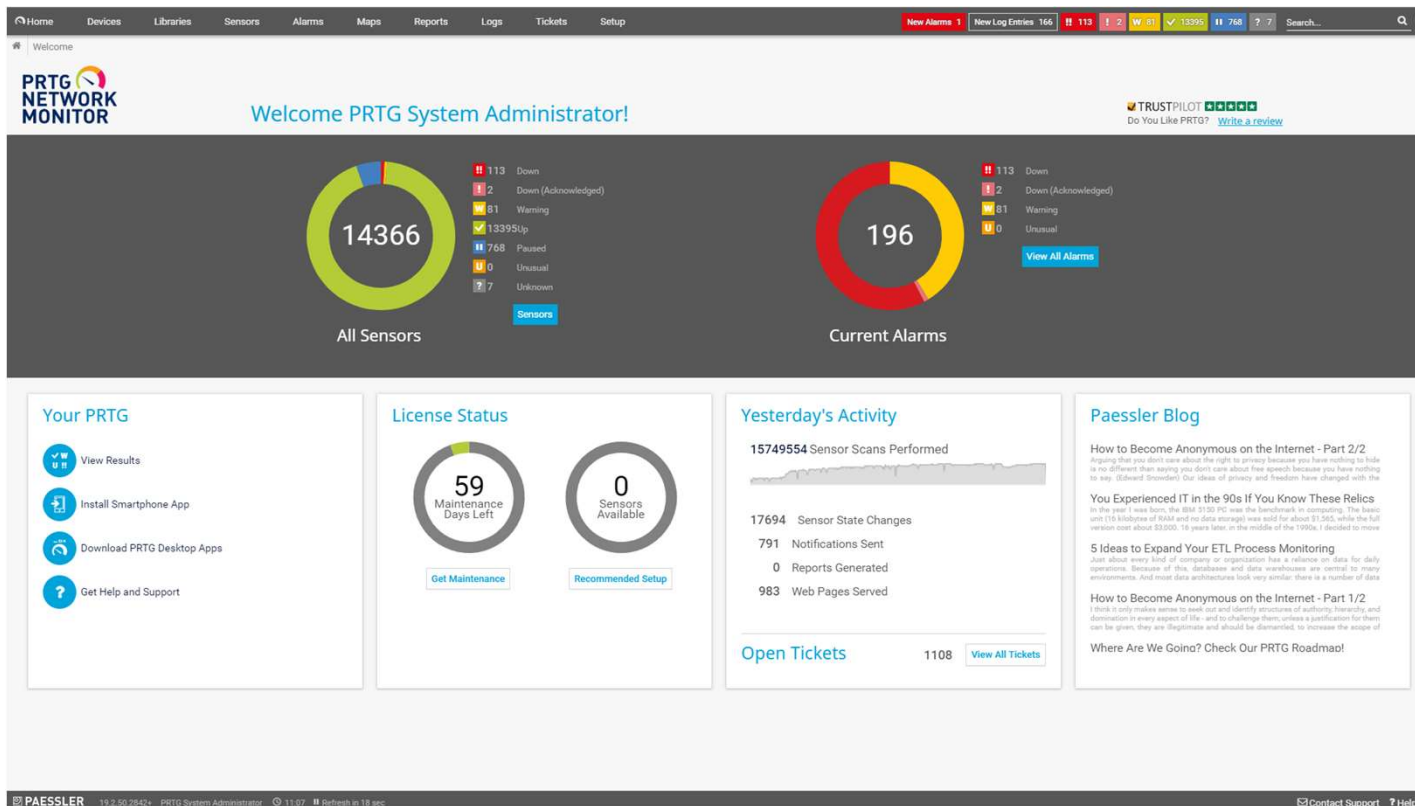
- Корректировка набора элементов
- Составление карт
- Корректировка иерархии групп
- Разработка нестандартных решений



# Финальная архитектура

- 1 сервер ядра (Core Server) - физический сервер
- 8 Удаленных зондов (2+2+1+1+1+1) – виртуальные сервера
- 14366 сенсоров
- 1715 устройств
- 15 749 554 сканирований в день (190 запросов в секунду)
- 30 пользователей (всего), 10 активных в момент времени
- 10 различных карт в активном использовании

# Финальная архитектура



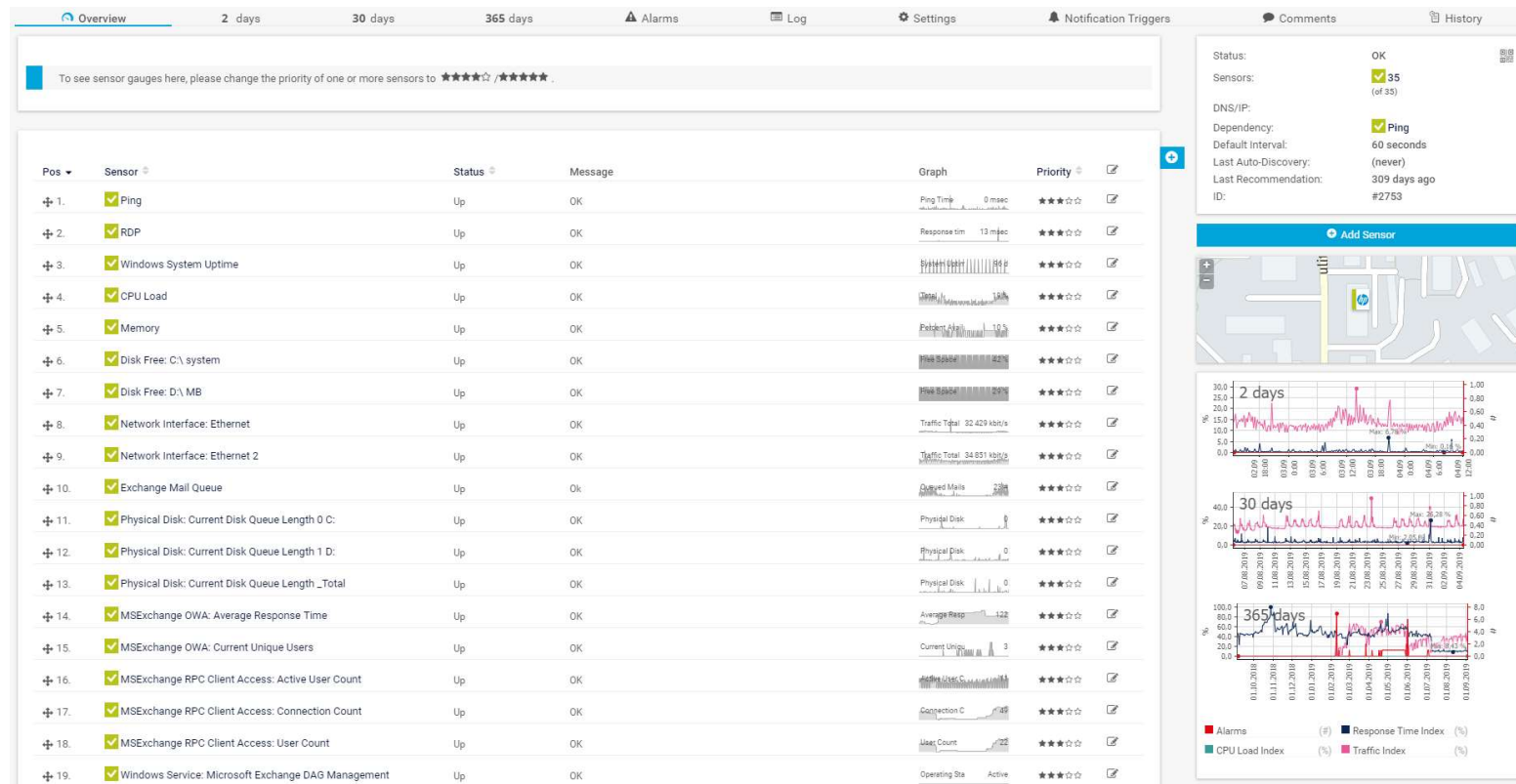
# Подключенные устройства

- Сервера: Windows + Linux + ESXI (+ модули управления)
- Файрволы
- Коммутаторы
- Маршрутизаторы
- Wi-fi (контроллеры + точки доступа)
- SAN\NAS-системы
- Кондиционеры
- ИБП + PDU + AVR
- Копировально-множительная техника
- Телефонные станции
- + различные точки сети, такие как веб-сайты, шлюзы провайдеров

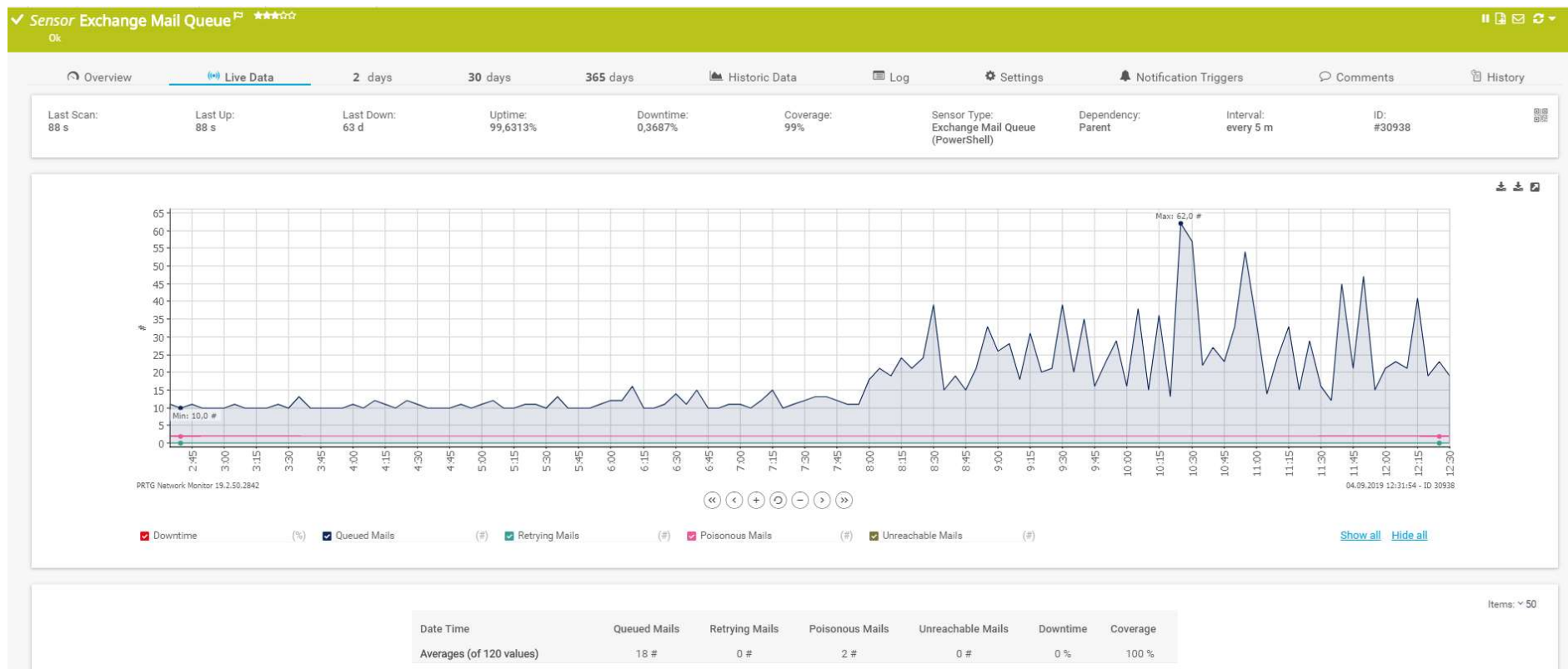
# Подключенные приложения

- Microsoft Exchange
- Microsoft SQL
- Microsoft Sharepoint
- 1С (Сервер + БД)
- SAP

# Сервер Microsoft Exchange (устройство)



# Очередь писем Exchange (стандартный сенсор)



# Состояние сервера HP (iLO) (стандартный сенсор)

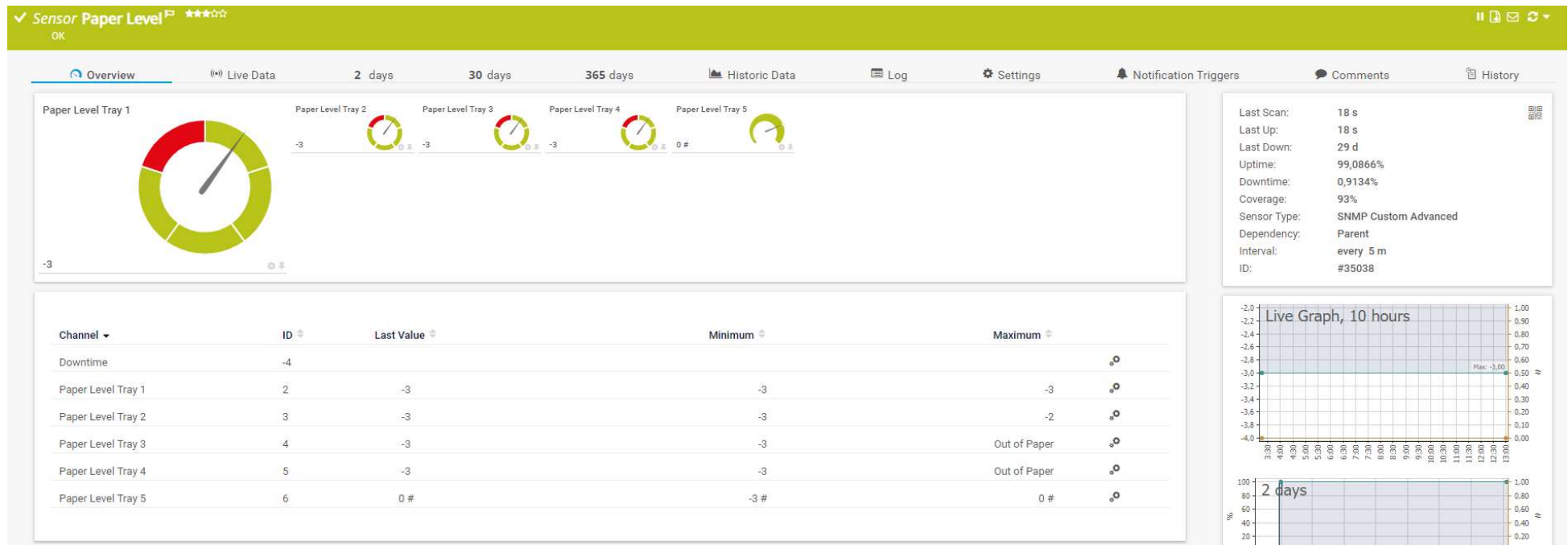


# Количество клиентов на точке доступа Wi-Fi (стандартный сенсор SNMP)

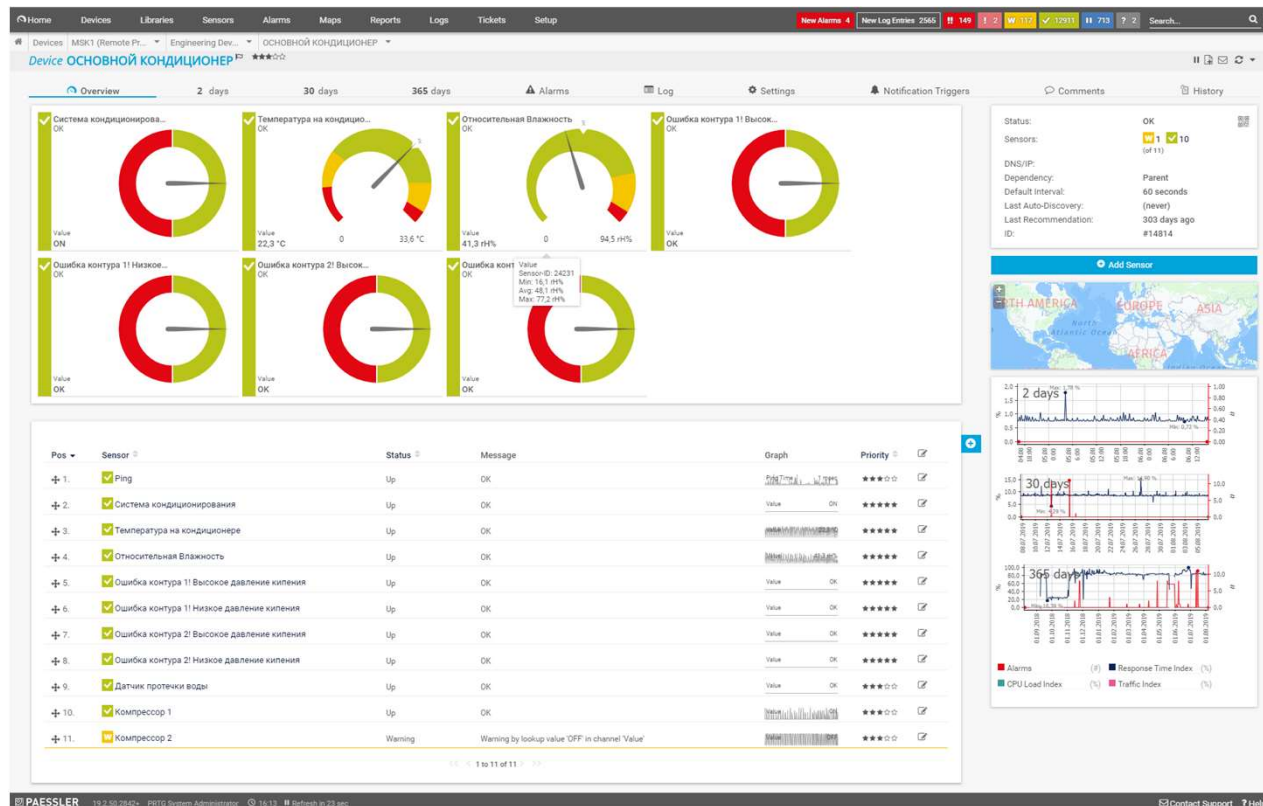




# Количество бумаги в лотках принтера (стандартный сенсор SNMP)



# Статус основного кондиционера (стандартный сенсор SNMP)



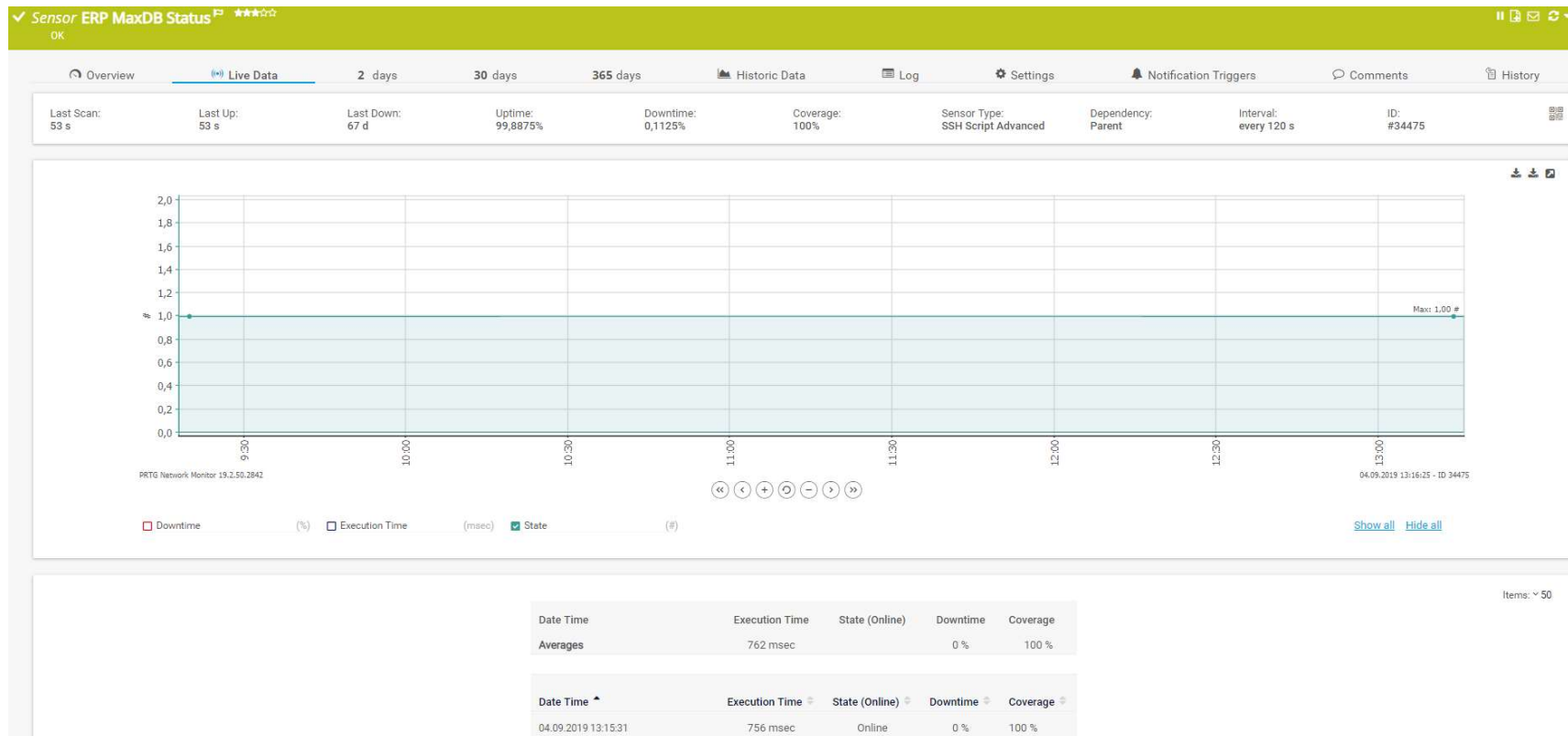
# Нестандартные решения

- ATC Siemens HiPath4000
- SAP
- SAN
- RDP

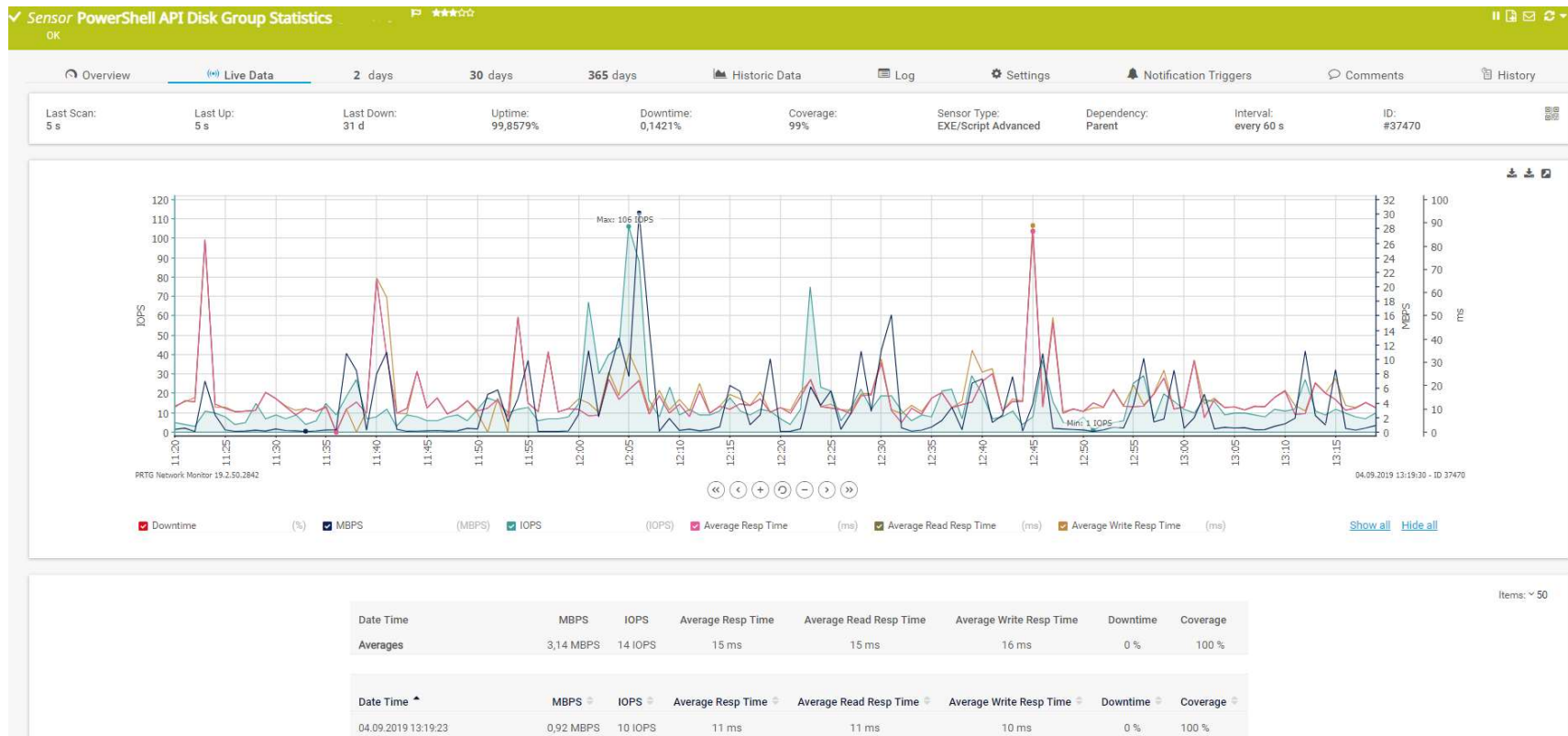
# ATC Siemens HiPath4000 (SSH-скрипт)



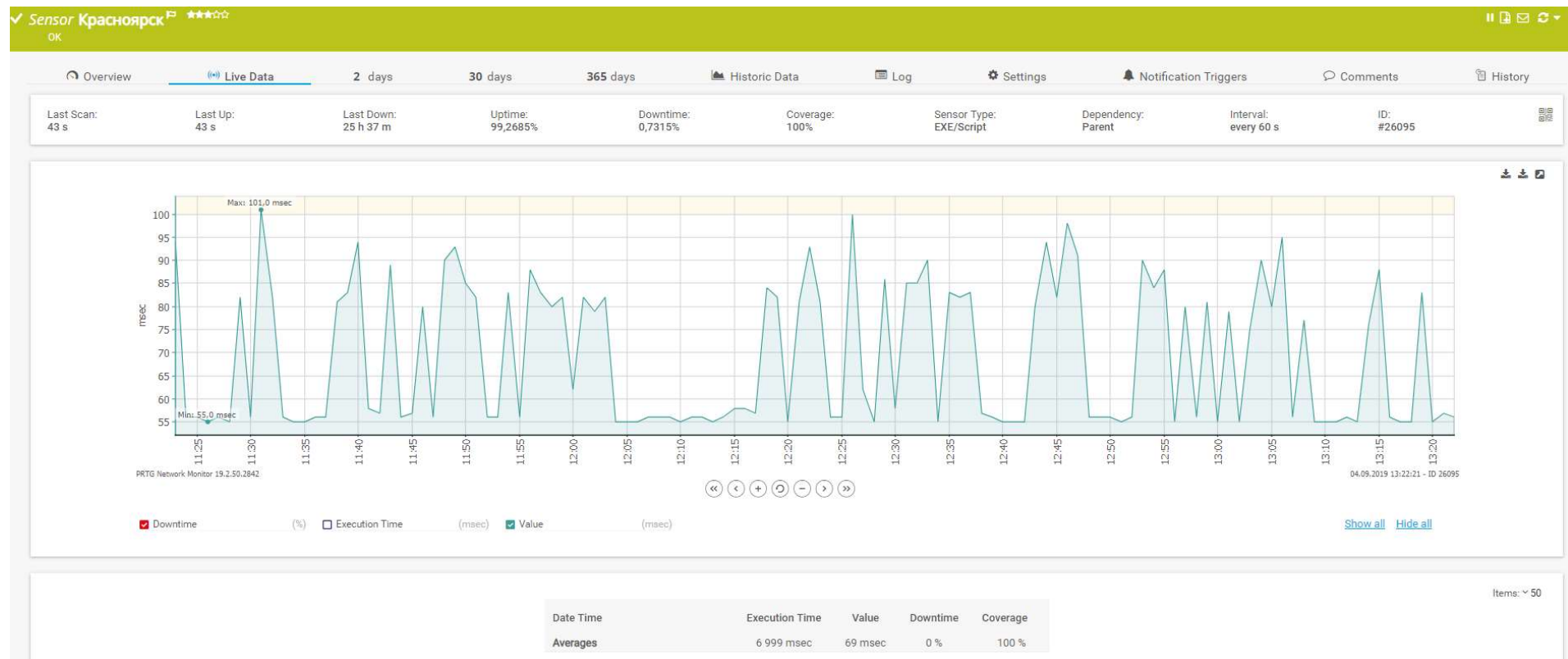
# SAP ERP (SSH-скрипт)



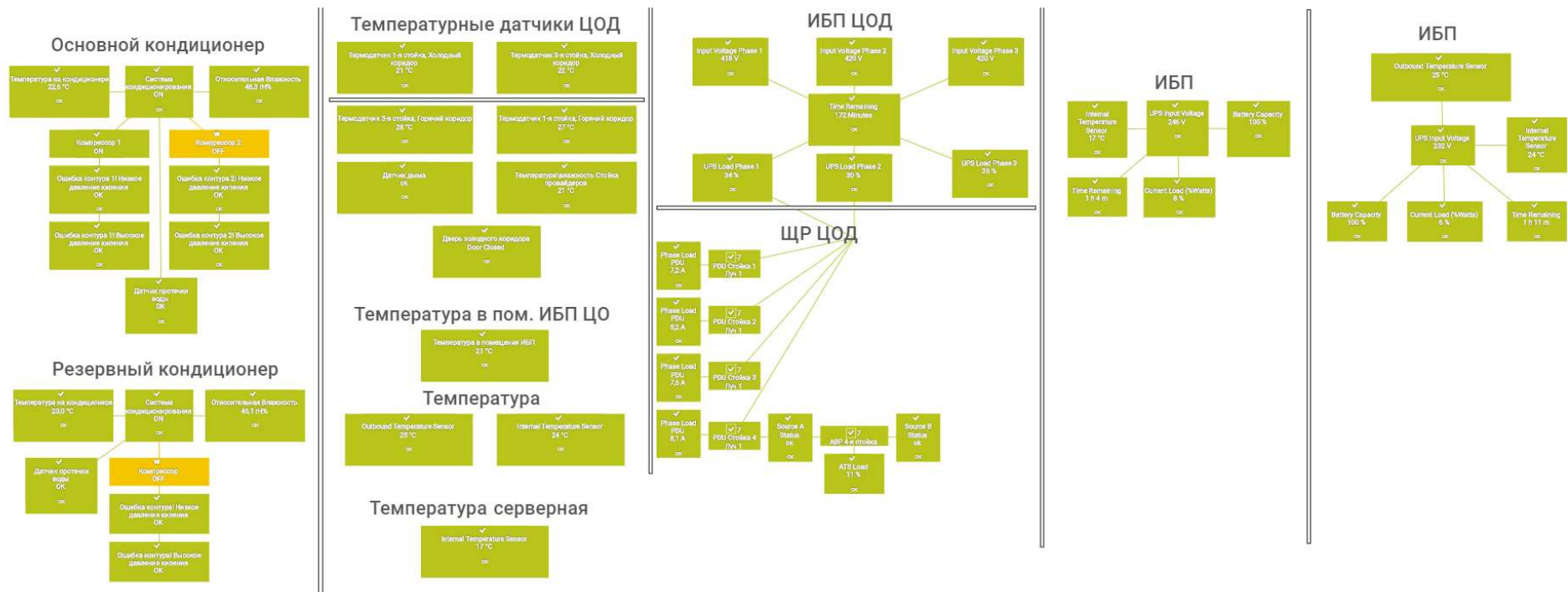
# SAN (PowerShell-скрипт)



# RDP (PowerShell-скрипт)

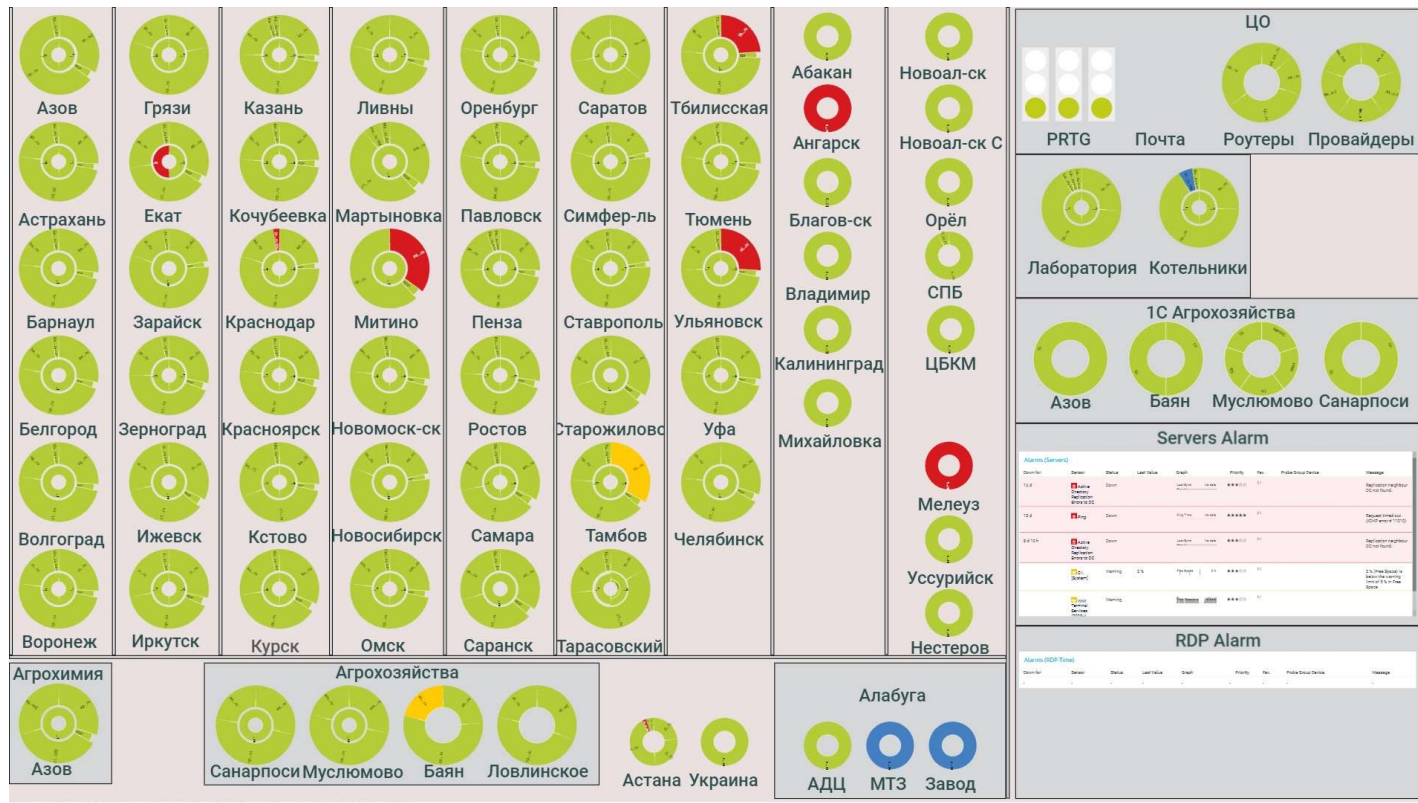


# Карта инженерных систем





# Карта региональных представительств



# Реальные ситуации

- Отключение каналов связи (переход на резервные каналы)
- Выход из строя дисков и блоков питания
- Высокое потребление CPU, памяти
- Уменьшение дискового пространства
- Накопление писем в очереди почтовых серверов
- Недоступность провайдеров
- Ошибки в конфигурациях оборудования или политиках
- Отключение кондиционеров
- Потеря питания

# Best practice

- Best practice от разработчиков
- Физические решения надежнее виртуальных
- Продумывайте систему отказоустойчивости для системы
- Оптимизируйте (следите) производительность
- Проводите регулярный аудит системы
- Используйте облегченные протоколы (PerfCounter вместо WMI)
- Используйте сервисные интервалы для обновления PRTG и Windows Update
- Не допускайте перенагрузки систем (Windows и PRTG)
- Используйте Factory sensor и Business Process
- Используйте MultiEdit
- Продумывайте пороговые значения
- Используйте Dependencies
- Контролируйте основную систему при помощи бесплатной версии
- Не забывайте добавлять исключения в антивирус
- Планируйте мониторинг до покупки оборудования или создания сервисов

# Формула эффективного мониторинга

- Удобная система + специалист в своей области (сеть, сервера, SAN и т.д.)
- Тесты, тесты, тесты

# Bonus

- До начала проекта PRTG уже использовали отдельные специалисты