



ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аналитическая **AIOps**-платформа для полного контроля над сложной IT-инфраструктурой

Каталог ИИ решений

ТИПОВЫЕ ПРОБЛЕМЫ ИТ-МОНИТОРИНГА

Масштаб:

- Сложный и меняющийся ИТ-ландшафт
- Множество источников различных данных
- Слабая связанность между источниками данных
- Растет число задач службы ИТ-мониторинга, а штат не увеличивается
- Высокий уровень «информационного шума»
- Постоянно растут расходы на мониторинг при развитии

Сложность решения проблем:

- Слабая автоматизация и ручное решение инцидентов
- Сильная зависимость от экспертов
- Сложность выявления корневых причин сбоев
- Сбои не прогнозируются, а устраняются по факту
- Отсутствие возможности интеллектуального анализа большого объема данных.
- Клиенты узнают о сбоях раньше ИТ-команды

ПРИМЕР КРУПНОЙ ОРГАНИЗАЦИИ

Рассмотрим типового крупного корпоративного заказчика (финансовый сектор, операторы связи...) со сложным, динамически изменяющимся IT-ландшафтом

Множество источников событий:

- Платформа работы с логами Splunk
- Собственная система мониторинга
- Log-файлы со всех серверов, платформ, БД, ...
- Множество самописных систем - журналы ошибок
- Банковские системы, АТМ
- Ошибки API
- Облачные сервисы, арендованные мощности, каналы связи

Это влечет за собой проблемы:

- Много источников - информационный шум
- Отсутствие полной объективной картины
- Медленный и ручной разбор инцидентов

Потребность изменить ситуацию:

- Понимать связи между аномальными событиями
- Быстрый поиск первопричины по всем источникам
- Оперативное обнаружение, локализация и решение инцидентов



AIOPS: ОТ РЕАКТИВНОГО КОНТРОЛЯ К ПРОАКТИВНОМУ УПРАВЛЕНИЮ

Традиционный подход:

Действия начинаются после возникновения проблемы — система отправляет оповещения при превышении пороговых метрик. Решение инцидентов осуществляется только по факту их влияния на бизнес-сервисы.

Традиционный подход:

AIOps использует ИИ и ML для автоматизации и оптимизации сбора, обработки, исследования данных ИТ мониторинга из множества источников, обогащения их полезным контекстом, детекции аномалий, анализа корреляционных связей, поиска коренных причин, прогнозирования и системного анализа проблем.

Системы мониторинга предоставляют детальные данные о состоянии систем, а AIOps помогает интерпретировать данные, уменьшать информационный шум и прогнозировать возможные сбои

Критерий	Реактивный подход	Проактивный подход
Обнаружение сбоев	По факту возникновения	До момента их возникновения, на ранних этапах за счет предсказания сбоев и детекции аномалий, прогнозирования и оценке рисков
Скорость реакции	Минуты или часы	Секунды за счет автоматизации обнаружения и локализации инцидентов
Автоматизация	Минимальная	Высокая
Влияние на бизнес	Убытки из-за простоев	Минимизация убытков, ускорение цифровой трансформации
Устранение проблем	Ручное, трудоёмкое	Автоматическое и оптимизированное
Нагрузка на ИТ-отдел	Высокая	Снижается за счет высокого уровня автоматизации
Риски повторений	Высокие	Минимальные, благодаря интеллектуальному анализу первопричин инцидентов, системному решению проблем и автоматизации (ИИ помощник, база знаний, прогнозирование, ...)

БОЛЬШЕ, ЧЕМ AIOPS

Аналитическая платформа предлагает расширенные возможности для углубленного исследования данных ИТ-мониторинга, выходя за рамки классического подхода AIOps

Сбор данных:

- Универсальный low-code коннектор OIM, с помощью которого можно подключить практически любую систему мониторинга - не ограничены готовыми коннекторами.
- Парсинг логов - LOG-FILE агент.

Управление изменениями:

- Гибкая настройка нормализации статуса поступающих данных с помощью low-code конструктора условий - извлечение событий, связанных с изменениями конфигурации ПО, оборудования, действиями администраторов, ...

Корреляция:

Построение карт причинно-следственных связей (корреляционные графы):

- статические модели ML корреляции;
- динамические модели ML корреляции (roadmap).

Детекция аномалий:

- Детектор аномалий последовательности (цепочек) событий. Позволяет обнаруживать недостающие ожидаемые события (отсутствие причины, следствия), задержку событий (следствий) (1.3.0).
- Детектор аномалий плотности событий. Позволяет фиксировать избыточно высокую или низкую плотность событий по сравнению с нормальным поведением. Решение позволит фиксировать в т.ч. аномалии в части информационной безопасности (roadmap).

БОЛЬШЕ, ЧЕМ AIOPS

Аналитическая платформа предлагает расширенные возможности для углубленного исследования данных ИТ-мониторинга, выходя за рамки классического подхода AIOps

Управление изменениями:

- ML кластеризация,
- ML классификация.

Позволяют выделить смыслы, разметить, структурировать, сгруппировать слабоструктурированные, неструктурированные данные, в т.ч. Log-файлы.

Автоматизация:

- Автоматическая оценка вероятностного прогноза развития инцидента (roadmap).
- Автоматическое построение карт ресурсов на основе поступающих данных (roadmap).

Инциденты:

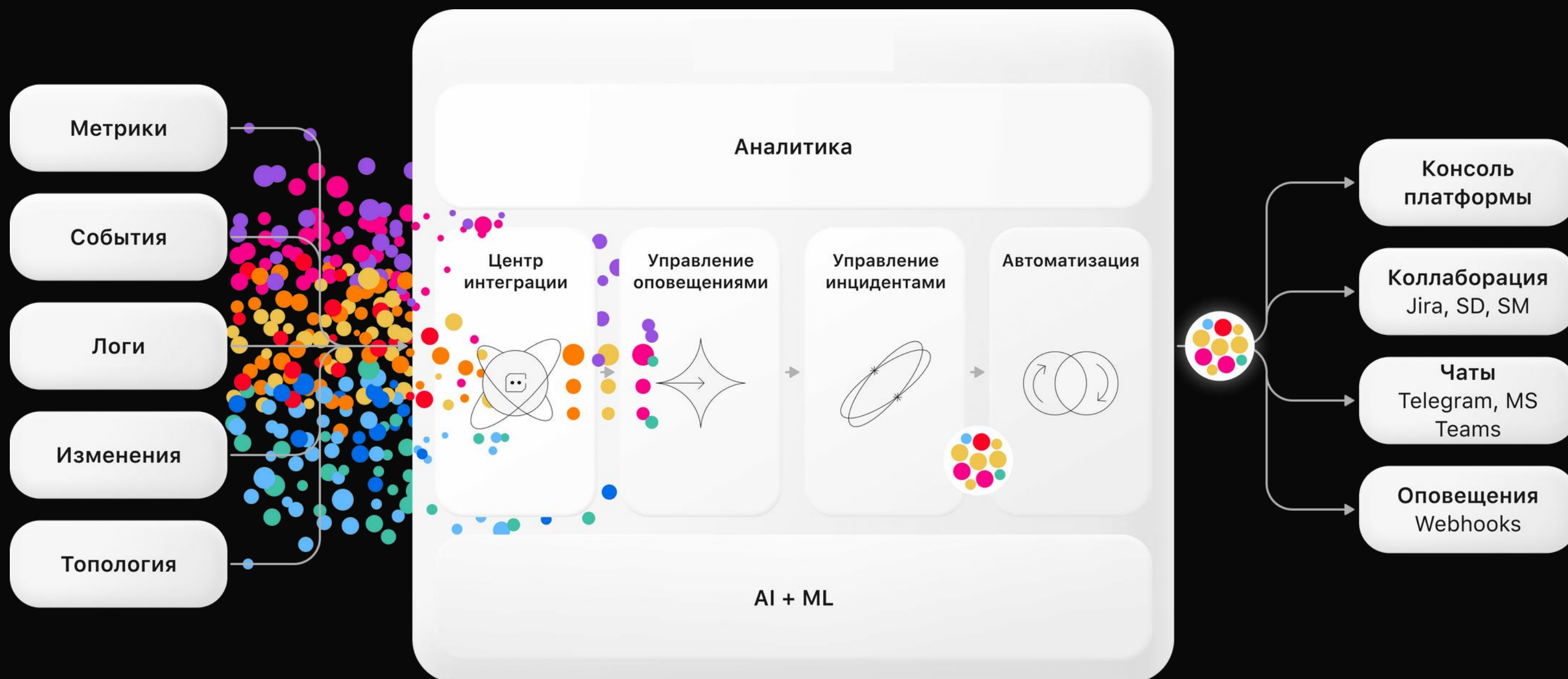
- История инцидента отражает хронологию связанных оповещений, изменений, аномалий.
- Карта причинно-следственных связей инцидента на базе алгоритмических и ML шаблонов корреляции.
- Учет несколько типов аномалий в инцидентах (roadmap).

Аналитика:

Инструменты системного анализа для поиска узких мест и уязвимостей (roadmap):

- Критические компоненты;
- Критические связи;
- Оценка и прогнозирование событий типа "черный лебедь".

КАК РАБОТАЕТ ПЛАТФОРМА?



КАК РАБОТАЕТ ПЛАТФОРМА?

Центр интеграции объединяет данные о событиях и изменениях из нескольких источников, предлагая готовые коннекторы к системам мониторинга и универсальные инструменты настройки пользовательских интеграций. В блоке реализован ETL- процесс.

Центр управления инцидентами формирует полную картину по каждому инциденту, включая набор связанных оповещений, изменений, аномалий, полный жизненный цикл (timeline), карту причинно-следственных связей, предоставляет набор инструментов для анализа, командной работы и решения инцидентов.

Центр управления оповещениями управляет жизненным циклом оповещений, изменений, аномалий, обогащает их полезным контентом (контекстуализация) с помощью набора алгоритмических правил и методов машинного обучения, детектирует аномальные события, исключает избыточную информацию.

Центр автоматизации организует совместную работу команд по локализованным инцидентам, своевременное уведомление пользователей всеми доступными средствами по сути возникающих проблем, предлагает готовые решения из базы знаний, подсказки и советы от встроенного чат-бота, автоматически эскалирует проблемы во внешние системы.

ML-ВОЗМОЖНОСТИ

Предлагаемая интеллектуальная платформа, использует силу ИИ и ML для трансформации подхода к управлению IT-инфраструктурой

Кластеризация:

Структурируйте и исследуйте наборы данных со всех доступных источников, создавайте ML-модели кластеризации на базе различных алгоритмов для поиска, анализа, систематизации, определения шаблонов групп схожих объектов.

Классификация:

Расширяйте возможности стандартных алгоритмических методов обогащения поступающих данных с помощью ML-классификации. Добавляйте новый полезный контекст к оповещениям, чтобы получить полную картину инцидентов для ускорения MTTR.

Корреляция:

Выстраивайте корреляционные графы или карты причинно-следственных связей между компонентами системы, которые позволяют прогнозировать развитие инцидентов, быстро находить первопричины сбоев (root cause analysis) и выявлять неожиданные зависимости, которые сложно заметить вручную

Поиск аномалий:

Находите аномалии, которые часто остаются незамеченными при традиционном мониторинге: локальные изменения в активности компонентов, которые не видны на обобщённых дашбордах; нестандартные последовательности событий, скрытые среди тысяч штатных операций; необычные ситуации, которые невозможно обнаружить вручную; аномальное поведение как отдельных метрик, так и их групп, указывающее на потенциальные риски.

КАКИЕ ЗАДАЧИ РЕШАЕТ ПЛАТФОРМА?

Сокращение информационного шума

Платформа анализирует поток данных, отфильтровывает лишние события и объединяет обогащенные полезным контентом оповещения, чтобы ваша команда могла сосредоточиться на решении ключевых инцидентов.

Системный анализ

Платформа предлагает набор интеллектуальных инструментов для комплексного анализа проблем, оценки состояния ИТ ландшафта, поиска узких мест.

Единый интерфейс для полного контроля

Интуитивно понятный интерфейс платформы объединяет данные со всех источников и предоставляет инструменты для интеллектуального анализа и управления.

Корреляция данных событий

Используя технологии искусственного интеллекта и машинного обучения, платформа определяет взаимосвязи между событиями, что позволяет находить корневые причины и предсказать потенциальные сбои.

Автоматизация решений инцидентов с помощью ИИ и ML

Обнаружение, локализация, оценка и прогнозирование рисков, ручное и автоматическое решение инцидентов с помощью встроенных ML моделей, сценариев эскалации и чат-бота.

Проактивная защита критически важных сервисов

Проактивный мониторинг аварий, изменений, аномалий и автоматизация задач помогают устранить простои и обеспечить надежность ИТ-сервисов даже при высоких нагрузках.

КАКИЕ ЗАДАЧИ РЕШАЕТ ПЛАТФОРМА?



Ускорение обнаружения, локализации и решения инцидентов (MTTR)



Снижение нагрузки на персонал, повышение эффективности ИТ-служб



Повышение качества ИТ услуг и сервисов, соблюдение SLA



Повышение уровня лояльности внутренних и внешних пользователей



ФЕДЕРАЛЬНЫЙ ЦЕНТР
ПРИКЛАДНОГО РАЗВИТИЯ
ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

СПАСИБО ЗА ВНИМАНИЕ!



ФЦПРИИ.РУ



t.me/fcprii