Proto Observability Platform

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Версия платформы: 203

Обозначение документа: ПРОТО.ОБП.203.И3.1

Вид документа: Руководство пользователя

Реестровая запись: № 14369 от 03.08.2022 (единый реестр российских программ для ЭВМ и баз данных)

Листов: 48

Год: 2026

СОДЕРЖАНИЕ

1. Введение

1.1. Область применения

Настоящее руководство определяет порядок работы пользователя с программным обеспечением **Proto Observability Platform** (далее — Система, платформа, ПО).

Система предназначена для комплексного наблюдения (observability) за состоянием информационных систем организации: приложений и микросервисов, серверной и виртуальной инфраструктуры, кластеров Kubernetes, баз данных, сетевого оборудования, а также за качеством цифрового опыта конечных пользователей веб- и мобильных приложений.

Руководство распространяется на все категории пользователей Системы, не обладающих правами администратора платформы. Действия, требующие административных привилегий (установка, обновление, настройка аутентификации, управление учётными записями и правами, настройка сроков хранения данных), описаны в документе **«Руководство администратора»**.

Документ подготовлен в соответствии с требованиями к содержанию документа «Руководство пользователя», установленными РД 50-34.698-90 (п. 3.4), с учётом положений ГОСТ 19.505-79 «ЕСПД. Руководство оператора. Требования к содержанию и оформлению» и ГОСТ Р 59795-2021.

Сведения о правовом статусе ПО. Программное обеспечение Proto Observability Platform включено в единый реестр российских программ для электронных вычислительных машин и баз данных. Запись в реестре № 14369 от 03.08.2022 произведена на основании поручения Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 03.08.2022 по протоколу заседания экспертного совета от 25.07.2022 № 1041пр. Подробные сведения приведены в «Руководстве администратора», п. 9.6.

1.2. Краткое описание возможностей

Система обеспечивает выполнение следующих групп функций:

Группа функций	Состав
Мониторинг приложений (APM)	Сбор в реальном времени метрик, ошибок, трейсов, логов, событий и бизнес-показателей с сервисов и приложений; визуализация на встроенных и пользовательских дашбордах; группировка сервисов в бизнес-приложения; анализ в разрезе окружений, команд и произвольных атрибутов
Распределённая трассировка	Сквозной анализ прохождения запроса через цепочку сервисов, диаграмма «водопад» (waterfall), детализация отдельных спанов, поиск узкого места
Мониторинг цифрового опыта (RUM)	Наблюдение за фронтендом веб- и мобильных приложений: APDEX, Web Vitals, Frustration signals, JS-ошибки, HTTP-запросы, ресурсы, сессии, пользователи, браузеры, геолокация; для мобильных приложений дополнительно — падения (crash) и производительность экранов
Мониторинг инфраструктуры	Хосты Linux и Windows, контейнеры, системы виртуализации, очереди сообщений, веб-серверы и серверы приложений, кеш-системы, Big Data, CI/CD-системы, почтовые системы (свыше 300 поддерживаемых технологий)
Мониторинг Kubernetes	Кластеры, ноды, неймспейсы, поды, деплойменты, демонсеты, сервисы
Мониторинг баз данных	SQL- и NoSQL-СУБД, агентный и безагентный («виртуальные БД») режимы, аналитика SQL-запросов
Мониторинг сети	Сетевое оборудование, проверки HTTP, DNS, TCP, TLS, SSH, NTP
Сбор и анализ логов	Централизованный сбор логов, поиск и анализ на языке LogsQL, визуализация объёмов и уровней серьёзности

Группа функций	Состав
Работа с метриками	Каталог метрик, визуальный и текстовый построитель запросов PromQL/MetricsQL, история и избранные запросы, анализ кардинальности метрик (начиная с версии 202)
Алертинг	Правила оповещений (встроенные и пользовательские), каналы доставки (email, Telegram, Webhook), политики маршрутизации, подтверждение и заглушение алертов, история и MTTR, оповещения о пропадании данных (No-Data)
Окна обслуживания	Объявление периодов регламентных работ с подавлением оповещений и инцидентов по заданным объектам; режимы «Сейчас», «Однократно» и «Регулярно», предпросмотр охвата, отображение окон на графиках (начиная с версии 202)
Выявление аномалий	Автоматическое построение базовых линий (baseline) ключевых показателей средствами машинного обучения с учётом суточной и недельной сезонности
Инциденты (AIOps)	Автоматическая корреляция связанных алертов в инциденты, жизненный цикл по ITIL, ИИ-сводка, ИИ-расследование первопричины, граф распространения (начиная с версии 201)
SLO	Определение целевых уровней обслуживания, бюджет ошибок, автоматические правила алертинга по скорости сжигания бюджета, отчёты о соответствии
Ресурсно-сервисная модель	Единый реестр ИТ-ресурсов и их взаимосвязей, граф зависимостей, справочники CI-классов
Кастомные дашборды	Конструктор дашбордов с виджетами «Текст» и «График», пять источников данных, вкладки и переменные-фильтры, специализированные виджеты «Соты здоровья» и «KPI-карточка», данные модуля «Инциденты» как источник (начиная с версии 202)
Отчёты по электронной почте	Регулярная рассылка дашборда в виде PDF-документа по расписанию либо по требованию, с историей запусков (начиная с версии 202)
Надёжность изменений	Соотношение выкатываемых изменений и изменений, закончившихся инцидентом (метрики класса DORA); сводная аналитика и журнал изменений (начиная с версии 203)
AI-аналитик	Чат по данным платформы: вопросы о состоянии сервисов на естественном языке с ответами, содержащими ссылки на конкретные сущности консоли (начиная с версии 203)
Экспорт и интеграции	Выгрузка в PDF, Excel, PNG; выгрузка трейса в открытых форматах (OTLP/JSON, Zipkin, Jaeger); экспорт журнала аудита в CSV и JSON; экспорт/импорт определений дашбордов; REST/GraphQL/OLAP API; интеграция с Grafana, SIEM, Service Desk/ITSM; приём ошибок из открытых Sentry SDK

Все собираемые данные хранятся исключительно в контуре Заказчика (on-premise, self-hosted) и не передаются во внешние облачные сервисы.

1.3. Уровень подготовки пользователя

Для эксплуатации Системы пользователь должен:

- владеть навыками работы с персональным компьютером и веб-браузером на уровне уверенного пользователя;
- знать предметную область — принципы функционирования сопровождаемых им информационных систем;
- быть ознакомлен с настоящим руководством.

Для выполнения расширенных операций (написание запросов PromQL/MetricsQL и LogsQL, создание правил алертинга, работа с OLAP-запросами и API) дополнительно требуется:

- понимание модели данных временных рядов и основ языка запросов PromQL;
- базовые представления о распределённой трассировке (трейс, спан, контекст);
- для интеграционных сценариев — навыки работы с REST API и форматом JSON.

Пользователи, впервые работающие с классом систем observability, могут приступать к эксплуатации после освоения разделов 3, 4.1, 4.2 и контрольного примера (раздел 6.1).

1.4. Перечень эксплуатационной документации

Обозначение	Наименование	Назначение
ПРОТО.ОБП.203.ИЗ.1	Руководство пользователя (настоящий документ)	Порядок работы с пользовательским интерфейсом
ПРОТО.ОБП.203.ИЗ.2	Руководство администратора	Установка, настройка, администрирование, восстановление
—	Описание функциональных характеристик ПО	Сведения для приобретателя и уполномоченных органов
—	Онлайн-документация вендора	Актуальные справочники метрик, языков запросов, подключения технологий
—	Release notes	Сведения об изменениях в очередной версии

1.5. Термины и сокращения

Термин / сокращение	Расшифровка
APM	Application Performance Monitoring — мониторинг производительности приложений
RUM / EUM	Real User Monitoring / End User Monitoring — мониторинг реального пользовательского опыта
APDEX	Application Performance Index — интегральный индекс удовлетворённости пользователей скоростью работы системы, принимает значения от 0 до 1
Трейс (trace)	Запись полного прохождения запроса через цепочку сервисов
Спан (span)	Отдельная операция внутри трейса (вызов метода, обращение к БД, HTTP-запрос)
Эндпоинт	Точка входа сервиса (операция, обрабатывающая запросы)
Метрика	Числовой показатель, измеряемый во времени
Лейбл (label)	Пара «ключ — значение», уточняющая принадлежность метрики или алерта
Алерт	Оповещение, сформированное при выполнении условия правила алертинга
Инцидент	Группа коррелированных алертов, объединённых платформой в одну сущность
Правило алертинга	Условие на языке PromQL/MetricsQL, при выполнении которого генерируется алерт
Канал оповещения	Адрес доставки уведомлений (email, Telegram, Webhook)
Политика оповещений	Правило маршрутизации алертов в каналы на основе лейблов
SLO	Service Level Objective — целевой уровень качества обслуживания
Бюджет ошибок	Допустимый объём нарушений SLO за период
MTTR	Mean Time To Repair — среднее время устранения
PCM	Ресурсно-сервисная модель

Термин / сокращение	Расшифровка
CI	Configuration Item — конфигурационная единица
PromQL / MetricsQL	Языки запросов к метрикам временных рядов
LogsQL	Язык запросов к логам
Baseline (базовая линия)	Ожидаемый диапазон значений показателя, рассчитанный автоматически
RBAC	Role-Based Access Control — ролевая модель управления доступом
SSO	Single Sign-On — единый вход
AIOps	Применение методов машинного обучения к задачам эксплуатации ИТ
Окно обслуживания	Заранее объявленный период регламентных работ по заданным объектам, на время которого оповещения и инциденты по ним подавляются
No-Data	Семейство встроенных правил алертинга, срабатывающих при прекращении поступления метрик от ранее наблюдавшегося источника
Флейм-граф	Представление трейса, в котором ширина блока пропорциональна длительности операции, а вложенность повторяет структуру вызовов
Критический путь	Цепочка спанов, определяющая общую длительность трейса
Кардинальность метрики	Число уникальных временных рядов, порождаемых метрикой и сочетаниями значений её лейблов
Соты здоровья (Honeycomb)	Виджет с плотной шестиугольной раскладкой, где одна ячейка соответствует одному объекту, а её цвет — состоянию объекта
Отчёт	Настроенная рассылка дашборда в виде PDF-документа по расписанию или по требованию
DSN	Строка адреса приёма событий, используемая Sentry SDK
DORA-метрики	Класс показателей надёжности процесса поставки изменений: частота выкатки изменений и доля изменений, приведших к инциденту
Маркер изменения	Отметка о релизе или развёртывании, передаваемая в платформу из конвейера CI/CD и отображаемая на графиках

2. Назначение и условия применения

2.1. Виды деятельности и функции, для автоматизации которых предназначена Система

Система предназначена для автоматизации следующих видов деятельности подразделений эксплуатации, разработки и сопровождения информационных систем:

1. **Контроль доступности и производительности** прикладных сервисов, инфраструктурных компонентов и бизнес-приложений в режиме реального времени.
2. **Диагностика инцидентов производительности** — определение затронутого сервиса, эндпоинта, инстанса, зависимого компонента и первопричины отклонения.
3. **Анализ первопричин (Root Cause Analysis)** на основе связанных трейсов, логов, метрик и событий.
4. **Контроль качества цифрового опыта** конечных пользователей веб- и мобильных приложений.
5. **Оповещение ответственных лиц** о нарушениях пороговых значений и об аномальном поведении показателей.
6. **Контроль соблюдения целевых уровней обслуживания (SLO/SLA)** и расходования бюджета ошибок.
7. **Учёт ИТ-ресурсов и их взаимосвязей** в ресурсно-сервисной модели.
8. **Контроль бизнес-показателей** (бизнес-операции, бизнес-процессы, бизнес-транзакции, KPI).
9. **Подготовка отчётности** о состоянии, доступности и производительности контролируемых объектов.

2.2. Условия применения

2.2.1. Требования к рабочему месту пользователя

Пользовательский интерфейс Системы является веб-приложением; установка клиентского ПО на рабочем месте не требуется.

Параметр	Значение
Браузер	Актуальная версия браузера на движке Chromium (Яндекс.Браузер, Chrome, Edge, Chromium) или Mozilla Firefox
Разрешение экрана	Не менее 1440 × 900; рекомендуется 1920 × 1080
Оперативная память рабочей станции	Не менее 8 ГБ (дашборды с большим числом виджетов увеличивают потребление памяти браузером)
Сетевой доступ	HTTP/HTTPS (порт 80 или 443) до сервера ProtoOBP Backend
Дополнительно	Включённые JavaScript и cookies; для экспорта файлов — разрешение на загрузку файлов

Операционная система рабочего места значения не имеет; поддерживаются в том числе отечественные ОС (Astra Linux, РЕД ОС, «Альт», ROSA) с браузером на движке Chromium.

2.2.2. Организационные условия

- Пользователю выдана учётная запись в Системе (собственная либо доменная — при подключённом SSO).
- Пользователю назначена роль, определяющая доступный набор разделов и объём видимых данных.

- Целевые объекты мониторинга подключены к Системе (установлены агенты, подключены трейсеры и источники метрик и логов).

2.2.3. Ограничения области видимости данных

Объём данных, доступных пользователю, определяется назначенными ему ролями. Ограничение может быть задано по трём измерениям: **сервисы**, **хосты**, **группы сервисов**. Фильтр применяется автоматически ко всем запросам данных — к виджетам дашбордов, обозревателю трейсов, обозревателю логов, браузеру метрик, разделам «Инфраструктура → Хосты», «Бизнес-приложения» и «SLO».

> **Внимание.** Если ожидаемый объект отсутствует в списках или интерфейс отображает панель «Доступ запрещён», это, как правило, следствие ограничения области видимости, а не сбой Системы. Обратитесь к администратору платформы.

3. Подготовка к работе

3.1. Состав и содержание дистрибутива

Установка ПО на рабочем месте пользователя не производится. Доступ к Системе осуществляется через веб-браузер по адресу, предоставленному администратором платформы (значение параметра `UI_URL`), например:

```
https://protoobp.company.local
```

Развёртывание серверной части и агентов выполняется администратором в соответствии с документом «Руководство администратора».

3.2. Порядок запуска Системы (вход)

1. Запустите веб-браузер.
2. В адресной строке введите адрес Системы, полученный от администратора.
3. При использовании самоподписанного сертификата браузер может вывести предупреждение о недоверенном соединении — в этом случае действуйте согласно регламенту, установленному в организации.
4. На странице входа:
   - при встроенной аутентификации — введите логин и пароль, нажмите кнопку входа;
   - при подключённом SSO (LDAP / OIDC) — нажмите кнопку с наименованием провайдера единого входа и выполните аутентификацию в корпоративной системе.
5. При первом входе по временному паролю Система потребует задать постоянный пароль.

После успешной аутентификации открывается основное окно Системы с меню навигации.

Завершение работы. Для выхода используйте пункт выхода в меню учётной записи. Закрытие вкладки браузера без выхода не завершает сессию немедленно.

3.3. Порядок проверки работоспособности

Система считается работоспособной и готовой к работе, если выполняются следующие условия:

№	Проверка	Ожидаемый результат
1	Страница входа открывается по адресу Системы	Отображается форма аутентификации
2	Выполнен вход под учётной записью пользователя	Открывается основное окно с меню навигации
3	Открыт раздел **Приложения → Сервисы**	Отображается список подключённых сервисов с актуальными значениями метрик
4	Открыт раздел **Инфраструктура → Хосты**	Отображается список контролируемых хостов
5	На дашборде выбран интервал «последние 15 минут»	Графики содержат данные, правая граница графика соответствует текущему времени
6	Открыт раздел **Алерты → Активные**	Отображается стена алертов либо сообщение об отсутствии активных алертов

Если данные на графиках отсутствуют или отстают более чем на несколько минут, выполните действия из раздела 5. Аварийные ситуации.

4. Описание операций

4.1. Общие принципы работы с интерфейсом

4.1.1. Структура основного окна

Основное окно Системы состоит из двух постоянных элементов и рабочей области:

- **боковое меню** (слева) — перечень разделов платформы. Меню свёрнуто до значков и разворачивается при наведении курсора. Разделы, недоступные пользователю по правам доступа, в меню не отображаются;
- **верхняя панель** — «хлебные крошки» текущего расположения, выбор периода наблюдения, кнопка обновления данных (с режимом автообновления), ссылка на документацию, переключатель темы оформления (светлая, тёмная или по настройке устройства) и меню учётной записи с перечнем назначенных ролей, выбором языка интерфейса (русский, английский) и выходом из Системы;
- **рабочая область** — дашборды, таблицы, графы, конструкторы;
- **панель действий** рабочей области — экспорт, настройка, переход к связанным разделам.

4.1.2. Разделы меню навигации

Разделы перечислены в том порядке, в котором они расположены в боковом меню.

Раздел	Подразделы	Назначение
Обзор	—	Стартовый экран со сводным дашбордом общего состояния: ключевые показатели, проблемы и аномалии по всем подключённым источникам
Приложения	Бизнес-приложения, Сервисы, Ошибки, Внешние сервисы, Виртуальные базы данных, Очереди сообщений, Настройки APM	Мониторинг производительности приложений (APM) и анализ ошибок
Цифровой опыт	Веб-приложения, Мобильные, Веб-транзакции, JS ошибки, Сессии, Пути, Настройки	Мониторинг реального пользовательского опыта (RUM)
Бизнес-аналитика	Транзакции, Бизнес-процессы, Настройки	Анализ бизнес-показателей поверх телеметрии приложений
Инфраструктура	Единый каталог источников по категориям	Инвентаризация и мониторинг инфраструктуры (единый каталог — начиная с версии 202)
Kubernetes	Навигатор, Кластеры, Неймспейсы	Мониторинг контейнерных платформ
Инциденты и Алерты	Инциденты, Активные Алерты, История Алертов, Надёжность изменений, Правила, Каналы оповещения, Политики оповещения, SLO, Окна обслуживания, Настройки Инцидентов	Оповещения, разбор инцидентов, цели уровня обслуживания и регламентные работы (объединённый раздел — начиная с версии 202; подраздел «Надёжность изменений» — начиная с версии 203)
Дашборды и отчёты	Дашборды, Отчёты	Пользовательские дашборды и регулярная рассылка отчётов (вкладка «Отчёты» — начиная с версии 202)
Трейсы	—	Traces Explorer — поиск и анализ распределённых трейсов
Метрики	Браузер, Конструктор, Кардинальность	Каталог метрик, построитель PromQL-запросов, анализ кардинальности (вкладка «Кардинальность» — начиная с версии 202)

Раздел	Подразделы	Назначение
Логи	—	Logs Explorer — поиск и анализ логов (начиная с версии 200)
РСМ	Каталог ресурсов, Настройки РСМ	Ресурсно-сервисная модель (начиная с версии 200)
AI-аналитик	—	Чат по данным платформы на естественном языке; требует настроенной языковой модели (начиная с версии 203)
Роли и доступ	Пользователи, Роли, Разрешения, Внешние группы, Журнал аудита, Проверка на ПДн	Управление доступом; только для администраторов при включённом RBAC (начиная с версии 200; вкладка «Проверка на ПДн» — начиная с версии 203)
Диагностика	Лицензия, Объём данных, Processor, Реестр конфигурации, Логи бэкенда	Сведения о работе самой платформы (пункты «Объём данных» и «Реестр конфигурации» — начиная с версии 203, доступны администраторам)

Состав отображаемых разделов зависит от прав назначенной роли.

Изменения расположения разделов в версии 202. Ранее самостоятельные разделы бокового меню — «Базы данных», «Сеть», «Очереди сообщений», «Веб-серверы» — перенесены внутрь раздела **Инфраструктура**, который стал единым каталогом источников. Разделы «Алерты» и «Инциденты» объединены в раздел **Инциденты и Алерты**. Ранее сохранённые адреса дашбордов продолжают работать.

Каталог «Инфраструктура». Раздел открывается витриной, на которой поддерживаемые технологии сгруппированы по категориям: хосты; сетевые устройства; проверки доступности (HTTP, DNS, TCP); базы данных; кеш-системы; очереди сообщений; веб-, прокси- и серверы приложений; системы виртуализации; Big Data; CI/CD; почтовые системы; Service Mesh; прочее. Внутри каждой категории источники разделены на **«Подключено»** и **«Доступно для подключения»**: подключённый источник открывает встроенный дашборд или список экземпляров, а карточка неподключённого ведёт к инструкции по подключению.

4.1.3. Выбор периода наблюдения

Период задаётся в верхней панели и применяется ко всем виджетам текущей страницы. Доступны быстрые интервалы (последние 15 минут, час, сутки, неделя и др.) и произвольный интервал с указанием даты и времени начала и окончания.

При выборе больших интервалов Система переходит на более грубую агрегацию данных (минутную, часовую, суточную) — это нормальное поведение, обусловленное схемой хранения.

4.1.4. Обновление данных

Кнопка **«Обновить»** в правом верхнем углу обновляет **значения метрик на текущем дашборде**. Она **не обновляет** состав списков объектов (например, перечень серверов или сервисов).

> **Важно.** Чтобы увидеть вновь подключённый объект (новый хост, новый сервис), обновите страницу браузера целиком (F5 / Ctrl+R).

4.1.5. Навигация «от симптома к причине»

Интерфейс построен по принципу последовательного углубления: с обзорного дашборда бизнес-приложения — к дашборду сервиса, далее — к эндпоинту, инстансу, конкретному трейсу, спану,

связанному логу и событию. Переход выполняется кликом по элементу графика, строке таблицы или ссылке в аннотации алерта.

4.2. Мониторинг приложений и сервисов (APM)

Раздел: `Приложения`

4.2.1. Подраздел «Бизнес-приложения»

Назначение. Анализ производительности и ошибок бизнес-приложений — логических групп сервисов — в разрезе окружения, команд и иных атрибутов.

Порядок работы:

1. Откройте `Приложения` → `Бизнес-приложения`.
2. Выберите период наблюдения.
3. При необходимости примените фильтры (окружение, команда и др.).
4. На встроенном дашборде оцените ключевые показатели группы: количество вызовов, время отклика, долю ошибок, APDEX, выявленные аномалии.
5. Для перехода к источнику проблемы кликните по проблемному элементу — откроется дашборд соответствующего сервиса.

4.2.2. Подраздел «Сервисы»

Назначение. Анализ работы отдельных сервисов по ключевым показателям.

Обзор всех сервисов. На обзорной странице отображается перечень подключённых сервисов с ключевыми показателями. Используйте сортировку и фильтрацию для выявления сервисов с наихудшими значениями APDEX, наибольшей долей ошибок или наибольшим временем отклика.

Дашборд сервиса. Кликните по имени сервиса. Дашборд сервиса предоставляет в реальном времени:

- ключевые метрики: количество вызовов, время отклика (среднее и перцентили), долю ошибок, APDEX;
- выявленные аномалии относительно базовой линии;
- список эндпоинтов с показателями по каждому;
- список инстансов сервиса, включая Runtime-метрики и данные о подах Kubernetes;
- связанные трейсы и логи;
- карту взаимосвязей сервиса с другими сервисами и инфраструктурными компонентами;
- события (в том числе маркеры релизов) и сработавшие оповещения.

Типовой сценарий диагностики:

1. На дашборде сервиса определите период деградации по графику времени отклика или доли ошибок.
2. Сопоставьте его с лентой событий — не совпадает ли деградация с релизом или изменением конфигурации.
3. Перейдите в список эндпоинтов и определите, затронуты ли все эндпоинты или отдельные.
4. Перейдите в список инстансов — локализована ли проблема на одном инстансе.
5. Откройте связанные трейсы медленных или ошибочных вызовов.
6. В трейсе найдите спан с наибольшей длительностью или с признаком ошибки.
7. При необходимости перейдите к логам соответствующего сервиса за тот же интервал.

4.2.3. Подраздел «Ошибки»

Сводная аналитика ошибок приложений: группировка по типам исключений, по эндпоинту и инстансу; динамика во времени; перечень затронутых сервисов и эндпоинтов; переход к трейсу и логам конкретной ошибки, а также к тексту исключения со стеком вызовов.

Начиная с версии 202 в этот же раздел попадают ошибки, полученные напрямую из приложений, инструментированных открытыми **Sentry SDK** (Python, JavaScript/Node.js, Java, Go, PHP, Ruby, .NET и другие). Такие ошибки отображаются наравне с ошибками, собранными трейсерами платформы: с группировкой, стек-трейсами, счётчиками, первым и последним появлением и динамикой во времени. Подключение выполняется администратором и разработчиками приложения — изменением адреса приёма (DSN) в настройках SDK, без переписывания кода и замены библиотеки.

4.2.3A. Прочие подразделы раздела «Приложения»

Подраздел	Содержание
Внешние сервисы	Производительность и доступность внешних HTTP-сервисов, к которым обращаются приложения: время ответа, коды ответов, ошибки
Виртуальные базы данных	Показатели баз данных, полученные безагентным способом — из анализа вызовов подключённых приложений, без установки агента на сервер СУБД
Очереди сообщений	Работа с очередями со стороны приложений: производители и потребители, задержки и ошибки обработки
Настройки APM	Управление сегментами сервисов и порогами APDEX

4.2.4. Бизнес-операции, бизнес-транзакции и бизнес-процессы

Система позволяет выделять отдельные транзакции в качестве **ключевых бизнес-операций** и отслеживать их отдельно от общей массы вызовов, а также обогащать транзакции бизнес-контекстом (например, идентификатором клиента, номером договора, суммой операции) с помощью правил извлечения бизнес-контекста.

Для ключевых бизнес-операций доступны собственные показатели, дашборды и правила алертинга.

Мониторинг бизнес-процессов обеспечивает сквозной контроль многошаговых процессов с визуализацией потока (BusinessFlow) и выявлением шагов, на которых происходят потери и задержки.

4.3. Анализ распределённых трейсов

Раздел: `Трейсы` (Traces Explorer), а также вкладки трейсов на дашбордах сервисов.

4.3.1. Ключевые понятия

- **Трейс** — полная запись прохождения одного запроса через цепочку сервисов.
- **Спан** — отдельная операция внутри трейса. Спаны образуют дерево: родительский спан вызывает дочерние.
- **Длительность спана** — время выполнения операции, включая вложенные вызовы.

4.3.2. Поиск трейсов

1. Откройте раздел `Трейсы`.
2. Задайте период наблюдения.

3. Задайте условия отбора:
   - **сервис** — сервис, породивший трейс;
   - **операция (эндпоинт)** — конкретная операция;
   - **длительность** — минимальная и/или максимальная;
   - **статус** — успешные / завершившиеся ошибкой.
4. Выполните поиск. Результат отображается списком трейсов с указанием времени начала, длительности, состава участвующих сервисов и признака ошибки.

4.3.3. Анализ трейса

Кликните по трейсу. Открывается диаграмма «водопад» (waterfall):

- по горизонтали — время; по вертикали — иерархия спанов;
- ширина полосы спана пропорциональна его длительности;
- спаны с ошибками выделяются цветом.

Кликните по спану, чтобы просмотреть его детали: сервис, операцию, длительность, теги (атрибуты), текст запроса к БД (в обфусцированном виде), сведения об ошибке.

Как читать диаграмму:

- «Ступенчатая лестница» — последовательные вызовы; общая длительность складывается из длительностей шагов;
- широкий спан в конце цепочки без вложенных — узкое место находится в самом этом компоненте (например, в СУБД);
- разрыв между окончанием одного спана и началом следующего — время, потраченное вне инструментированного кода (ожидание в очереди, сетевая задержка, работа неинструментированного участка);
- множество коротких однотипных спанов подряд — характерный признак проблемы «N+1 запрос».

4.3.3А. Флейм-граф трейса

Начиная с версии 202 в детальном просмотре трейса рядом с диаграммой «водопад» доступна вкладка **«Флейм-граф»**. Ширина блока пропорциональна длительности операции, вложенность повторяет структуру вызовов, цвет соответствует сервису.

Дерево спанов при сотнях операций приходится прокручивать; флейм-граф размещает весь трейс на одном экране и сразу показывает, где сосредоточено время и какая ветвь вызовов его формирует.

Работа с флейм-графом:

Действие	Как выполняется
Детализация (дрилл-даун)	Клик по блоку масштабирует граф на выбранное поддерево. Путь отображается «хлебными крошками» — от пункта «Весь трейс» до текущего спана; возврат — кликом по любому уровню или кнопкой **«Сбросить зум»**
Детали спана	`Ctrl + клик` (`⌘ + клик` в macOS) по блоку открывает карточку спана
Поиск спанов	Фильтр по имени операции со счётчиком совпадений
Критический путь	Подсвечивает цепочку спанов, определяющую общую длительность трейса
Сжать паузы	Схлопывает длительные простои (ожидание в очереди, асинхронные вызовы), чтобы фактическая работа занимала большую часть ширины. Кнопка появляется только при наличии таких пауз
Линейка времени	Закреплена сверху: на любом уровне вложенности видно, в какой момент трейса выполняется операция

Спаны, завершившиеся ошибкой, обведены красной рамкой с сохранением цвета сервиса. На очень крупных трейсах часть спанов может не отрисовываться — над графом выводится пометка с числом непоказанных спанов.

4.3.3Б. Выгрузка трейса в открытых форматах

Начиная с версии 202 в просмотре трейса доступно меню **«Экспорт трейса»**: выбранный трейс сохраняется в файл в одном из открытых форматов — **OTLP/JSON**, **Zipkin v2 JSON** или **Jaeger JSON**.

Выгруженный трейс можно приложить к обращению в службу технической поддержки, передать команде разработки или открыть в стороннем средстве анализа — данные остаются переносимыми.

4.3.4. Типовые сценарии

Сценарий	Порядок действий
Поиск причины медленных запросов	Отбор трейсов сервиса с длительностью выше перцентиля → анализ waterfall → определение спана-«долгожителя»
Разбор ошибки	Отбор трейсов со статусом «ошибка» → переход к спану с ошибкой → анализ тегов и стека
Проверка после релиза	Сравнение трейсов до и после маркера релиза за одинаковые интервалы
Поиск «N+1»	Анализ трейса на предмет серий одинаковых спанов обращений к БД
Быстрый поиск узкого места в длинном трейсе	Вкладка «Флейм-граф» → «Критический путь» → детализация по самому широкому блоку
Передача трейса разработчикам или в поддержку	«Экспорт трейса» → выбор формата (OTLP/JSON, Zipkin, Jaeger)

4.4. Поиск и анализ логов

Раздел: `Логи` (Logs Explorer). Доступен начиная с версии 200.

4.4.1. Режимы построения запроса

Обозреватель логов поддерживает два режима:

- **Визуальный режим** — построение запроса через элементы интерфейса: фильтры и пайпы (этапы обработки). Подходит пользователям, не знакомым с синтаксисом LogsQL.
- **Режим «Чистый LogsQL»** — прямой ввод запроса с подсветкой синтаксиса и автодополнением.

Режимы синхронизированы: запрос, построенный визуально, отображается в текстовом виде. Обратное преобразование возможно не для всех конструкций — при переключении из текстового режима в визуальный сложный запрос может быть не разобран; в этом случае продолжите работу в текстовом режиме.

4.4.2. Порядок работы

1. Откройте раздел `Логи`.
2. Задайте временной диапазон.
3. Постройте запрос:

   - в визуальном режиме — добавьте фильтры (по сервису, хосту, уровню серьёзности, тексту сообщения, произвольным полям) и при необходимости пайпы (агрегация, извлечение полей, сортировка, ограничение количества);
   - в режиме LogsQL — введите запрос, например:

```
service:exact("payment-service") AND level:exact("error")
```

4. Выполните запрос.
5. Проанализируйте результат:
   - **гистограмма объёма логов** — распределение количества записей во времени с цветовой индикацией уровней серьёзности; позволяет визуально локализовать всплеск;
   - **таблица записей** — перечень лог-записей; поддерживается режим отображения JSON;
   - **панель деталей записи** — полный состав полей выбранной записи.
6. При необходимости уточните запрос, используя контекстное меню легенды гистограммы (например, отфильтровать по конкретному уровню).

4.4.3. Рекомендации

- Начинайте с широкого запроса и узкого временного диапазона, затем сужайте условия.
- Для поиска причин инцидента задавайте интервал, охватывающий момент начала алерта минус 5–15 минут.
- Точное сопоставление (`exact`) выполняется быстрее подстрочного поиска — используйте его при известном значении поля.
- Результаты запроса ограничены областью видимости, назначенной вашей роли: хосты сопоставляются с полем `hostname`, сервисы — с полем `service`.

4.5. Работа с метриками и PromQL

Раздел: `Метрики`

4.5.1. Браузер метрик

Браузер метрик представляет каталог всех доступных метрик:

- **список метрик** с поиском по имени;
- **детали метрики** — описание, тип (counter, gauge, histogram, summary), единицы измерения;
- **исследование лейблов** — перечень лейблов метрики и их фактических значений.

Используйте браузер, чтобы выяснить, какая метрика содержит нужный показатель и какими лейблами её можно разрезать.

4.5.2. Построитель запросов

Визуальный режим. Запрос собирается из элементов интерфейса: выбор метрики, добавление фильтров по лейблам, выбор функции агрегации и группировки, задание временного окна. Формируемый запрос отображается в текстовом виде.

Режим «Чистый PromQL». Прямой ввод выражения с подсветкой синтаксиса, автодополнением и валидацией. Пример:

```
round(avg(system_cpu_system{host=~".*central1.internal"}) by (host), 0.1)
```

Переключение между режимами выполняется кнопкой; сложные выражения могут быть недоступны для разбора визуальным режимом.

4.5.3. Анализ результатов

Результат запроса доступен на вкладках:

Вкладка	Содержание
График	Временные ряды результата
Таблица	Табличное представление значений
Статистика	Сводные показатели по рядам
Объяснение	Разбор структуры запроса и порядка вычисления
Производительность	Стоимость выполнения запроса, число обработанных рядов и точек

Результаты можно экспортировать.

4.5.3А. Анализ кардинальности метрик

Начиная с версии 202 в разделе `Метрики` доступна вкладка **«Кардинальность»**. Она отвечает на вопрос, какие метрики и лейблы расходуют базу временных рядов, и позволяет найти метки, чрезмерно увеличивающие объём хранения (идентификаторы запросов, пользователей или сессий, попавшие в лейблы), до того как это скажется на скорости запросов и на свободном месте на дисках.

Сводные показатели:

Показатель	Смысл
Всего серий	Общее число временных рядов в хранилище метрик
Пар «лейбл=значение»	Число уникальных сочетаний лейбла и его значения
Уникальных имён метрик	Количество различных собираемых метрик

Фильтры: количество отображаемых строк («Топ»), дата среза, ограничение среза PromQL-селектором (например, `{service="cart"}`), разрез по выбранному лейблу, отбор только незапрашиваемых метрик.

Таблицы среза: топ метрик по числу серий; лейблы по числу серий; лейблы по числу уникальных значений; топ пар «лейбл=значение»; распределение серий по значениям выбранного лейбла.

Для метрик дополнительно отображаются число обращений и время последнего обращения (либо «никогда»). Метрики, к которым ни разу не выполнялись запросы, отмечены полосой слева — это кандидаты на отключение при сборе.

> **Порядок разбора.** Откройте «Лейблы по числу уникальных значений» → найдите лейбл с аномально большим числом значений → постройте по нему разрез и убедитесь, что в значениях содержатся идентификаторы → обратитесь к команде разработки или к администратору платформы для исключения такого лейбла на стороне инструментирования или сбора.

4.5.4. История и избранные запросы

Выполненные запросы сохраняются в **истории** с указанием текста запроса, времени выполнения и результата. Часто используемые запросы можно сохранить в **избранное** для повторного применения.

4.5.5. Решение типовых проблем с запросами

Симптом	Вероятная причина и действие
Запрос не возвращает данных	Проверьте точность имени метрики и значений лейблов через

Симптом	Вероятная причина и действие
	браузер метрик; убедитесь, что выбранный период содержит данные; проверьте, входит ли объект в вашу область видимости
Ошибка «No data» при использовании `rate()`	Временное окно функции меньше интервала сбора метрики — увеличьте окно (например, до `5m`)
Запрос выполняется слишком долго	Сузьте период; добавьте фильтры по лейблам; уменьшите кардинальность группировки
Неожиданные значения на графике	Проверьте тип метрики: к counter применяются `rate`/`increase`, к gauge — `avg`/`max`/`min`
Визуальный режим не разбирает запрос	Продолжите работу в режиме «Чистый PromQL»

4.6. Мониторинг цифрового опыта (RUM)

Раздел: `Цифровой опыт`

4.6.1. Веб-приложения

Подраздел отображает ключевые показатели производительности и ошибки фронтенда в разрезе страниц и версий:

- **APDEX** — интегральная удовлетворённость пользователей;
- **Web Vitals** — показатели загрузки и отзывчивости страниц;
- **Frustration signals** — признаки раздражения пользователя (повторные клики, «клики в пустоту», перезагрузки);
- **JS-ошибки** — ошибки исполнения на стороне браузера;
- **HTTP-запросы и ресурсы** — обращения фронтенда к бэкенду и загрузка ресурсов;
- **Сессии и пользователи** — записи пользовательских сессий;
- **Браузеры и геолокации** — распределение аудитории.

4.6.2. Мобильные приложения

Подраздел предоставляет те же группы показателей для приложений iOS и Android, дополненные:

- **падениями приложения (crash)** — количество, стек, затронутые версии и устройства;
- **производительностью экранов** — время отрисовки и отклика.

4.6.2А. Прочие подразделы раздела «Цифровой опыт»

Подраздел	Содержание
Веб-транзакции	Ключевые бизнес-транзакции фронтенда — отдельная аналитика по важным для бизнеса пользовательским сценариям
JS ошибки	Реестр и анализ JavaScript-ошибок веб-приложений с группировкой, динамикой и детализацией. Начиная с версии 202 поддерживается приём ошибок из Sentry SDK
Сессии	Поиск и анализ пользовательских сессий: список с фильтрами, временная шкала действий и воспроизведение записи сессии (session replay), начиная с версии 201
Пути	Анализ путей пользователей (см. п. 4.6.4), начиная с версии 201
Настройки	Управление ключевыми бизнес-транзакциями фронтенда и правилами их автоматического определения

Начиная с версии 202 в модуле цифрового опыта улучшено распознавание устройств: добавлена **классификация ботов** (поисковые, скрейперы, SEO и отдельно AI-краулеры — GPTBot, ClaudeBot,

PerplexityBot, Bytespider, краулеры Яндекса), а также **распознавание встроенных браузеров** мобильных приложений (поисковые приложения, мессенджеры и другие). Это позволяет отделять трафик реальных браузеров от трафика внутри приложений. Новые характеристики отображаются в секции «Устройство» карточки трейса и спана.

4.6.3. Трейсы сессий

Трейсы сессий связывают действия пользователя в браузере или мобильном приложении со сквозными вызовами на бэкенде — это позволяет от жалобы пользователя перейти к конкретной серверной операции.

4.6.4. Анализ путей (User Journeys)

Диаграмма путей показывает последовательность переходов пользователей между страницами:

- **чтение диаграммы** — узлы соответствуют страницам, связи — переходам, толщина связи пропорциональна числу переходов;
- **режимы анализа** — от выбранной страницы вперёд (куда уходят) или назад (откуда приходят);
- **сводка и сравнение периодов** — сопоставление поведения пользователей за разные интервалы;
- **здоровье страниц** — показатели производительности и ошибок по каждой странице пути;
- **переход к сессиям** — от узла диаграммы к конкретным пользовательским сессиям.

> **Рекомендация.** Качество диаграммы напрямую зависит от качества названий страниц. Если на диаграмме преобладают узлы с однотипными или техническими названиями, обратитесь к команде разработки для настройки осмысленных наименований страниц.

4.7. Мониторинг инфраструктуры, Kubernetes, БД и сети

4.7.1. Инфраструктура

Раздел: `Инфраструктура`

Начиная с версии 202 раздел представляет собой единый каталог источников. Витрина каталога группирует поддерживаемые технологии по категориям; внутри каждой категории источники разделены на **«Подключено»** и **«Доступно для подключения»**.

Категория каталога	Содержание
Хосты	Серверы Linux и Windows: загрузка процессора, памяти, дисков, сети; события; проблемы; ошибки проверок; контейнеры, относящиеся к хосту
Базы данных	СУБД с установленным агентом: PostgreSQL, MySQL, MongoDB, Oracle, ClickHouse, Elasticsearch, MS SQL, DB2, Cassandra и другие. По MySQL дополнительно доступна детальная аналитика SQL-запросов и связанных с ними ошибок
Системы виртуализации	VMware vSphere (обзор vCenter, ESXi-хосты, дата-центры, кластеры, хранилища данных, виртуальные машины), Яндекс Облако, Базис.DynamiX. Объекты виртуализации обнаруживаются автоматически и попадают в ресурсно-сервисную модель (начиная с версии 201)
Сетевые устройства и проверки доступности	Сетевое оборудование, активные проверки по протоколам HTTP, DNS, TCP
Очереди сообщений	Kafka, RabbitMQ, ActiveMQ, IBM MQ и другие

Категория каталога	Содержание
Веб-, прокси- и серверы приложений	Nginx, Apache HTTPd, Tomcat, WebLogic, WebSphere, IIS, HAProxy и другие
Кеш-системы, Big Data, CI/CD, почтовые системы, Service Mesh, прочее	Остальные подключённые технологии

4.7.2. Kubernetes

Подраздел	Содержание
Навигатор	Инвентарь объектов кластеров на одном экране с вкладками «Обзор», «Кластеры», «Рабочие нагрузки», «Поды», «Узлы». Позволяет переходить от кластера к неймспейсу, рабочей нагрузке, поду и его контейнерам. Объекты кластера автоматически попадают в ресурсно-сервисную модель (начиная с версии 201)
Кластеры	Производительность и проблемы кластеров в разрезе нод, подов, деплойментов, демонсетов
Неймспейсы	Ключевые метрики и проблемы в разрезе подов, деплойментов, демонсетов, сервисов

4.7.3. Базы данных

Дашборды СУБД доступны в категории **«Базы данных»** каталога `Инфраструктура`. Показатели баз данных, полученные безагентным способом, вынесены в подраздел `Приложения` → `Виртуальные базы данных` (см. п. 4.2.3А).

4.7.4. Сеть

Показатели сетевого оборудования и результаты сетевых проверок (HTTP, DNS, TCP, TLS, SSH, NTP) доступны в категориях **«Сетевые устройства»** и **«Проверки доступности»** каталога `Инфраструктура`. Доступность и время отклика внешних HTTP-сервисов, к которым обращаются приложения, отображаются в подразделе `Приложения` → `Внешние сервисы`.

4.8. Оповещения (алертинг)

Раздел: `Инциденты и Алерты`

> **Изменение в версии 202.** Ранее самостоятельные разделы «Алерты» и «Инциденты» объединены в один раздел бокового меню — **«Инциденты и Алерты»**. Он содержит подразделы: Инциденты, Активные Алерты, История Алертов, Правила, Каналы оповещения, Политики оповещения, SLO, Окна обслуживания, Настройки Инцидентов.

4.8.1. Модель оповещений

Оповещения строятся на трёх связанных сущностях:

Сущность	Назначение
Правило алертинга	Условие на языке PromQL/MetricsQL, при выполнении которого генерируется алерт
Политика оповещений	Маршрутизация: какие алерты (по лейблам) в какой канал направлять
Канал оповещения	Адрес доставки: email, Telegram, Webhook

Порядок работы связки: правило срабатывает → политика сопоставляет лейблы алерта со своими условиями (матчерами) и выбирает канал → канал доставляет уведомление.

4.8.2. Просмотр активных алертов

`Инциденты и Алерты` → `Активные Алерты` — стена алертов в состоянии `firing`, обновляемая автоматически. Карточки сгруппированы по критичности (`CRITICAL`, `WARNING`) и по правилу/категории; счётчик вверху показывает общее число активных алертов.

На карточке отображаются сервис, описание алерта, длительность и (при наличии соответствующей аннотации) ссылка на дашборд источника проблемы.

Доступные действия:

- **Подтверждение (acknowledge)** — отметка о том, что алерт принят в работу;
- **Заглушение (silence)** — временное подавление уведомлений по алертам, подходящим под заданные лейблы, на указанный срок. Применяется, когда команда уже занимается проблемой и повторные уведомления не требуются.

4.8.3. История алертов

`Инциденты и Алерты` → `История Алертов` — журнал сработавших алертов за выбранный период.

График **«Активные алерты»** показывает динамику числа алертов по уровням критичности. Таблица **«История»** содержит столбцы:

Столбец	Значение
Сост.	Состояние алерта (активен / разрешён)
Критичность	`CRITICAL` или `WARNING`
Описание	Текст из описания правила
Где	Сервис или объект, к которому относится алерт
Начало / Конец	Время начала и завершения срабатывания
Длит-ть (мин)	Продолжительность срабатывания
Контекст	Переход к связанному дашборду или объекту

Вкладки **Обзор**, **Анализ** и **MTTR** предоставляют сводную аналитику, включая среднее время устранения. Результаты можно выгрузить кнопкой **«Экспорт»**.

4.8.4. События

`Инциденты и Алерты` → `История Алертов` → вкладка `События` — лента событий инфраструктуры и приложений: события Kubernetes (`Unhealthy`, `FailedMount` и др.), маркеры релизов из CI/CD, изменения конфигурации.

Диаграммы «События по типу» и «События по источнику» показывают распределение; таблица содержит столбцы: Сообщение, Время, Тип, Хост, Источник, Контекст.

События используются для сопоставления отклонений с изменениями — например, чтобы установить, что всплеск ошибок совпал с релизом.

4.8.5. Каналы оповещений

`Инциденты и Алерты` → `Каналы оповещения`. Поддерживаются три типа каналов.

Общие поля:

Поле	Обяз.	Описание
Название	Да	Уникальное описательное имя (до 64 символов); допускаются латинские

Поле	Обяз.	Описание
		и кириллические буквы, цифры, дефис, подчёркивание, пробелы
Тип	Да	`Электронная почта`, `Telegram` или `Webhook`. При смене типа специфичные поля очищаются
Комментарий	Нет	Произвольная заметка до 500 символов
Отправлять завершённые?	Нет	Направлять ли уведомления о разрешившихся алертах
Отключить проверку SSL	Нет	Включайте только при использовании самоподписанного сертификата

Поля канала «Электронная почта»:

Поле	Обяз.	Описание
Кому	Да	Email получателя
От кого	Да	Адрес отправителя
SMTP сервер	Да	В формате `хост:порт`, например `smtp.example.com:587`
Имя пользователя SMTP	Нет	Учётная запись для аутентификации
Пароль SMTP	Нет	Хранится в зашифрованном виде
hello имя хоста	Нет	По умолчанию `localhost`
Требовать TLS	Нет	Требовать TLS для SMTP-соединения

Поля канала «Telegram»:

Поле	Обяз.	Описание
Telegram ID	Да	Идентификатор чата (`chat_id`), целое число, может быть отрицательным
Токен бота	Да	Хранится в зашифрованном виде
API URL	Нет	По умолчанию `https://api.telegram.org`
ID ветки сообщений	Нет	Идентификатор topic для форумных групп

Поля канала «Webhook»:

Поле	Обяз.	Описание
Webhook URL	Да	Адрес приёма HTTP POST; должен начинаться с `http://` или `https://`
Максимум алертов	Нет	Максимальное число алертов в одном сообщении
Таймаут	Нет	Максимальное время ожидания ответа приёмника

Проверка настроек канала электронной почты. Начиная с версии 202 в форме канала доступна кнопка **«Отправить тестовое письмо»** — параметры почтового сервера проверяются сразу при настройке, а не в момент первой реальной тревоги.

Что следует учитывать:

- тестовое письмо проверяет **только транспорт SMTP**; чтобы оповещения действительно доходили, канал должен быть привязан к политике, а политика — применена;
- при ошибке сообщение указывает этап сбоя — соединение с сервером, TLS, аутентификация или отправка;
- если параметр **«Требовать TLS»** выключен, выводится предупреждение: соединение не шифруется, и при аутентификации `LOGIN` пароль SMTP будет передан открытым текстом. Включите TLS, если сервер это поддерживает;

- проверка ограничена по частоте: при слишком частых нажатиях интерфейс предложит повторить через несколько секунд.

> **Ограничения.** Тип существующего канала изменить нельзя — создайте новый канал. Канал нельзя удалить, пока он используется хотя бы в одной политике: сначала отвяжите его от политик. При редактировании секретные значения (пароли, токены) не отображаются: оставьте поле пустым, чтобы сохранить прежнее значение.

4.8.6. Политики оповещений

`Инциденты и Алерты` → `Политики оповещения`. Политики проверяются по возрастанию значения поля «Порядок».

Поле	Обяз.	Описание
Лейблы группировки	Да	Лейблы, по которым алерты объединяются в одно сообщение (например, `alertname`, `service`). Для отключения группировки используется значение `...`
Каналы оповещения	Да	Канал доставки (должен быть создан заранее)
Матчеры	Да (≥1)	Условия сопоставления лейблов алерта
Продолжение	Нет	`Выкл.` — обработка алерта прекращается на первой совпавшей политике; `Вкл.` — алерт обрабатывается и последующими политиками
Порядок	Да	Приоритет проверки, от 1 до 100
Комментарий	Нет	Описание политики или ссылка на регламент (до 500 символов)

Матчер состоит из трёх частей: **ключ** (имя лейбла), **оператор** (`=` равно, `!=` не равно, `=~` соответствует регулярному выражению, `!~` не соответствует), **значение**. Несколько матчеров в одной политике объединяются по «И».

Примеры матчеров:

Цель	Матчер
Любой алерт (политика-перехватчик)	`alertname =~ .*`
Алерты определённого семейства	`alertname =~ Аномалия.*`
Только сервисные (APM) алерты	`type = apm`
Алерты конкретного сервиса	`service = payment-service`
Только критичные	`severity = CRITICAL`
Только инфраструктурные	`type = infra`
Конкретная технология	`technology = postgres`
Всё, кроме предупреждений	`severity != WARNING`

Политику-«перехватчик» (`alertname =~ .*`) размещайте последней (наибольшее значение поля «Порядок»), чтобы она обрабатывала алерты, не подошедшие под более специфичные политики.

Типовые лейблы встроенных правил, пригодные для построения матчеров:

Лейбл	Типовые значения
`alertname`	Имя сработавшего правила
`severity`	`CRITICAL`, `WARNING`
`type`	`apm`, `infra`, `licensing`
`component_type`	`service`, `endpoint`, `application`, `db`, `host`, `k8s`, `container`,

Лейбл	Типовые значения
	`queue`, `web_server`, `virtualization`
`technology`	`postgres`, `mysql`, `mongodb`, `redis`, `kafka`, `nginx`, `elasticsearch`, `vsphere`, `k8s_node`, `k8s_pod` и др.
`rule_type`	`SLA`, `APDEX`, `anomaly_calls`, `anomaly_resptime`, `anomaly_errors`, `cpu`, `ram` и др.
`service`, `service_id`, `service_group`	Из метрики
`endpoint`, `opName`	Из метрики

> Матчеры сопоставляются именно с **лейблами**; аннотации (`summary`, `dashboard`) для маршрутизации не используются.

4.8.7. Правила алертинга

`Инциденты и Алерты` → `Правила`. Доступны фильтры по типу (встроенные / пользовательские), группе и статусу, а также поиск по названию.

Встроенные правила поставляются «из коробки», периодически обновляются вендором, не подлежат редактированию и удалению, но могут быть **отключены** или **скопированы** для последующего изменения копии.

Поля формы создания правила:

Поле	Обяз.	Описание
Название	Да	Краткое описание сути правила (до 64 символов)
Группа	Да	Логическая группа правил. **Только латинские буквы, цифры и подчёркивание**; без пробелов и кириллицы
Критичность	Да	`CRITICAL` или `WARNING`; сохраняется как лейбл `severity`
Описание	Да	Понятное описание (до 200 символов); сохраняется как аннотация `summary`, попадает в текст уведомления
Выражение	Да	Условие на PromQL/MetricsQL (до 10 000 символов) с подсветкой синтаксиса
`for`	Нет	Длительность непрерывного выполнения условия до перехода алерта в `firing` (`30s`, `5m`, `1h`, `1d`, `1w`). До её истечения алерт находится в статусе `pending`
`keep_firing_for`	Нет	Длительность удержания статуса `firing` после прекращения выполнения условия
Лейблы	Нет	Дополнительные пары «ключ — значение» для группировки и маршрутизации
Аннотации	Нет	Метаданные алерта; зарезервированные ключи `dashboard`, `dashboardHost`, `dashboardContainer` формируют ссылки на дашборды
`debug`	Нет	Вывод отладочной информации в логи
Статус	—	`включено` / `отключено`. Новое правило создаётся **отключённым**

> **Зарезервированные ключи.** Лейбл `severity` задаётся полем «Критичность», аннотация `summary` — полем «Описание». Не задавайте их вручную в блоках «Лейблы» / «Аннотации».

Предпросмотр выражения. В форме правила нажмите **«Показать график»** и выберите интервал — Система построит график по текущему выражению, что позволяет проверить корректность условия до включения правила.

Действия над правилами:

Действие	Применимо к
Просмотр	Все правила
Редактирование	Пользовательские
Создать копию	Все правила (основной способ кастомизации встроенного правила)
Отключить / Включить	Все правила
Удалить	Только пользовательские

> **Важно.** После любого изменения правил или политик нажмите **«Применить»**. Без этого изменения не активируются. Новые настройки вступают в силу в течение примерно одной минуты.

4.8.8. Автоматическое выявление аномалий

Система средствами машинного обучения автоматически строит базовую линию (ожидаемый диапазон) для ключевых показателей каждого сервиса и ключевой транзакции с учётом суточной и недельной сезонности. Ручная настройка порогов не требуется.

При выходе значения за верхнюю границу базовой линии срабатывают встроенные правила группы `ANOMALY`. Такие алерты полезны для выявления отклонений, не описываемых фиксированным порогом (например, аномального падения числа операций в рабочие часы).

4.8.8A. Оповещения о пропадании данных (No-Data)

Начиная с версии 202 доступно семейство встроенных правил группы **`NO_DATA`** — оповещение о том, что ранее наблюдавшийся источник перестал присылать метрики.

Зачем это нужно. Обычные пороговые правила проверяют условие, пока данные поступают. Если экспортёр, агент или сама цель выходят из строя, метрика перестаёт поступать, ряд исчезает — и все пороговые правила по этому источнику молча замолкают вместе с ним. Источник фактически перестаёт наблюдаться, но ни одно правило об этом не сообщает: проблему замечают позже, по пустому графику.

Правила группы `NO_DATA` срабатывают, когда источник, присылавший метрики в течение последних суток, перестаёт их присылать (данные не поступают дольше нескольких минут). Правила настраиваются так же, как обычные правила алертинга (см. п. 4.8.7), и отображаются в общем списке в отдельной группе.

> **Учёт регламентных работ.** Плановые работы, оформленные окном обслуживания (см. п. 4.9A) на соответствующий хост или сервис, не поднимают оповещений о пропадании данных: остановленный на время работ источник — ожидаемое молчание, а не сбой.

4.8.9. Правила алертинга по SLO

При создании SLO Система автоматически формирует набор правил по скорости расходования бюджета ошибок:

- **быстрое сжигание** (fast burn, 14.4× / 1 ч) — внезапная деградация, при которой бюджет будет исчерпан за несколько часов;
- **медленное сжигание** (slow burn, 6× / 6 ч) — устойчивое, но менее резкое превышение допустимого уровня ошибок;
- **контроль объёма** (volume guard) — подавление ложных срабатываний при резком падении трафика;
- **исчерпание бюджета** — фиксация факта нарушения SLO.

Эти правила отображаются в общем списке, но **не редактируются напрямую** — для изменения условий измените параметры соответствующего SLO.

4.8.10. Надёжность изменений

Подраздел: `Инциденты и Алерты` → `Надёжность изменений`. Доступен начиная с версии 203.

Подраздел показывает, сколько изменений выкатывается и какая их часть заканчивается инцидентом, — это показатели класса **DORA**, характеризующие надёжность процесса поставки изменений.

Подраздел состоит из двух вкладок:

Вкладка	Содержание
Сводная аналитика надёжности	Обобщённые показатели за выбранный период
Журнал изменений	Перечень выкаченных изменений с их результатом

Показатели считаются по маркерам релизов и развёртываний (см. п. 4.8.4) и по инцидентам платформы (см. п. 4.9). **Дополнительной настройки не требуется** — при условии, что маркеры изменений передаются в платформу из конвейера CI/CD и модуль инцидентов работает.

> **Условие достоверности.** Если маркеры релизов и развёртываний в платформу не передаются, показатели надёжности изменений будут неполными: платформа не сможет соотнести инциденты с изменениями. Порядок передачи маркеров из конвейера CI/CD уточните у администратора платформы.

4.9. Инциденты

Раздел: `Инциденты`. Доступен начиная с версии 201.

4.9.1. Назначение

При отказе одного компонента, как правило, срабатывает не один алерт, а серия связанных: отказ пода влечёт ошибки зависимых сервисов, нарушение SLO, рост задержек. Модуль «Инциденты» автоматически коррелирует связанные алерты и объединяет их в одну сущность, снижая шум и ускоряя реагирование.

4.9.2. Атрибуты инцидента

Атрибут	Описание
Критичность	Наивысшая критичность среди входящих алертов: `Критический`, `Высокий`, `Средний`, `Низкий`
Этап	Текущая фаза жизненного цикла
Охват	Количество связанных алертов и затронутых ресурсов
Влияние	Оценка масштаба с числом затронутых ресурсов
Ответственный	Пользователь, назначенный на работу с инцидентом
Возраст	Время с момента создания и время последнего обновления

4.9.3. Список инцидентов

`Инциденты` → `Список инцидентов` показывает активные и недавние инциденты по доступным пользователю сервисам; список обновляется автоматически.

Панель фильтров позволяет отбирать инциденты по этапу, критичности, ответственному и сервису, а также выполнять полнотекстовый поиск по названию и сводке. Переключатель **«Только мои инциденты»** оставляет инциденты, назначенные текущему пользователю. Счётчик активных фильтров и кнопка **«Сбросить фильтры»** расположены над таблицей. Размер страницы выбирается внизу (10 / 20 / 50 / 100).

4.9.4. Карточка инцидента

Карточка состоит из трёх зон:

- **степпер этапов** вверху — текущая фаза и переход между этапами;
- **панель AIOPS** в центре — вкладки `Причина проблемы`, `Сводка`, `Расследование`, а также таймлайн и хронология;
- **правая колонка** — ответственный, затронутые ресурсы, связанные алерты.

В шапке отображаются критичность, влияние, возраст, время создания и последнего обновления, заголовок (доступен для переименования) и кнопка **«Объединить с…»**.

4.9.5. Этапы жизненного цикла (ITIL)

1. **Обнаружен** — инцидент создан корреляцией алертов.
2. **Диагностика** — выполняется поиск причины.
3. **Устранение** — причина найдена, выполняются восстановительные действия.
4. **Закрыт** — проблема решена.

Переход между этапами выполняется вручную; часть переходов (например, автоматическое закрытие после разрешения всех входящих алертов) Система выполняет самостоятельно. Названия и порядок этапов настраиваются администратором.

4.9.6. ИИ-сводка и ИИ-расследование

Вкладка «Сводка» содержит автоматически сгенерированное описание инцидента: что произошло, когда, какие сервисы затронуты, как развивалась ситуация. Рядом с заголовком отображается время последнего обновления; при последующем изменении инцидента появляется отметка `Устарело`. Кнопка **«Обобщить»** запускает повторную генерацию.

Вкладка «Расследование» запускает анализ первопричины: в отличие от сводки, описывающей *что* произошло, расследование отвечает на вопрос *почему*. Результат содержит уровень уверенности, цепочку первопричины, перечень затронутых сервисов и рекомендации.

> **Условие доступности.** ИИ-функции работают только при подключённой администратором внешней языковой модели. Если подключение не выполнено, кнопки «Суммаризировать», «Расследовать» и «Постмортем» недоступны.
>
> **Рекомендация по применению.** Результат работы языковой модели носит рекомендательный характер и подлежит проверке специалистом. Не используйте ИИ-выводы как единственное основание для действий, влияющих на промышленную эксплуатацию.

4.9.7. Прочие возможности

- **Затронутые ресурсы, связанные алерты и граф распространения** — визуализация охвата инцидента и путей его распространения по зависимостям.
- **Таймлайн и хронология** — последовательность событий инцидента.
- **Объединение инцидентов** — слияние сущностей, относящихся к одной проблеме.
- **Назначение ответственного** — закрепление инцидента за пользователем.

- **Черновик постмортема** — автоматически формируемая заготовка отчёта о разборе инцидента.

4.9A. Окна обслуживания

Раздел: `Инциденты и Алерты` → `Окна обслуживания`. Доступен начиная с версии 202.

4.9A.1. Назначение

Плановые работы — перезапуск сервиса, обновление базы данных, миграция стенда, работы на площадке — выглядят для системы мониторинга так же, как авария: показатели проседают, источники замолкают, правила алертинга срабатывают. Дежурная смена получает поток оповещений о событии, о котором и так знала заранее.

Окно обслуживания — заранее объявленный период работ по конкретным объектам. Пока окно активно, срабатывания по этим объектам не поднимают инциденты и не рассылаются по каналам оповещения, но остаются в истории алертов с пометкой **«Обслуживание»** — данные для последующего разбора и аудита не теряются.

4.9A.2. Список окон

Таблица со всеми окнами; доступны поиск по названию и фильтр по статусу.

Колонка	Описание
Название	Название окна
Область действия	Сводка объектов, попадающих в окно; при большом их числе — «+N ещё»
Расписание	«Однократно» с датами начала и окончания либо «Регулярно» с днями недели, временем, длительностью и часовым поясом
Статус	«Активно», «Запланировано», «Завершено» или «Отменено»
Следующий запуск	Ближайшее срабатывание — для регулярных окон

4.9A.3. Создание окна

Нажмите **«Создать окно»** и заполните форму.

Поле	Обяз.	Описание
Название	Да	Отображается в списке, в пометке подавленного алерта и на графиках
Описание	Нет	Здесь удобно указать номер заявки на изменение и ответственного
Область действия	Да	Объекты, попадающие под подавление (см. п. 4.9A.4)
Расписание	Да	Режим и период действия окна (см. п. 4.9A.5)

4.9A.4. Область действия

Тип области	Описание
Хосты	Выбор из обнаруженных хостов
Сервисы	Выбор из известных платформе сервисов
Группы сервисов	Бизнес-приложения; под окно попадают все входящие в группу сервисы
Расширенный (метки)	Условия по меткам алерта: метка, оператор и значение — для нестандартных срезов (окружение, кластер, экземпляр)

Правила комбинирования:

- несколько хостов или сервисов **в одной области** — «любой из перечисленных»;
- условия по меткам **внутри одной области** объединяются по «И»;
- разные области объединяются по «ИЛИ».

4.9А.5. Расписание

Режим	Назначение и параметры
Сейчас	Окно начинается немедленно — для незапланированных работ, о которых стало известно в момент начала
Однократно	Разовые работы: начало (дата и время) и длительность в часах; время окончания отображается под полем. Доступны кнопки-предустановки типовой длительности
Регулярно	Повторяющиеся работы: дни недели (с предустановками «Будни», «Выходные», «Все дни»), время начала, длительность в минутах, часовой пояс и необязательное поле «Повторять до» — дата окончания серии. Без него серия бессрочна

> **Часовой пояс.** Расписание регулярного окна считается в выбранном часовом поясе, а не в поясе браузера и не в UTC. Для распределённых площадок это принципиально: окно «02:00 будни» должно означать ночь на площадке, а не в другом регионе.

4.9А.6. Предпросмотр охвата

До сохранения формы под областью действия отображается строка вида: «Под окно попадёт 14 алертов (3 активных) из 250 за 24 ч». Это оценка по фактическим срабатываниям за последние сутки — сколько алертов заглушило бы такое окно. Список можно раскрыть и просмотреть конкретные алерты и их состояние.

Предпросмотр закрывает основной риск неверно заданной области: слишком широкая область заглушит лишнее, слишком узкая не заглушит ничего. **Если строка сообщает, что совпадений не найдено, область почти наверняка задана неверно.**

4.9А.7. Что происходит во время окна

Пока окно активно, для попавших в область объектов:

- срабатывания **не создают инциденты**;
- оповещения **не отправляются** ни по одному каналу (электронная почта, Telegram, Webhook и др.);
- срабатывания **записываются в историю алертов** с пометкой «Обслуживание»; в карточке алерта видно, каким именно окном вызвано подавление;
- правила обнаружения пропадания данных (No-Data, см. п. 4.8.8А) не поднимают оповещений.

Объекты вне области действия окна обрабатываются как обычно — окно на одном сервисе не заглушает остальную инсталляцию.

4.9А.8. Окна на графиках

Активные и запланированные окна отображаются полосой на графиках дашбордов вместе с отметками изменений — релизами и развёртываниями. Регулярные окна показываются на весь период повторений в пределах видимого интервала времени.

Это снимает типовой вопрос при разборе: «провал на графике — это авария или плановые работы?» — ответ виден на самом графике, без перехода в другой раздел.

4.9А.9. Отмена и удаление окна

Действие	Результат
Отменить окно	Прекращает текущее или ближайшее срабатывание. Окно сохраняется в списке со статусом «Отменено»; для регулярного окна серия повторений продолжается со следующего срабатывания
Удалить	Удаляет окно целиком. Если окно было активно, подавление прекращается немедленно

> **Рекомендация.** Отмену следует предпочитать удалению: она сохраняет след того, что работы планировались.

4.9А.10. Права доступа и аудит

Раздел управляется ресурсом ролевой модели **«Окна обслуживания»** (`maintenance_window`). Пользователи без права просмотра раздел не видят. Создание, изменение, отмена и удаление окон фиксируются в журнале аудита с состоянием «до» и «после» — видно, кто и как менял область действия или расписание.

4.10. Управление SLO

Раздел: `SLO`

4.10.1. Ключевые понятия

- **SLI** — показатель качества обслуживания (доля успешных запросов, доля быстрых запросов).
- **SLO** — целевое значение SLI за период (например, 99,5 % успешных запросов за 30 дней).
- **Бюджет ошибок** — допустимый объём нарушений: при цели 99,5 % бюджет составляет 0,5 % запросов.
- **Скорость сжигания (burn rate)** — темп расходования бюджета относительно равномерного.

4.10.2. Порядок работы

1. Откройте раздел `SLO` — отображается список определённых SLO с текущим состоянием, остатком бюджета ошибок и трендом.
2. Для создания нажмите кнопку добавления и задайте параметры SLO: контролируемый объект (сервис, эндпоинт), тип показателя, целевое значение, период, метки и владельца.
3. Сохраните SLO. Система автоматически сформирует связанные правила алертинга (см. п. 4.8.9).
4. Для анализа откройте детали SLO: динамика SLI, расход бюджета ошибок, история нарушений.
5. Для отчётности используйте **отчёт о соответствии SLO** за выбранный период.

4.10.3. Права доступа

Операции с SLO ограничиваются правами роли; возможна выдача прав на редактирование только выделенных SLO (например, SLO конкретной команды).

4.11. Ресурсно-сервисная модель (PCM)

Раздел: `PCM`. Доступен начиная с версии 200.

4.11.1. Назначение

PCM представляет единый реестр ИТ-ресурсов (серверы, сервисы, базы данных, иные элементы инфраструктуры) и их взаимосвязей, а также визуализирует граф зависимостей. Модель используется для оценки влияния отказа одного компонента на связанные с ним бизнес-сервисы.

4.11.2. Работа с ресурсами

- **Список ресурсов** — реестр с поиском и фильтрацией по типу, CI-классу, статусу.
- **Создание ресурса** — ручное добавление ресурса с указанием типа, атрибутов и взаимосвязей.
- **Детали ресурса** — карточка со свойствами, связями и связанными данными мониторинга.
- **Редактирование ресурса** — изменение атрибутов и связей.

4.11.3. Автоматическое обнаружение ресурсов

Система автоматически обнаруживает ресурсы по данным мониторинга. Обнаруженный ресурс проходит жизненный цикл **Provisional → Confirmed**: первоначально он получает статус предварительного (`Provisional`) и подлежит подтверждению ответственным лицом, после чего переходит в статус подтверждённого (`Confirmed`).

4.11.4. Настройка справочников

Подраздел настройки позволяет управлять справочниками: типами ресурсов, типами взаимосвязей, CI-классами и CI-подклассами. Операции доступны при наличии соответствующих прав.

4.12. Кастомные дашборды

Раздел: `Дашборды и отчёты` → вкладка `Дашборды`

4.12.1. Создание дашборда

1. Откройте раздел `Дашборды и отчёты`.
2. Нажмите **«+ Дашборд»**.
3. Введите название и нажмите **«Создать»** — откроется конструктор с пустой рабочей областью.
4. Добавьте и настройте виджеты.
5. Нажмите **«Сохранить»** в правом верхнем углу. Для отмены создания используйте кнопку с красным крестиком рядом с кнопкой сохранения.

4.12.2. Типы виджетов

Тип	Описание
Текст	Произвольный текст с базовым форматированием и ссылками. Применяется для пояснений, регламентов, ссылок на инструкции
График	Визуализация данных; поддерживает несколько источников данных и типов визуализации

Виджеты перемещаются и масштабируются в пределах рабочей области; количество виджетов на дашборде не ограничено. Настройка виджета выполняется через меню с тремя точками → **«Изменить»**.

4.12.3. Источники данных виджета-графика

Источник	Назначение и особенности
OLAP Мастер	Управляемый режим построения графиков по APM- и EUM-метрикам: выбор метрики из курируемого каталога, выбор сервиса и эндпоинта; запрос формируется автоматически. Рекомендуется как основной
PromQL	Произвольные запросы к метрикам Prometheus. На один виджет можно добавить до 5 запросов кнопкой **«+ Запрос»**; результаты отображаются на одном графике
LogsQL	Визуализация данных логов. Режим **Hits** — динамика количества записей, соответствующих запросу; режим **Stats** — результаты агрегатных запросов с пайпом `stats`. Доступен с версии 200
OLAP экспертный режим	Полный доступ к OLAP-движку (measures, dimensions, filters, timeDimensions) и расширенный набор визуализаций: поток бизнес-процесса (BusinessFlow), геокарта (GeoMap), граф связей (DirectedGraph), горизонтальная столбчатая диаграмма, составная карточка
Базовый режим	Устаревший источник на базе GraphQL API. Сохранён для обратной совместимости; для новых виджетов не рекомендуется

Инциденты как источник данных. Начиная с версии 202 данные модуля «Инциденты» доступны в OLAP-режимах наравне с APM- и EUM-метриками. Это позволяет собрать дашборд надёжности штатным конструктором и показывать его руководству или смежным командам, не предоставляя доступ к самому модулю инцидентов.

Показатели: всего инцидентов; открытые, решённые и закрытые; разбивка по критичности (критичные, серьёзные, незначительные, низкий приоритет); открытые критичные и открытые серьёзные; MTTR (минуты); средняя и максимальная длительность; затронуто ресурсов; связано алертов; сводный статус здоровья.

Разрезы: критичность, статус (детектирование, диагностика, решение, закрытие), влияние, причина корреляции, ответственный, заголовок и описание, длительность, число затронутых ресурсов и связанных алертов, время создания, решения и закрытия. Временная ось строится по времени создания инцидента.

Примеры виджетов: «MTTR по неделям» (линейная диаграмма), «Инциденты по критичности» (круговая), «Открытые критичные» (KPI-карточка), «Инциденты с наибольшей длительностью» (таблица).

Пример запроса PromQL:

```
round(avg(system_cpu_system{host=~".*central1.internal"}) by (host), 0.1)
```

Пример запроса LogsQL (режим Hits):

```
service:exact("payment-service") AND level:exact("error")
```

4.12.3A. Виджет «Соты здоровья»

Начиная с версии 202 доступен виджет **«Соты здоровья»** (Honeycomb) — плотная раскладка из шестиугольников: одна ячейка соответствует одному объекту (сервису, хосту, поду, устройству), цвет ячейки — его текущему состоянию. Сотни объектов помещаются на один экран, проблемные видны сразу, без прокрутки таблицы.

Виджет доступен на источниках данных **PromQL**, **OLAP Мастер** и **OLAP экспертный режим** и используется на встроенных дашбордах платформы, включая переработанный дашборд «Обзор».

Цветовая карта (состояние берётся из числового значения запроса):

Значение	Состояние	Цвет
`0`	Нет проблем	зелёный
`1`	Предупреждение	жёлтый
`2`	Критический	красный
иное или отсутствует	Неизвестно	серый

Настройки виджета: заголовок и подзаголовок; лейбл группировки (для PromQL — имя метки, по которой ячейки раскладываются на отдельные карточки, например `service_group`; пусто — единая плоская раскладка); включение перехода по клику на ячейку к дашборду соответствующей сущности. Для источников «OLAP Мастер» и «OLAP экспертный режим» группировка задаётся вторым измерением запроса.

Над каждой группой выводится полоса распределения состояний и счётчик объектов. Наведение на ячейку показывает имя объекта, состояние и дополнительные поля запроса. На очень крупных инсталляциях число ячеек ограничено 2000: сначала отображаются проблемные объекты, а над сотами выводится пометка «Показано N из M».

Порядок добавления: добавьте виджет типа «График» → выберите источник данных → выберите тип визуализации «Соты здоровья» → введите запрос, возвращающий состояние `0/1/2` в разрезе объектов → при необходимости укажите лейбл группировки → сохраните дашборд.

4.12.3Б. Виджет «KPI-карточка»

Начиная с версии 202 доступен виджет **«KPI-карточка»** (Scorecard) — значение показателя со статусом по заданным порогам и полосой распределения «хорошо / требует улучшения / плохо». Применяется для вывода отдельных ключевых показателей, в том числе Web Vitals.

4.12.4. Вкладки и переменные дашборда

- **Вкладки** позволяют разделить дашборд на тематические страницы (например, «Обзор», «Ошибки», «Инфраструктура»).
- **Переменные (фильтры)** — параметры, значения которых подставляются в запросы виджетов. Позволяют одним элементом управления переключать весь дашборд между сервисами, окружениями или хостами.

4.12.5. Операции с дашбордами

Доступны переименование, копирование, удаление, а также экспорт и импорт определения дашборда (см. п. 4.14).

4.12.6. Рекомендации по построению дашбордов

- Размещайте на верхнем уровне 4–8 показателей, отвечающих на вопрос «всё ли в порядке»; детализацию выносите на отдельные вкладки.
- Для каждого виджета указывайте единицы измерения в названии.
- Используйте текстовые виджеты для ссылок на регламенты реагирования — это сокращает время реакции дежурной смены.
- Ограничивайте период по умолчанию: дашборды с большим числом PromQL-виджетов на длинных интервалах создают заметную нагрузку.

4.13. Отчёты по электронной почте

Раздел: `Дашборды и отчёты` → вкладка `Отчёты`. Доступен начиная с версии 202.

4.13.1. Назначение

Отчёты — механизм регулярной рассылки состояния системы тем, кто не работает в интерфейсе платформы ежедневно: руководителям, владельцам сервисов, смежным командам, заказчику по договору обслуживания.

Отчёт собирается из **существующего дашборда**: платформа отрисовывает дашборд за завершившийся отчётный период, сохраняет его в **PDF** и отправляет письмом списку получателей. Отдельный конструктор отчётов не требуется — если дашборд уже настроен, его можно поставить на рассылку.

Вкладка отображается пользователям с правом администратора на ресурс `reports`.

4.13.2. Список отчётов

Колонка	Описание
Имя	Название отчёта; используется в теме письма по умолчанию и в имени файла вложения
Дашборд	Дашборд-источник. Если дашборд удалён, отображается «Дашборд недоступен»
Расписание	Сводка вида «Ежедневно в 09:00», «Еженедельно, Пн в 09:00», «Ежемесячно, 1-го в 09:00»
Получатели	Адреса, на которые направляется письмо
Вкл.	Переключатель. Выключенный отчёт сохраняется, но не отправляется по расписанию
Последний запуск	Время и результат последней отправки

Действия по строке: **«Отправить сейчас»**, **«История»**, **«Изменить»**, **«Удалить»**.

4.13.3. Создание отчёта

Нажмите **«Создать отчёт»** и заполните форму.

Поле	Обяз.	Описание
Имя	Да	Отображается в списке и в теме письма по умолчанию
Дашборд	Да	Выбор из пользовательских дашбордов, доступен поиск по имени
Периодичность	Да	«Ежедневно», «Еженедельно» или «Ежемесячно»
Время отправки	Да	Время суток в выбранном часовом поясе
День недели	Условно	Только для еженедельной периодичности
День месяца	Условно	Только для ежемесячной периодичности, значения 1–28
Часовой пояс	Да	Расписание считается в нём, а не в UTC и не в поясе браузера
Получатели	Да	Один или несколько адресов; адрес вводится и подтверждается клавишей `Enter`
Тема письма	Нет	По умолчанию — `Отчёт ProtoOBP: <имя отчёта> за <период>`
Переменные дашборда	Нет	JSON-объект со значениями переменных дашборда (см. п. 4.13.5)

> **День месяца.** Диапазон ограничен значениями 1–28, чтобы ежемесячный отчёт направлялся в одну и ту же дату в любом месяце, включая февраль.

4.13.4. Отчётный период

Отдельно задавать период не требуется — он определяется периодичностью и всегда охватывает **завершившийся** интервал, а не текущий.

Периодичность	Период отчёта
Ежедневно	Предыдущие календарные сутки (00:00–24:00)
Еженедельно	Предыдущая календарная неделя, с понедельника по воскресенье
Ежемесячно	Предыдущий календарный месяц

Границы периода считаются в часовом поясе отчёта. Период печатается в теле письма и в нижнем колонтитуле PDF-документа, поэтому у получателя не остаётся сомнений, за какой интервал собраны данные.

4.13.5. Переменные дашборда

Если дашборд использует переменные (см. п. 4.12.4), их значения задаются в поле **«Переменные дашборда»** JSON-объектом:

```
{"serviceId": "cGF5bWVudC1zZXJ2aWNl"}
```

> **Важно.** Для дашбордов уровня сервиса и любых других, где виджеты опираются на переменную, переменные **обязательны** — без них отчёт придёт пустым.

4.13.6. Отправка вручную и история запусков

Действие **«Отправить сейчас»** ставит внеочередной запуск в очередь; расписание при этом не меняется. Используйте его, чтобы проверить вёрстку отчёта и доставку письма сразу после настройки, не дожидаясь планового времени.

Действие **«История»** открывает панель со всеми запусками отчёта.

Поле	Описание
Статус	«Выполняется», «Успех» или «Ошибка»
Запуск	«По расписанию» или «Вручную»
Запланирован	Плановое время запуска
Начат	Фактическое время начала
Задержка	Разница между плановым и фактическим временем
Длительность	Время сборки и отправки
Размер	Размер PDF-вложения

У неуспешных запусков доступна кнопка **«Показать ошибку»** с текстом сбоя и копированием в буфер обмена — это первое, что следует приложить к обращению в службу технической поддержки. Отдельно помечаются запуски **с предупреждениями**: письмо отправлено, но часть виджетов дашборда не отрисовалась (например, источник данных не ответил).

> **Повторные отправки.** Ошибки отрисовки повторяются один раз автоматически. Ошибки отправки письма **не повторяются** — иначе получатели рисковали бы получить дубликаты одного отчёта.

4.13.7. Типовые сценарии

Сценарий	Настройка
Еженедельная сводка для руководства	Дашборд с ключевыми показателями сервиса → отчёт «Еженедельно, Пн 09:00» → получатели: руководитель направления и владелец сервиса
Ежемесячный отчёт по договору обслуживания	Дашборд с SLO и доступностью → отчёт «Ежемесячно, 1-го» → получатели со стороны заказчика. PDF пригоден для приложения к акту
Ежедневный контроль критичного бизнес-процесса	Дашборд бизнес-процесса → ежедневный отчёт дежурной смене, чтобы утренняя проверка начиналась с фактов, а не с ручного обхода экранов

> **Условие работоспособности.** Отправку отчётов выполняет отдельный сервис платформы с собственными параметрами почтового сервера — они не берутся из настроек канала оповещения по электронной почте. Параметры задаются администратором при установке. Если они не заданы, платформа работает штатно, но запуски отчётов завершаются с ошибкой, видимой в истории.

4.14. Экспорт данных и отчётность

Операция	Порядок выполнения	Результат
Экспорт дашборда в PDF	Меню действий дашборда → экспорт в PDF	Файл PDF со снимком дашборда за выбранный период
Сохранение изображения виджета в файл	Меню виджета → сохранить изображение	Файл PNG
Копирование изображения виджета	Меню виджета → сохранить изображение в буфер обмена	Изображение в буфере обмена
Выгрузка таблицы в Excel	Меню виджета → сохранить таблицу как Excel	Файл электронной таблицы
Просмотр данных виджета	Меню виджета → просмотр данных	Табличное представление данных, лежащих в основе графика
Экспорт определения дашборда	Меню действий дашборда → экспорт определения	Файл с описанием дашборда для переноса между установками
Импорт определения дашборда	Раздел «Дашборды» → импорт	Дашборд, восстановленный из файла определения
Экспорт истории алертов	`Инциденты и Алерты` → `История Алертов` → «Экспорт»	Файл с перечнем срабатываний за период
Выгрузка трейса	Просмотр трейса → «Экспорт трейса» → выбор формата	Файл OTLP/JSON, Zipkin v2 JSON или Jaeger JSON (начиная с версии 202)
Экспорт журнала аудита	`Роли и доступ` → `Журнал аудита` → экспорт	Файл CSV или JSON со всей выборкой по текущим фильтрам (начиная с версии 202)
Регулярная рассылка дашборда	`Дашборды и отчёты` → `Отчёты` (см. п. 4.13)	PDF-документ, направляемый получателям по расписанию
Экспорт результатов запроса метрик	Вкладка результатов в разделе «Метрики» → экспорт	Файл с результатами запроса

> **Внимание.** Выгружаемые файлы могут содержать сведения об архитектуре и состоянии информационных систем организации. Обращайтесь с ними в соответствии с внутренними требованиями к защите служебной информации и требованиями законодательства о защите информации.

4.15. Программный доступ к данным (API)

Система предоставляет программные интерфейсы для интеграции с внешними системами — BI-инструментами, системами отчётности, скриптами автоматизации.

4.15.1. Состав интерфейсов

Назначение	Тип интерфейса
Выгрузка данных телеметрии (OLAP)	REST (CubeJS API)
Запросы к метрикам	PromQL-совместимый HTTP API
Запросы к логам	HTTP API LogsQL
Загрузка внешних логов	REST/HTTP, мультиформатный (OTLP, Elasticsearch, JSON, Loki, DataDog)
Маркеры событий (аннотации)	Grafana-совместимый API `/api/annotations` (с версии 201)
Приём алертов от внешних систем	Alertmanager webhook
Управление правилами алертинга	REST с описанием OpenAPI/Swagger
Получение данных для UI	GraphQL

4.15.2. Аутентификация запросов

Начиная с версии 200 ролевая модель включена по умолчанию. Все запросы к `/cubejs-api/*` должны содержать действительный Bearer-токен, выданный сервисом аутентификации. Запрос без токена возвращает `401 TOKEN_MISSING`.

Порядок подключения внешнего клиента:

1. Обратитесь к администратору платформы с заявкой на создание **отдельной учётной записи для интеграции** с минимально необходимым набором прав (право просмотра на требуемые сервисы).
2. Получите access-токен:

```
ACCESS_TOKEN=$(curl -s -X POST \
  "https://<адрес_платформы>/realms/protoobp/protocol/openid-connect/token" \
  -H "Content-Type: application/x-www-form-urlencoded" \
  -d "grant_type=password" \
  -d "client_id=ui" \
  -d "username=$INTEGRATION_USER" \
  -d "password=$INTEGRATION_PASSWORD" \
  | jq -r '.access_token')
```

3. Выполните запрос к API, передав токен в заголовке:

```
curl -s -X POST "https://<адрес_платформы>/cubejs-api/v1/load" \
  -H "Authorization: Bearer $ACCESS_TOKEN" \
  -H "Content-Type: application/json" \
  -d '{
    "query": {
      "measures": ["Calls.count"],
      "dimensions": ["Calls.service"],
      "timeDimensions": [{"dimension": "Calls.date", "dateRange": "today"}]
    }
  }'
```

Сервисы, на которые у учётной записи нет прав, в результат не включаются.

4.15.3. Замечания по эксплуатации интеграций

- **Время жизни токена** — около 5 минут. Длительно работающие интеграции должны обновлять токен по `refresh_token` либо запрашивать новый перед каждым обращением.
- **Отдельная учётная запись на каждую интеграцию** — упрощает аудит и отзыв прав. Не используйте личные учётные записи сотрудников в интеграциях.
- **Хранение реквизитов** — пароли и токены интеграционных учётных записей размещайте в системе управления секретами организации, а не в тексте скриптов и не в системах контроля версий.
- **Миграция со старых версий** — скрипты, работавшие с OLAP API версии 199 без аутентификации, на версии 200 и выше получают `401 TOKEN_MISSING`; их необходимо перевести на схему с Bearer-токеном.

4.16. AI-аналитик

Раздел: `AI-аналитик`. Доступен начиная с версии 203.

Раздел представляет собой чат по данным платформы: вопросы о состоянии сервисов задаются на естественном языке, а ответы содержат ссылки на конкретные сущности консоли — сервисы, хосты, инциденты, — по которым можно сразу перейти к соответствующему разделу.

Порядок работы:

1. Откройте раздел `AI-аналитик`.
2. На старте предлагается набор готовых вопросов — выберите подходящий либо сформулируйте свой.
3. Изучите ответ и при необходимости перейдите по ссылкам на упомянутые в нём сущности.

> **Условие доступности.** Раздел работает только при подключённой администратором внешней языковой модели. Порядок подключения приведён в «Руководстве администратора», п. 4.3.
>
> **Рекомендация по применению.** Ответ языковой модели носит справочный характер и подлежит проверке по исходным данным платформы. Не используйте его как единственное основание для действий, влияющих на промышленную эксплуатацию. Те же ограничения распространяются на ИИ-функции модуля «Инциденты» (п. 4.9.6).

5. Аварийные ситуации

В настоящем разделе описаны действия пользователя при нарушении штатных условий эксплуатации. Действия, требующие доступа к серверной части, выполняются администратором платформы.

5.1. Классификация ситуаций и действия пользователя

№	Признак ситуации	Вероятная причина	Действия пользователя
1	Страница Системы не открывается, браузер сообщает о невозможности установить соединение	Недоступен сервер платформы или отсутствует сетевой доступ	Проверить сетевую доступность рабочего места; убедиться в корректности адреса; обратиться в службу технической поддержки
2	Ошибка аутентификации при вводе верных реквизитов	Учётная запись заблокирована, срок действия пароля истёк, недоступен провайдер SSO	Обратиться к администратору платформы
3	Раздел меню отсутствует, отображается панель «Доступ запрещён»	Недостаточно прав назначенной роли либо ограничена область видимости данных	Обратиться к администратору платформы с обоснованием необходимости доступа
4	Дашборд открывается, но данные отсутствуют или устарели	Прекращена передача данных от агента или трейсера; выбран период без данных; объект вне области видимости	Проверить корректность выбранного периода и фильтров; обновить страницу целиком; при сохранении признака — обратиться в техническую поддержку с указанием сервиса/хоста и интервала
5	Новый подключённый хост или сервис не отображается в списке	Список объектов не обновляется кнопкой «Обновить»	Обновить страницу браузера целиком (F5). Если объект не появился в течение 2–5 минут — обратиться к администратору
6	Уведомление об алерте не доставлено	Не нажата кнопка «Применить»; правило отключено; алерт в статусе `pending`; лейблы алерта не совпадают с матчерами политики; неверны реквизиты канала	Выполнить проверку по перечню п. 5.2
7	Запрос PromQL или LogsQL завершается с ошибкой или не возвращает данных	Ошибка синтаксиса; неверные имена метрик и лейблов; слишком широкий период	Выполнить проверку по п. 4.5.5; сузить период; сверить имена в браузере метрик
8	Страница отвечает медленно, браузер потребляет много памяти	Большое число виджетов и/или длительный период наблюдения	Сократить период; разнести виджеты по вкладкам; закрыть неиспользуемые вкладки браузера
9	Экспорт файла не выполняется	Блокировка загрузки файлов в браузере	Разрешить загрузку файлов с адреса Системы в настройках браузера
10	Кнопки ИИ-функций инцидента недоступны либо отсутствует раздел «AI-аналитик»	Не подключена внешняя языковая модель	Обратиться к администратору платформы
10д	В подразделе «Надёжность изменений» показатели пусты или явно занижены	В платформу не передаются маркеры релизов и развёртываний из конвейера CI/CD	Обратиться к администратору платформы либо к команде сопровождения конвейера (п. 4.8.10)
10а	Отчёт не поступил получателям	Не заданы параметры почтового сервера отчётности; отчёт выключен переключателем;	Открыть «История» отчёта, изучить статус и текст ошибки; при ошибке транспорта

№	Признак ситуации	Вероятная причина	Действия пользователя
		ошибка отрисовки или отправки	обратиться к администратору платформы
10б	Отчёт пришёл пустым	Дашборд использует переменные, значения которых не заданы в настройках отчёта	Задать значения в поле «Переменные дашборда» (п. 4.13.5)
10в	Оповещения не приходят, хотя правило срабатывает; в истории алерты помечены «Обслуживание»	Действует окно обслуживания, охватывающее объект	Открыть карточку алерта и определить окно; при необходимости отменить окно (п. 4.9А.9)
10г	Предпросмотр охвата окна обслуживания сообщает, что совпадений не найдено	Область действия окна задана неверно	Проверить состав области действия; при использовании меток — сверить их с фактическими лейблами алертов (п. 4.9А.6)
11	Отображаются сообщения об ошибках компонентов платформы, разделы работают нестабильно	Нарушение работоспособности серверной части	Немедленно обратиться в службу технической поддержки, приложив снимок экрана, точное время и наименование раздела
12	Обнаружены признаки несанкционированного доступа: неизвестные действия в журнале аудита, изменение правил или каналов без ведома ответственных, вход под учётной записью в нерабочее время	Возможная компрометация учётных данных	Немедленно уведомить администратора платформы и подразделение информационной безопасности организации. Не удалять записи журналов. Сменить пароль после указания администратора

5.2. Порядок проверки при недоставке уведомления об алерте

1. Убедиться, что после изменения правил и политик нажата кнопка **«Применить»**.
2. Проверить, что правило находится в статусе `включено`.
3. Проверить статус алерта: он должен быть `firing`, а не `pending` (условие должно продержаться время, заданное в поле `for`).
4. Сверить лейблы алерта с матчерами политики (например, `severity = WARNING`).
5. Проверить реквизиты канала (адрес получателя, токен бота, идентификатор чата, адрес webhook).
6. Проверить порядок политик: более приоритетная политика с выключенным параметром «Продолжение» могла перехватить алерт.

5.3. Порядок обращения в службу технической поддержки

При обращении подготовьте:

- наименование раздела Системы и выполнявшуюся операцию;
- точное время возникновения ситуации (с указанием часового пояса);
- наименование сервиса, хоста или иного объекта;
- текст сообщения об ошибке и снимок экрана;
- идентификатор учётной записи, под которой выполнялась операция.

Сбор технических журналов серверной части выполняется администратором платформы в порядке, установленном «Руководством администратора».

5.4. Ограничения при аварийных ситуациях

- Не выполняйте массовое удаление правил, каналов и политик в попытке восстановить работоспособность — это приведёт к потере конфигурации оповещений.
- Не отключайте встроенные правила алертинга без согласования с ответственным за мониторинг.
- Не передавайте реквизиты доступа третьим лицам, включая сотрудников технической поддержки; для диагностики используйте выделенные учётные записи.

6. Рекомендации по освоению

6.1. Контрольный пример

Контрольный пример предназначен для проверки готовности пользователя к самостоятельной работе. Ожидаемое время выполнения — 30–45 минут.

Задача

Настроить оповещение о превышении доли ошибок сервиса и убедиться в его доставке, после чего провести разбор ситуации средствами Системы.

Шаг 1. Создание канала доставки

1. Откройте `Инциденты и Алерты` → `Каналы оповещения`, нажмите **«Добавить»**.
2. Укажите **Название** — `Telegram дежурной смены`, **Тип** — `Telegram`.
3. Заполните **Токен бота** и **Telegram ID** (идентификатор чата).
4. Сохраните канал.

Шаг 2. Создание правила алертинга

1. Откройте `Инциденты и Алерты` → `Правила`, нажмите **«Добавить»**.
2. Заполните поля:
   - **Название**: `Высокая доля ошибок сервиса`;
   - **Группа**: `GENERAL`;
   - **Критичность**: `WARNING`;
   - **Описание**: `Доля ошибок сервиса выше 5% в течение 5 минут`;
   - **Выражение**:

```
    avg(services_errorcallsperc{service="credit-bureau-service"}) by (service,
service_id) > 5
```

(замените `credit-bureau-service` на имя вашего сервиса);

   - **for**: `5m`.
3. Нажмите **«Создать»**, затем переведите правило в статус `включено`.
4. Нажмите **«Применить»**.

Шаг 3. Создание политики маршрутизации

1. Откройте `Инциденты и Алерты` → `Политики оповещения`, нажмите **«Добавить»**.
2. В **Лейблах группировки** оставьте `alertname` и `service`.
3. В **Каналах оповещения** выберите `Telegram дежурной смены`.
4. Добавьте матчер: ключ `severity`, оператор `=`, значение `WARNING`.
5. Задайте **Порядок** — `1`, сохраните.
6. Нажмите **«Применить»**.

Шаг 4. Проверка

При превышении долей ошибок сервиса значения 5 % дольше пяти минут:

- алерт появится в разделе `Инциденты и Алерты` → `Активные Алерты`;
- уведомление поступит в указанный чат.

Если уведомление не получено — выполните проверку по перечню п. 5.2.

Шаг 5. Разбор ситуации

1. Из карточки алерта перейдите к дашборду сервиса.
2. Определите период деградации и сопоставьте его с лентой `Инциденты и Алерты` → `История Алертов` → вкладка `События` — не совпадает ли он с релизом.
3. Определите, все ли эндпоинты сервиса затронуты, и локализована ли проблема на отдельном инстансе.
4. Перейдите к трейсам ошибочных вызовов, найдите спан с ошибкой.
5. В разделе `Логи` выполните запрос по этому сервису за тот же интервал с фильтром по уровню `error`.
6. Зафиксируйте вывод: затронутый компонент, предполагаемая причина, момент начала.

Критерии успешного выполнения

- Канал, правило и политика созданы и применены.
- Алерт отображается в разделе «Активные» и присутствует в истории.
- Уведомление доставлено в канал.
- Выполнен переход от алерта к трейсу и логам, определён затронутый компонент.

6.2. Рекомендуемая последовательность освоения

Этап	Содержание	Разделы руководства
1	Вход в Систему, навигация, выбор периода, обновление данных	3, 4.1
2	Работа с дашбордами сервисов и бизнес-приложений	4.2
3	Анализ трейсов и логов	4.3, 4.4
4	Оповещения: просмотр активных, история, события	4.8.2–4.8.4
5	Настройка собственных оповещений (контрольный пример)	4.8.5–4.8.7, 6.1
6	Работа с метриками и PromQL	4.5
7	Создание пользовательских дашбордов	4.12
8	Инциденты, SLO, PCM	4.9, 4.10, 4.11
9	Экспорт данных и программный доступ	4.13, 4.14

6.3. Рекомендации по организации эксплуатации

- **Единые соглашения об именовании.** Согласуйте в организации соглашения об именовании сервисов, окружений, групп правил алертинга и тегов. Группы правил должны именоваться только латиницей.
- **Регламент реагирования.** Для каждого правила алертинга с критичностью `CRITICAL` определите ответственное подразделение и порядок действий; ссылку на регламент разместите в комментарии политики или в текстовом виджете дашборда.
- **Контроль шума.** Регулярно (не реже одного раза в квартал) пересматривайте перечень правил: отключайте правила, срабатывания которых систематически не приводят к действиям.
- **Проверка после изменений.** После каждого релиза контролируемой системы сверяйте показатели с маркером релиза в ленте событий.
- **Разграничение доступа.** Запрашивайте только те права, которые необходимы для выполнения должностных обязанностей.

7. Приложения

Приложение А. Соответствие документа требованиям нормативных документов

Требование	Нормативный документ	Раздел настоящего документа
Область применения, краткое описание возможностей, уровень подготовки пользователя, перечень эксплуатационной документации	РД 50-34.698-90, п. 3.4.1	1.1–1.4
Виды деятельности и функции, для автоматизации которых предназначено ПО; условия применения	РД 50-34.698-90, п. 3.4.2	2.1, 2.2
Состав и содержание дистрибутива, порядок загрузки, порядок проверки работоспособности	РД 50-34.698-90, п. 3.4.3	3.1–3.3
Описание операций: наименование, условия, подготовительные и основные действия, ресурсы	РД 50-34.698-90, п. 3.4.4	4.1–4.14
Действия в случае несоблюдения условий выполнения операций; действия по восстановлению; действия при обнаружении несанкционированного вмешательства	РД 50-34.698-90, п. 3.4.5	5.1–5.4
Рекомендации по освоению, контрольный пример	РД 50-34.698-90, п. 3.4.6	6.1–6.3
Назначение и условия применения, характеристики, обращение к программе, сообщения оператору	ГОСТ 19.505-79	1.2, 2.2, 3.2, 5.1

Приложение Б. Перечень значимых ограничений версии

Ограничение	Раздел
Кнопка «Обновить» не обновляет списки объектов — требуется полная перезагрузка страницы	4.1.4
Имя группы правил алертинга — только латиница, цифры и подчёркивание	4.8.7
Встроенные правила алертинга не редактируются и не удаляются — только отключаются или копируются	4.8.7
Изменения правил и политик применяются только после нажатия кнопки «Применить» (до ~1 минуты)	4.8.7
Тип существующего канала оповещения изменить нельзя	4.8.5
Канал, используемый в политике, не может быть удалён	4.8.5
Правила алертинга по SLO не редактируются напрямую	4.8.9
Источник данных LogsQL для виджетов доступен с версии 200	4.12.3
Разделы «Логи», «РСМ», «Роли и доступ» доступны с версии 200	4.1.2
Модуль «Инциденты» и API маркеров событий доступны с версии 201	4.9, 4.15.1
Разделы «Алерты» и «Инциденты» объединены в раздел «Инциденты и Алерты» с версии 202	4.1.2, 4.8
Разделы «Базы данных», «Сеть», «Очереди сообщений», «Веб-серверы» перенесены в каталог «Инфраструктура» с версии 202	4.1.2, 4.7.1

Ограничение	Раздел
Окна обслуживания, отчёты по электронной почте, правила No-Data, флейм-граф и выгрузка трейса, вкладка «Кардинальность», виджеты «Соты здоровья» и «KPI-карточка», инциденты как источник данных, приём ошибок из Sentry SDK — доступны с версии 202	4.9А, 4.13, 4.8.8А, 4.3.3А, 4.3.3Б, 4.5.3А, 4.12.3А, 4.12.3Б, 4.2.3
Подраздел «Надёжность изменений», раздел «AI-аналитик», вкладка «Проверка на ПДн», пункты диагностики «Объём данных» и «Реестр конфигурации» — доступны с версии 203	4.8.10, 4.16, 4.1.2
Раздел «AI-аналитик» требует подключения внешней языковой модели администратором	4.16
Показатели надёжности изменений достоверны только при передаче маркеров релизов из CI/CD	4.8.10
Пункты диагностики «Объём данных» и «Реестр конфигурации» доступны только администраторам; «Реестр конфигурации» — только на чтение	4.1.2
Вкладка «Отчёты» доступна только пользователям с правом администратора на ресурс `reports`	4.13.1
День месяца для ежемесячного отчёта ограничен значениями 1–28	4.13.3
Отчёт по дашборду с переменными без заданных значений переменных приходит пустым	4.13.5
Ошибки отправки письма отчёта автоматически не повторяются	4.13.6
Окно обслуживания подавляет оповещения, но не скрывает срабатывания из истории алертов	4.9А.7
Число ячеек виджета «Соты здоровья» ограничено 2000	4.12.3А
На очень крупных трейсах часть спанов может не отображаться на флейм-графе	4.3.3А
ИИ-функции требуют подключения внешней языковой модели администратором	4.9.6
Базовый режим источника данных виджетов является устаревшим	4.12.3
Время жизни access-токена API — около 5 минут	4.15.3

Приложение В. Единицы измерения и шкалы

Показатель	Шкала / единицы	Интерпретация
APDEX	0 … 1	1 — все пользователи удовлетворены; 0 — неприемлемый пользовательский опыт
Доля ошибок	%	Доля вызовов, завершившихся ошибкой
Время отклика	мс	Приводится как среднее и как перцентили
Длительность спана	мс	Включает время вложенных вызовов
Критичность алерта	`CRITICAL`, `WARNING`	Задаётся полем «Критичность» правила
Критичность инцидента	Критический, Высокий, Средний, Низкий	Наивысшая среди входящих алертов

Показатель	Шкала / единицы	Интерпретация
MTTR	мин	Среднее время устранения
Бюджет ошибок	% / доля периода	Остаток допустимых нарушений SLO

Пороговое значение `APDEX T` (граница удовлетворительного времени отклика) задаётся администратором для каждого сервиса; значение по умолчанию — 500 мс. Транзакции классифицируются как: удовлетворительные (быстрее `APDEX T`), приемлемые (быстрее `4 × APDEX T`), неудовлетворительные (медленнее `4 × APDEX T` либо завершившиеся ошибкой).

Конец документа