



## РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ ИНДЕКСЛОГ

### 1. Введение

Пользователь системы ИндексЛог – аналитик данных, в его обязанности входит анализ данных, хранящихся в системе, построение визуализаций, создание информационных панелей – дашбордов – из этих визуализаций. Для выполнения этих обязанностей ему предоставляется доступ к чтению данных и доступ к построению визуализаций. Также пользователь в соответствии со своей должностью и областью ответственности может иметь доступ к встроенным информационным панелям приложений АРМ, Инфраструктурного мониторинга, Мониторинга доступности и приложениям Безопасности. Краткие инструкции по пользованию этими приложениями включены в решение, поэтому в данном Руководстве будет рассмотрено использование возможностей визуализации ИндексЛог\_Аналитика.

### 2. Принцип работы визуализаций в ИндексЛог\_Аналитика

Решение ИндексЛог\_Аналитика представляет собой фронтэнд приложение стека ИндексЛог. Его основные функции – упрощение отправки в ИндексЛог\_Поиск REST API-запросов и визуализация результатов, возвращаемых ИндексЛог\_Поиск.

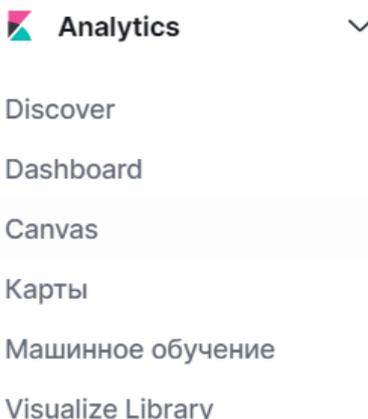
Поисковые запросы ИндексЛог\_Поиск имеют два типа: search и aggregation. Запросы типа aggregation используются для распределения на группы, суммирования и проведения математических и статистических операций над ними. Агрегации разбивают данные на bucket'ы и возвращают их в формате JSON. На основе bucket'ов и строятся все визуализации в ИндексЛог\_Аналитика. Визуализации можно затем сохранить и добавить на информационную панель (далее - дэшборд) для создания представления данных, удобного для анализа данных пользователя.

### 3. Создание Визуализации в ИндексЛог\_Аналитика

Вкладка Visualize позволяет создавать визуализации на основе запросов ИндексЛог\_Поиск без необходимости создавать запрос вручную. Визуализации создаются в удобном интерфейсе и имеют широкие возможности настройки.

Для создания визуализации:

1. Откройте левую боковую панель навигации и кликните на вкладку «Visualize Library».





2. Нажмите кнопку «Создать визуализацию».

3. Выберите стандартный инструмент создания визуализаций «Lens».



### Lens

Создавайте визуализации перетаскиванием с помощью нашего редактора. Переключайтесь между типами визуализаций в любое время.  
*Рекомендуется для большинства пользователей.*

4. Выберите тип визуализации:

- таблица;
- гистограммы: вертикальные, вертикальные складываемые, процентные гистограммы вертикальные, горизонтальные, горизонтальные складываемые, процентные гистограммы горизонтальные;
- метрики и шкалы: вертикальные и горизонтальные шкалы, метрика;
- графики и области: графики, областные диаграммы, процентные областные диаграммы;
- тепловые карты;
- географические карты;
- пропорции: вафельные диаграммы, древовидные карты, кольцевые диаграммы, круговые диаграммы, мозаики.

#### Тип визуализации

Цель и единственное значение

-  Вертикаль...  Технический предпросмотр
-  Горизонал...  Технический предпросмотр
-  Метрика  Технический предпросмотр
-  Устаревшая метрика 

Линия и площадь

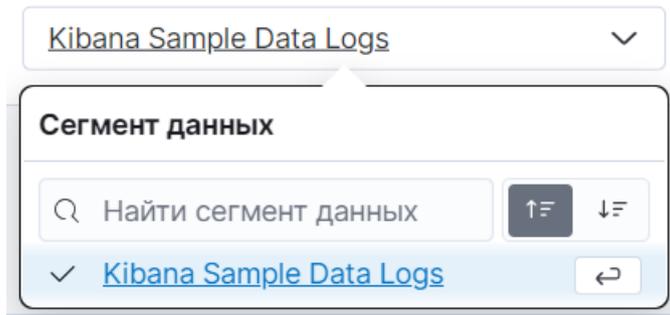
-  **Линия**
-  Область
-  Площадь наложенная
-  Процент площади

Величина

-  Тепловая карта 



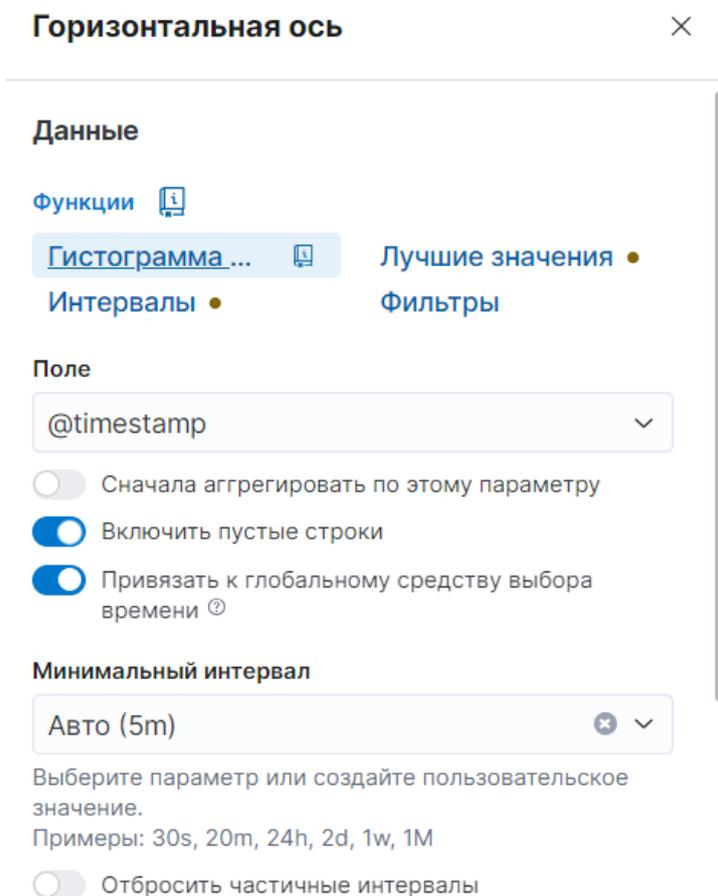
5. Выберите сегмент данных для визуализации.



6. Добавьте данные на вертикальную ось. Выберите метрику агрегации для оси Y визуализации:

- метрические агрегации: подсчет, среднее, сумма, минимум, максимум, стандартное отклонение, количество уникальных значений, медиана (50%), процентные ряды, топ значений;
- агрегации родительских источников информации: производная, кумулятивная сумма, скользящее среднее, последовательный дифференциал;
- агрегации родственного источника: среднее по bucket'у, сумма по bucket'у, минимум и максимум по bucket'у.

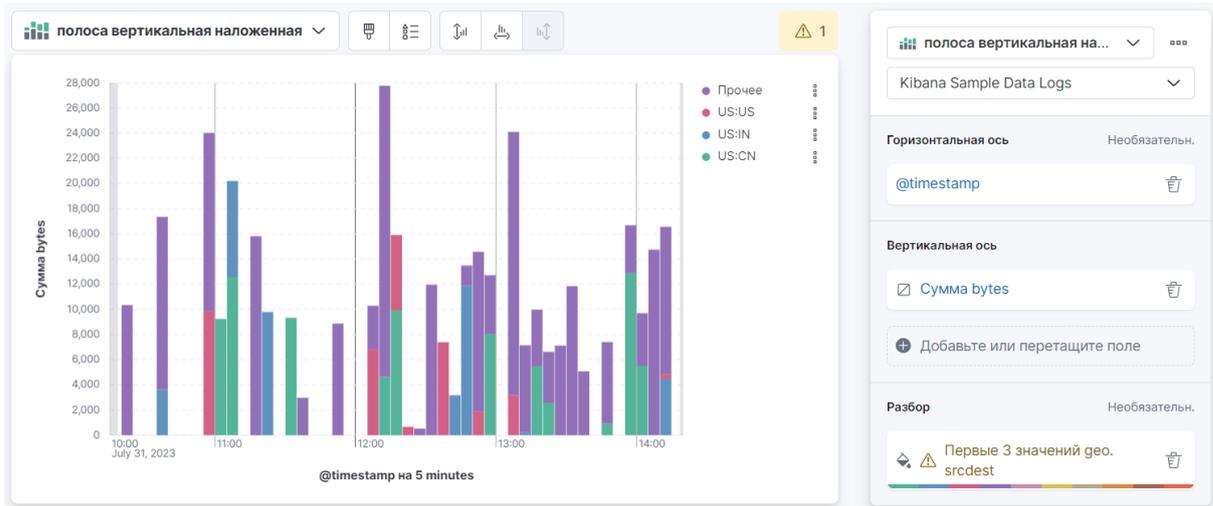
7. Добавьте данные на горизонтальную ось. Выберите для оси X агрегацию по bucket'у: гистограмма дат, спектр, выражения, фильтры, знаковые выражения.





## 8. При необходимости добавьте данные для разбивки

В качестве примера построена агрегация типа «складываемая вертикальная гистограмма» на сегменте данных логов. Визуализация предоставляет количество байтов лога, полученные за выбранный период времени с разбивкой по направлению передачи данных.



### Обзор параметров визуализаций в ИндексЛог.

Графики, диаграммы и областные диаграммы строятся по двум осям.

Для оси Y (вертикальной) доступны следующие агрегации:

- **Подсчет.** Агрегация подсчета возвращает чистый подсчет элементов в выбранном шаблоне индекса.
- **Среднее.** Данная агрегация возвращает среднее значение по числовому полю. Выберите поле из выпадающего списка.
- **Сумма.** Возвращает общую сумму по числовому полю. Выберите поле из выпадающего списка.
- **Минимум.** Возвращает минимальное значение по числовому полю. Выберите поле из выпадающего списка.
- **Максимум.** Возвращает максимальное значение по числовому полю. Выберите поле из выпадающего списка.
- **Кол-во уникальных значений.** Кардинальная агрегация возвращает число уникальных значений в поле. Выберите поле из выпадающего списка.
- **Стандартное отклонение.** Агрегация общей статистики возвращает стандартное отклонение данных в числовом поле. Выберите поле из выпадающего списка.
- **Лучшие значения.** Агрегация топовых значений возвращает один или больше топовых значений из специального поля в вашем документе. Выберите поле из выпадающего списка, тип сортировки документов, количество значений, которые нужно вернуть.
- **Процентиль.** Агрегация процентов разделяет значения числового поля на заданные диапазоны. Выберите поле из выпадающего списка, затем определите одну или больше областей в полях Процентили.



- **Процентильный ранг.** Агрегация процентного ранга возвращает процентное ранжирование по выбранному числовому полю. Выбирайте поле из выпадающего списка, затем определите один или больше значений процентного ранга в полях Значения.
- **Производная.** Агрегация производной подсчитывает производную определенных метрик.
- **Кумулятивная сумма.** Агрегация накопительной суммы подсчитывает накопительную сумму определенных метрик в родительской гистограмме.
- **Скользящее среднее.** Агрегация скользящего среднего будет вставлять окно сквозь данные и писать среднее значение этого окна.
- **Последовательное дифференцирование.** Последовательное дифференцирование — это метод, где значения во временном ряде отнимаются от самих себя в другой временной период или задержки.
- **Среднее по bucket'y.** Среднее сегмента вычисляет среднее значение определенных метрик в агрегации родственных источников.
- **Сумма по bucket'y.** Высчитывает сумму значений определенной метрики в агрегации родственного источника.
- **Минимум по bucket'y.** Возвращает минимальное значение определенной метрики в агрегации родственного источника.
- **Максимум по bucket'y.** Возвращает максимальное значение определенной метрики в агрегации родственного источника.

По горизонтальной оси доступны следующие агрегации:

- **Временная гистограмма.** Временная гистограмма построена на основе числового поля и организована по дате. Вы можете определить временные рамки для интервалов в секундах, минутах, часах, днях, неделях, месяцах или годах. Вы также можете определить интервал по умолчанию, выбрав Польз. в качестве интервала и указав число и единицу времени в текстовом поле. По умолчанию единицами временного интервала являются: s для секунд, m для минут, h для часов, d для дней, w для недель, y для лет. Различные единицы поддерживают различные уровни точности, вплоть до одной секунды. Интервалы подписываются в начале интервала, используя ключ-дату, который возвращается из ИндексЛог\_Поиск. Для примера, на всплывающей подсказке для месячного интервала будет отображаться первый день месяца.
- **Гистограмма.** Стандартная гистограмма строится на основе числового поля. Определите целочисленный интервал для этого поля. Range. С помощью агрегации рангов вы можете определить ранги для значений числового поля. Кликните Добавить диапозорн для добавления набора конечных точек ранга. Кликните красный символ (x), чтобы удалить ранг.
- **Диапазон дат.** Агрегация временного ранга сообщает значения, которые находятся в указанном диапазоне дат. Вы можете указать диапазоны дат, используя математические выражения даты. Кликните Добавить диапазон, чтобы добавить набор конечных точек ранга
- **IPv4 Range.** Агрегация IPv4 ранга позволяет вам определить диапазоны IPv4 адресов. Кликните Add Range, чтобы добавить набор конечных точек ранга. Кликните красный символ (x), чтобы удалить ранг.
- **Термины.** Агрегация значений позволяет вам определить верхние или нижние n элементов данного поля для отображения, упорядоченные по количеству или пользовательской метрике.



- **Фильтры.** Вы можете определить набор фильтров для данных. Возможно указать фильтр как строку запроса или в формате JSON, так же как и в поисковой вкладке Discover. Кликните Добавить фильтр, чтобы добавить другой фильтр. Кликните кнопку сноски, чтобы открыть поле подписи, где вы можете напечатать имя для отображения на визуализации.
- **Важные термины.** Выводит результаты экспериментальной агрегации знаковых значений.