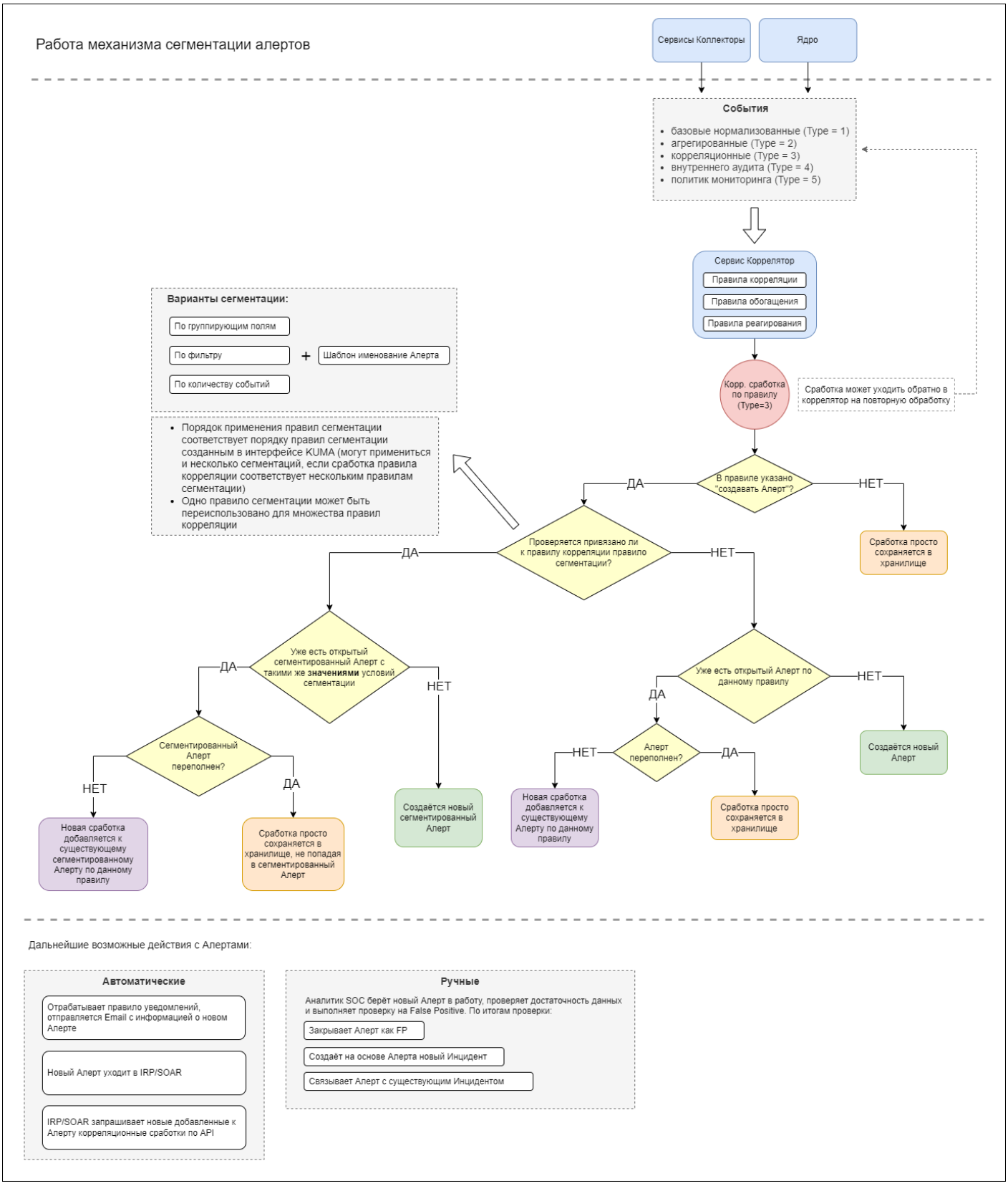
Сегментация правил корреляции

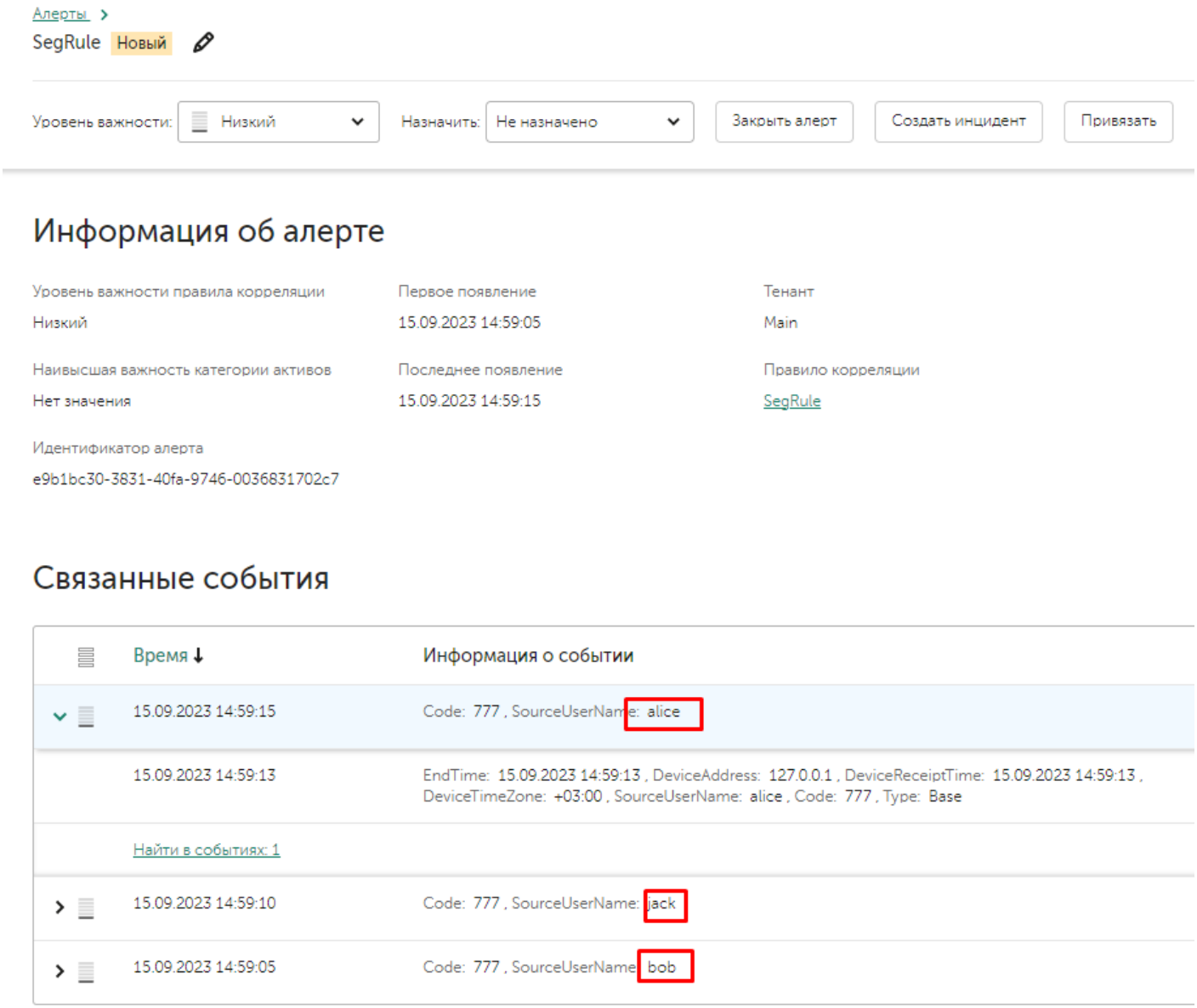
По умолчанию, если в коррелляторе какое-то правило корреляции сработает несколько раз, все созданные в результате этого корреляционные события будут присоединены к одному алерту. Правила сегментации алертов дают возможность определить условия, при которых на основе таких однотипных корреляционных событий будут создаваться разные алерты.

> Порядок применения правил сегментации соответсвует порядку правил сегментации созданным в интерфейсе KUMA (могут примениться и несколько сегментаций, если сработка правила корреляции соответствует нескольким правилам сегментации)

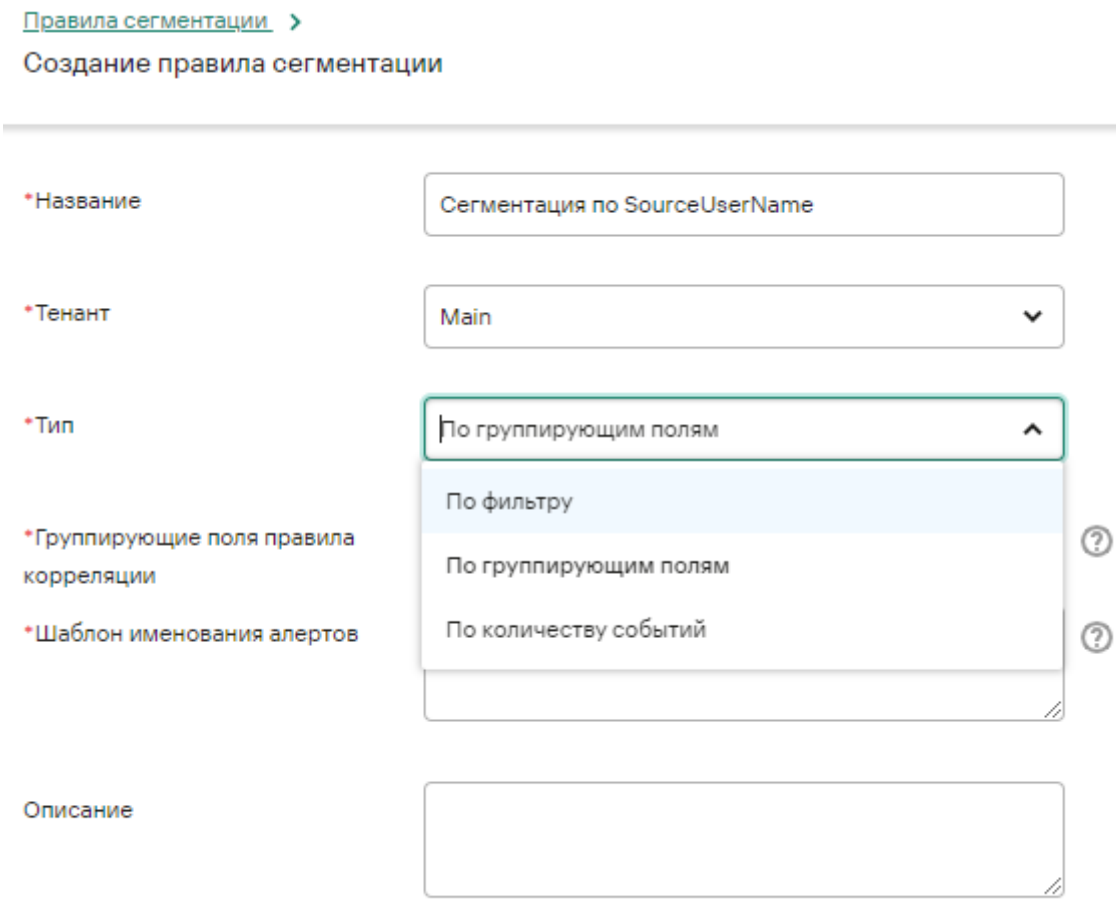
Блок-схема работы сегментации (спасибо за наработку интегратору):



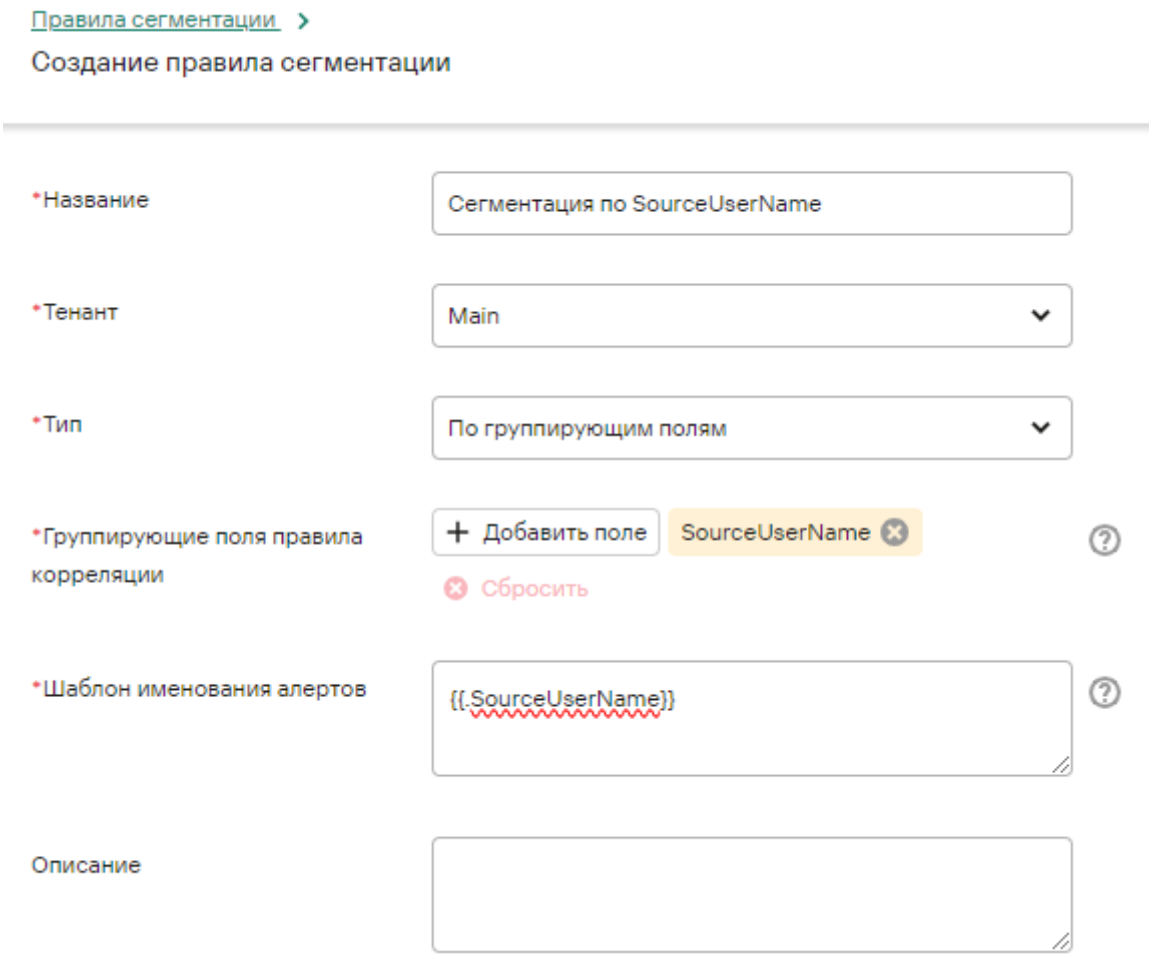
Пример работы, есть правило корреляции, которое срабатывает на событие с полем Code равное "777" с разными занчениями SourceUserName, все сработки правила складваются в один Алерт, мы хотим создать отдельные алерты для отдельных пользователей:



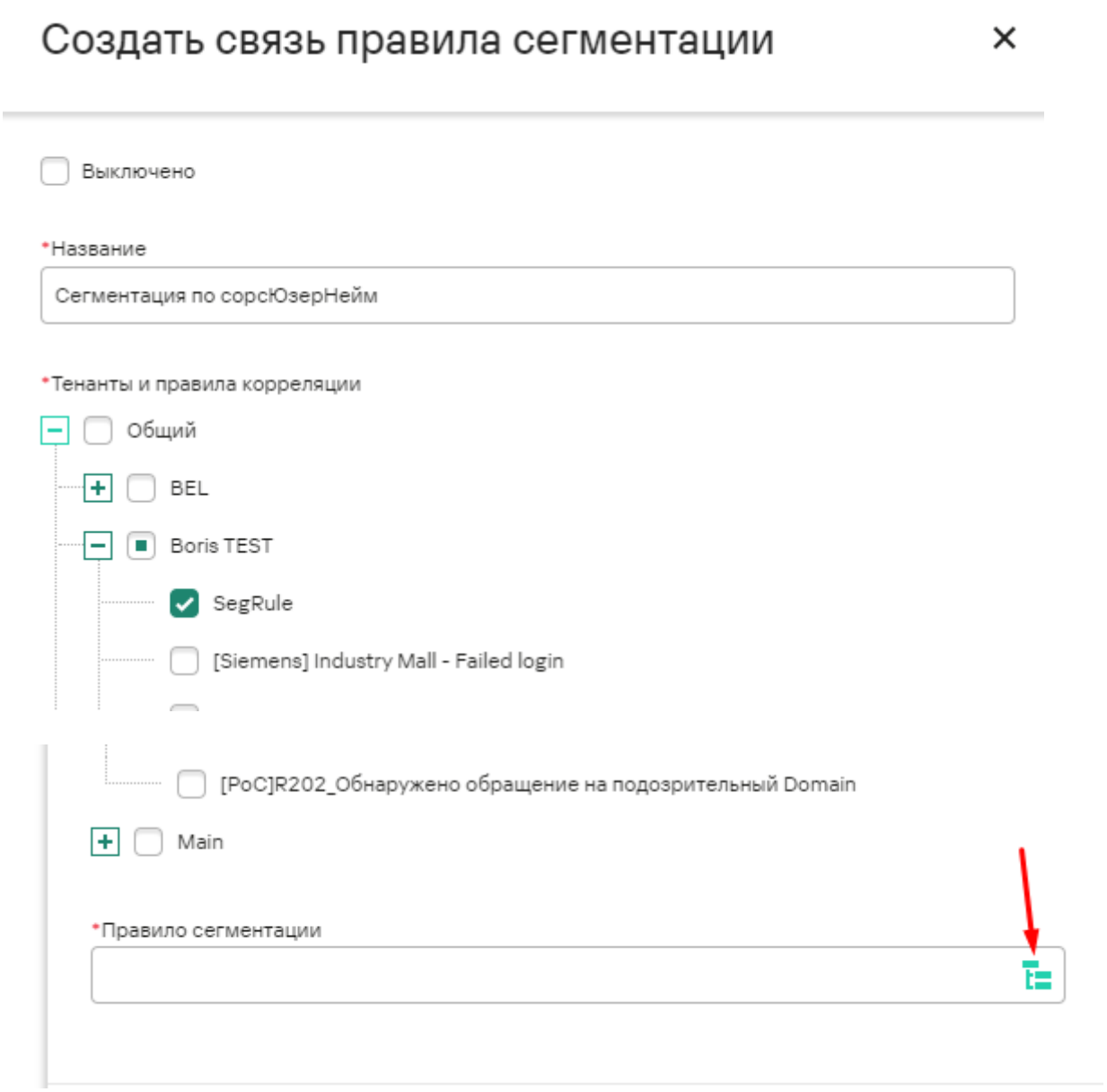
Для этог онужно создать правило сегментации ипривязать его к правилу корреляции. Перейдите в **Ресурсы - Правила сегментации** и нажмите на кнопку **Добавить правило сегментации**. В нашем случае подойдет тип **По группирующим полям**:

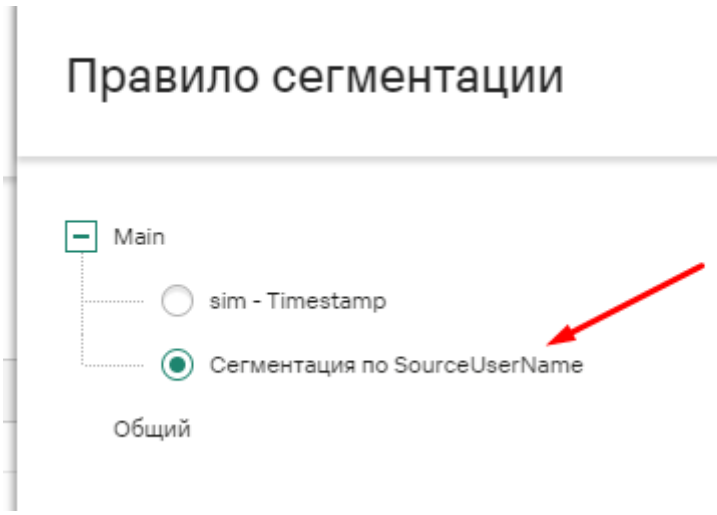


Указываем свой шаблон именования и группирующее поле - используем поля имени пользователя и **Сохраняем**:

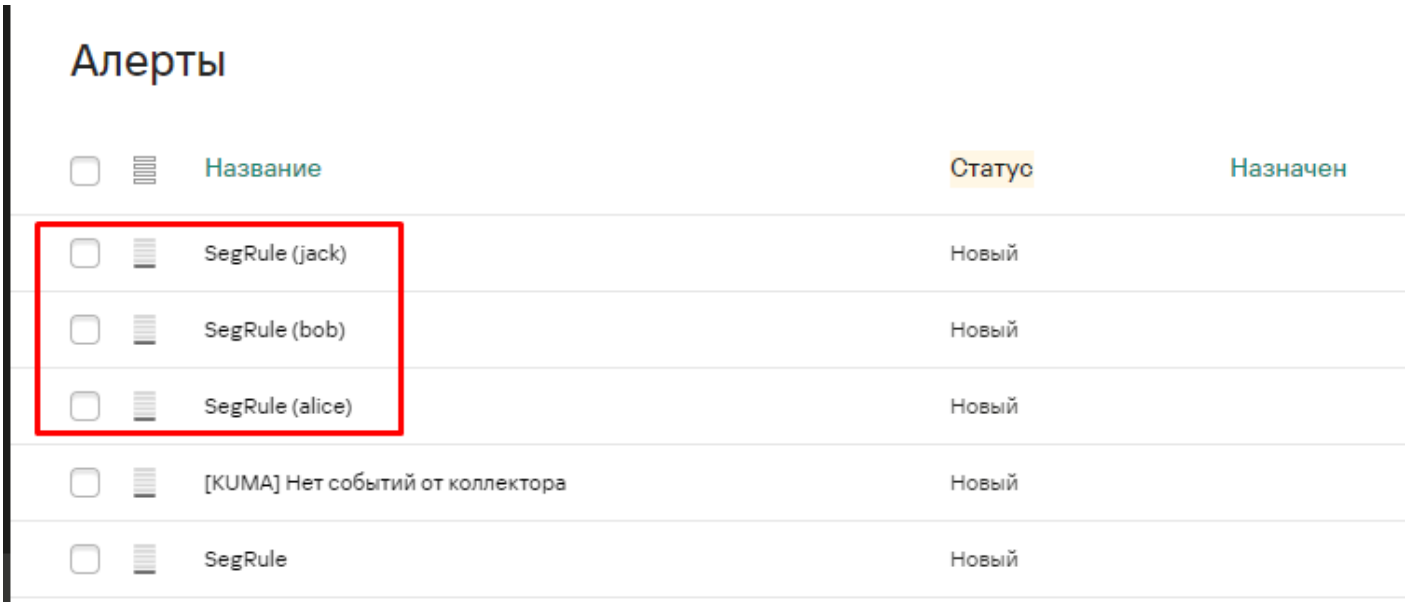


Далее необходимо привязать правило сегментации к нашему правилу корреляции. Это делается в **Параметры - Алерты - вкладка Сегментация**. Выбираем необходимый тенант, нажимаем кнопку Добавить, Указываем название, Выбираем правило корреляции и добавлем правило сегментации, затем на каждом шаге все **Сохраняем**.





По итогу, при появлении событий удовлетворяющих правилу корреляции мы получим отдельные алерты на основе SourceUserName.



Аналогичным образом можно использовать и другие типы правил сегментации.

Revision #6
Created 15 September 2023 11:46:11 by Boris Rzr
Updated 7 July 2024 08:24:17 by Koala