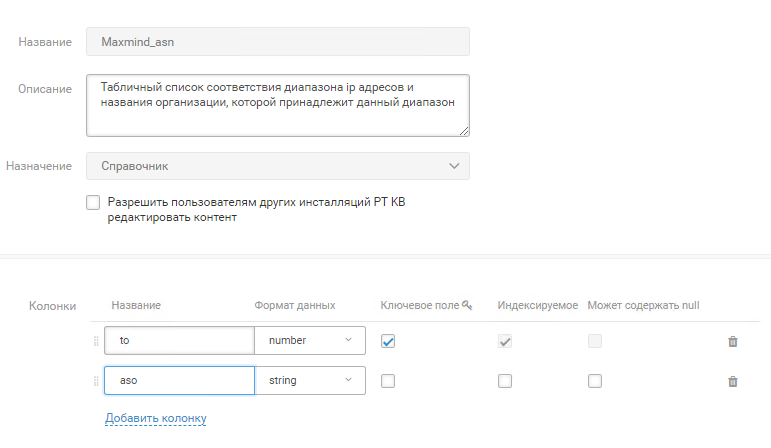
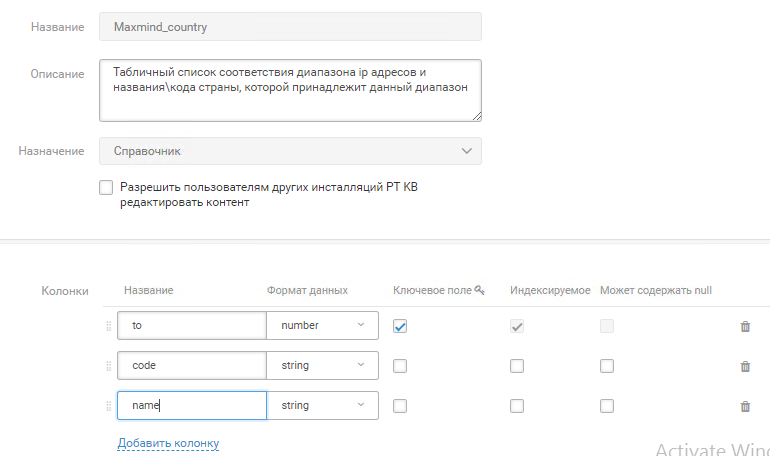
**Инструкция подготовки SIEM 19.1 для работы с обогащением geoip сетевых соединений**

1. Через PTKB создать табличный список «Maxmind\_asn» типа справочник с полями, как показано на скриншоте



Нажать кнопку «Сохранить»

1. Выбрать созданный список, нажать кнопку импорт, выбрать csv файл asn\_range\_final, дождаться завершения импорта (должно импортироваться 422558 записей),нажать кнопку «установить в PT Maxpatrol SIEM»
2. Через PTKB создать табличный список «Maxmind\_country» типа справочник с полями, как показано на скриншоте



1. Выбрать созданный список, нажать кнопку импорт, выбрать csv файл country\_range\_final, дождаться завершения импорта (должно импортироваться 310192 записей),нажать кнопку «установить в PT Maxpatrol SIEM»
2. Через PTKB создать правило обогащения «Maxmind\_geoip» с текстом, приведенным в архиве. Нажать кнопку «Валидация», Нажать кнопку «установить в PT Maxpatrol SIEM»

Если необходимо выводить в события не название страны, а её код, то

* $result1["$country"] поменять на $result1["$code"]
* qhandler {

$country = name

}

Поменять на

qhandler {

$code = code

}