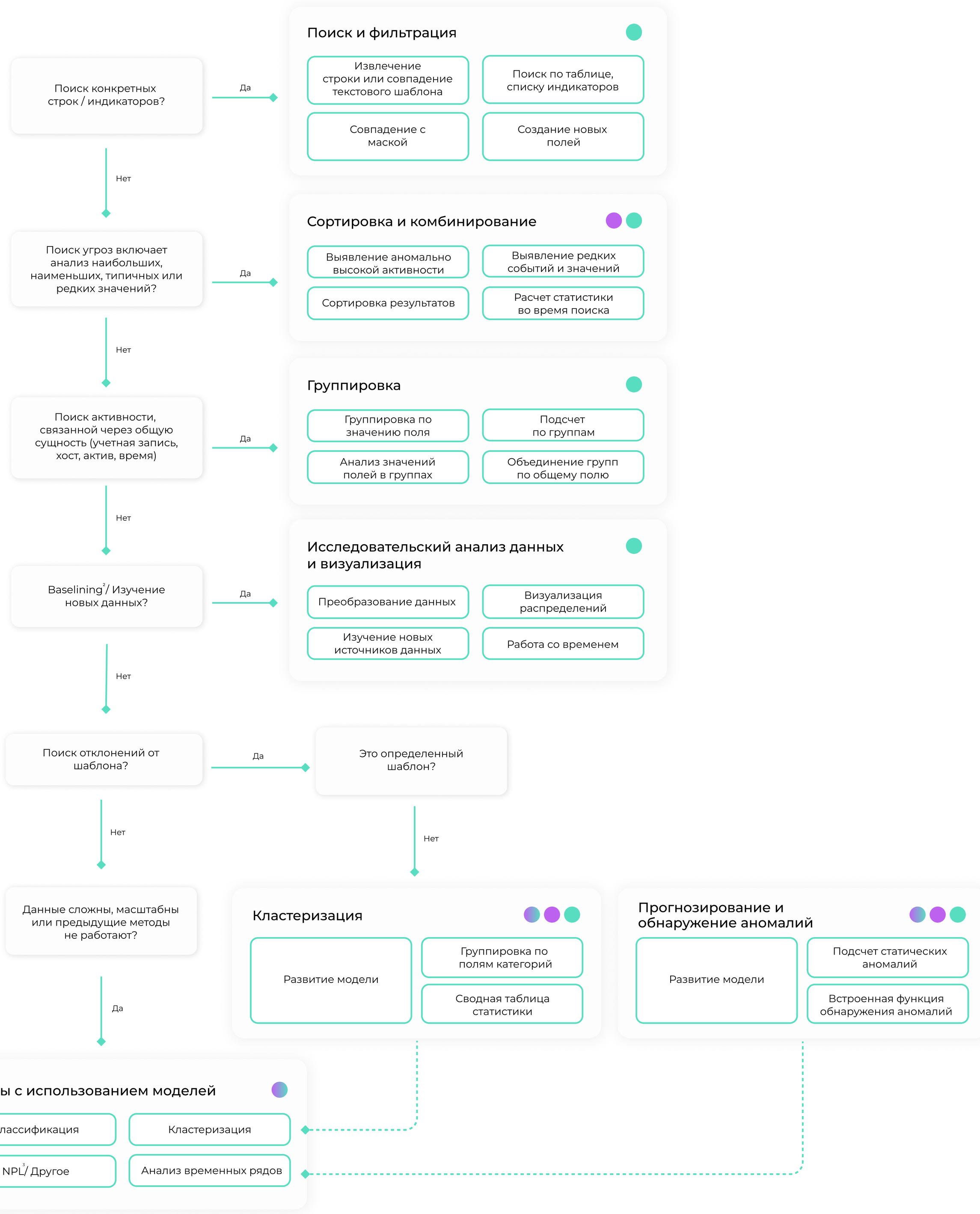
Методология поиска угроз (Threat Hunting)

Активный поиск угроз (threat hunting) — проактивное обнаружение вредоносной деятельности в IT-инфраструктуре, которая не была обнаружена автоматическими системами. Моделью зрелости данного процесса является PEAK, поэтапный фреймфорк для поиска угроз.

Наиболее распространенные методы PEAK[1]

- M-ATH (Model-Assisted Threat Hunts)
- Baselining[2]
- Основанные на гипотезах

Блок-схема по выявлению угроз



[1] **PEAK** (Threat Hunting Framework) - Prepare Execute Act with Knowledge

[2] **Baselining -** процесс создания и документирования эталонного состояния системы, сети или приложения, который используется для сравнения текущей производительностью

[3] **NPL** (Natural Language Processing) - подраздел машинного обучения, позволяющий компьютерам понимать и работать с человеческим языком