Предупреждение инсайдерских угроз на основе выявления аномального поведения пользователей

д.т.н., проф. Шелухин О.И.,

к.т.н., доц. Осин А.В,

кафедра ИБ

МТУСИ

Определение аномального поведения

Нетипичная активность (как правило связано с временными рамками)

Необычная география

Неожиданные действия пользователей (функционал, которым не пользовались ранее или пользовались редко)

Предупреждения от системы безопасности (многократные попытки входа, использование VPN и т.д.)

Попытки повышения привилегий

Какие типы аномального поведения бывают

Угрозы

Злоумышленные действия

Ошибки пользователей

Компрометация учетных записей

Не так как обычно

Нетипичная активность

Избыточное потребление ресурсов

Смена шаблона поведения

СкачкИ

Резкая смена поведения

Смена контекста

Системные предупреждения

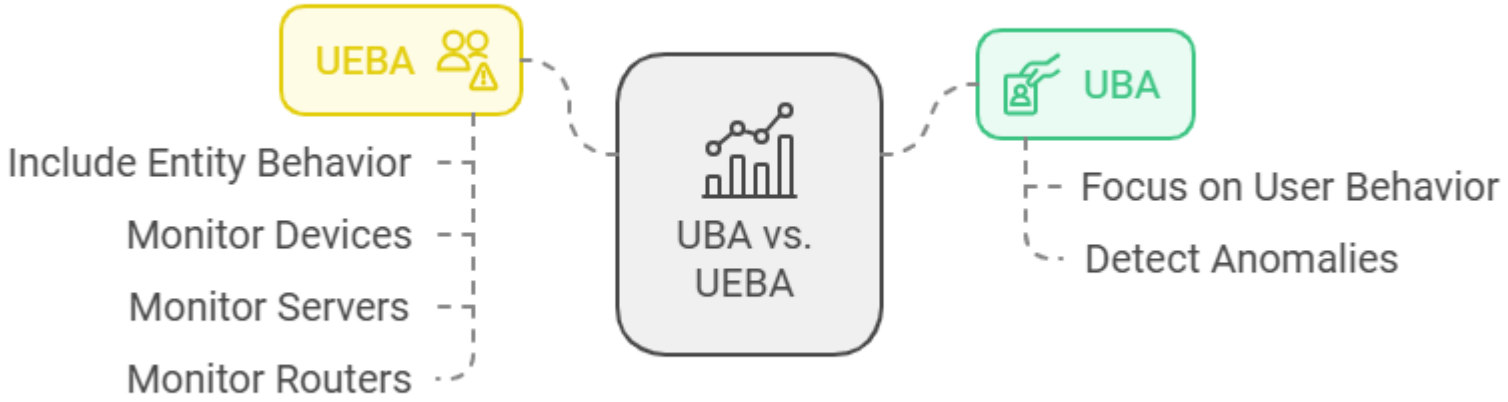
Кто актор?

Инсайдеры

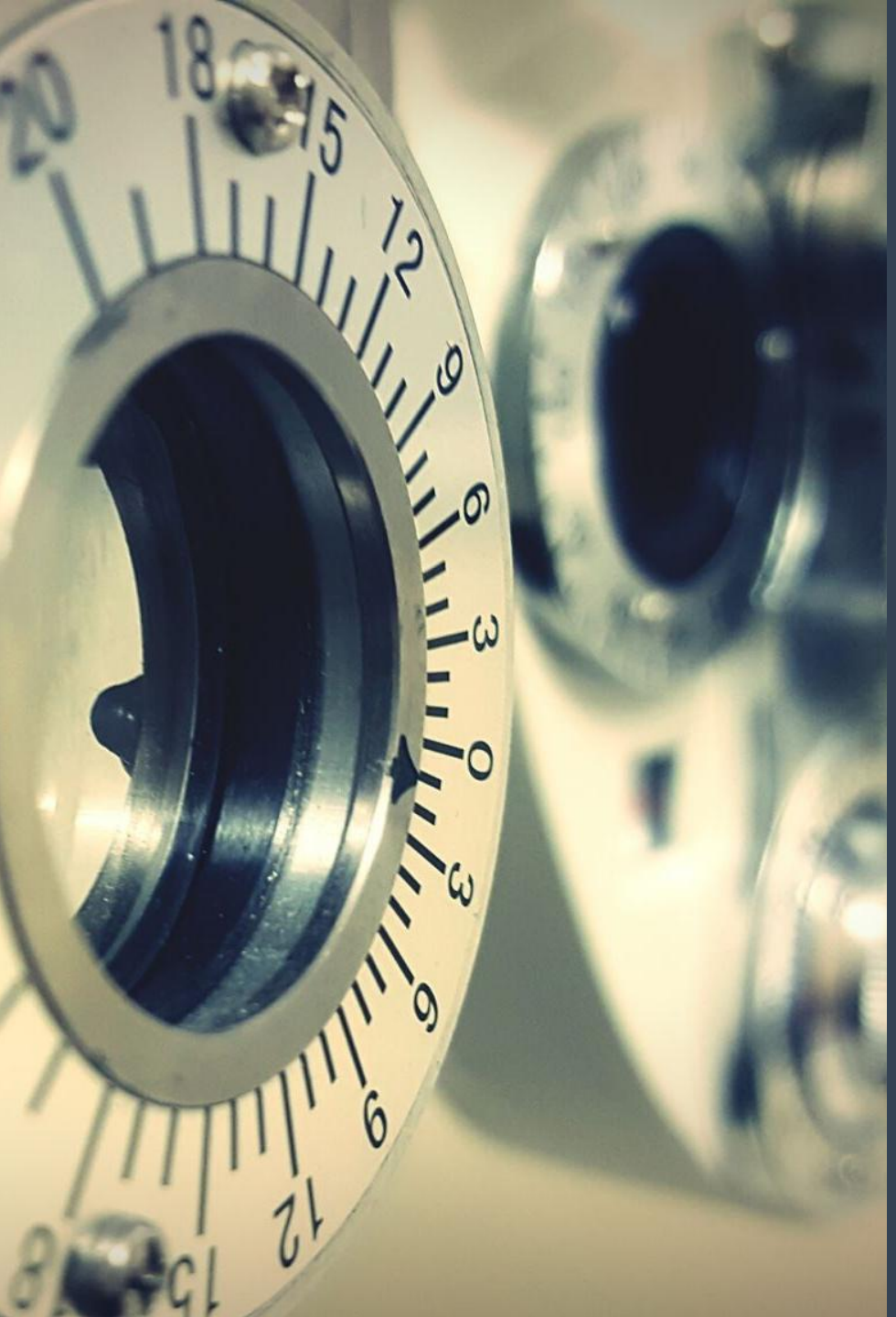
Хакеры

Внешние манипуляторы

UBA vs. UEBA

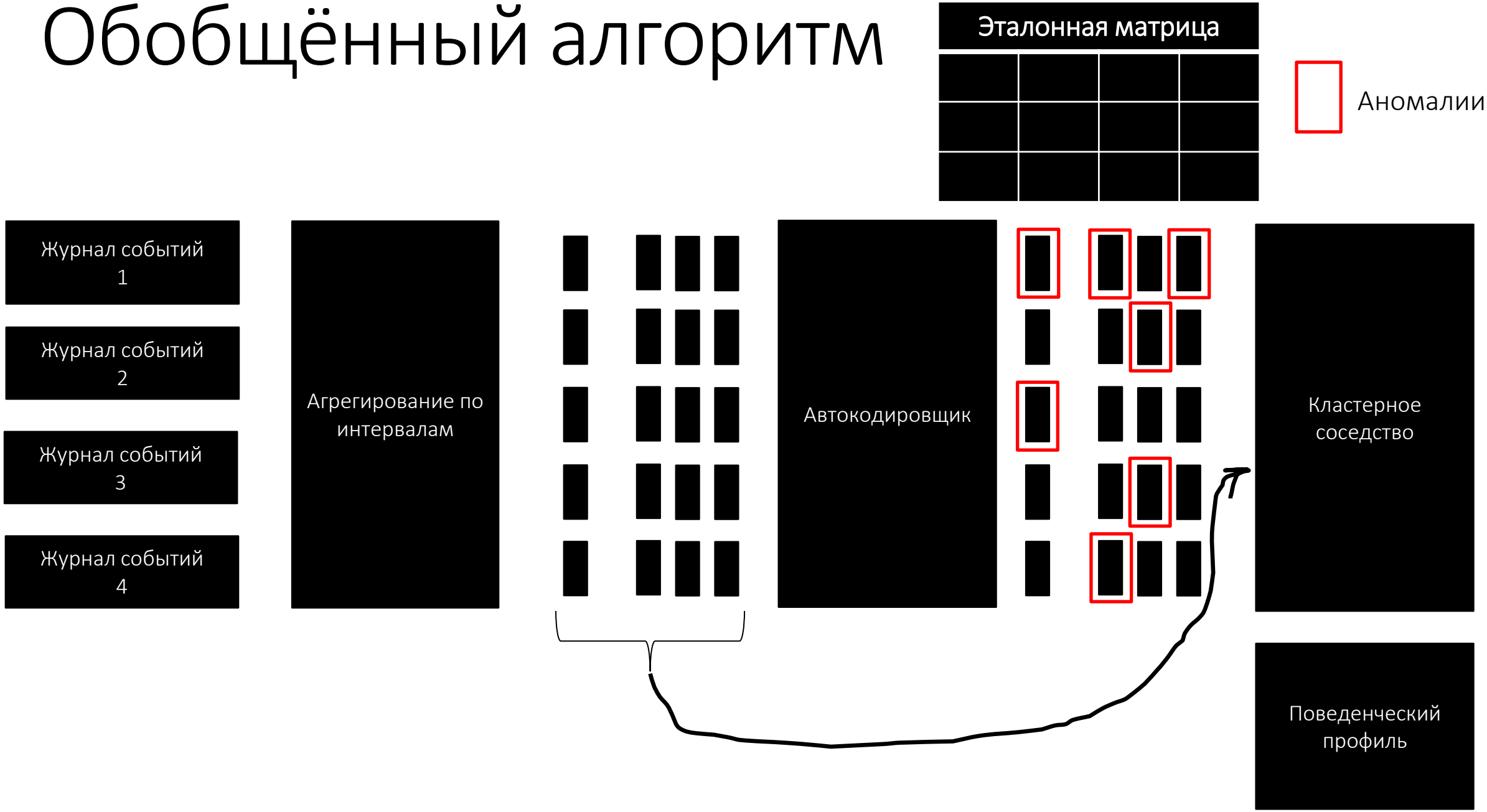


Характеристика	UBA (User Behavior Analytics)	UEBA (User and Entity Behavior Analytics)
Фокус анализа	Только пользователи	Пользователи + устройства, системы, сети
Основная цель	Выявление аномалий в поведении людей	Выявление аномалий во всей IT-инфраструктуре
Противодействие	Внутренним угрозам (инсайдеры, скомпрометированные аккаунты)	Внешним и внутренним угрозам (вирусы, боты, утечки, атаки)
Примеры аномалий	Вход из необычного места, скачивание большого объема данных	Взломанные серверы, боты, зараженные устройства
Технологии	Машинное обучение, статистический анализ	Более продвинутая аналитика с SIEM и машинным обучением



Как построить поведенческий профиль и оценить аномальную активность?

Обобщённый алгоритм



Примеры данных


```
{
  "crm_user_club_id": 3,
  "crm_user_fio": "Ежова Олеся ",
  "crm_user_role": "manager",
  "data": [
    {
      "active": 0,
      "created_at": 1730821584,
      "end_at": 1730821584,
      "inactive": 18262,
      "metric_id": 8122,
      "path": "/clients/index",
      "start_at": 1730803322
    },
```


Пользовательская активность


```
{
  "crm_user_club_id": 3,
  "crm_user_fio": "Ежова Олеся ",
  "crm_user_role": "manager",
  "data": [
    {
      "average_press_time": 0,
      "average_speed": 0,
      "created_at": 1730883890,
      "end_at": 1730883890,
      "metric_id": 13021,
      "path": "/schedule/index",
      "start_at": 1730883795,
      "symbols_typed": null
    },
```


Клавиатурный почерк


```
{
  "crm_user_club_id": 3,
  "crm_user_fio": "Ежова Олеся ",
  "crm_user_role": "manager",
  "data": [
    {
      "average_acceleration": 0,
      "average_speed": 0,
      "created_at": 1730821584,
      "end_at": 1730821584,
      "left_clicks": 0,
      "metric_id": 8091,
      "path": "/clients/index",
      "right_clicks": 0,
      "scroll_down": 0,
      "scroll_up": 0,
      "start_at": 1730803322
    },
```


Параметры курсора


```
{
  "crm_user_club_id": 3,
  "crm_user_fio": "Ежова Олеся ",
  "crm_user_role": "manager",
  "data": [
    {
      "copied_at": 1731295445,
      "created_at": 1731295445,
      "data": "393 003,00",
      "metric_id": 2360,
      "path": "/statistics/sell-all-items-list"
    },
```


Содержимое буфера обмена


```
  "crm_user_club_id": 3,
  "crm_user_fio": "Ежова Олеся ",
  "crm_user_role": "manager",
  "data": [
    {
      "created_at": 1730821584,
      "event_at": 1730803322,
      "metric_id": 4333,
      "path": "/clients/index",
      "type": "updatedUserHash"
    },
```


События пользователя

Идеология кластерного соседства

1 шаг

Формирование бутстрепов атрибутов

2 шаг

По каждому сочетанию атрибутов вычисляется кластерное пространство

3 шаг

Фиксируется кластер, к которому отнесён образец

4 шаг

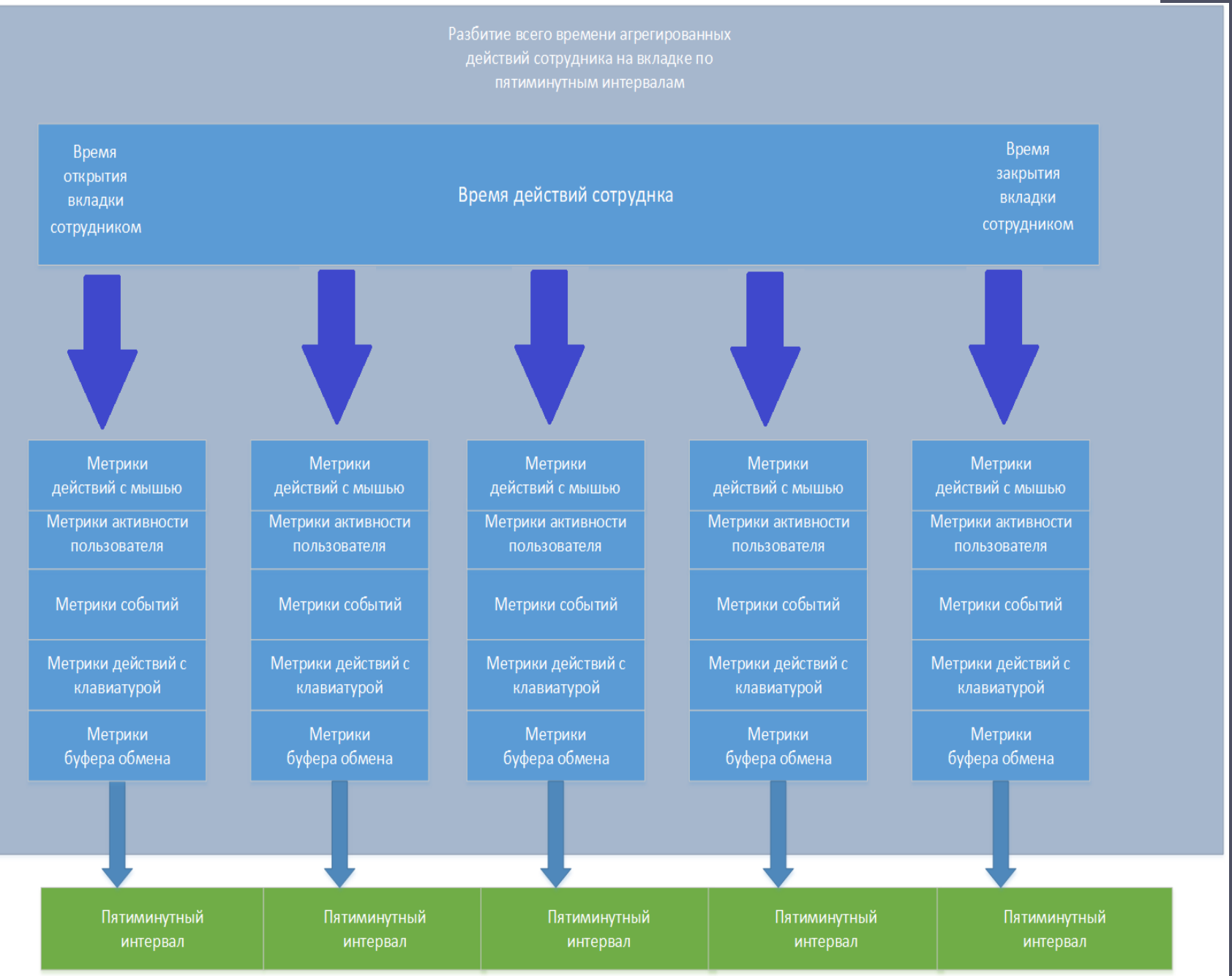
Объект фиксируется в каждом кластере каждого бутстрепа

5 шаг

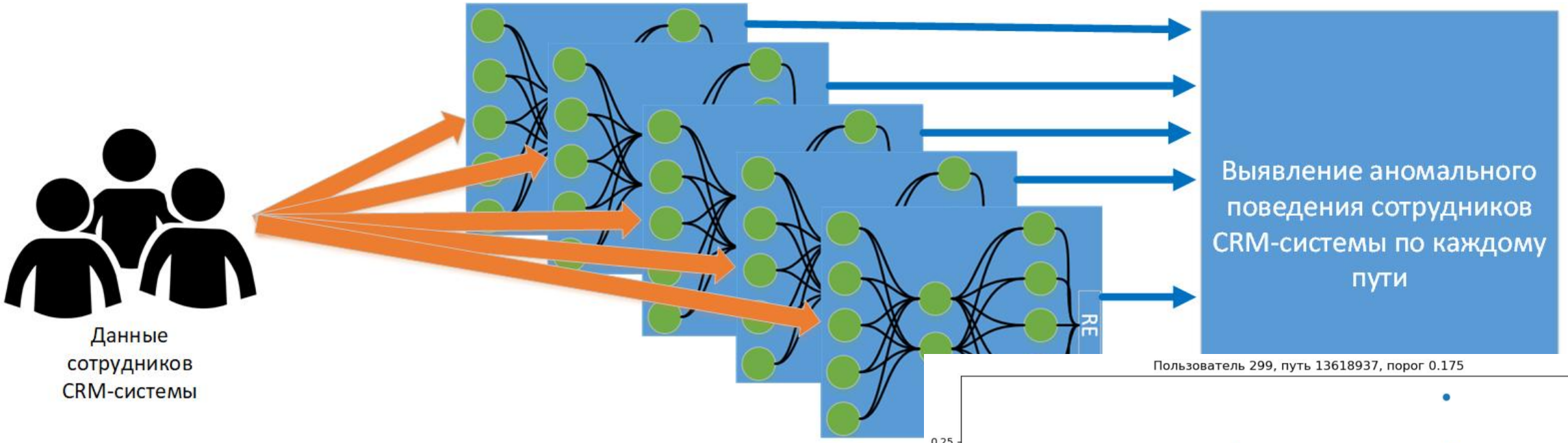
Вычисляется процент объектов разного типа для найденного кластера

6 шаг

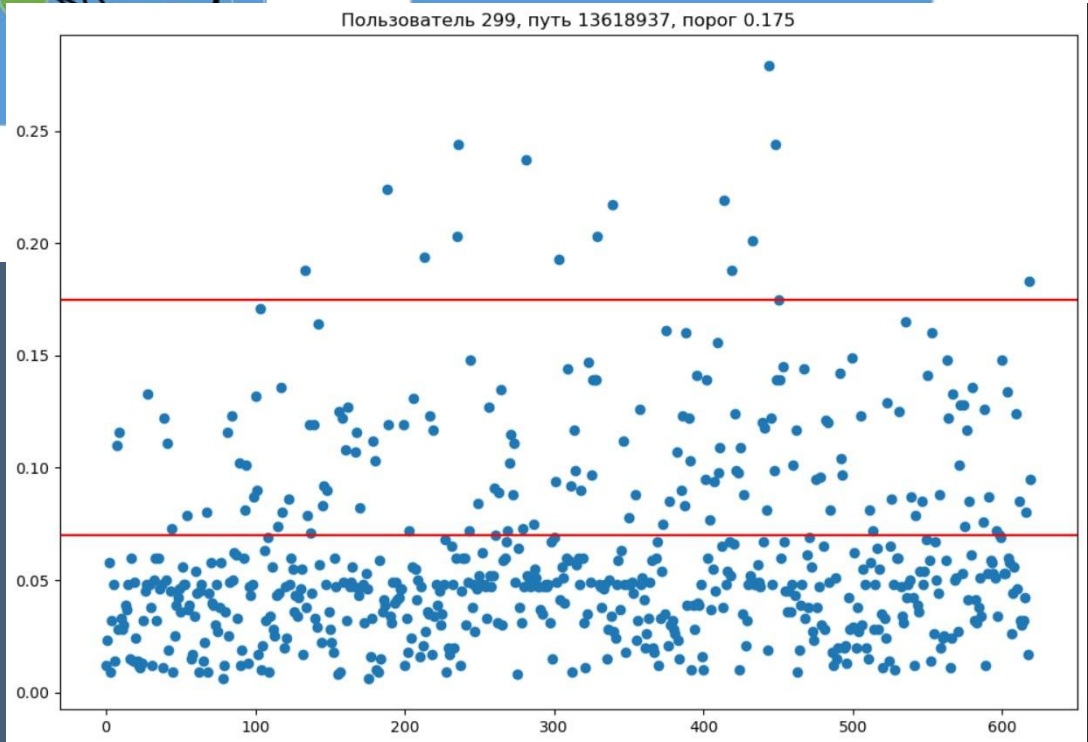
Строится поведенческий профиль объекта по каждому следу в кластерном пространстве для каждого бутстрепа



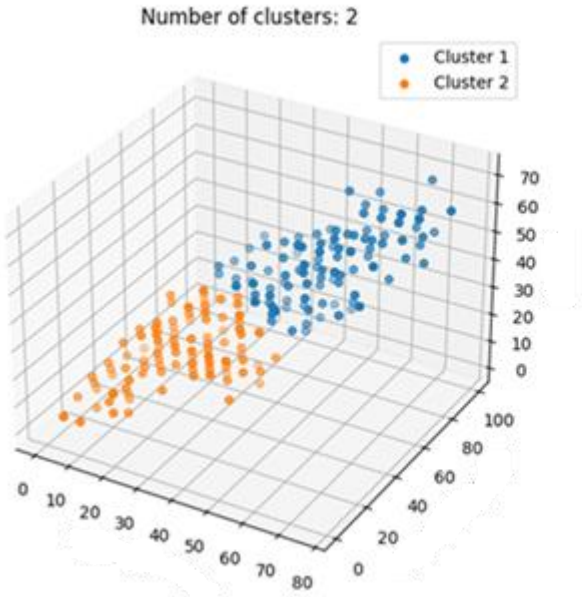
Какие данные собираем...

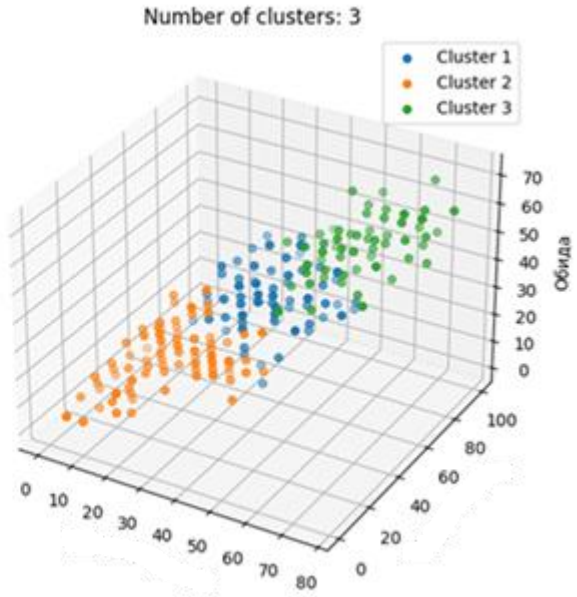


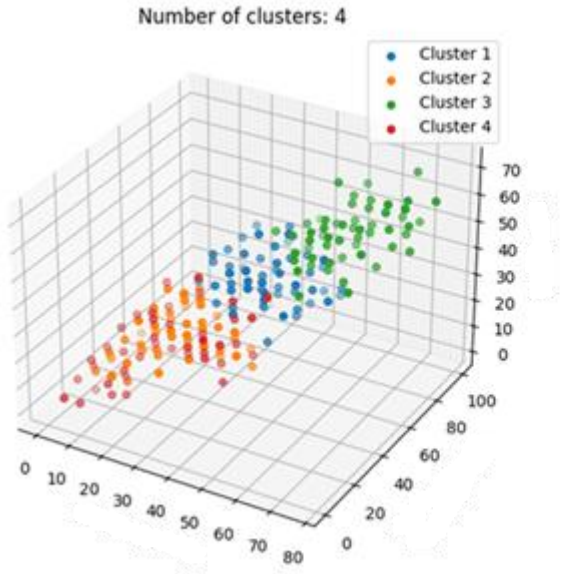
Выделяем группы...

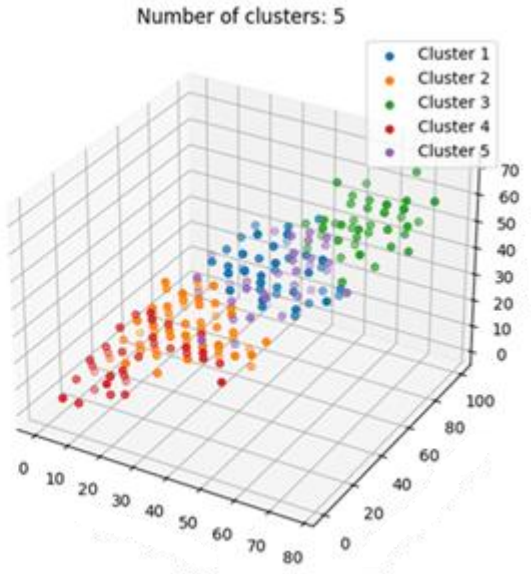


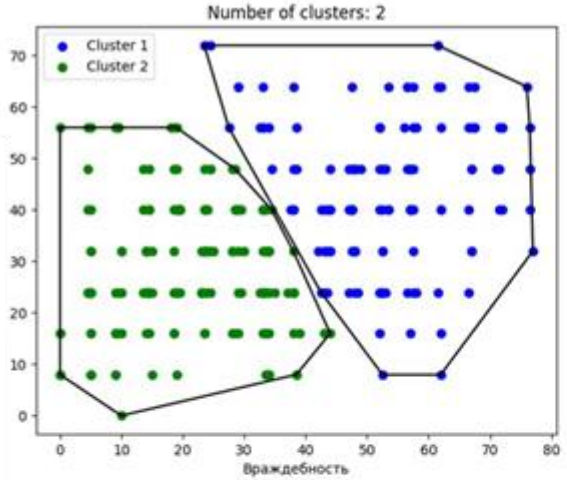
Выделение кластеров для подпространств

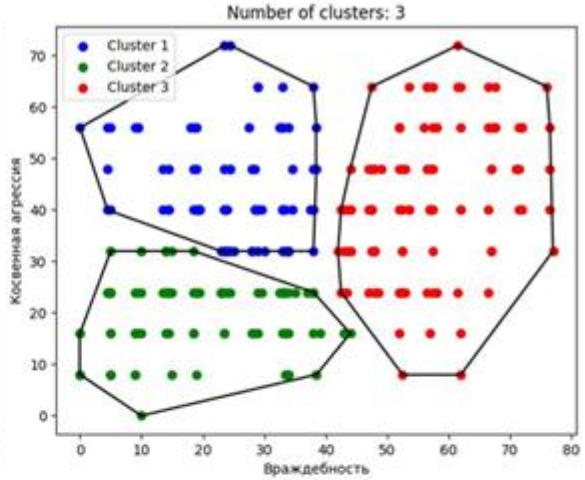


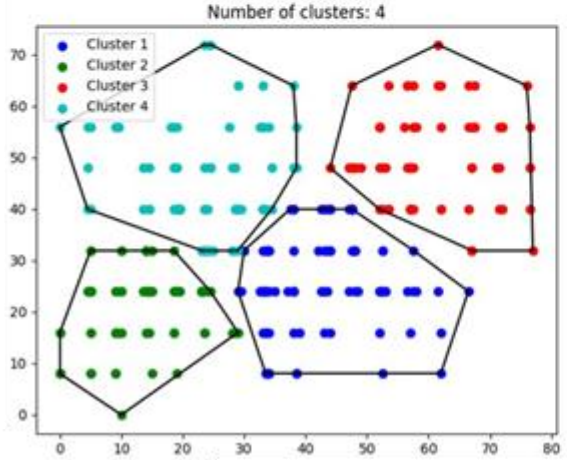


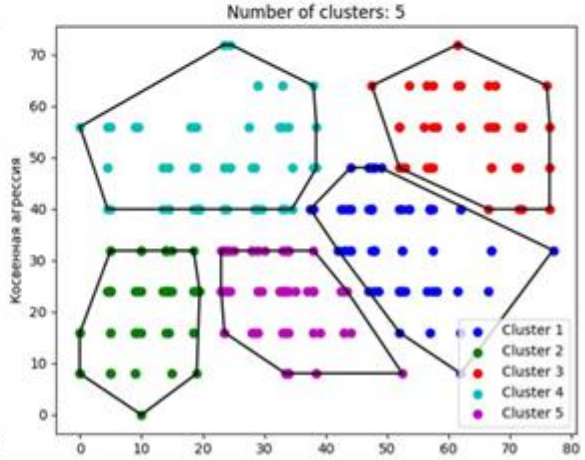


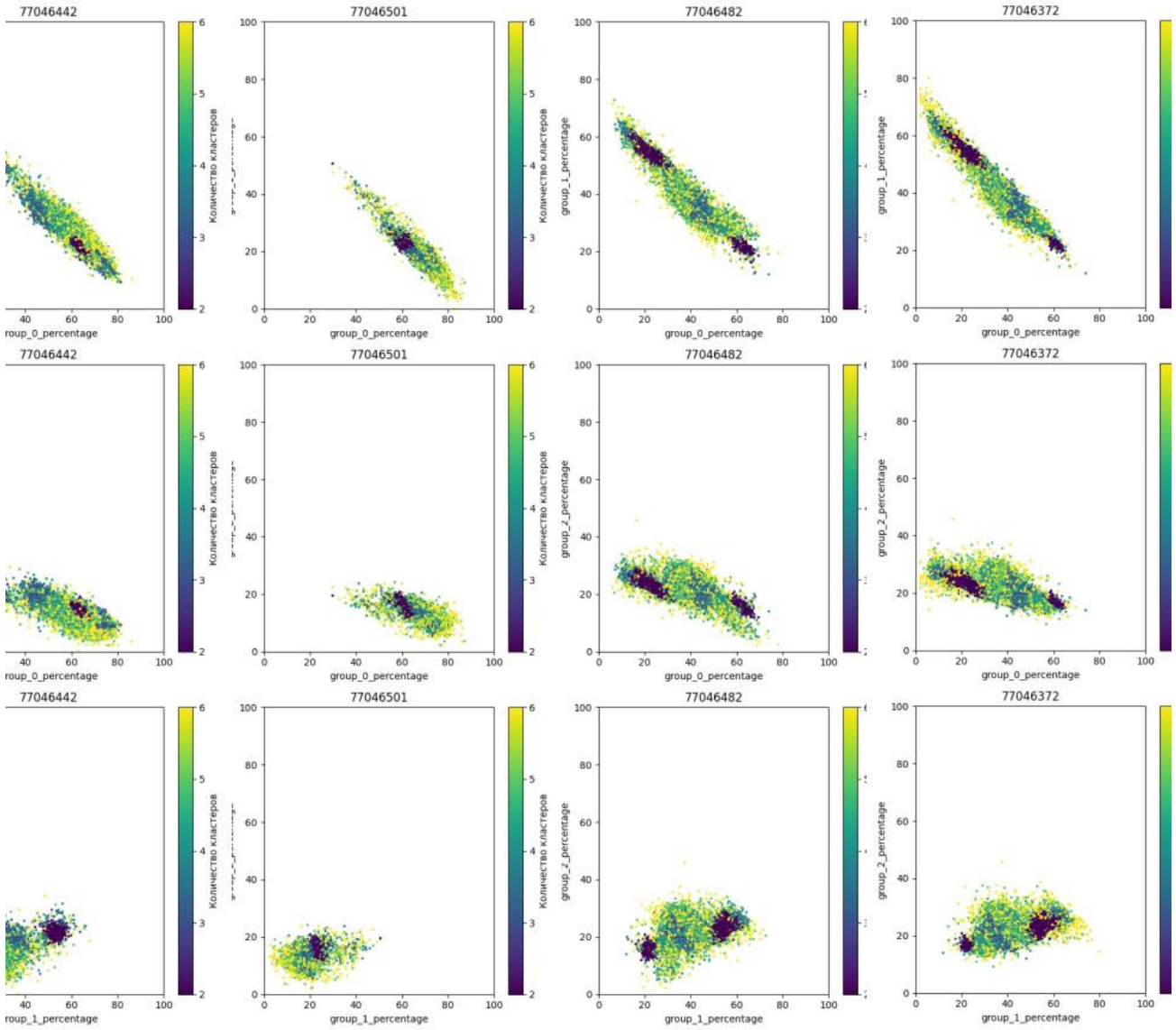




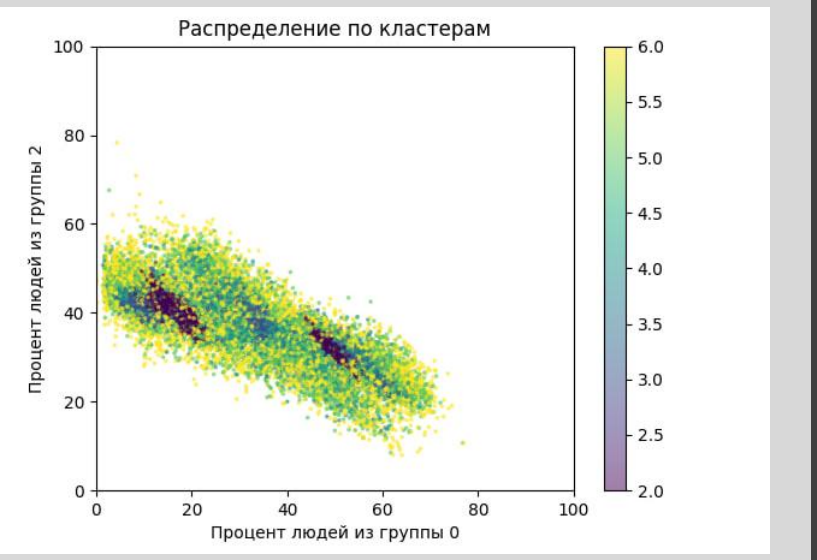


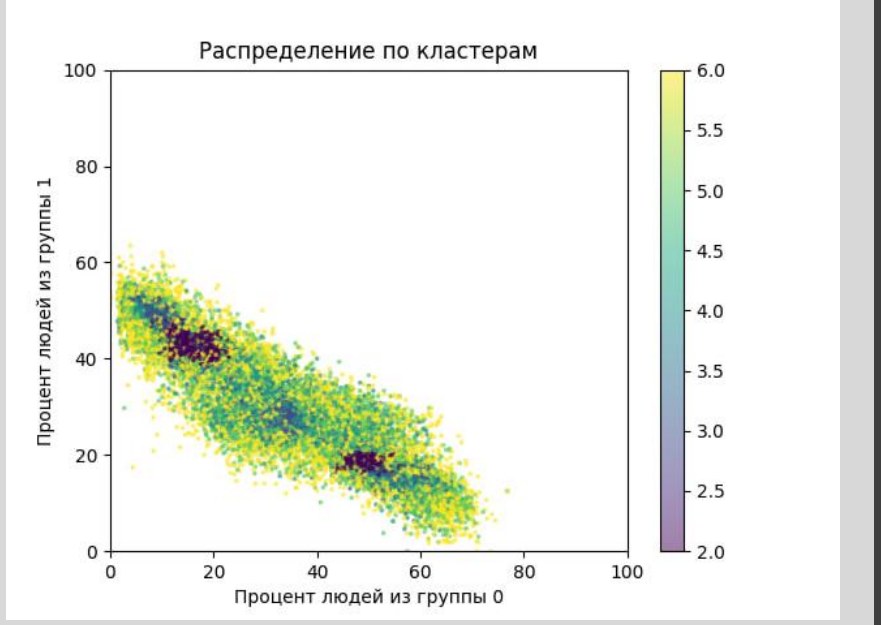


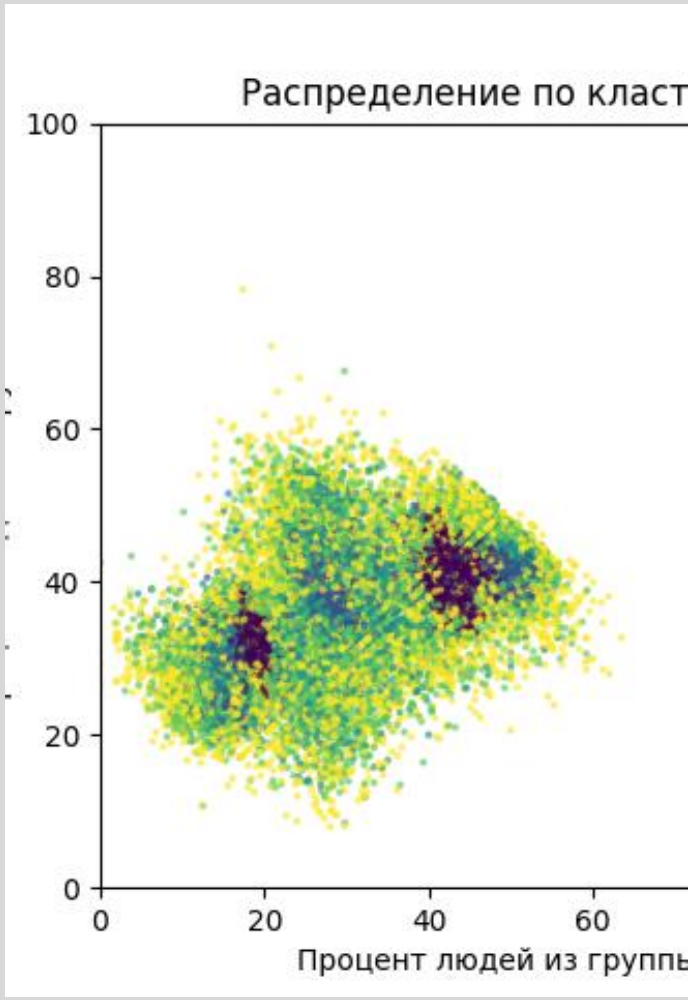




Поведенческие профили пользователей

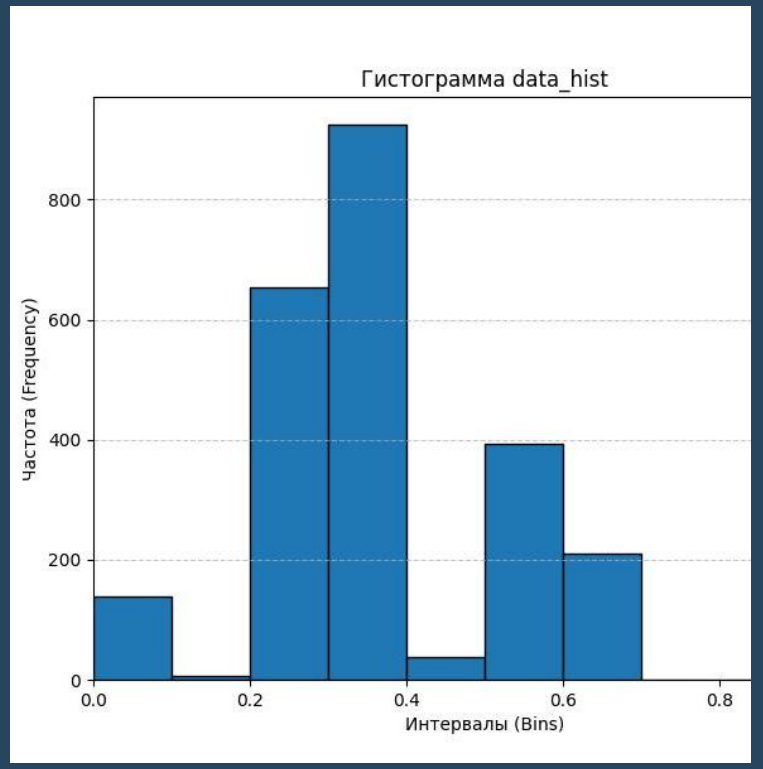


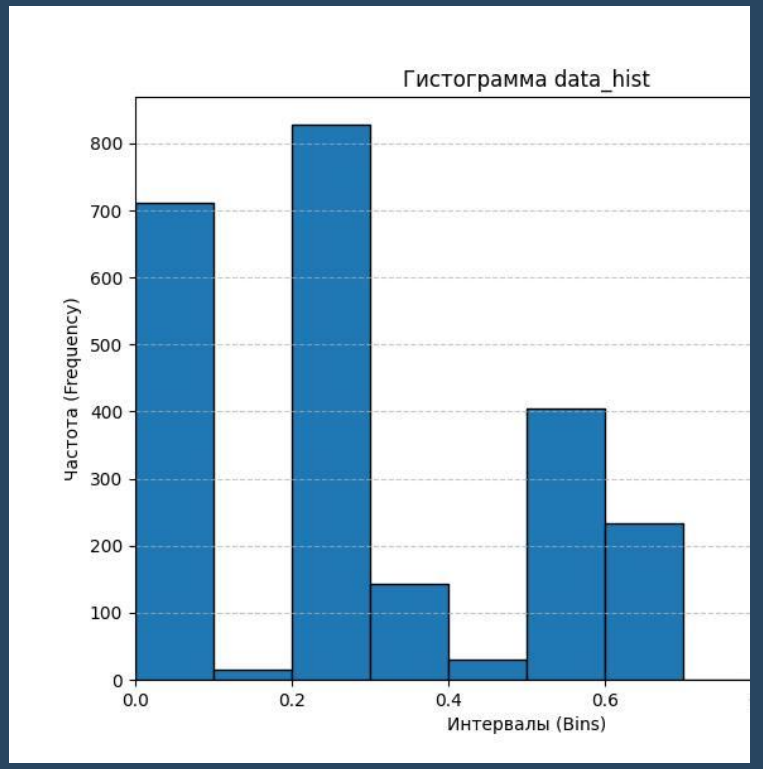


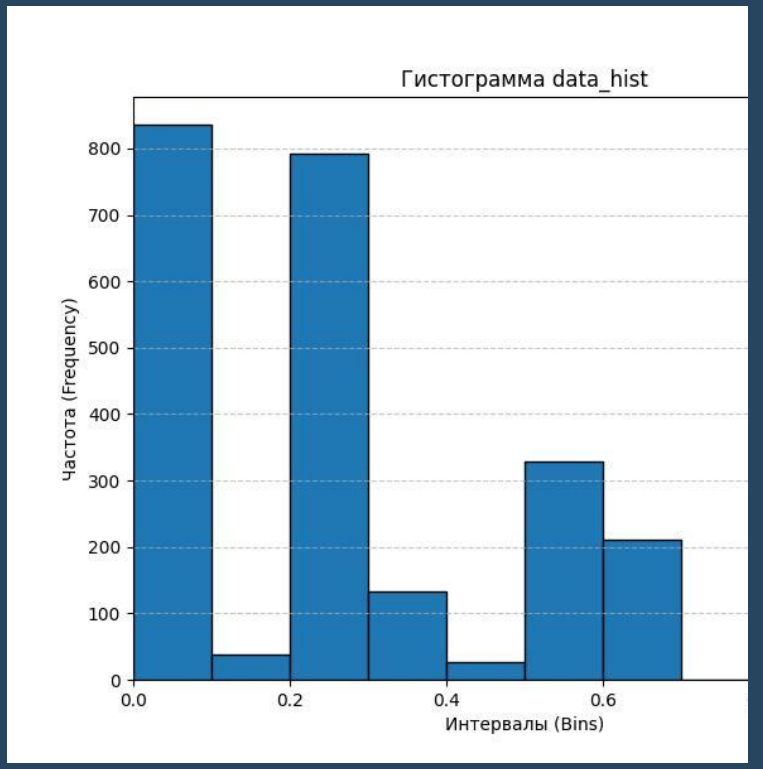


Распределение по всем кластерам

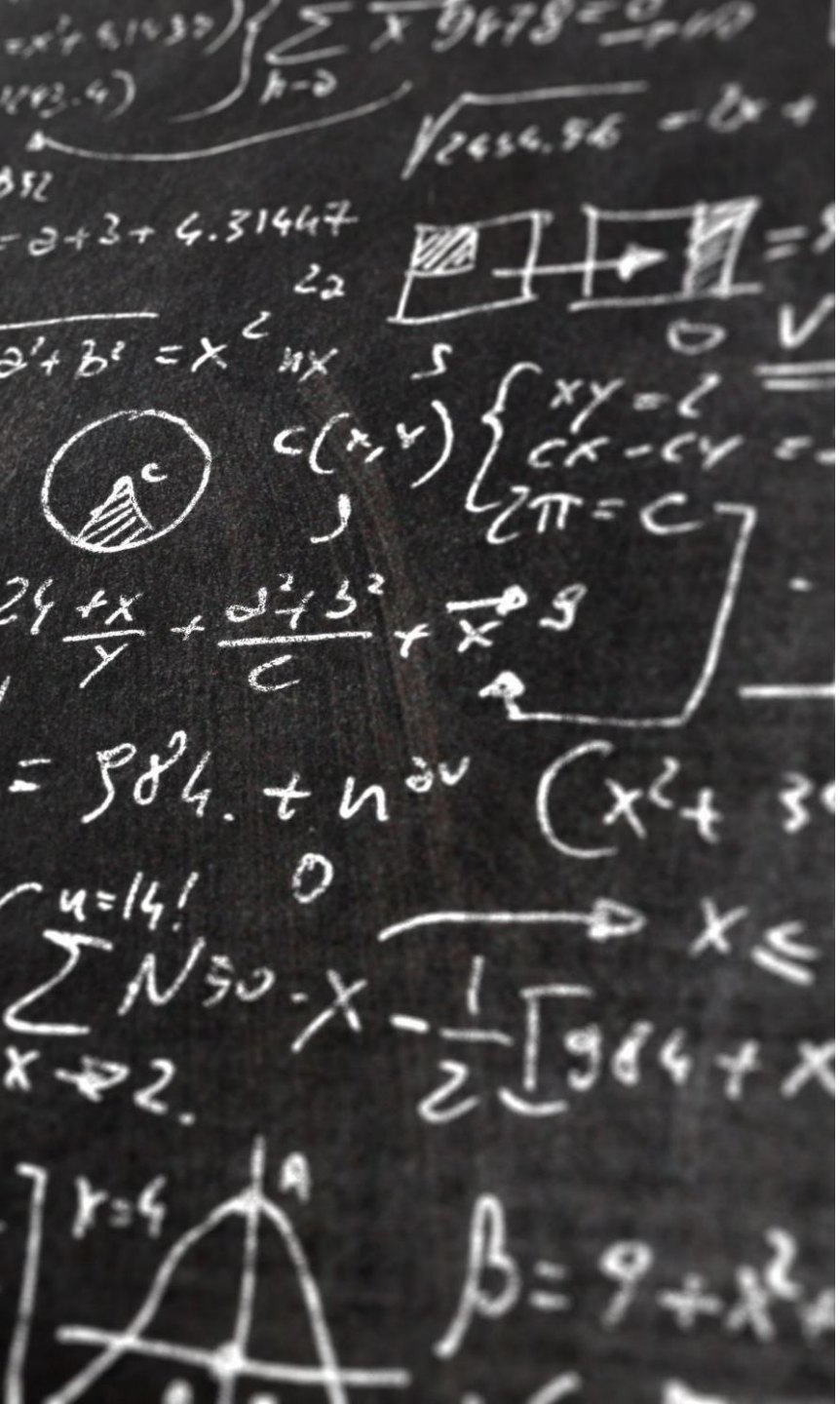
Здесь показано как выглядят смешанные поведенческие профили для всех пользователей, включённых в эксперимент







Индекс аномального поведения



Что в итоге…

- Внедрение поведенческого профиля в анализ поведения (UEBA, UBA).
- Построение теории поведенческих профилей
- Формализация процесса оценки индекса аномальной активности
- Разработка методологии оценки аномальной активности на длинных интервалах времени.

Спасибо за внимание!