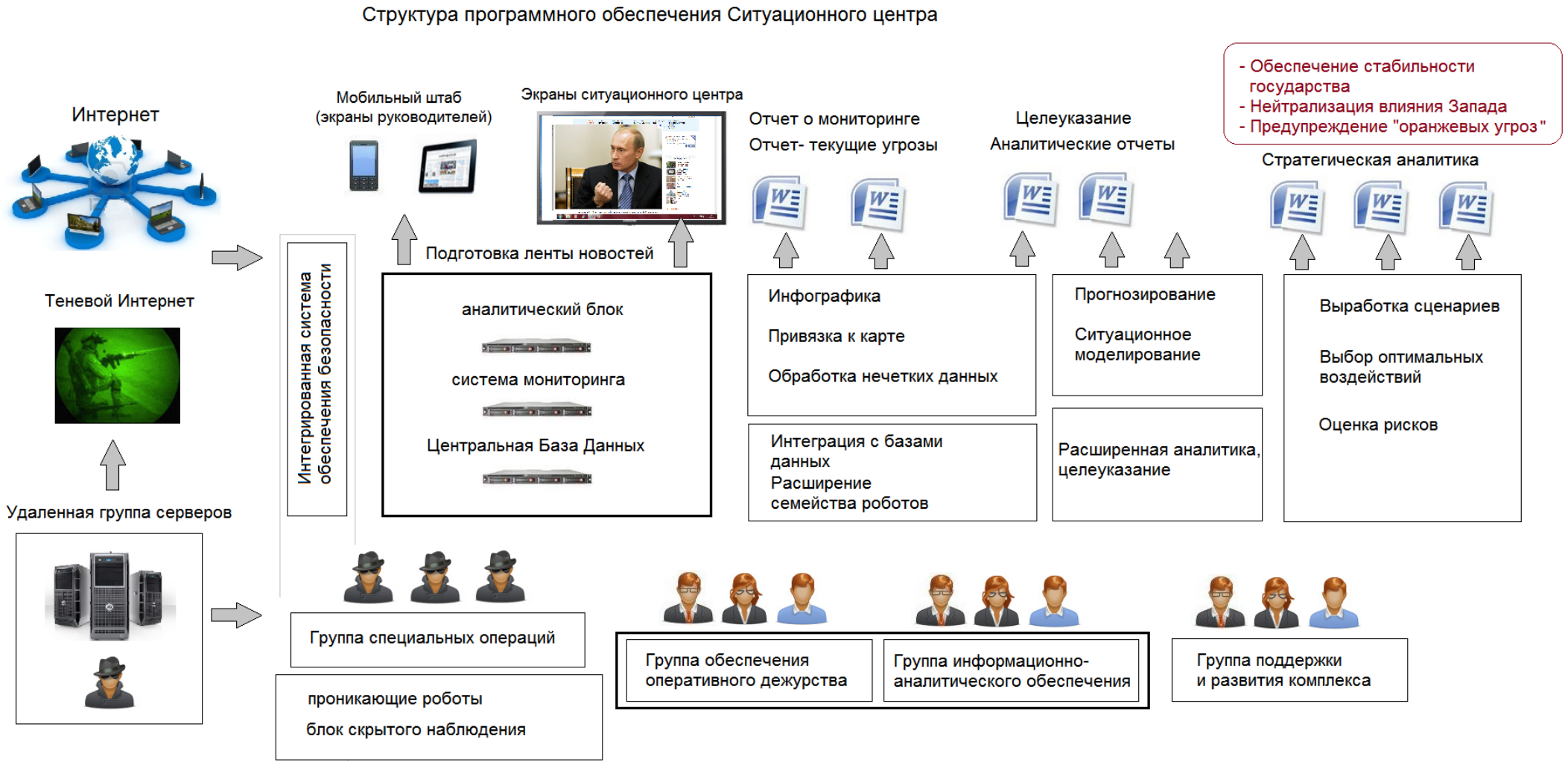
Система контроля оперативной обстановки в цифровом пространстве

Масалович Андрей Игоревич

Цель – раннее обнаружение и предупреждение информационных атак и противоправных действий

- Информационное обеспечение руководства
- Раннее обнаружение информационных угроз и оперативно-значимой информации
- Мониторинг активности и выявление информационных атак в социальных сетях;
- Активное информационное противоборство и парирование рисков;
- Контроль защищенности собственных информационных ресурсов.

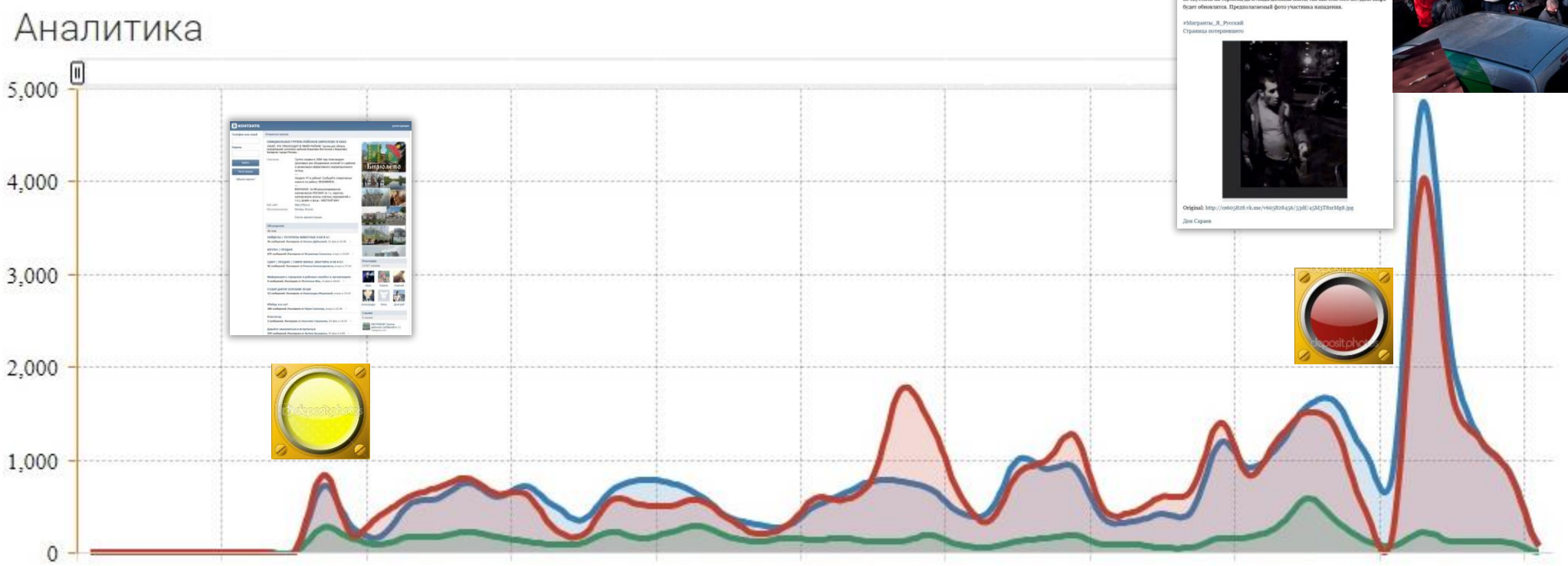
Система контроля оперативной обстановки Avalanche – основа построения ситуационных центров



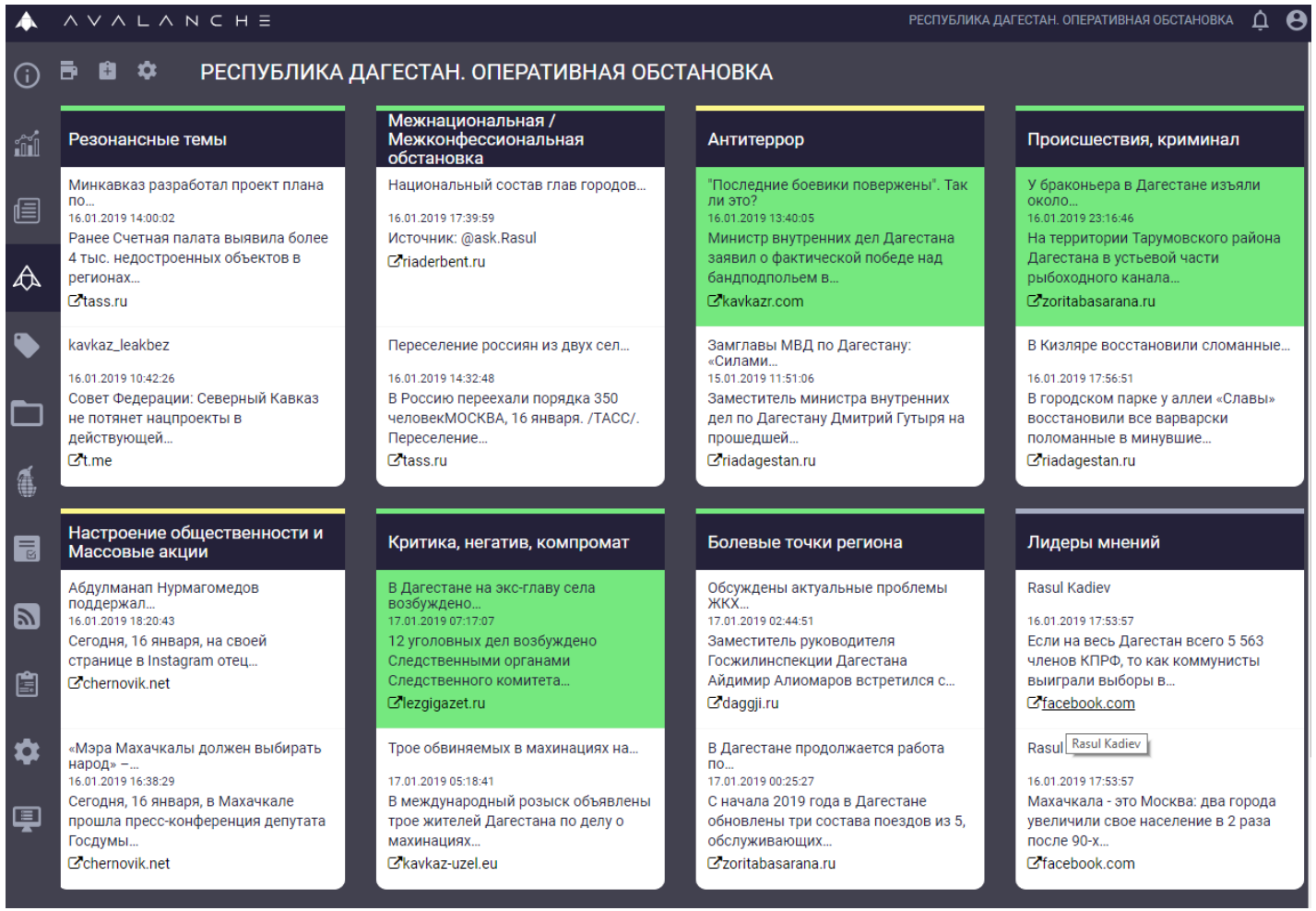
Пример упущенного контроля над ситуацией

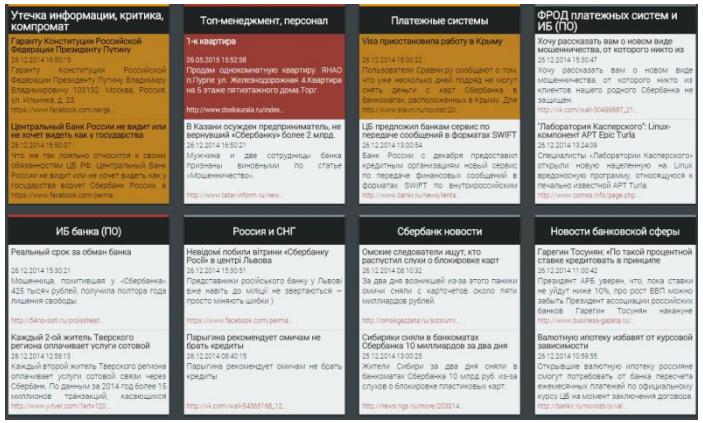
- Бирюлево, 10-13 октября 2013

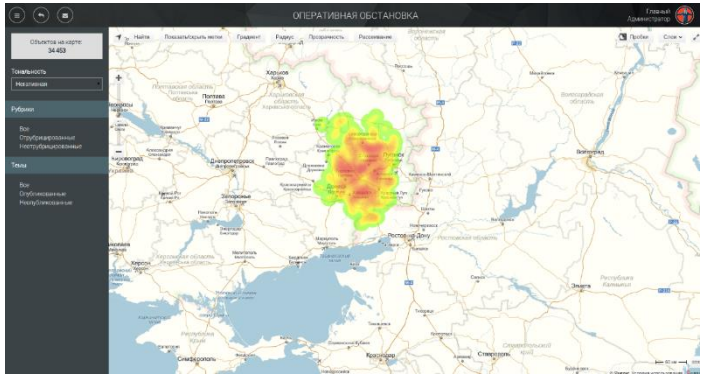
Отличие системы контроля обстановки от традиционного мониторинга



Контроль оперативной обстановки в регионе – Республика Дагестан

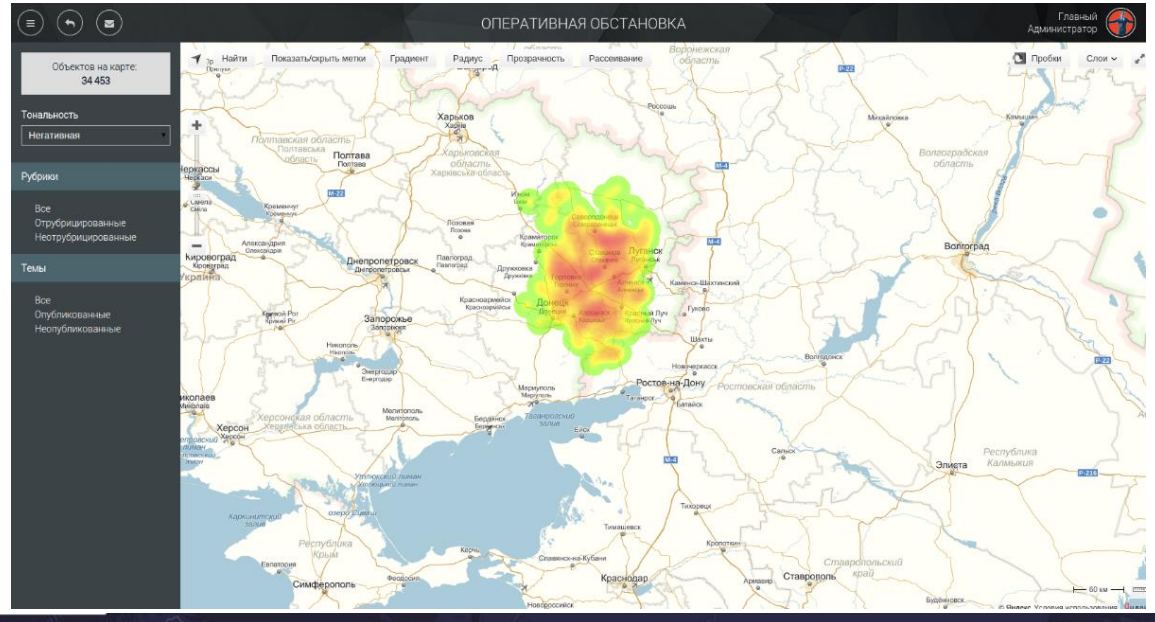


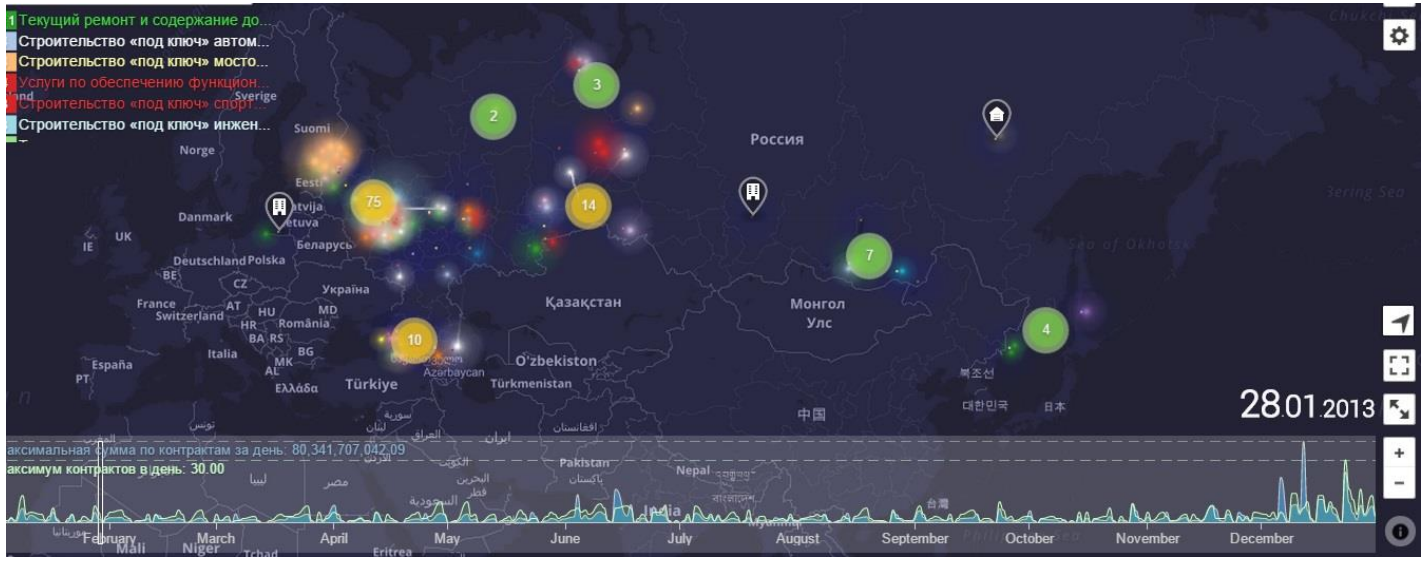




AVALANCHE

Тепловая карта активности в социальных сетях





AVALANCHE

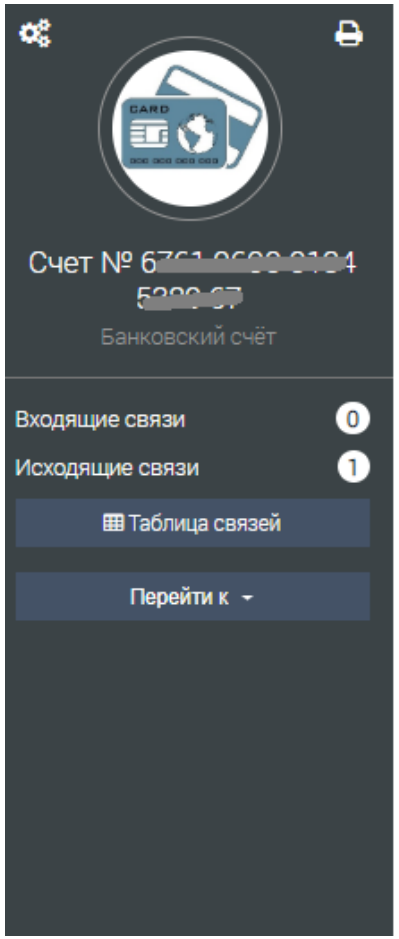
Оперативное оповещение руководителей

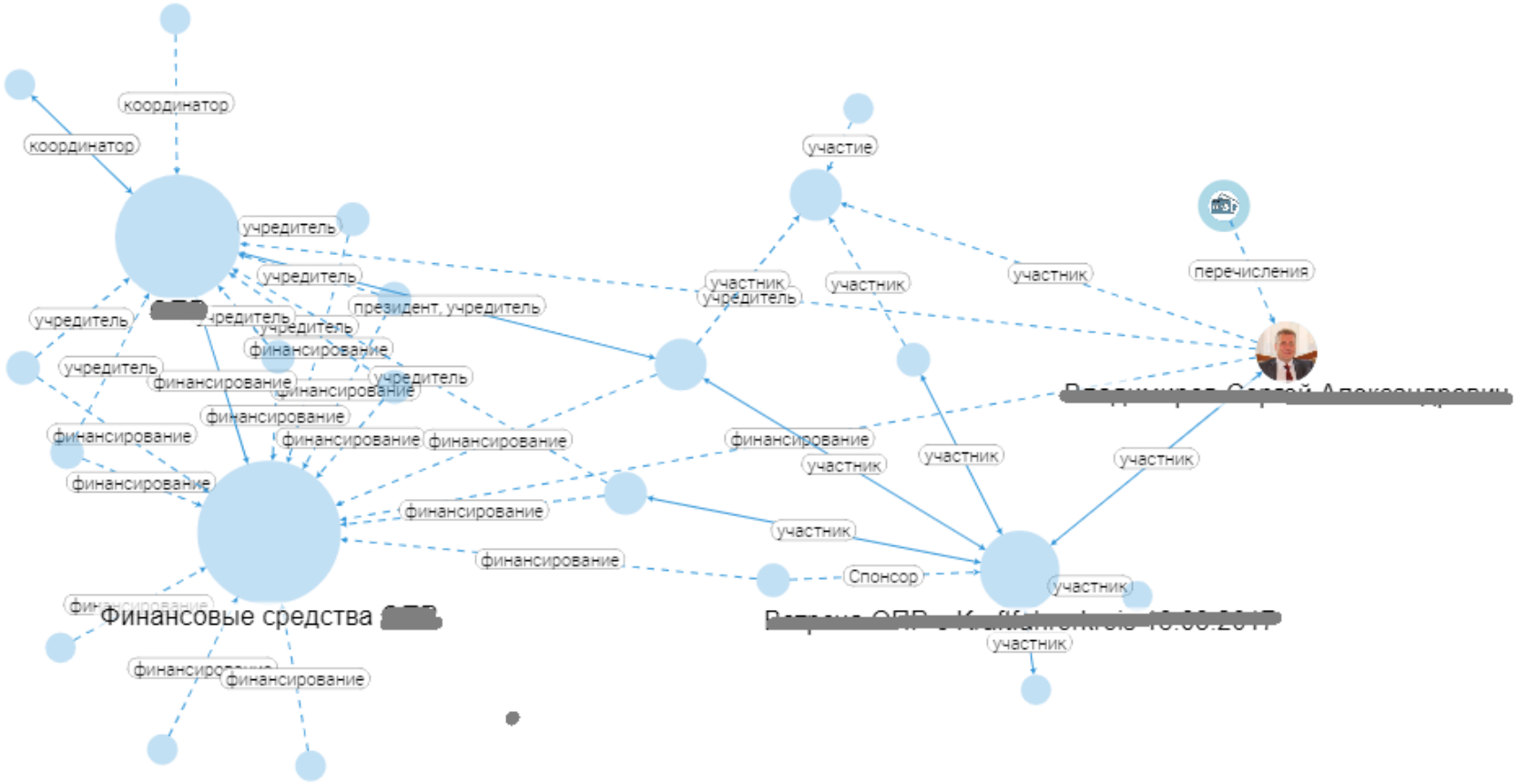
Анализ активности в социальных сетях: Муфтият Дагестана

Движение Карфаген в социальных сетях (Дагестан)

Пример: мониторинг беспорядков при повышении тарифов на систему Платон

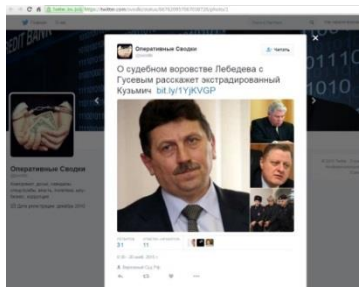
Организаторы беспорядков: Анализ графов связей

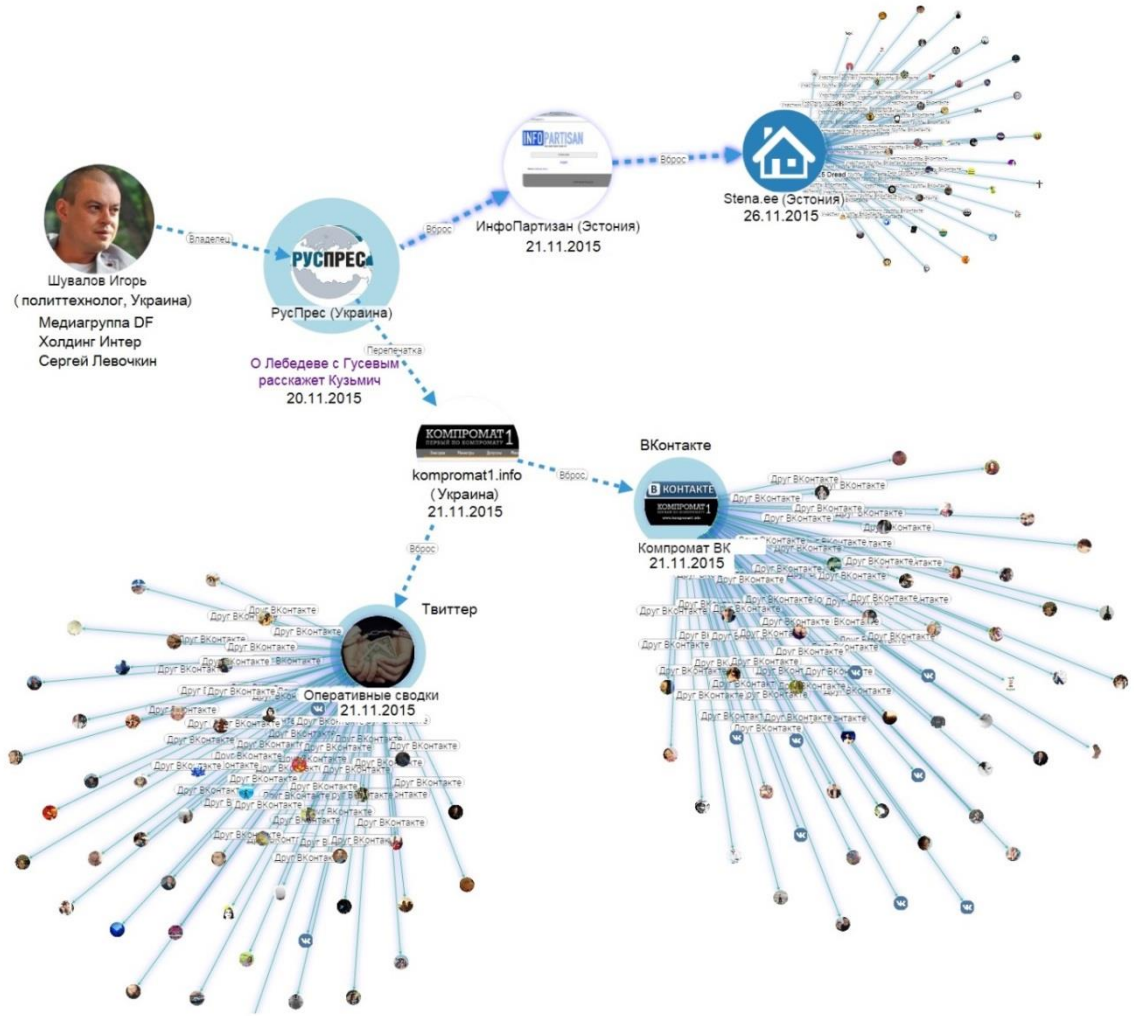




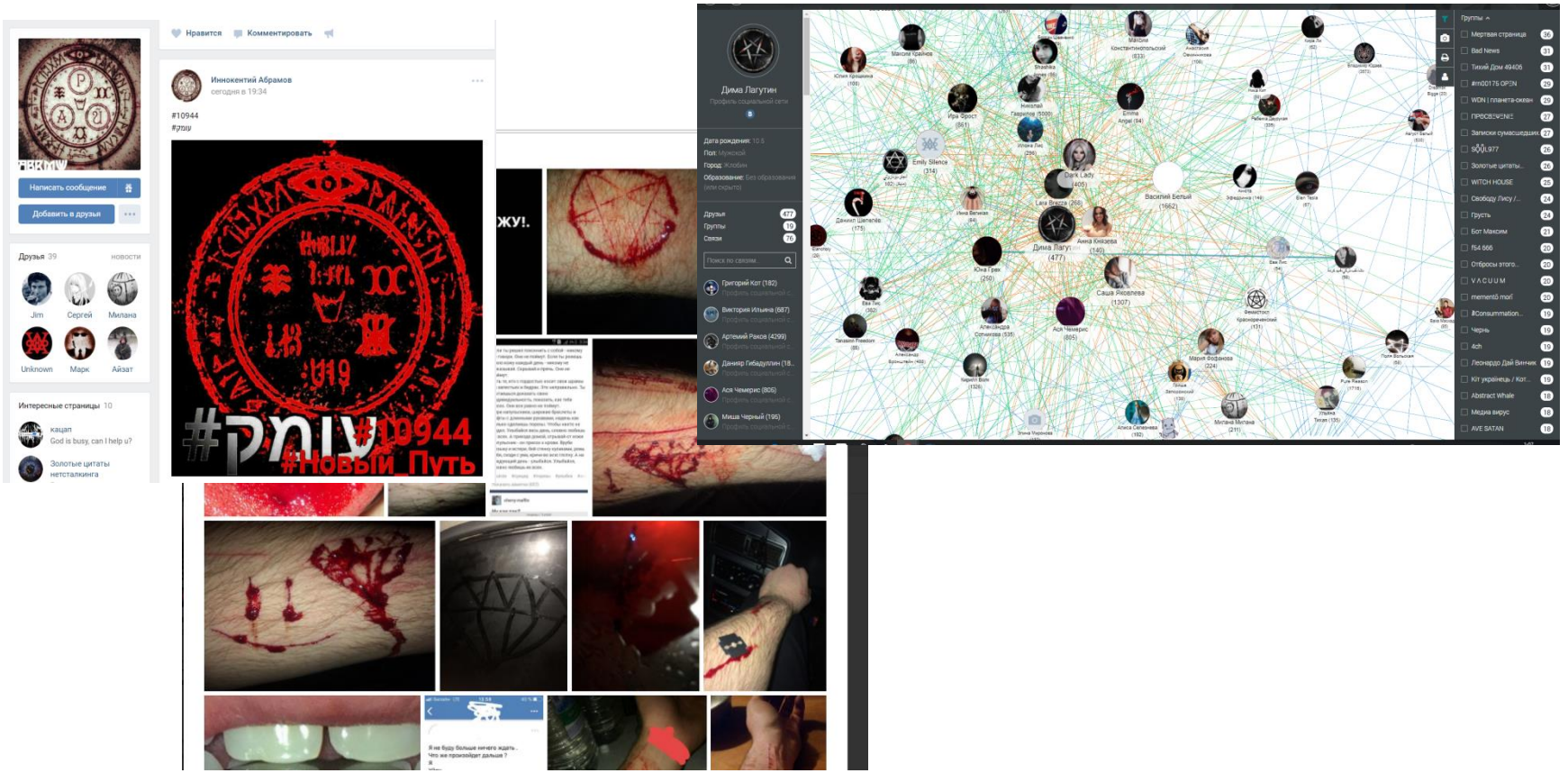
AVALANCHE

Анализ источников информационных вбросов





«Синий кит», «Красная сова»
суицидные группы подростков



Технологии многоуровневого вовлечения

Как это устроено?

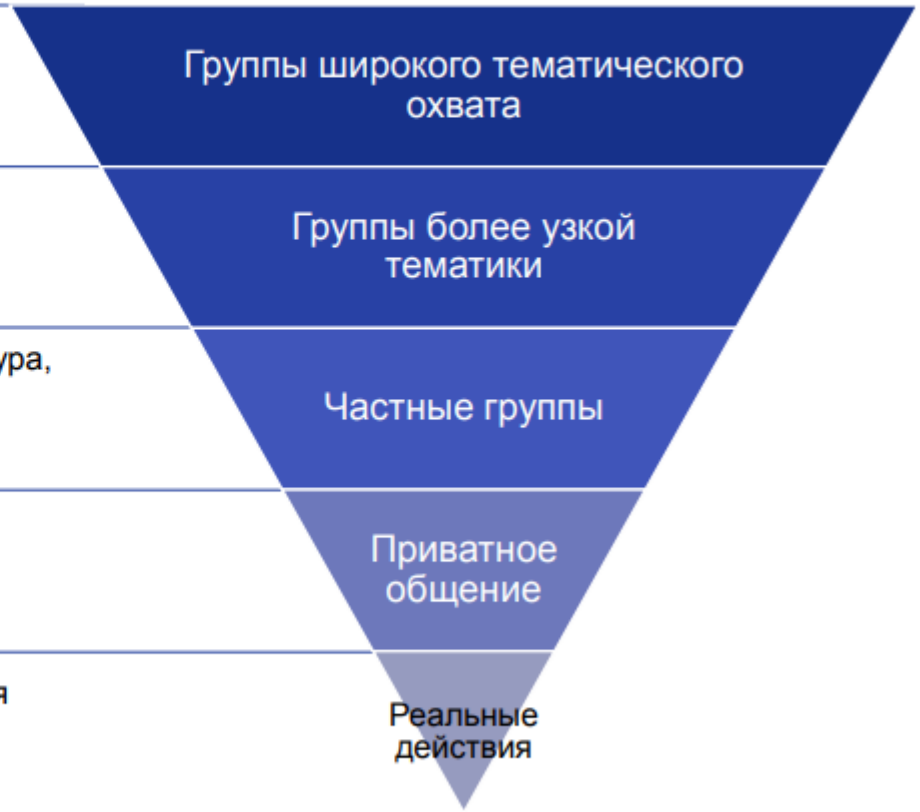
Группы по темам (самоубийства, травля, депрессия): общая информация, пропаганда темы, доступно для всех

Для тех, кто «созрел». Есть условия вступления. Чтоб оставаться членом, надо выполнять задания. Появляется иерархия власти.

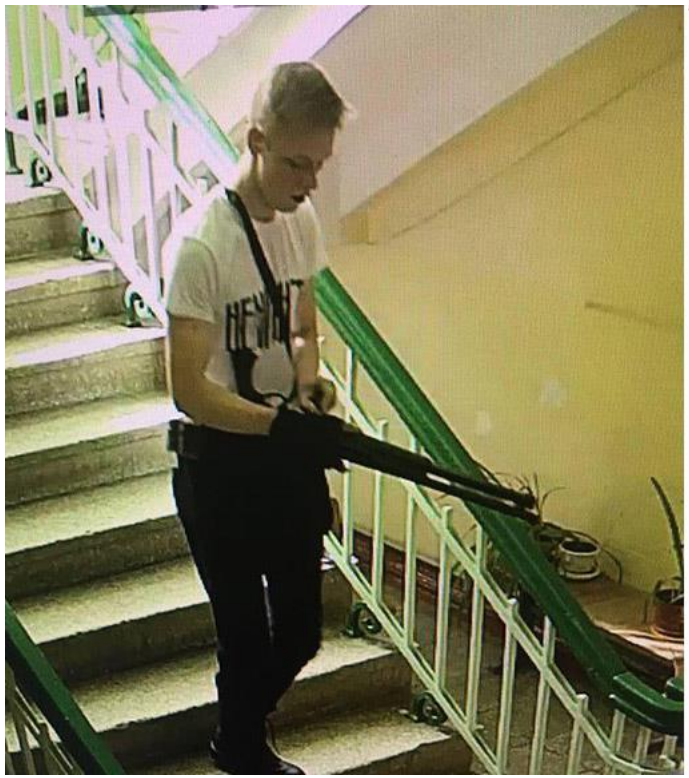
Конкретное течение в теме. Есть собственная культура, которую надо соблюдать, чтоб быть «своим»

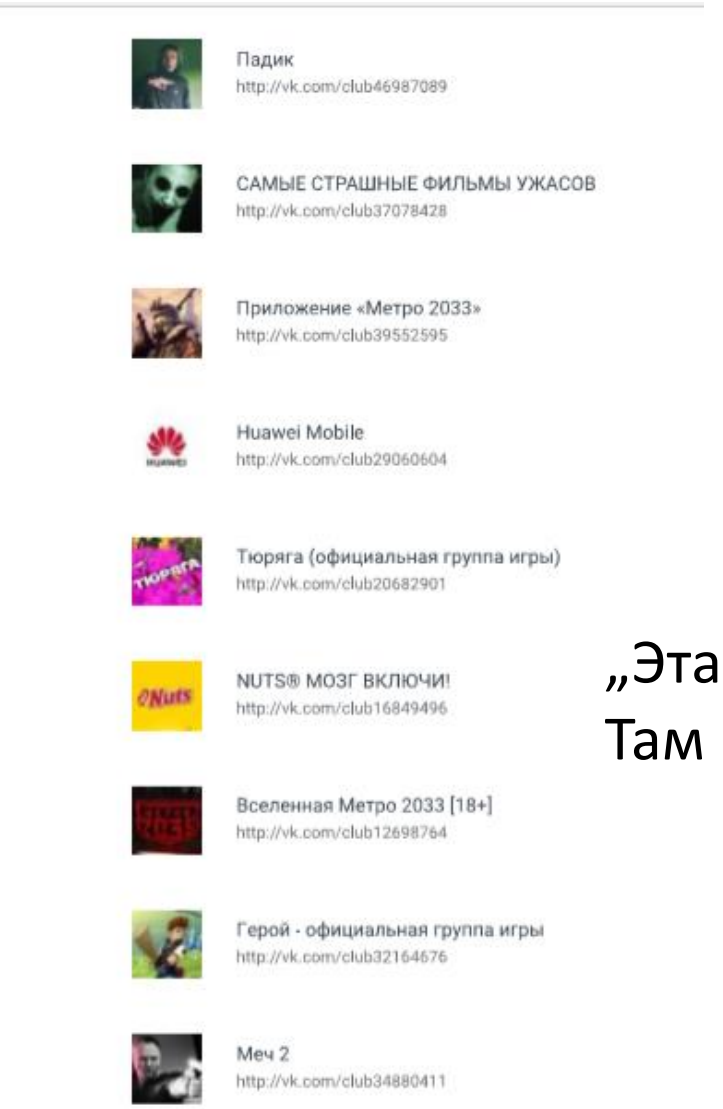
«Избранные» переводятся в закрытые чаты и личные сообщения. Появляется реальный статус в реальном мире.

Выполнение заданий, поступающих виртуально, для реального мира. Создается ощущение близости, повышается статус в группе. Даются бонусы.



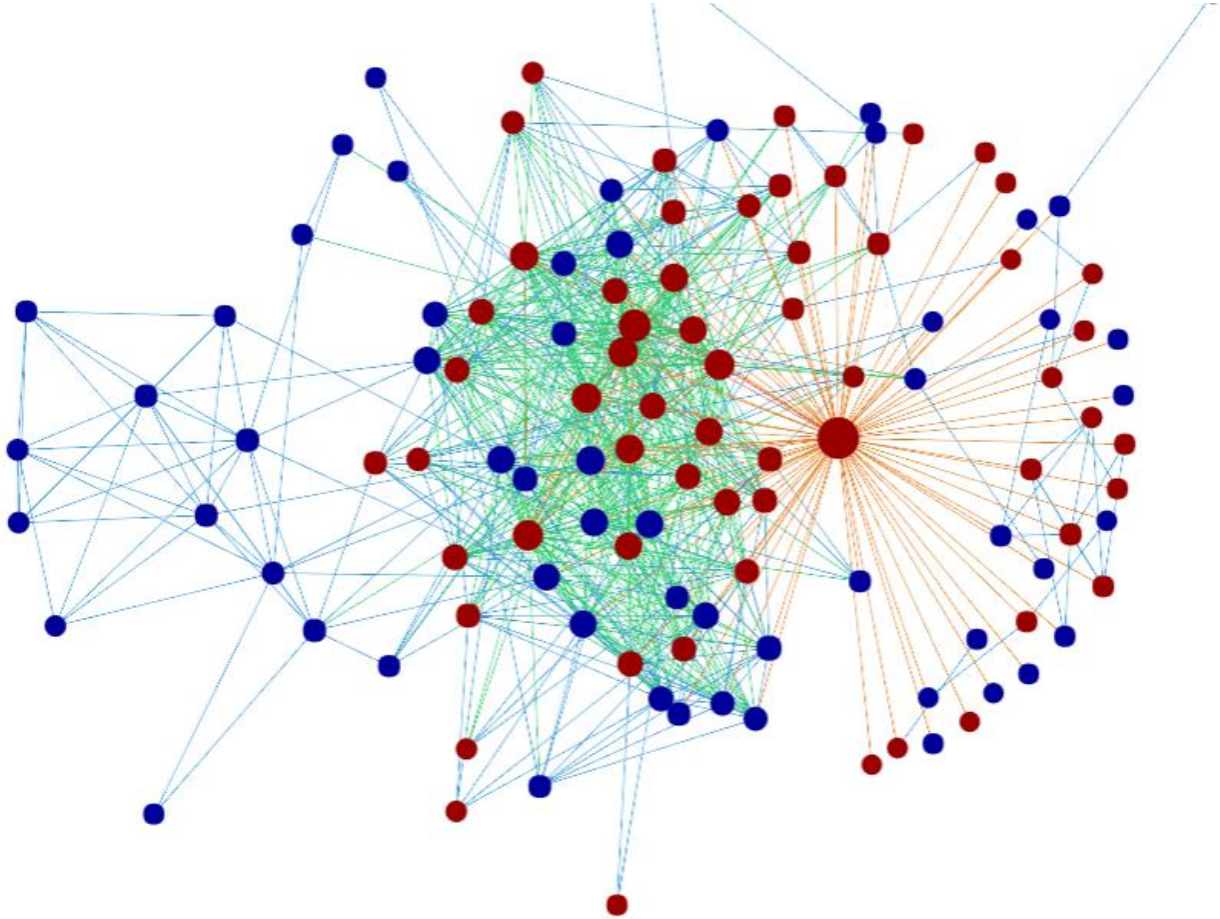
«Керченский стрелок»

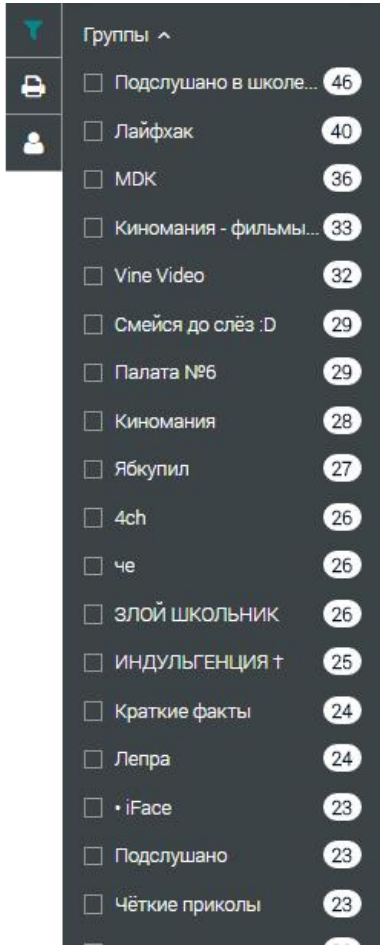




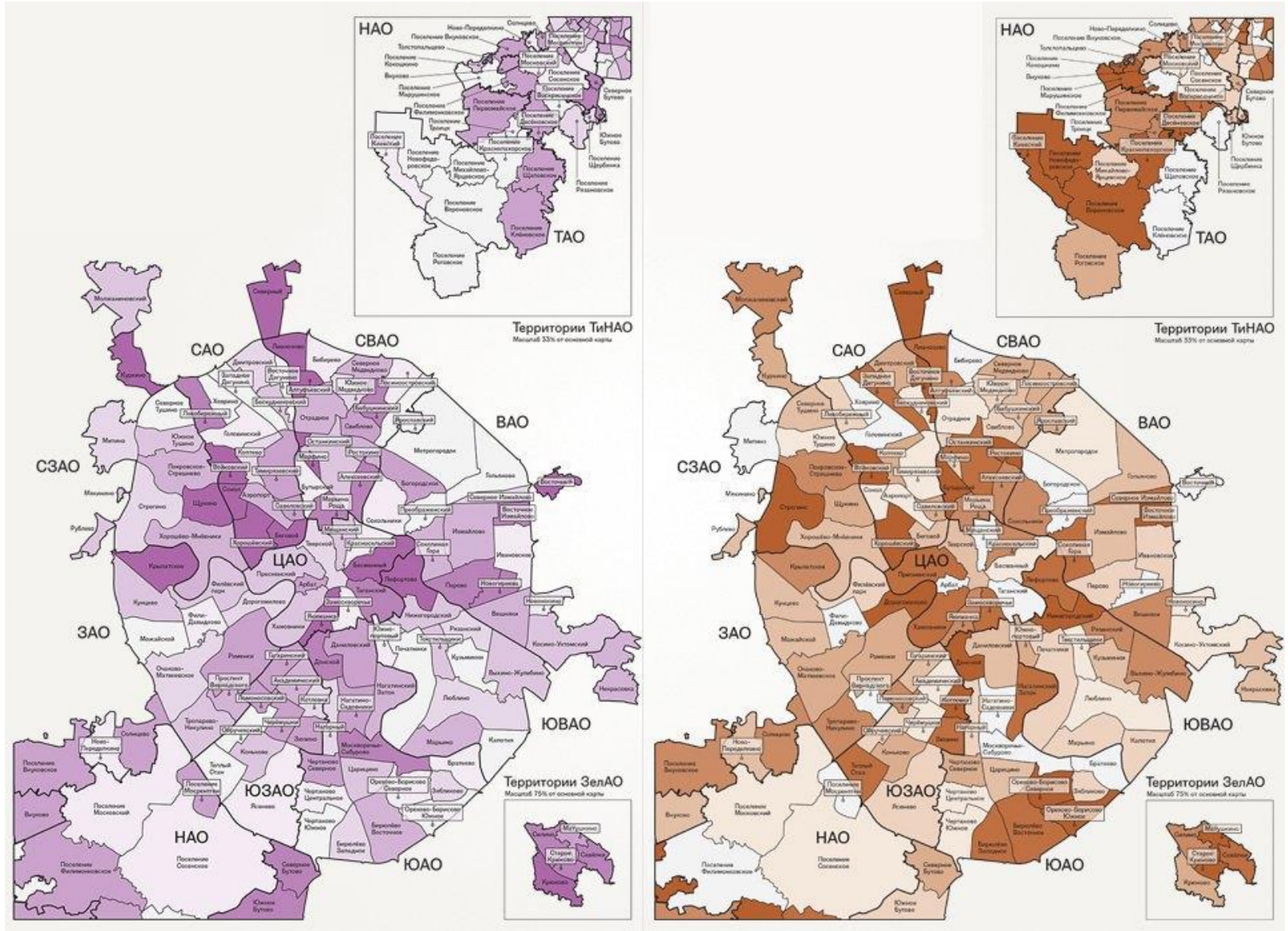
„Эта игра из меня чуть психа не сделала. Там все несправедливо к людям“

Социальный портрет - подросток

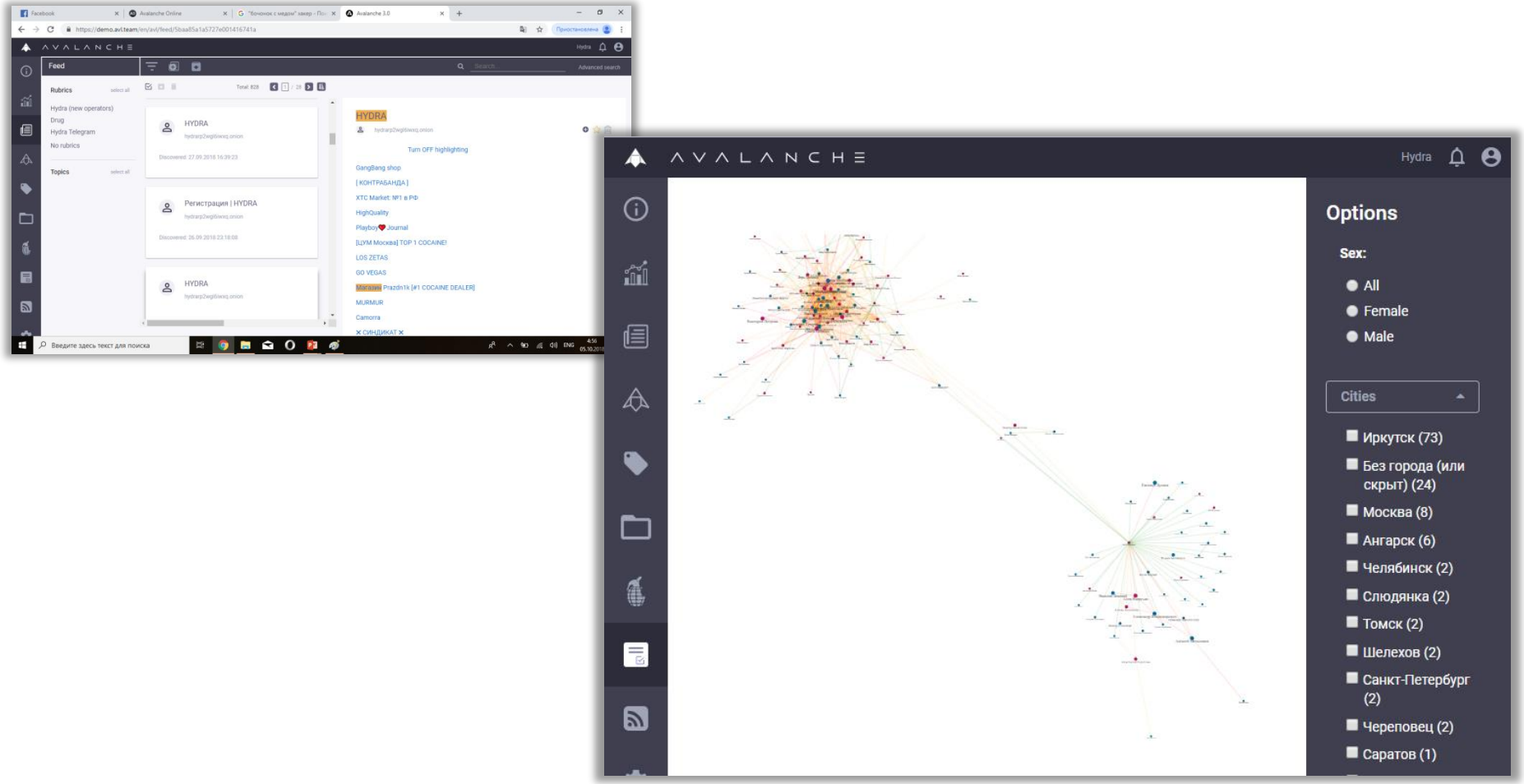




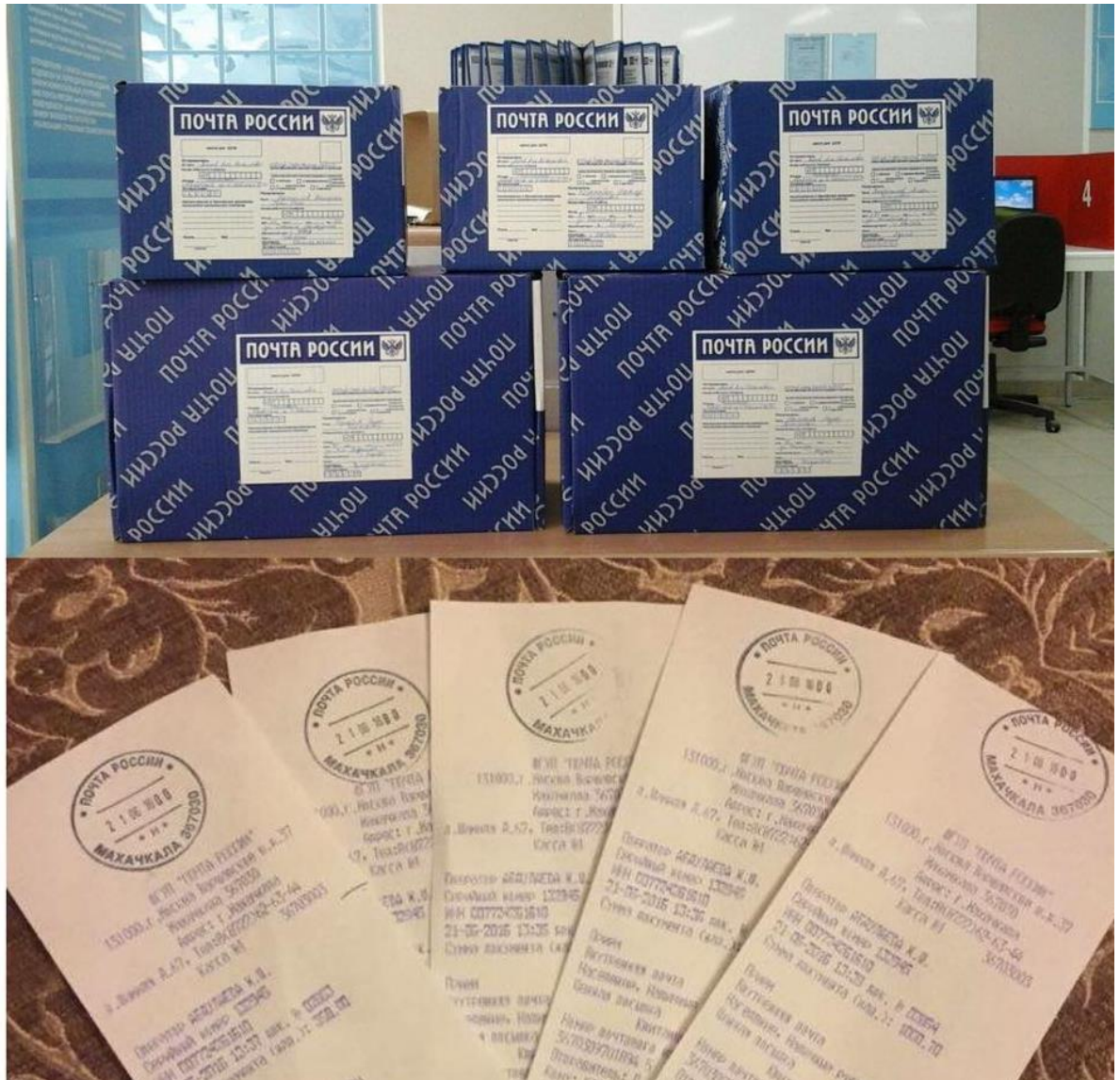
Тепловые карты обстановки в городе



Работа в «сером» и «черном» интернете (TOR и др) – пример групп Hydra



Разведка по открытым источникам



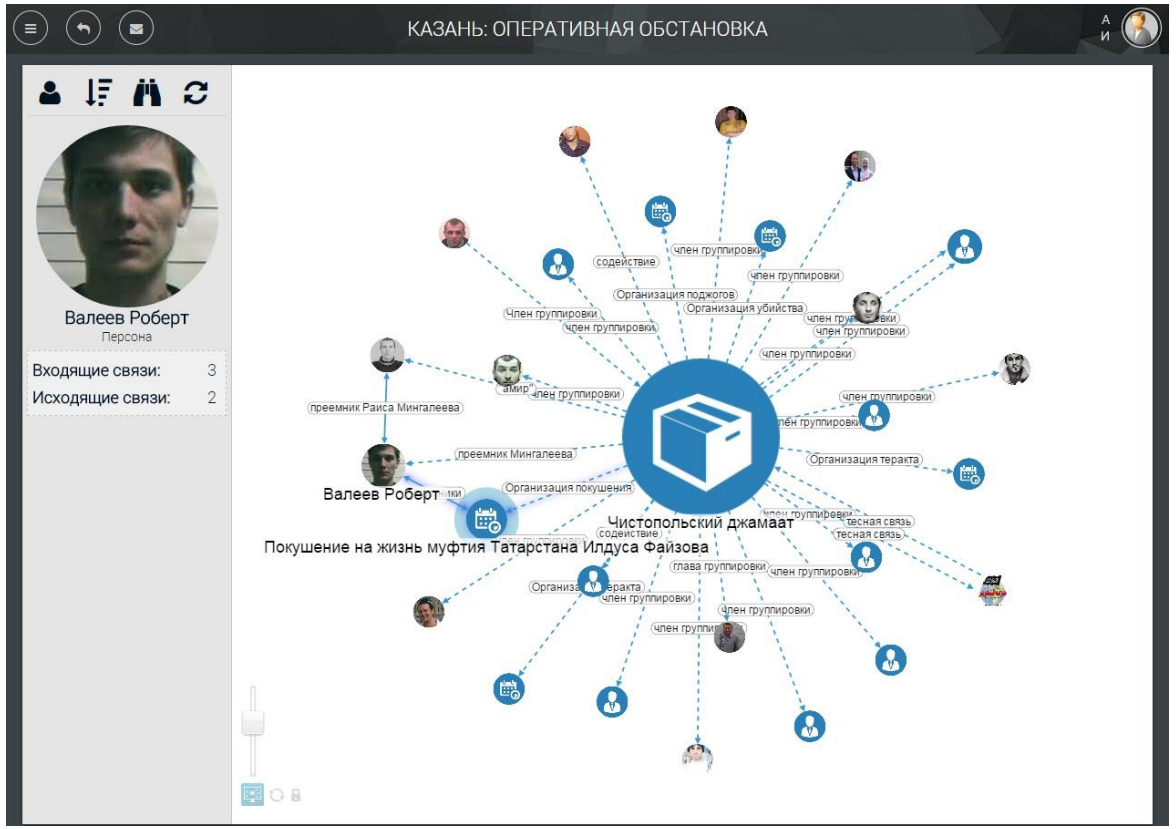
Пример: контроль оперативной обстановки

Казань, чемпионат мира по водным видам спорта, 2015

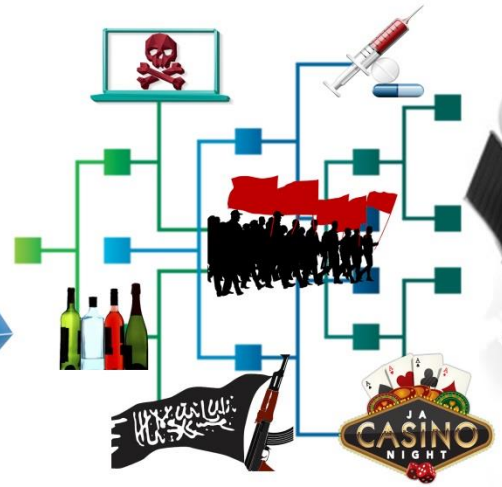
FINA WORLD CHAMPIONSHIPS
KAZAN
RUSSIA 2015

- Общая обстановка
- Освещение ЧМ, критика
- Митинги, выступления
- Радикалы, оппозиция
- Межконфессиональные
- Межнациональные
- Правонарушения
- Радикальный ислам
- Критика полиции

Анализ связей остатков группировки «Чистопольский джамаат»



Ситуационный центр органов государственной власти по мониторингу угрозообразующих факторов жизнедеятельности города Москвы



Мониторинг угрозообразующих факторов жизнедеятельности г. Москвы В СМИ и сети Интернет

Ситуационный центр правительства города Москвы

Автоматизированный механизм поиска и анализа

Оценка и идентификация криминогенной информации в сети интернет

Хранение и систематизация данных по объектам и видам угроз

Сигнализация угроз и рисков

Принятие решения на основе аналитических результатов

ЧТО ДЕЛАТЬ?

- **Люди** – Обучить
- **Процессы** - Настроить
- **Технологии** – Внедрить

ЛЮДИ

- Китай открывает 5 учебных центров по кибербезопасности по 10 000 специалистов
- Сингапур оценивает свои потребности в специалистах по ИБ в 15 000 человек

Первый шаг – ЭКСПРЕСС-КУРСЫ

- *Для руководителей*
- *Для специалистов*
- *Для пользователей*

Основам безопасности можно научить за один день

ПРОЦЕССЫ

Контроль обстановки в киберпространстве

AVALANCHE

ТЕХНОЛОГИИ

- Системы контроля оперативной обстановки
- Системы раннего предупреждения
- Аналитическая обработка больших данных
- Ситуационные центры нового поколения

Первый шаг – системы контроля оперативной обстановки

Технологическая платформа **Avalanche** в арсенале Ситуационных центров

- Технология разработана более 15лет назад
- Комплекс интернет-разведки, мониторинга и анализа
- Более 20 типов поисковых роботов
- Контроль «серого» (глубинного) Интернета
- Автоматические «светофоры» уровня угроз
- Раннее обнаружение информационных атак

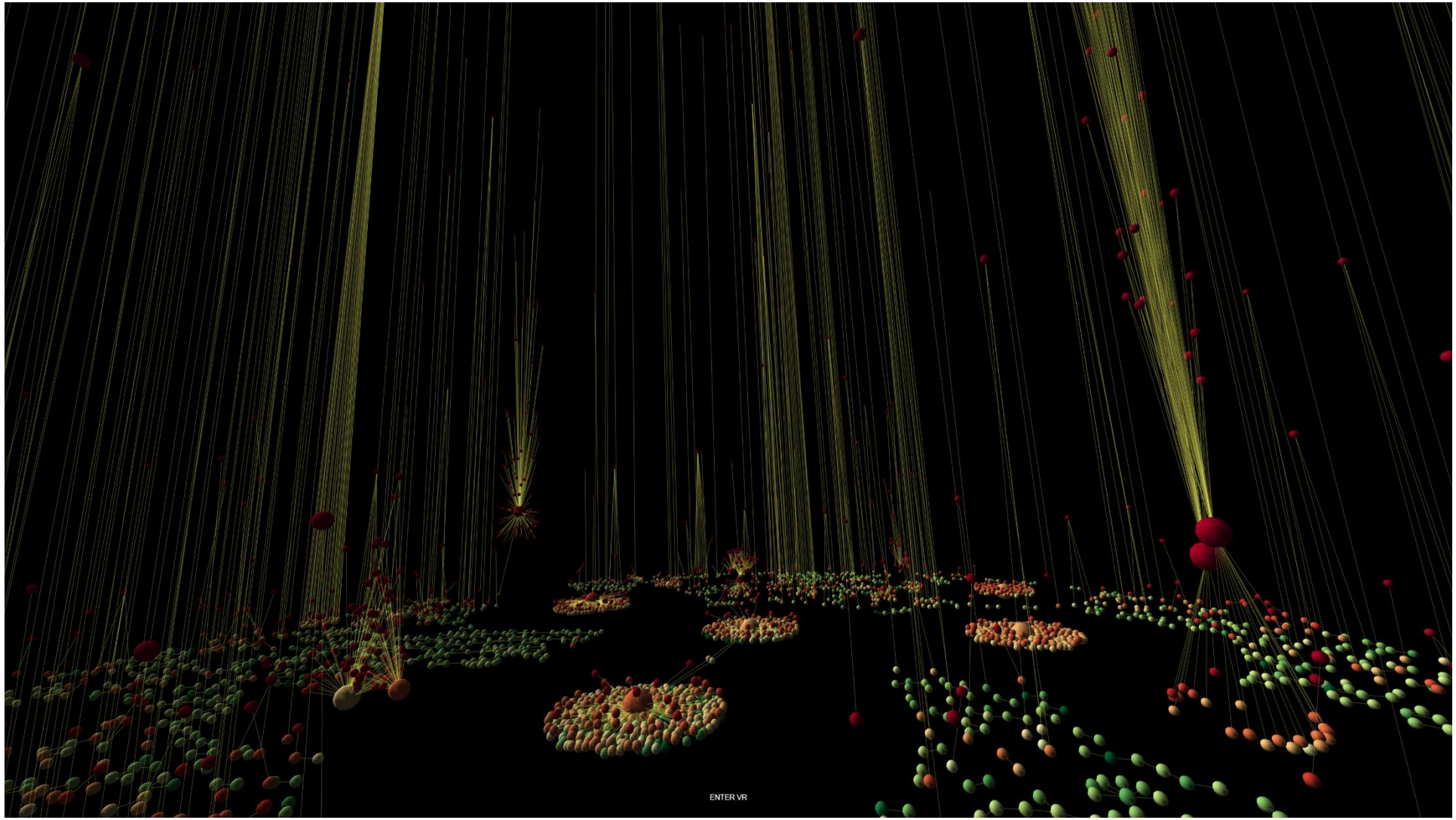
Система контроля оперативной обстановки

- Своя матрица интересов и угроз для каждого подразделения
- Разделение прав доступа по ролям, проектам, персонам
- Одно- или двухфакторная авторизация
- Защищенное хранение, шифрованный трафик
- Ведение логов активности сотрудников
- Мгновенное оповещение о важных событиях
- Комплексный мониторинг – СМИ, соцсети, «серый интернет»
- Контроль источников угроз и оперативной информации
- Расширяемый набор источников, рубрик и тем
- Автоматическое отображение уровня угроз («светофоры»

Step to the Web

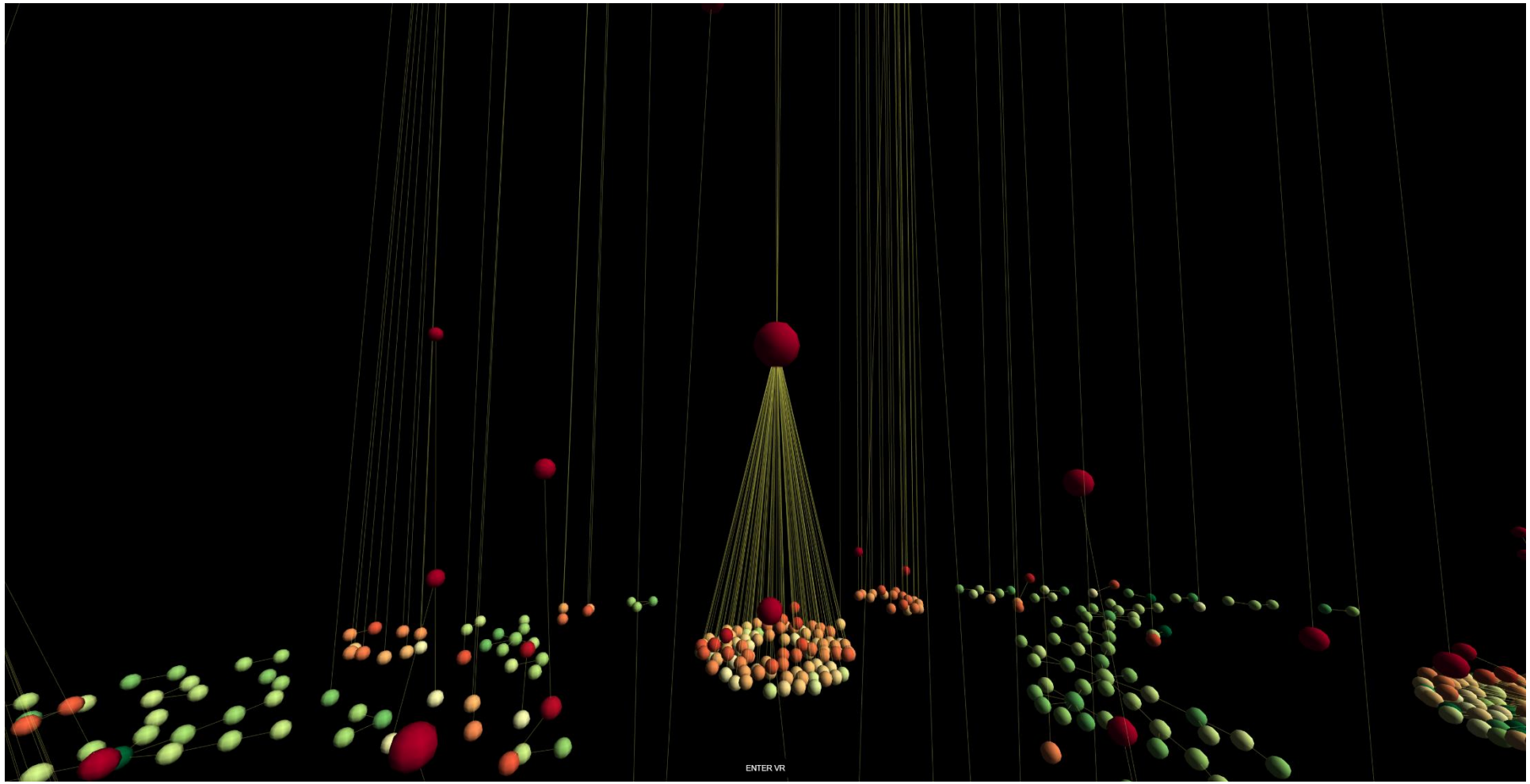
AVALANCHE

One minute inside Twitter



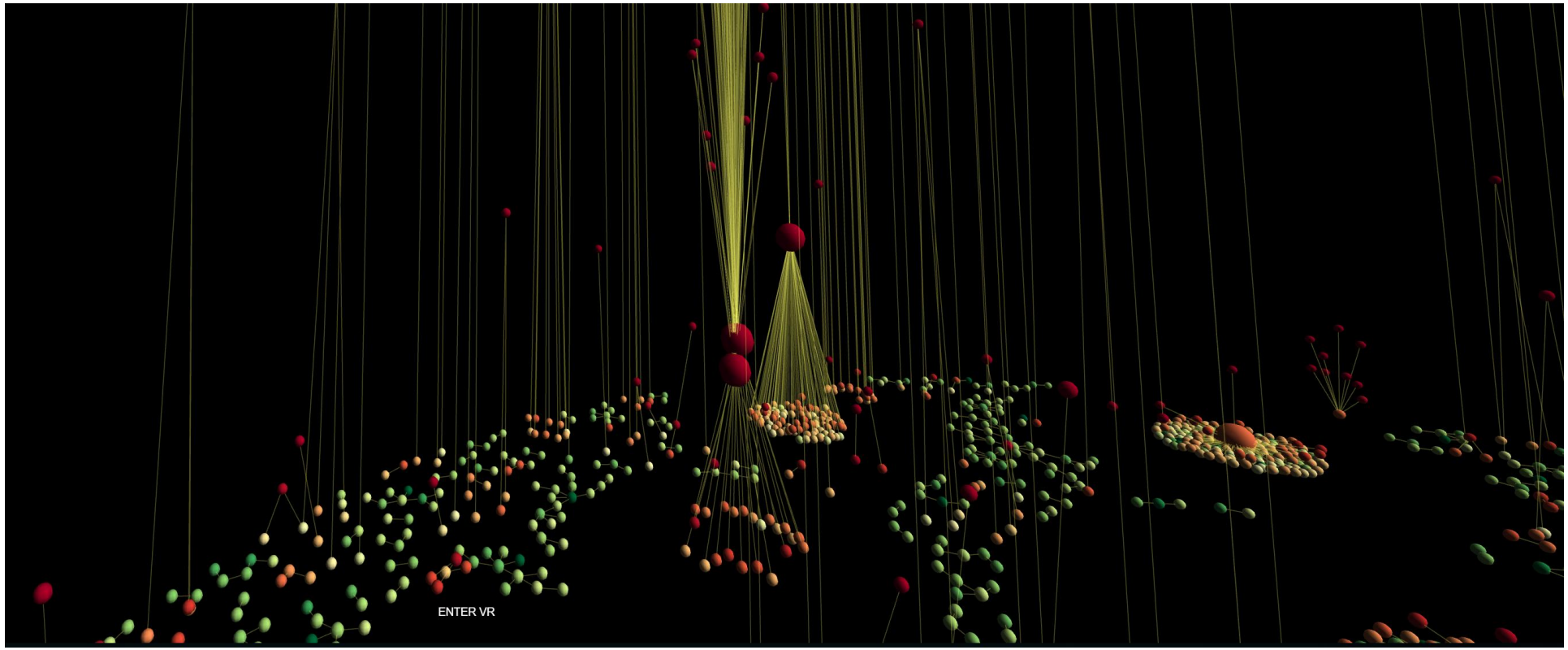
AVALANCHE

The Leader



AVALANCHE

Real People and Botnets



AVALANCHE

Дополнительная информация