

Система контроля оперативной обстановки в цифровом пространстве

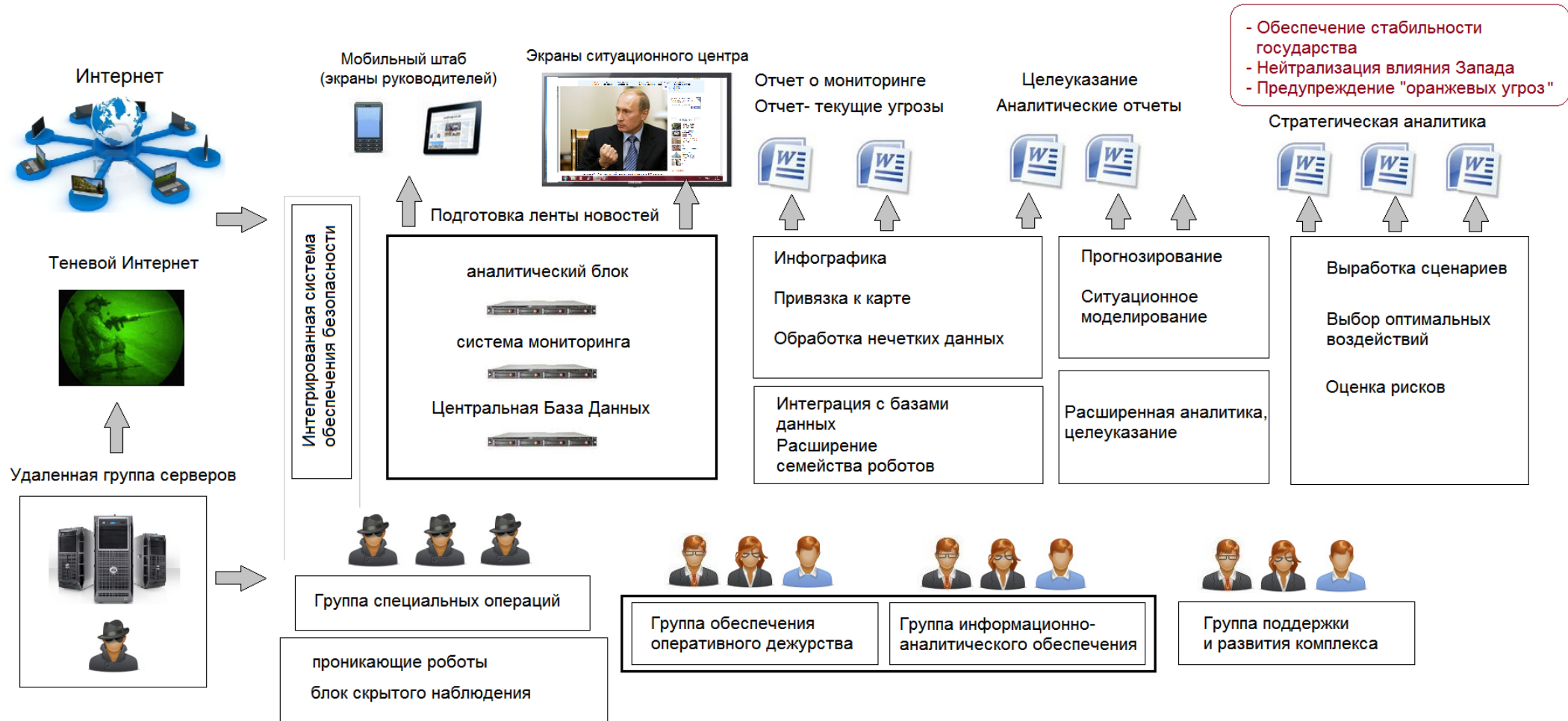
Масалович Андрей Игоревич

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

Структура программного обеспечения Ситуационного центра

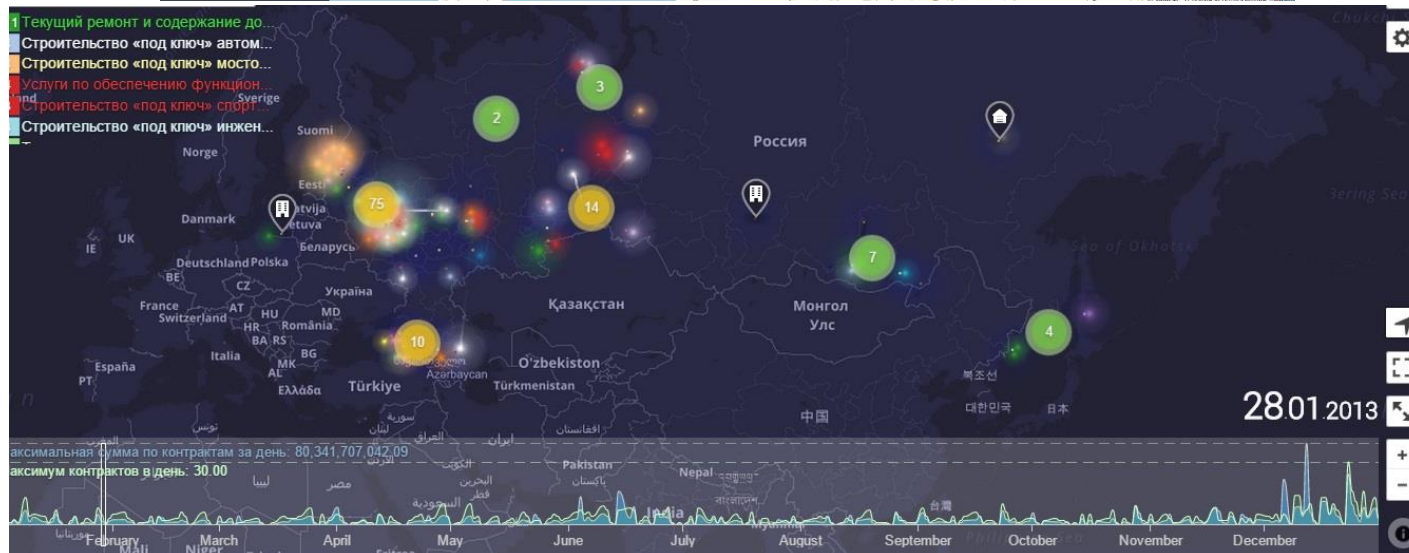
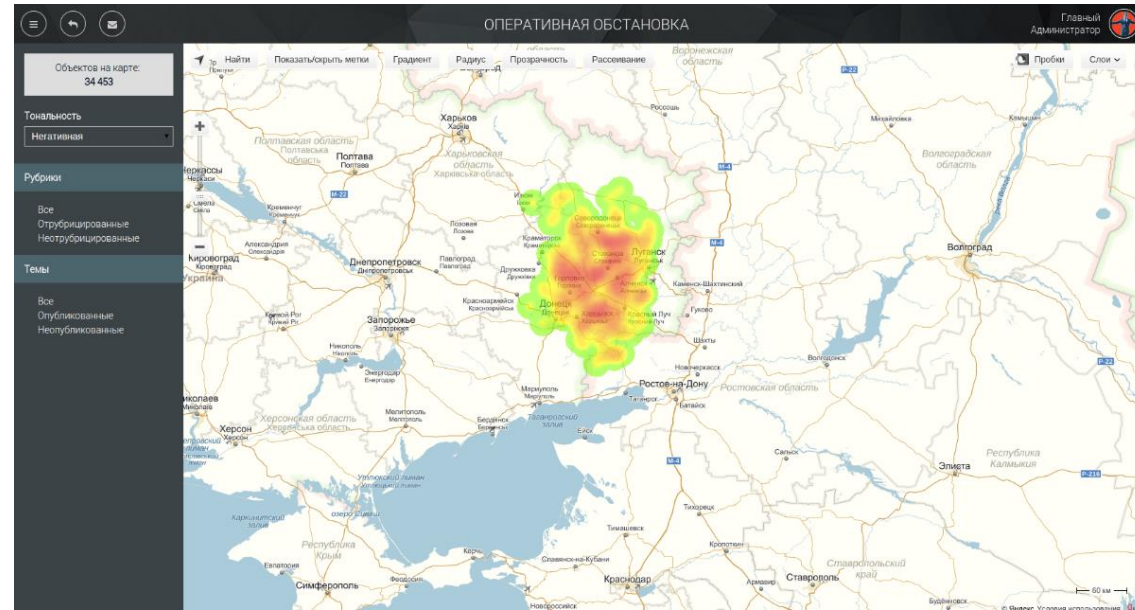


Пример упущенного контроля над ситуацией

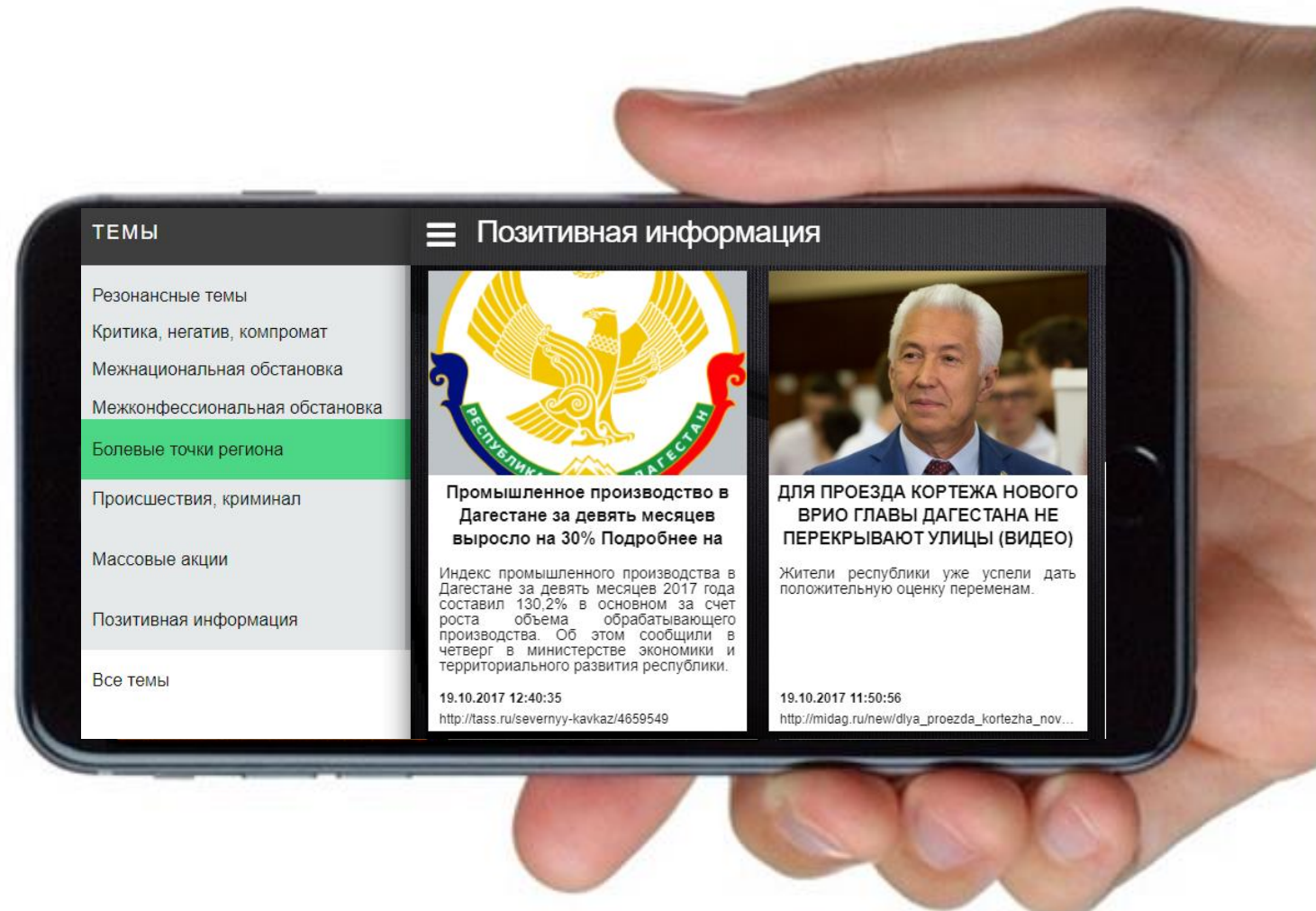
- Бирюлево, 10-13 октября 2013



Тепловая карта активности в социальных сетях



Оперативное оповещение руководителей



Анализ активности в социальных сетях: Муфтият Дагестана



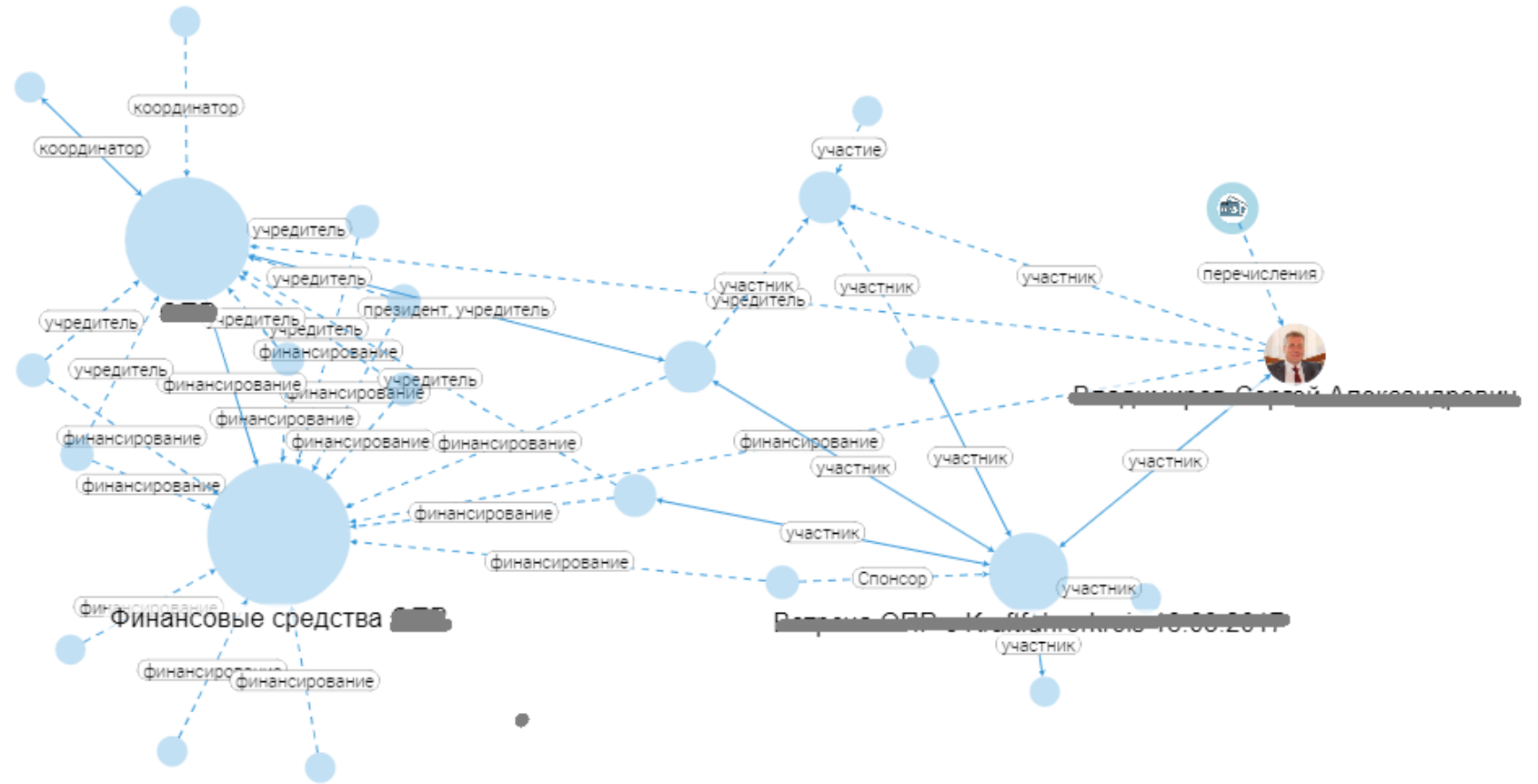
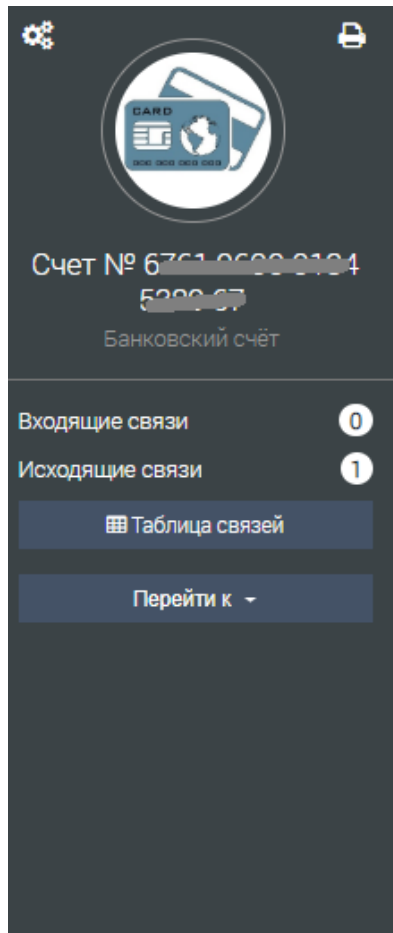
Движение Карфаген в социальных сетях (Дагестан)



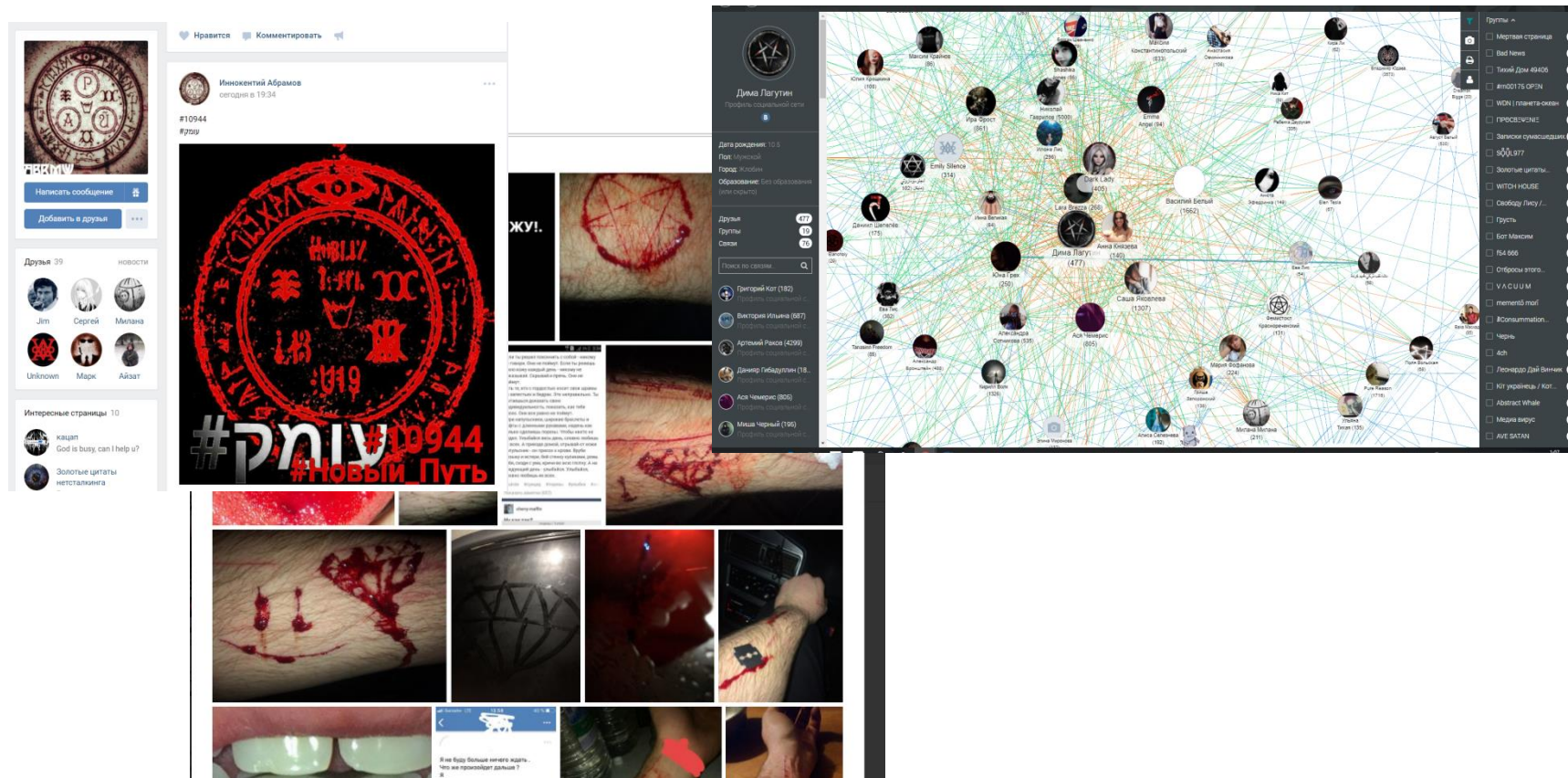
Пример: мониторинг беспорядков при повышении тарифов на систему Платон



Организаторы беспорядков: Анализ графов связей



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



Технологии многоуровневого вовлечения



Крибрум 2018

Угрозы социальных медиа для подростков

Как это устроено?

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

Группы широкого тематического охвата

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

Группы более узкой тематики

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

Частные группы

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

Приватное общение

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

Реальные действия

«Керченский стрелок»



Падик
<http://vk.com/club46987089>



САМЫЕ СТРАШНЫЕ ФИЛЬМЫ УЖАСОВ
<http://vk.com/club37078428>



Приложение «Метро 2033»
<http://vk.com/club39552595>



Huawei Mobile
<http://vk.com/club29060604>



Тюряга (официальная группа игры)
<http://vk.com/club20682901>



NUTS® МОЗГ ВКЛЮЧИ!
<http://vk.com/club16849496>



Вселенная Метро 2033 [18+]
<http://vk.com/club12698764>



Герой - официальная группа игры
<http://vk.com/club32164676>

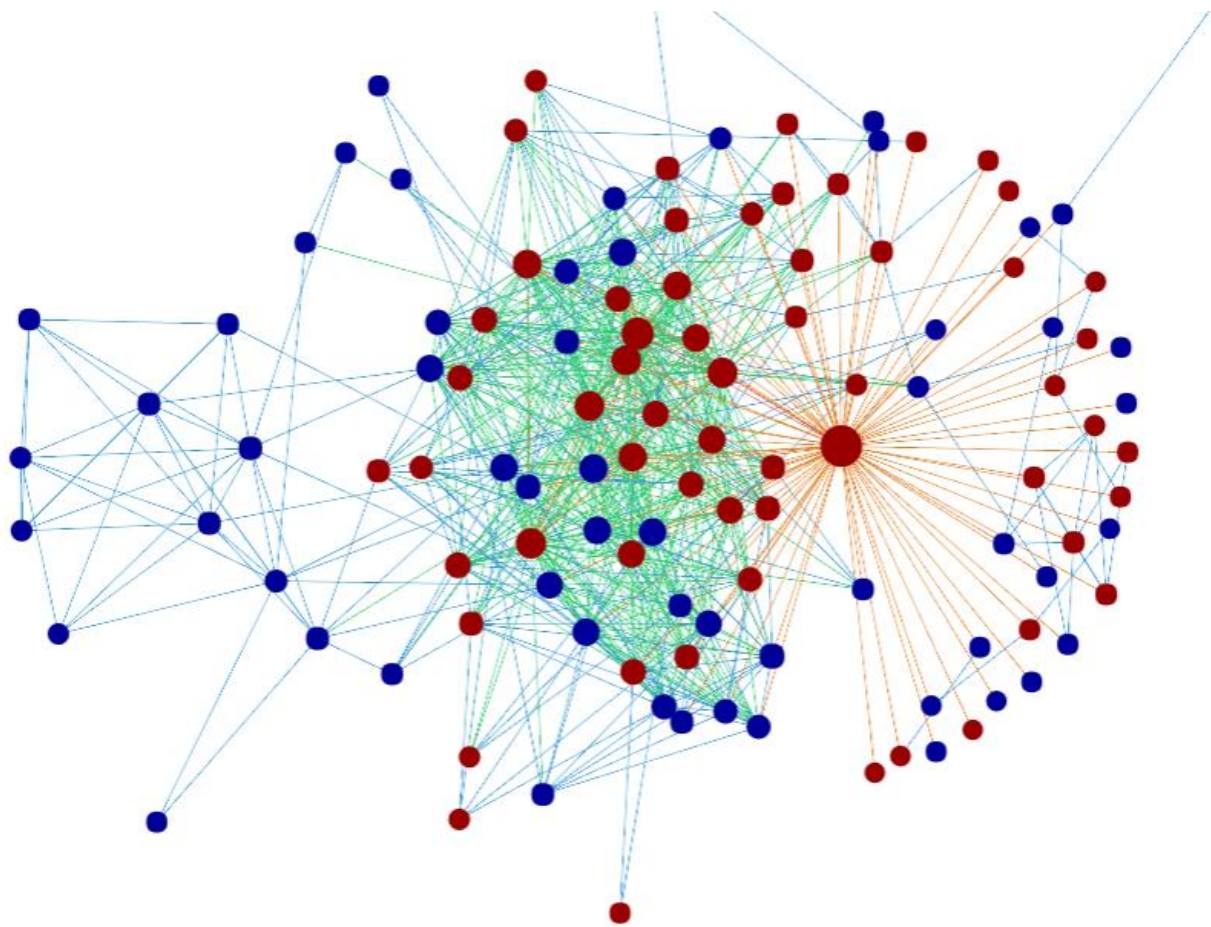


Меч 2
<http://vk.com/club34880411>



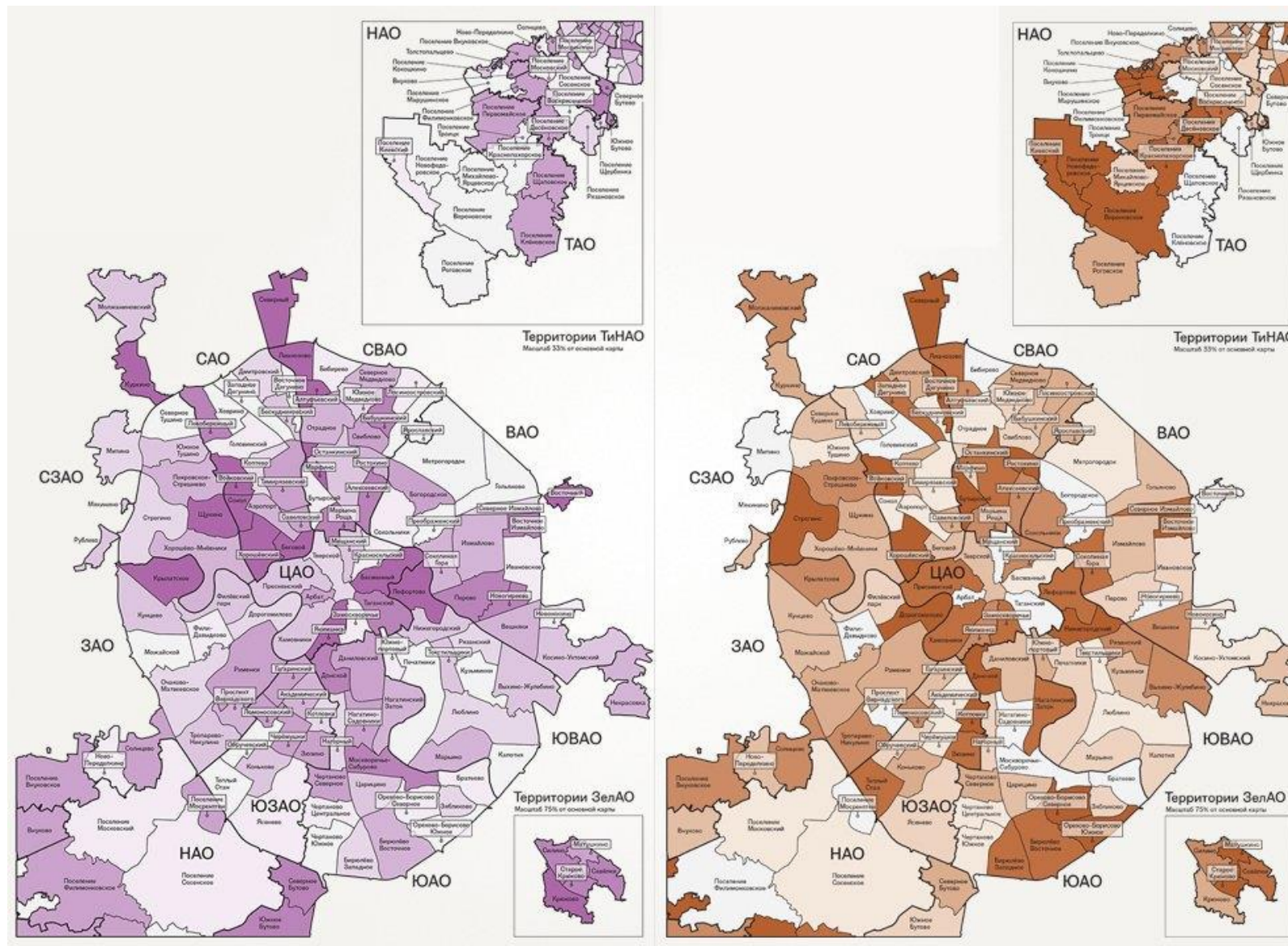
„Эта игра из меня чуть психа не сделала.
Там все несправедливо к людям“

Социальный портрет - подросток

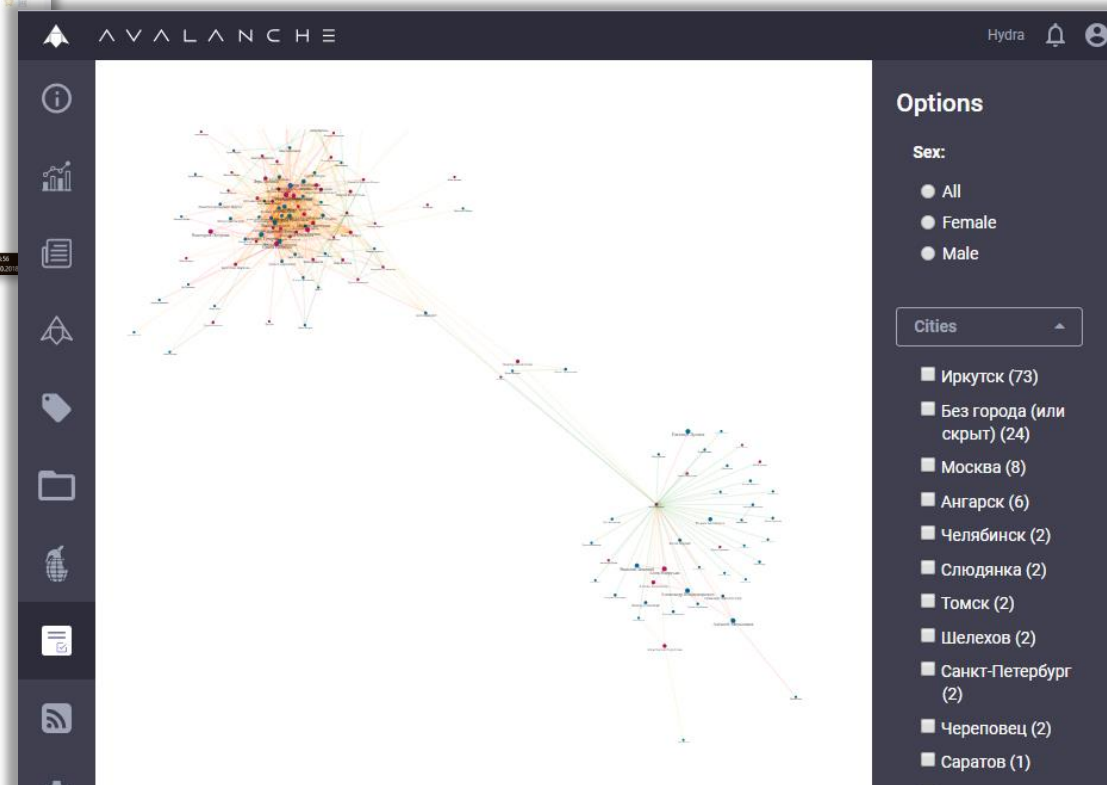
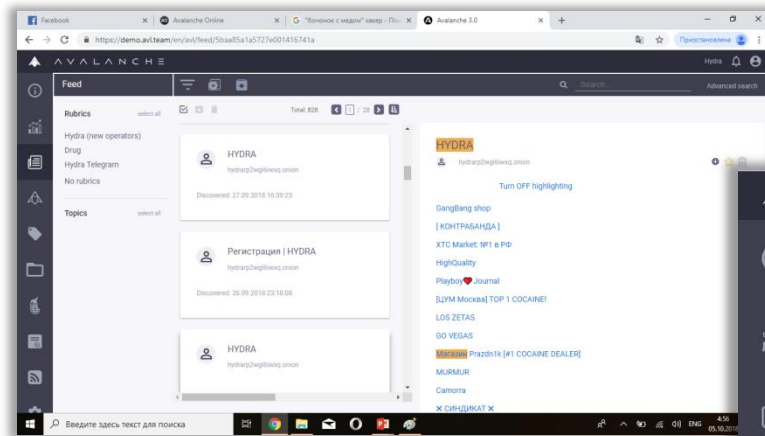


Группы ^	
<input type="checkbox"/>	Подслушано в школе... 46
<input type="checkbox"/>	Лайфхак 40
<input type="checkbox"/>	МДК 36
<input type="checkbox"/>	Киномания - фильмы... 33
<input type="checkbox"/>	Vine Video 32
<input type="checkbox"/>	Смейся до слёз :D 29
<input type="checkbox"/>	Палата №6 29
<input type="checkbox"/>	Киномания 28
<input type="checkbox"/>	Ябкупил 27
<input type="checkbox"/>	4ch 26
<input type="checkbox"/>	че 26
<input type="checkbox"/>	ЗЛОЙ ШКОЛЬНИК 26
<input type="checkbox"/>	ИНДУЛЬГЕНЦИЯ † 25
<input type="checkbox"/>	Краткие факты 24
<input type="checkbox"/>	Лепра 24
<input type="checkbox"/>	• iFace 23
<input type="checkbox"/>	Подслушано 23
<input type="checkbox"/>	Чёткие приколы 23

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



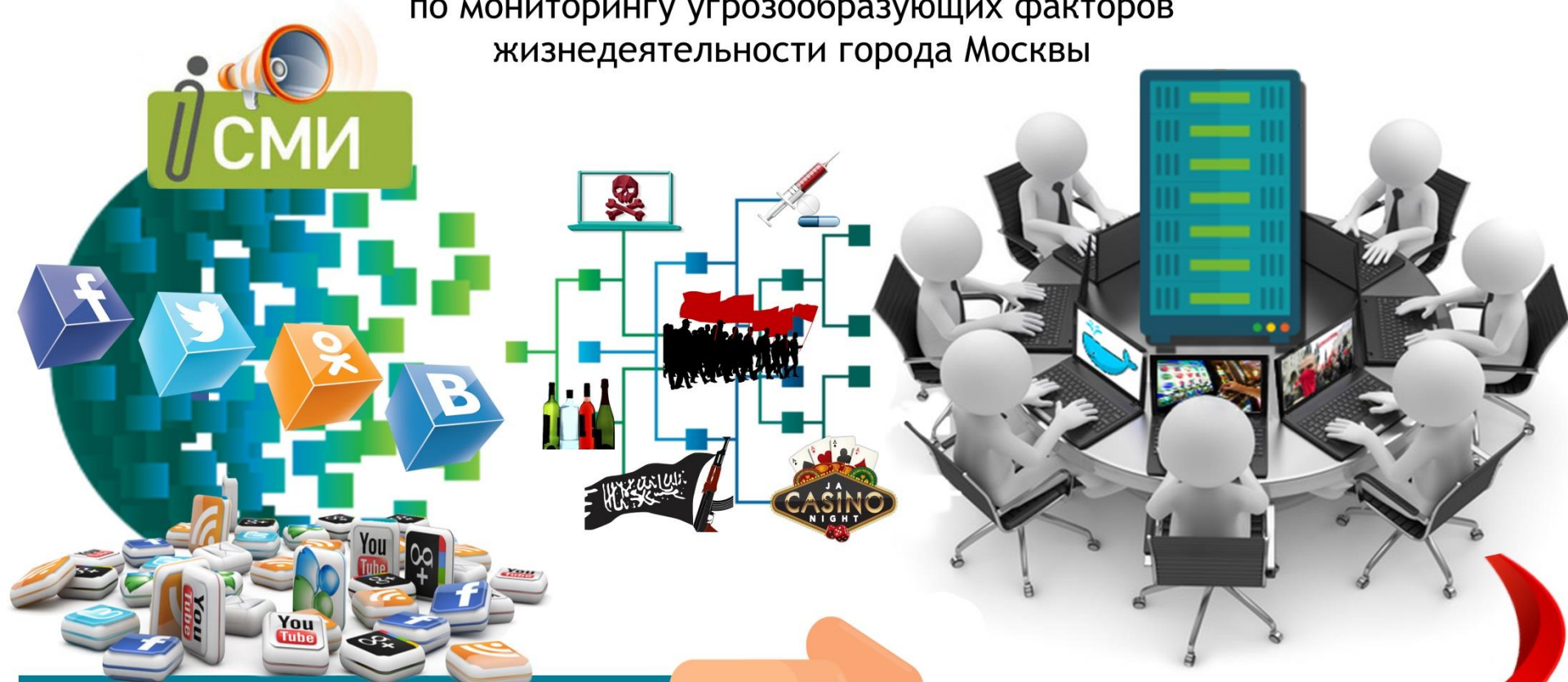
FINA WORLD CHAMPIONSHIPS
KAZAN
RUSSIA 2015

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

КАЗАНЬ: ОПЕРАТИВНАЯ ОБСТАНОВКА

Общая обстановка в городе Спорт кончился, скоро выборы: главные медиаперсоны РТ в мае-2015 01.06.2015 19:01:15 Метшин и Мухаметшин растут в цитируемости, Минниханов побивает новые рекорды, а его конкуренты по праймериз стали чаще попадать в новости. Как http://info.tatcenter.ru/artic... Верховный суд Татарстана признал законным отказ исполкома Казани в 01.06.2015 18:04:32 Верховный суд Татарстана оставил без удовлетворения жалобу главы партии «Яблоко» Руслана Зинатуллина, который просил отменить решение Вахитовского http://triboona.ru/post/7545	Освещение ситуации вокруг ЧМ/ критика организации ЧМ Иностранным строителям объектов ЧМ-2018 по футболу упростят въезд в 02.06.2015 07:37:38 Предусмотрена возможность при выдаче решений о въезде не учитывать распределение квоты на иностранных граждан и квоты на выдачу разрешений на http://www.tatar-inform.ru/new... Алексей Сорокин: «Отставка Толстых на подготовку к ЧМ-2018 не повлияет» 01.06.2015 15:48:51 Директор оргкомитета «Россия-2018» поделился мнением об отставке главы РФС Николая Толстых со своего поста. http://www.tatar-inform.ru/new...	Выборы Президента, митинги и политические акции Либералы в Татарстане выбросили «белый флаг» 02.06.2015 00:00:32 При первом президенте Татарстана Минтимере Шаймиеве в регионе существовал так называемый круглый стол партий и общественно-политических http://www.ng.ru/ng_politics/2... МАРШ МИРА В ПЕТЕРБУРГЕ ПРОИДЕТ В ФОРМАТЕ НАРОДНОГО СХОДА 17.09.2014 13:00:28 Администрация Санкт-Петербурга не согласовала проведение в Санкт-Петербурге «Марша мира», запланированного на 21 сентября. Поэтому акция пройдет в городе не https://vk.com/event770031497w...	Радикальные и оппозиционные политические партии Радикальный ислам под красным флагом 01.06.2015 14:00:34 Оппозиционные партии в регионах привлекают в свои ряды исламистов http://lenta.ru/articles/2015/... Зачем Геннадий Зюганов принял в ряды КПРФ в Татарстане религиозного 27.05.2015 11:22:26 Татарский национал-сепаратист Наиль Набиуллин, возглавляющий националистический Союз татарской молодежи «Азатлык», и адепт идеологии http://kazanfirst.ru/feed/4712...
Межконфессиональные, межнациональные конфликты Законодатели Поволжья сверяют вектор приоритетов 30.05.2015 04:52:53 «На вопросы гармонизации межнациональных и межконфессиональных отношений нужно обращать особое внимание. На примере Татарстана могут http://rt-online.ru/articles/ru... Рустам Минниханов: «Вы, наверное, помните события, связанные с 29.05.2015 18:53:04 «Чрезвычайно чувствительные и delicate» темы обсуждали сегодня законодатели Поволжья в Казанской ратуше. Замполпреда в ПФО, передавая http://www.business-gazeta.ru/...	Происшествия и правонарушения Нурлатский «Адмирал»: в Татарстане опять сорел торговый центр 01.06.2015 19:10:30 Из плана проверок пожарной безопасности, которые прокатились по всей республике, объект по неизвестной причине был вычеркнут. http://www.business-gazeta.ru/... Родственница президента Вера Путина победила на выборах в МО «Владимирский 16.09.2014 21:29:02 Санкт-Петербург, 16 сентября (Олег Саломатин). Двухродная племянница президента РФ Вера Путина сохранила свой депутатский мандат в МО «Владимирский округ» показав лучший http://www.bal-info.ru/2014/09...	Религиозный экстремизм/ радикальный ислам I Международная исламская конференция по профилактике 02.06.2015 11:00:12 В работе конференции примут участие ведущие отечественные и зарубежные религиозные и светские специалисты, члены дипломатического корпуса. http://www.tatar-inform.ru/new... Радикальный ислам под красным флагом 01.06.2015 14:00:34 Оппозиционные партии в регионах привлекают в свои ряды исламистов http://lenta.ru/articles/2015/...	Деятельность правоохранительных органов Прокуратура нашла нарушения в мэрии Казани и спортшколе после ДТП со 01.06.2015 23:59:27 Прокуратура Казани после проведенной по факту ДТП в Нижегородской области с детьми-каратистами из Казани проверки нашла нарушения в комитете мэрии города http://prokazan.ru/news/view/1... Прокуратура потребовала от ректора КГАСУ наказать виновных в нарушении 01.06.2015 20:00:30 Сегодня прокуратура Татарстана сообщила, что в адрес ректора Казанского Государственного архитектурно-строительного университета (КГАСУ) http://www.kommersant.ru/doc/2...

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



УГРОЗЫ
РИСКИ
ПОЗИТИВ

РЕШЕНИЕ

ПРАВИТЕЛЬСТВО МОСКВЫ


The dashboard on the tablet shows a traffic light indicator with red, yellow, and green lights. Below it is a grid of news items with colored headers: 'Аварии', 'Общественно-политическая жизнь', 'Культурная жизнь', 'Увлечения', 'Мода и стиль', 'СЭМ', and 'Характер'. The text in the grid is small and mostly illegible.



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



 Текущая деятельность ГБУ г.Москвы «МИЦ»

 Планируемая деятельность с помощью интеллектуального комплекса мониторинга и анализа информационных материалов в сети Интернет

Ситуационный центр правительства города Москвы



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

Главные новости ○ Ситуация в стране ○ Военные конфл... ○ Чрезвычайные ... ● Минобороны ● Сопредельные с... ○


Киберпространство



Сирийские хакеры взломали сайт Forbes

Хакеры из группировки «Сирийской электронной армии» (SEA) взломали сайт американского журнала Forbes и ряд принадлежащих изданию и его сотрудникам аккаунтов в сети микроблога Twitter.


Добавлено 14.02.2014 16:28
www.vz.ru



В DARPA разрабатывается система использования смартфонов на поле боя

В управлении перспективных исследовательских программ министерства обороны США (DARPA) пришли к выводу, что привычка постоянно сверяться с мобильным помощником может стать на поле боя преимуществом для американских войск. В среду появились сообщения о начале разработок системы связи, которая бы


Добавлено 14.02.2014 12:00
www.ci2b.info



Белый дом представил госучреждениям США список рекомендаций по защите от

Администрация Белого дома сообщила о выпуске списка рекомендаций для защиты инфраструктуры частных компаний и госучреждений от киберугроз. Президент США Барак Обама приветствовал это нововведение. Около года назад глава государства в своем выступлении, посвященном положению дел в стране,

Добавлено 13.02.2014 14:48
itar-tass.com



Администрация США представила новую концепцию кибербезопасности

Президент Обама назвал эту инициативу поворотным моментом в обеспечении защиты от хакерских атак

Добавлено 13.02.2014 14:43
www.golos-ameriki.ru

Во Франции сменился начальник генштаба

Глава генштаба ВС Франции адмирал Эдуар Гийо официально ушел в отставку. В честь него на площади Инвалидов в Париже прошла торжественная церемония, во время которой президент республики Франсуа Олланд лично поблагодарил Гийо за заслуги перед Фра...

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 15 лет 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

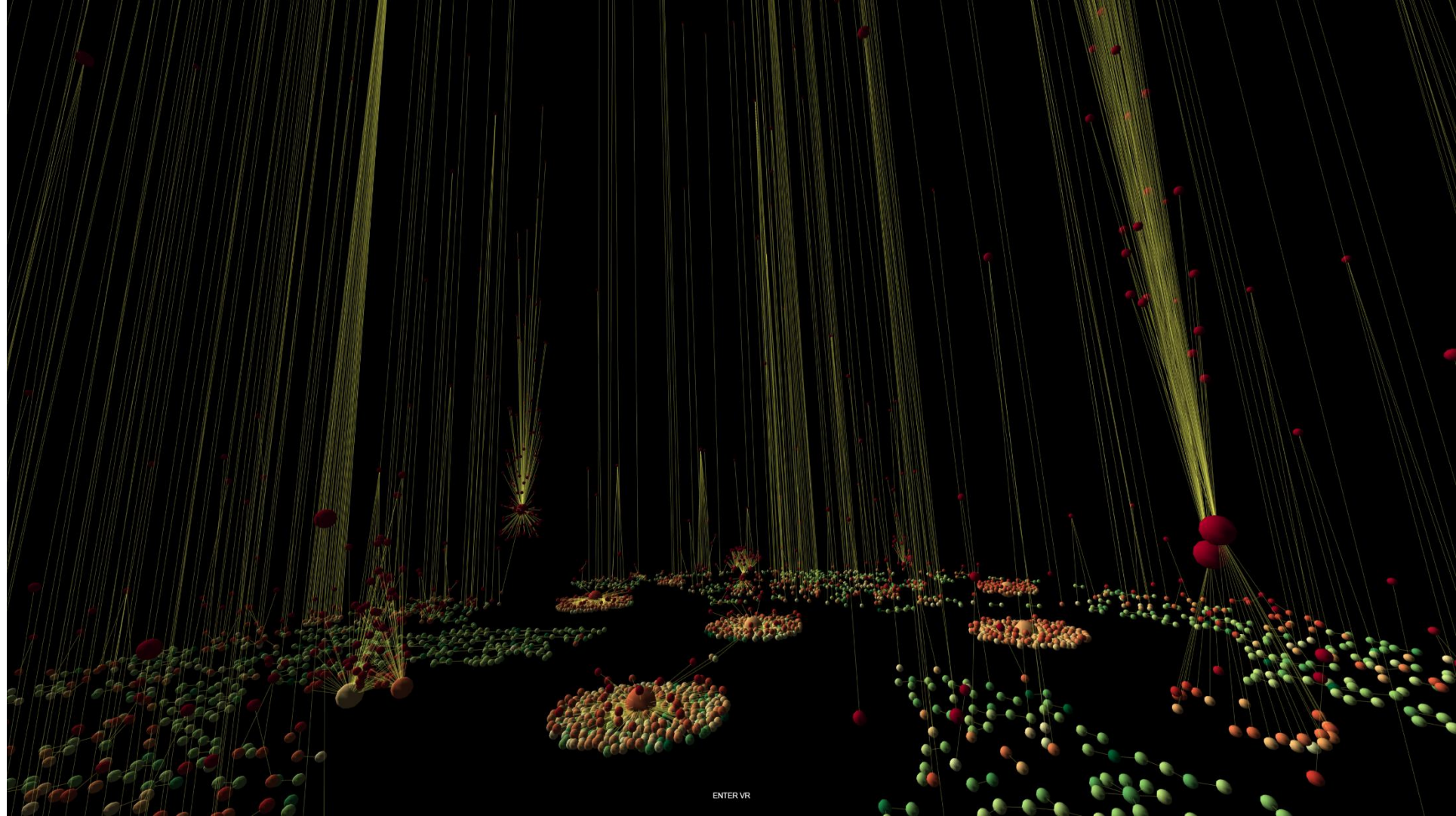
- Своя матрица интересов и угроз для каждого подразделения
- Разделение прав доступа по ролям, проектам, персонам
- Одно- или двухфакторная авторизация
- Защищенное хранение, шифрованный трафик
- Ведение логов активности сотрудников
- Мгновенное оповещение о важных событиях
- Комплексный мониторинг – 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



A V A L A N C H E

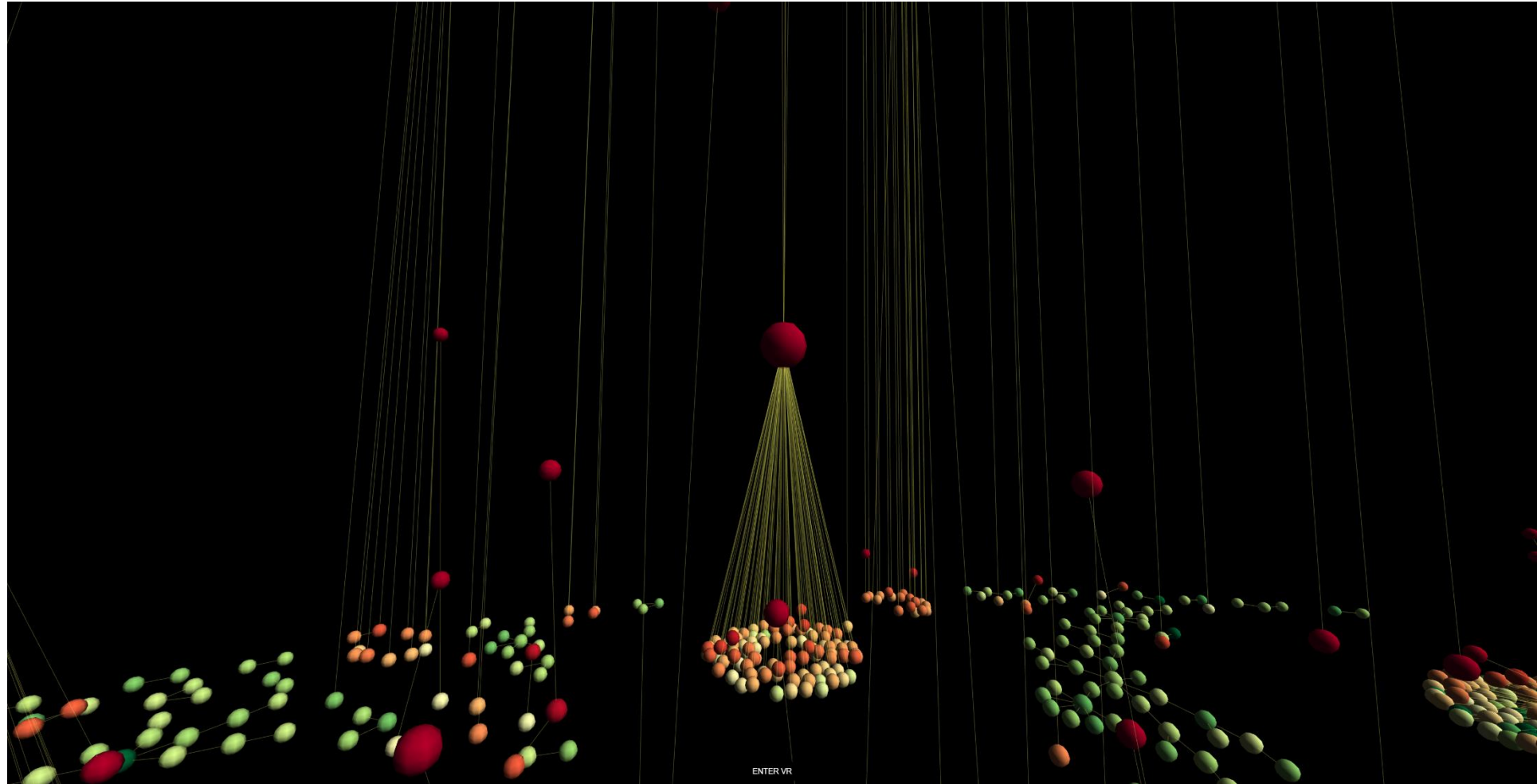
One minute inside Twitter



ENTER VR

AVANCE

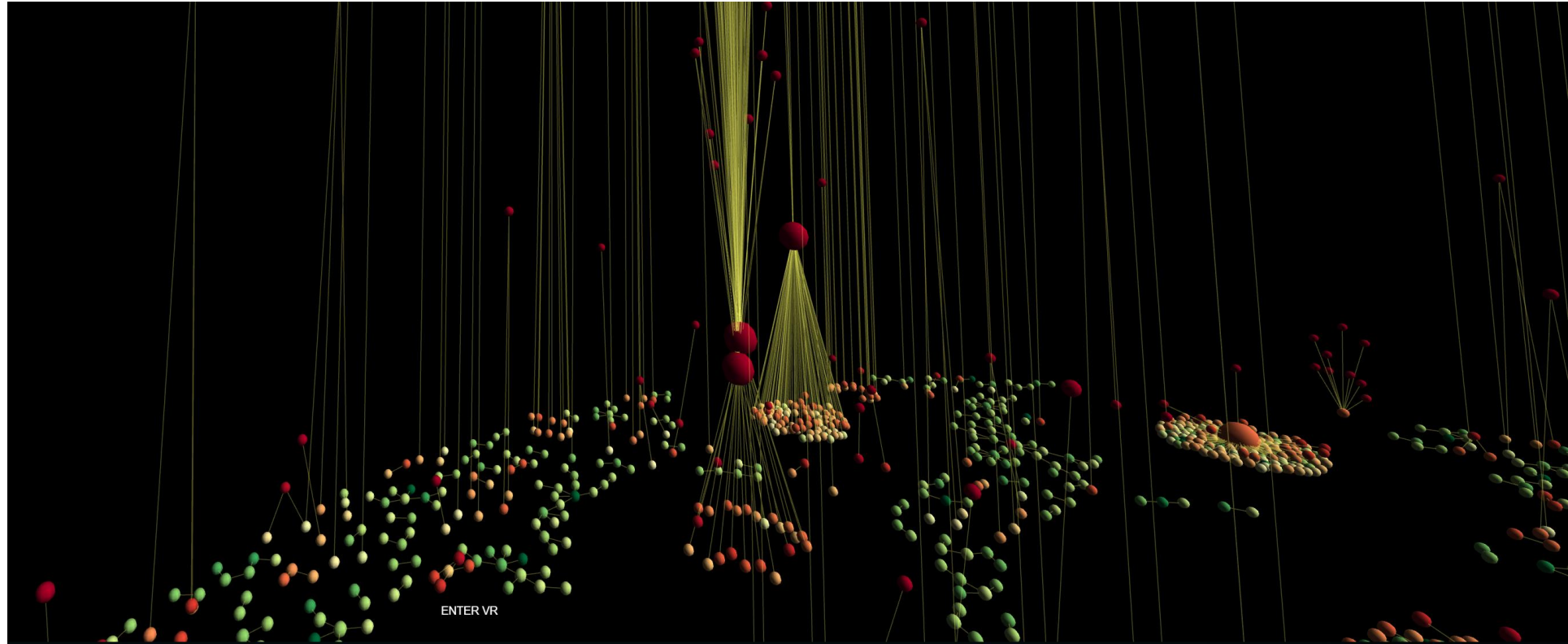
The Leader



ENTER VR

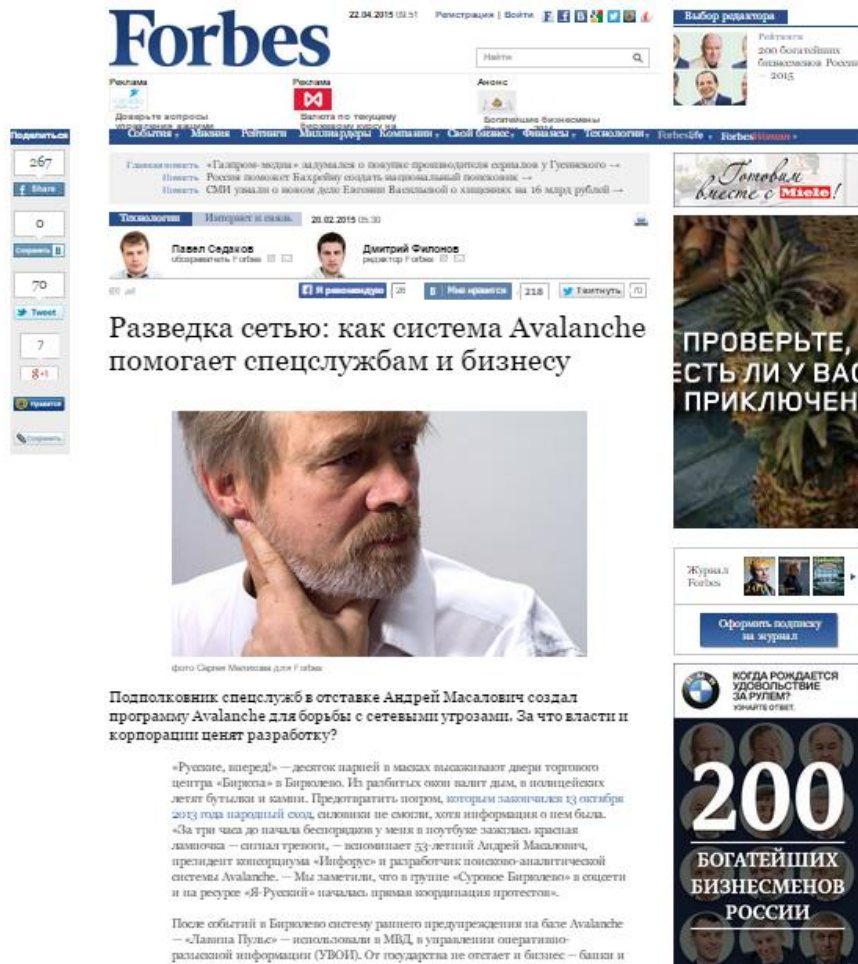
AVANCE

Real People and Botnets



AVANCE

Дополнительная информация



Forbes 22.04.2015 08:51

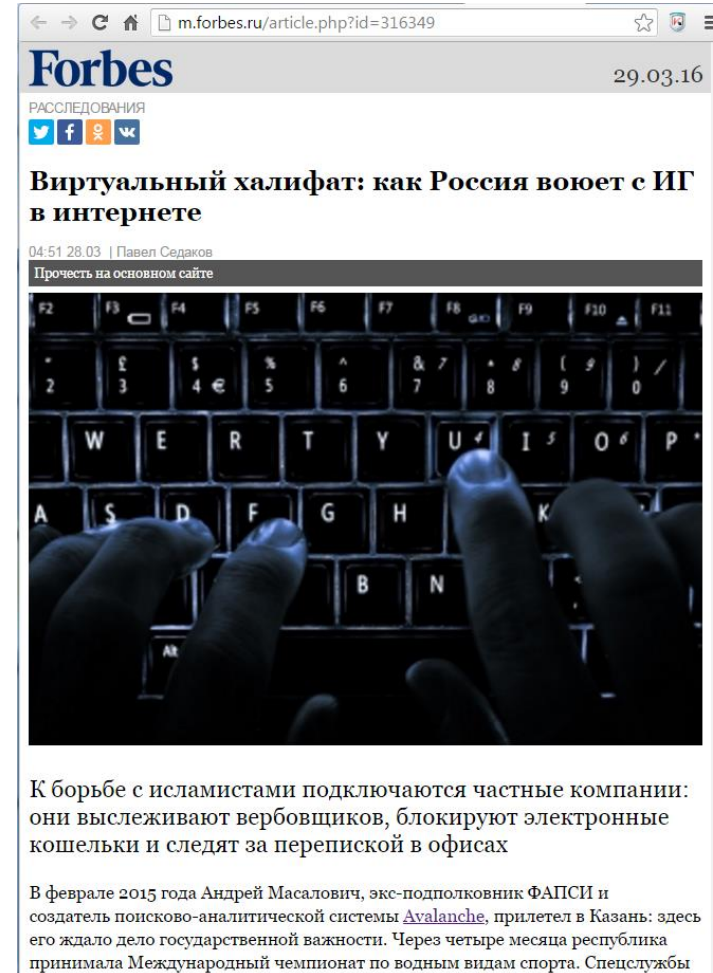
Выбор редактора: Рейтинги 200 богатейших бизнесменов России 2015

Разведка сетью: как система Avalanche помогает спецслужбам и бизнесу

Подполковник спецслужб в отставке Андрей Масалович создал программу Avalanche для борьбы с сетевыми угрозами. За что власти и корпорации ценят разработку?

«Русские, вперед!» — десктоп парней в масках высказывают двери торгового центра «Бирюза» в Бирюлево. Из разбитых окон валит дым, в полицейских летят бутылки и камни. Предотвратить погром, которым закончился 13 октября 2013 года шарашиный сход, силовиков не смогли, хотя информация о нем была. «За три часа до начала беспорядков у меня в ноутбуке загорелась красная лампочка — сигнал тревоги», — вспоминает 53-летний Андрей Масалович, президент корпорации «ИнФорум» и разработчик поисково-аналитической системы Avalanche. — Мы заметили, что в группе «Суровое Бирюлево» в соцсети и на ресурсе «Я-Русский» началась активная координация протестов.

После событий в Бирюлево систему раннего предупреждения на базе Avalanche — «Лампа Пульс» — использовали в МВД в управлении оперативно-разыскной информацией (УВОИ). От государства не отпал и бизнес — банки и



m.forbes.ru/article.php?id=316349

Forbes 29.03.16

РАССЛЕДОВАНИЯ

Виртуальный халифат: как Россия воюет с ИГ в интернете

04:51 28.03 | Павел Седаков

Прочсть на основном сайте

К борьбе с исламистами подключаются частные компании: они выслеживают вербовщиков, блокируют электронные кошельки и следят за перепиской в офисах

В феврале 2015 года Андрей Масалович, экс-подполковник ФАПСИ и создатель поисково-аналитической системы **Avalanche**, прилетел в Казань: здесь его ждало дело государственной важности. Через четыре месяца республика принимала Международный чемпионат по водным видам спорта. Спецслужбы