СЫГРАТЬ НА ОПЕРЕЖЕНИЕ:

арсенал бизнес-разведки для раннего предупреждения угроз бизнесу, репутации и устойчивому развитию

МАСАЛОВИЧ
Андрей Игоревич
am@inforus.biz
(964) 577-2012

ЛАВИНА ПУЛЬС

Технология **Avalanche** – интернет-разведка в арсенале Ситуационных центров

- Технология разработана более 10 лет назад
- Комплекс интернет-разведки и мониторинга
- Более 20 типов поисковых роботов
- Контроль «серого» (глубинного) Интернета
- Автоматические «светофоры» уровня угроз
- Раннее обнаружение информационных атак

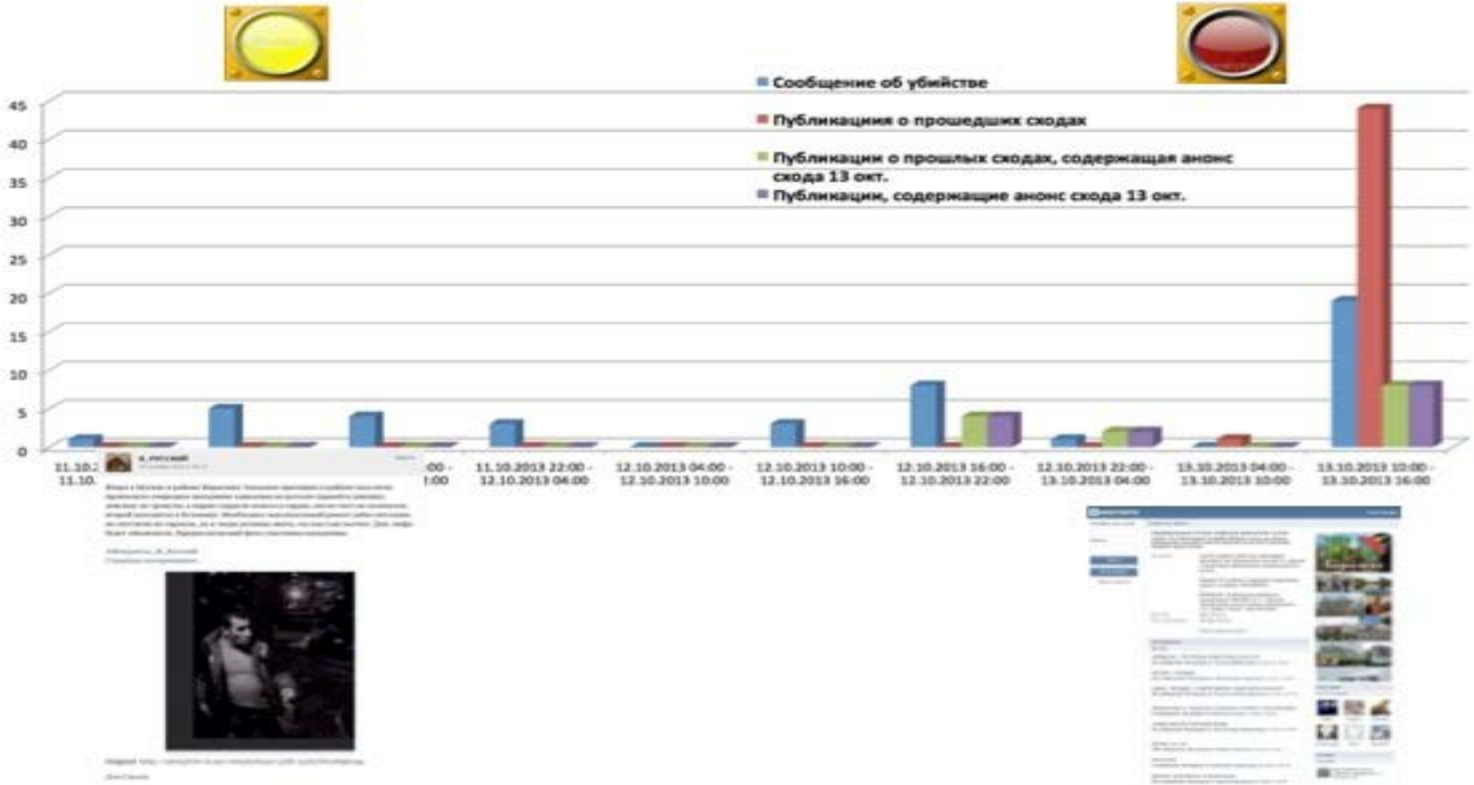
Цели развертывания комплекса

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

Пример упущенного контроля над ситуацией

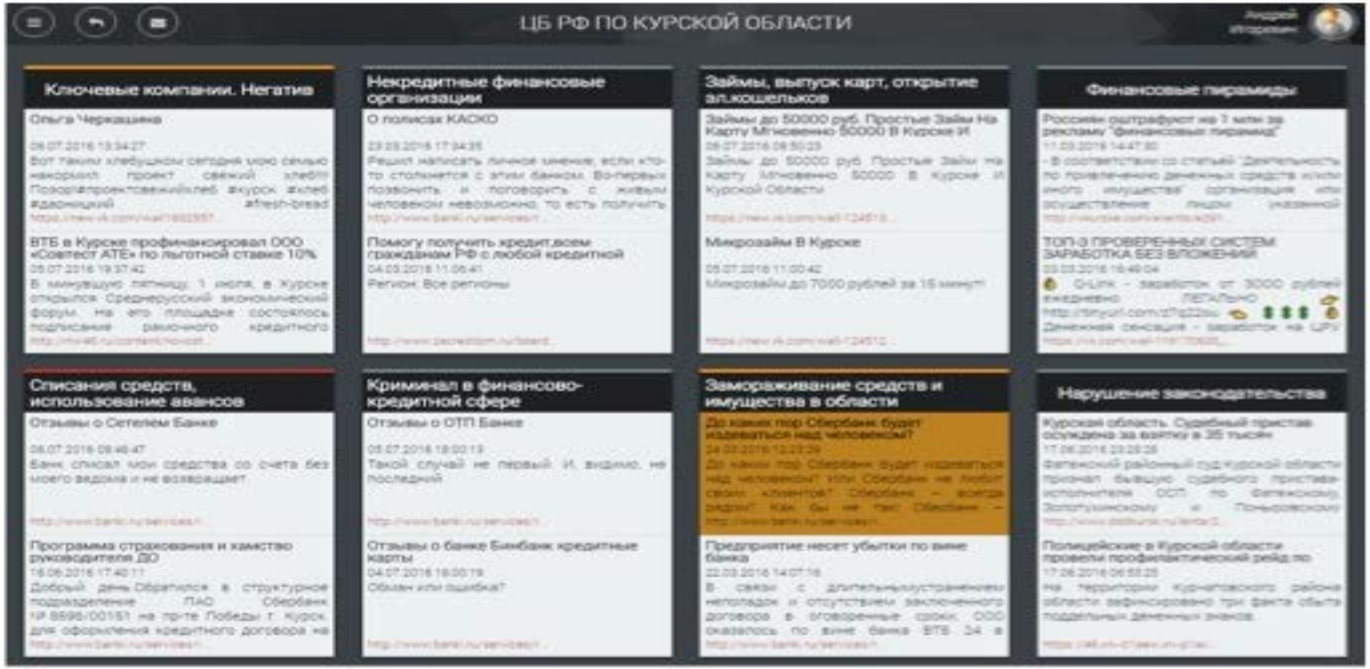
Бирюлево, 10-13 октября 2013

Мониторинг СМИ или система раннего предупреждения?



AVALANCHE

Система контроля оперативной обстановки



- 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»)

AVALANCHE

Персонификация для каждого руководителя

- 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

Проблемы, которые выявляет комплекс

- Угрозы бизнесу, репутации, устойчивому развитию
- Критика, компромат, негатив в адрес банка
- Утечки коммерческой тайны, конфиденциальной и внутренней информации
- Утечки персональных данных
- Конфликты интересов банка и его менеджмента
- Риски проникновения в банк криминальных элементов
- Недобросовестная конкуренция
- Противоправные действия менеджмента
- Новые схемы мошенничества, фрода в ДБО и др.
- И т.д.

Экран руководителя - планшет и смартфон

AVALANCHE

Поиск на нескольких языках одновременно

РОСНЕФТЬ. АКТИВЫ

Андрей Игоревич

Рубрики

- Все
- Отрубрицированные
  - Активы de
  - Активы it
  - Активы ru
  - Активы ua
- Неотрубрицированные

Темы

- Все
- Опубликованные
  - Активы (немецкий язык)
  - Активы (украинский язык)
  - Активы (итальянский язык)
  - Активы (русский язык)
- Неопубликованные

В корзине

ОПУБЛИКОВАНО

Bp: Rosneft cede quota 20% progetto siberiano Taas

Il colosso energetico russo Rosneft ha ceduto al gruppo britannico Bp una partecipazione del 20% nel progetto siberiano Taas

12.02.2016 14:48:42 30.11.2015 14:47:49 http://www.iltempo.i...

ОПУБЛИКОВАНО

Rosneft: «Resteremo nel capitale di Saras con il 12%»

Non ridurranno ulteriormente la loro partecipazione, ora al 12%, e continueranno a lavorare per aumentare l'efficienza di Saras, che considerano tuttora un investimento strategico nel campo della raffinazione petrolifera. E sono molto lieti della "svolta cinese" di Pirelli

Активы it

12.02.2016 14:38:40 23.10.2015 14:38:18 http://www.ilsole24o...

ОПУБЛИКОВАНО

Sechin (Rosneft): manteniamo il 12% in Saras e lavoriamo per più efficienza

Non ridurranno ulteriormente la loro partecipazione, rimasta al 12%, e continueranno a lavorare per aumentare l'efficienza di Saras. A Verona, all'apertura del quarto Forum eurasiatico - vertice economico che sta diventando un punto di riferimento del dialogo nella "Grande Eurasia", organizzato dall'Associazione Conoscere Eurasia e dal Forum economico internazionale di San Pietroburgo - le prime attenzioni sono per Igor Sechin, presidente e amministratore delegato di Rosneft, prima per produzione al mondo tra le compagnie petrolifere quotate.

Найдено новостей: 45

Поиск по тексту

Расширенный поиск

Источник

Поиск по источнику

Дата публикации

От

До

Дата создания

От

До

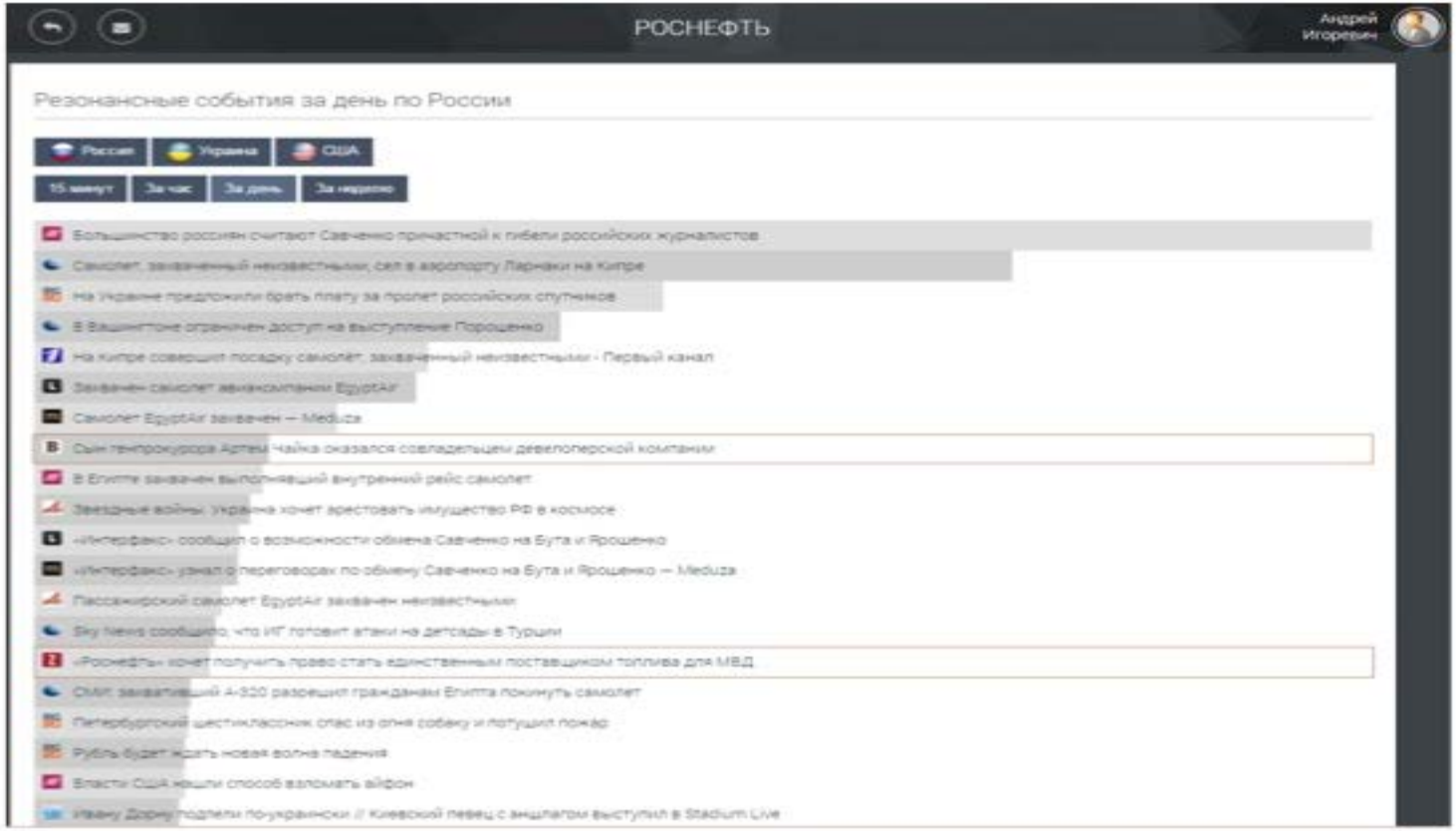
- Перевернуть ленту
- Отключить подсветку
- Не показывать дубликаты

Важность

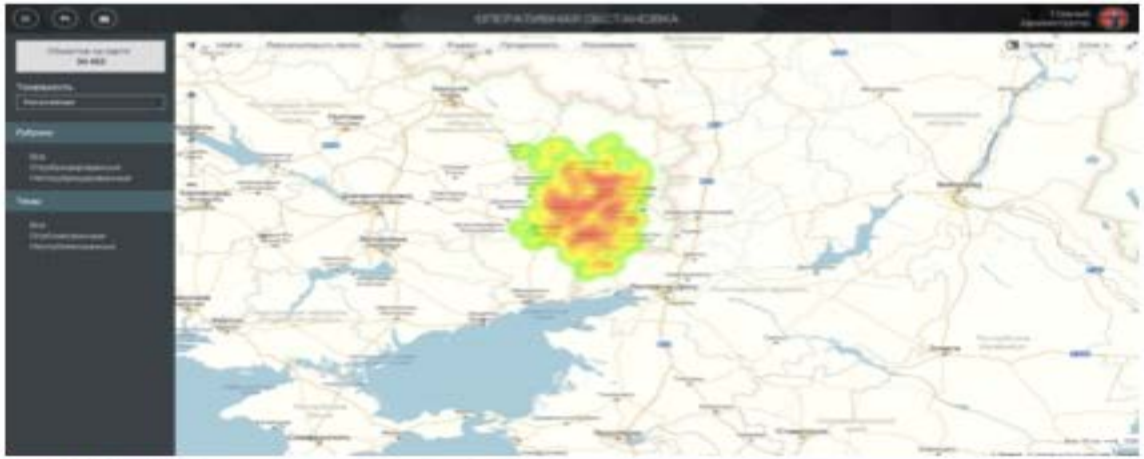
Все

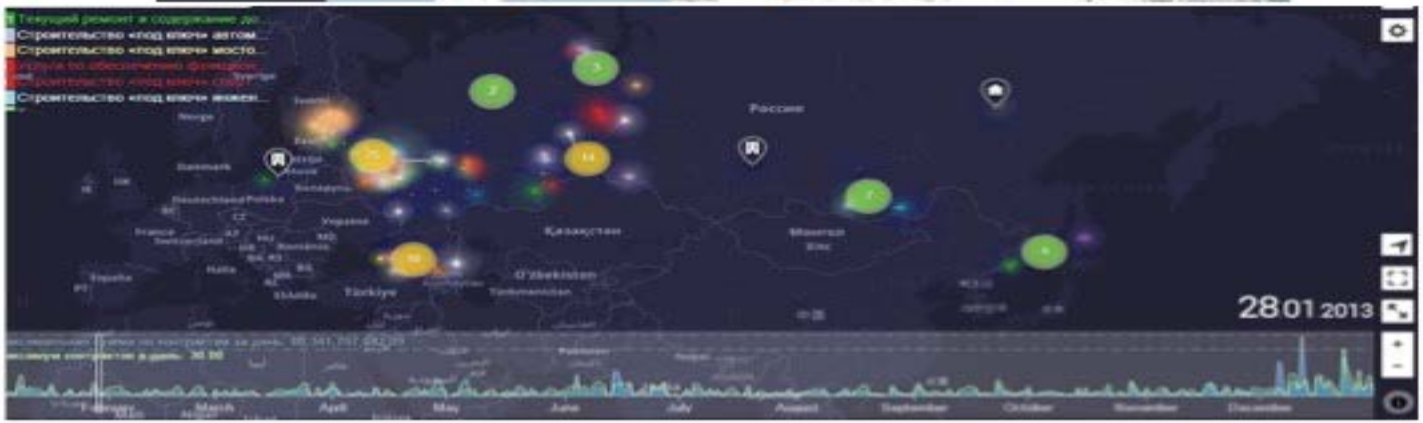
Тональность

Выделение резонансных тем



Тепловая карта активности в социальных сетях

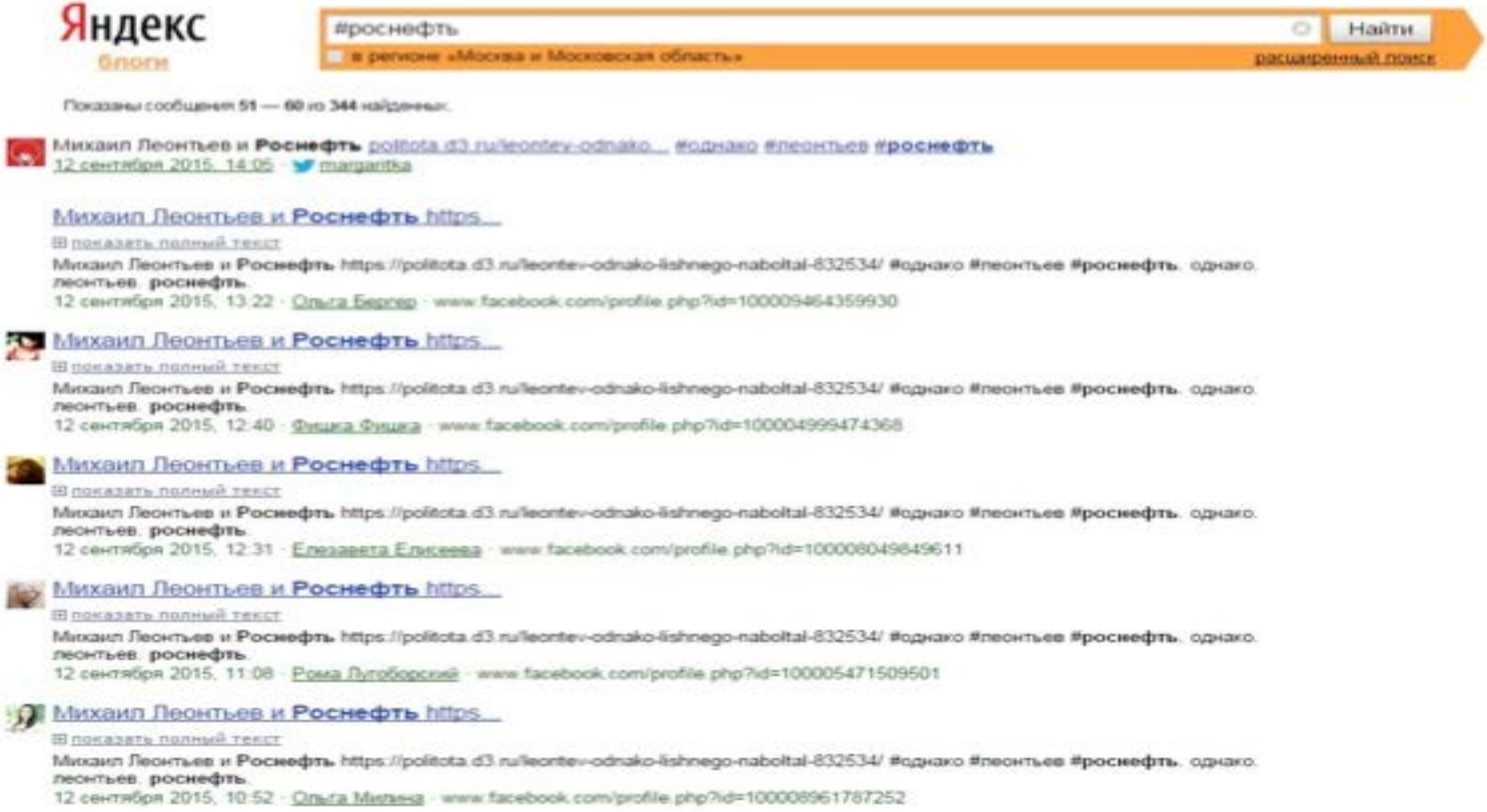




AVALANCHE

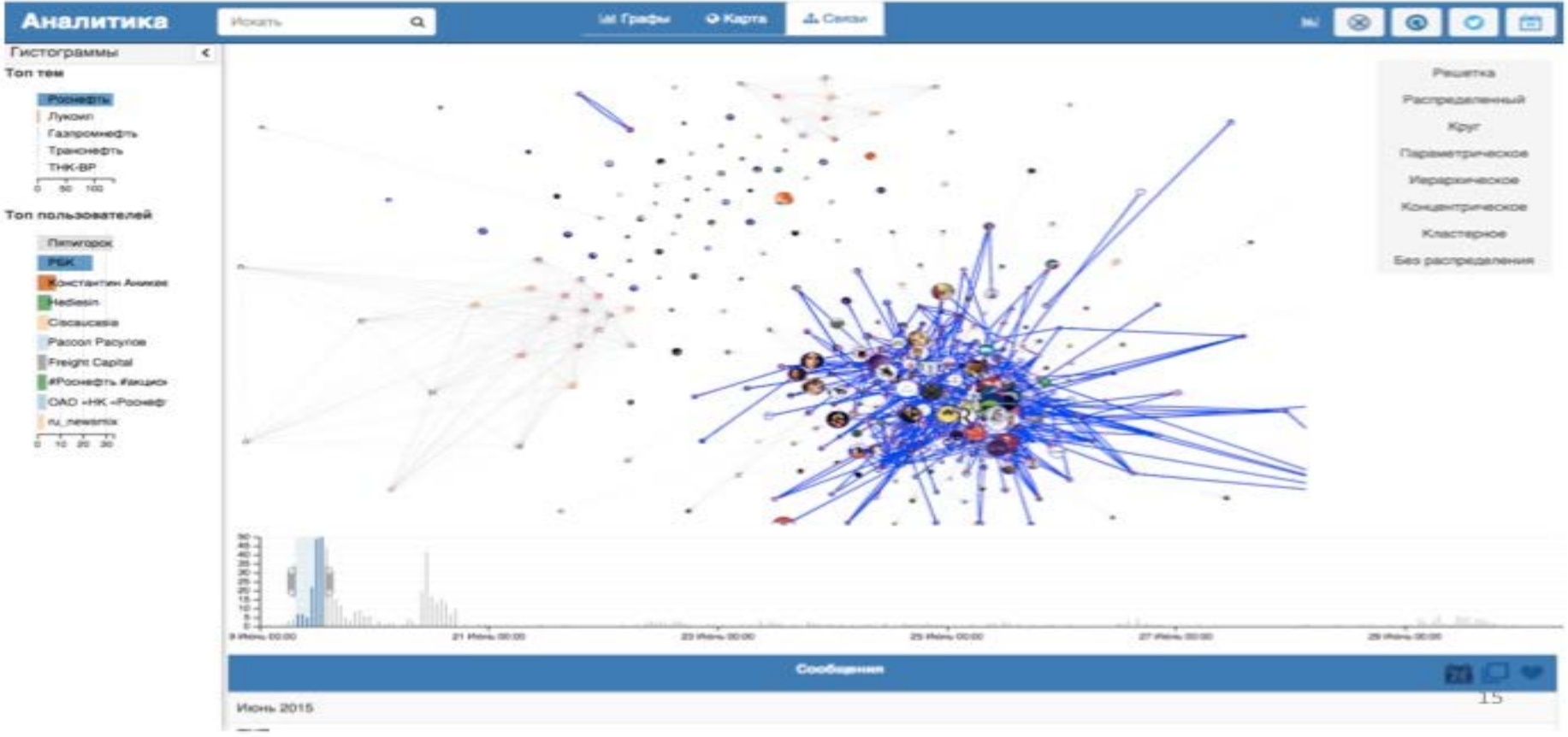
Анализ информационных всплесков

Выявление ссылочных взрывов



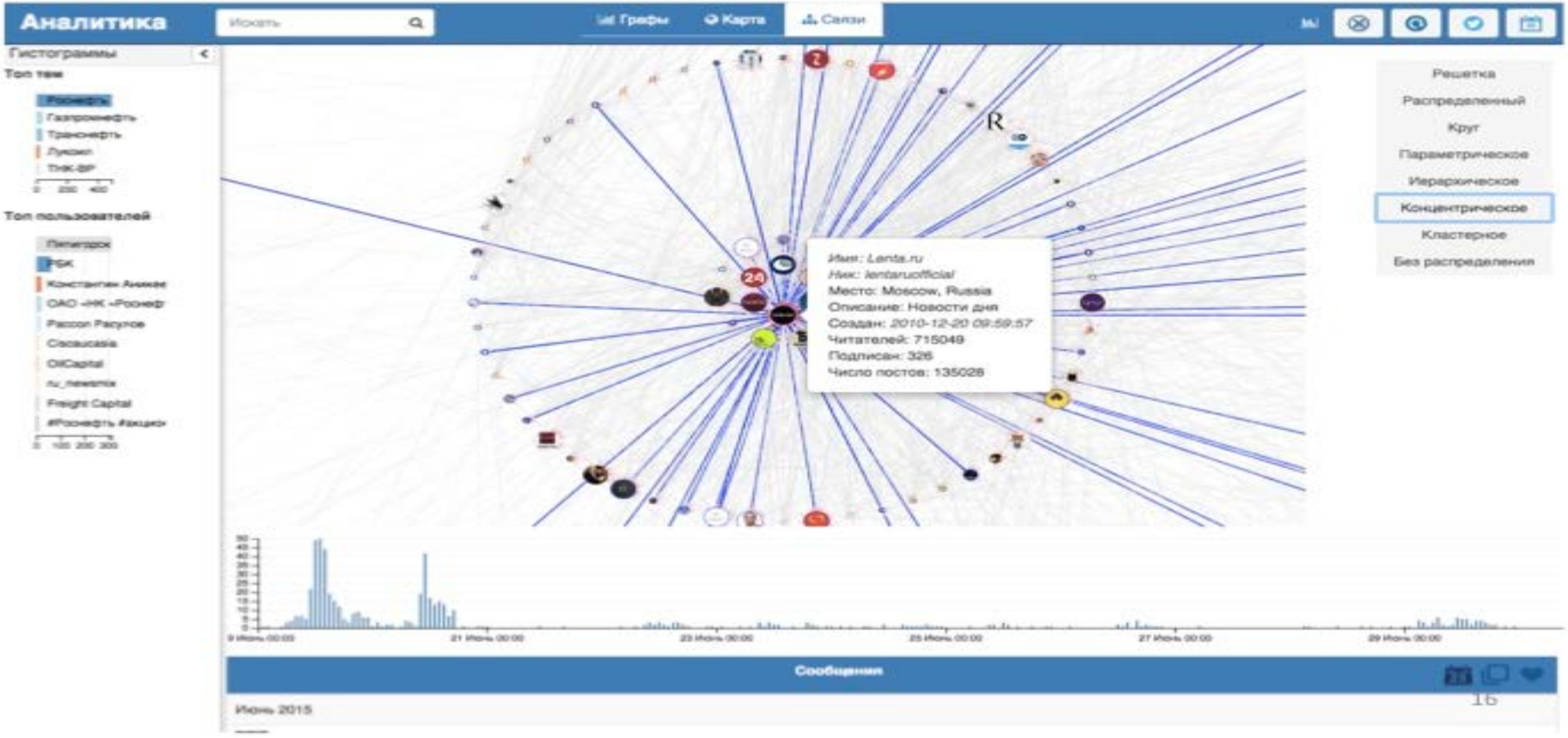
AVALANCHE

Анализ активности в социальных сетях

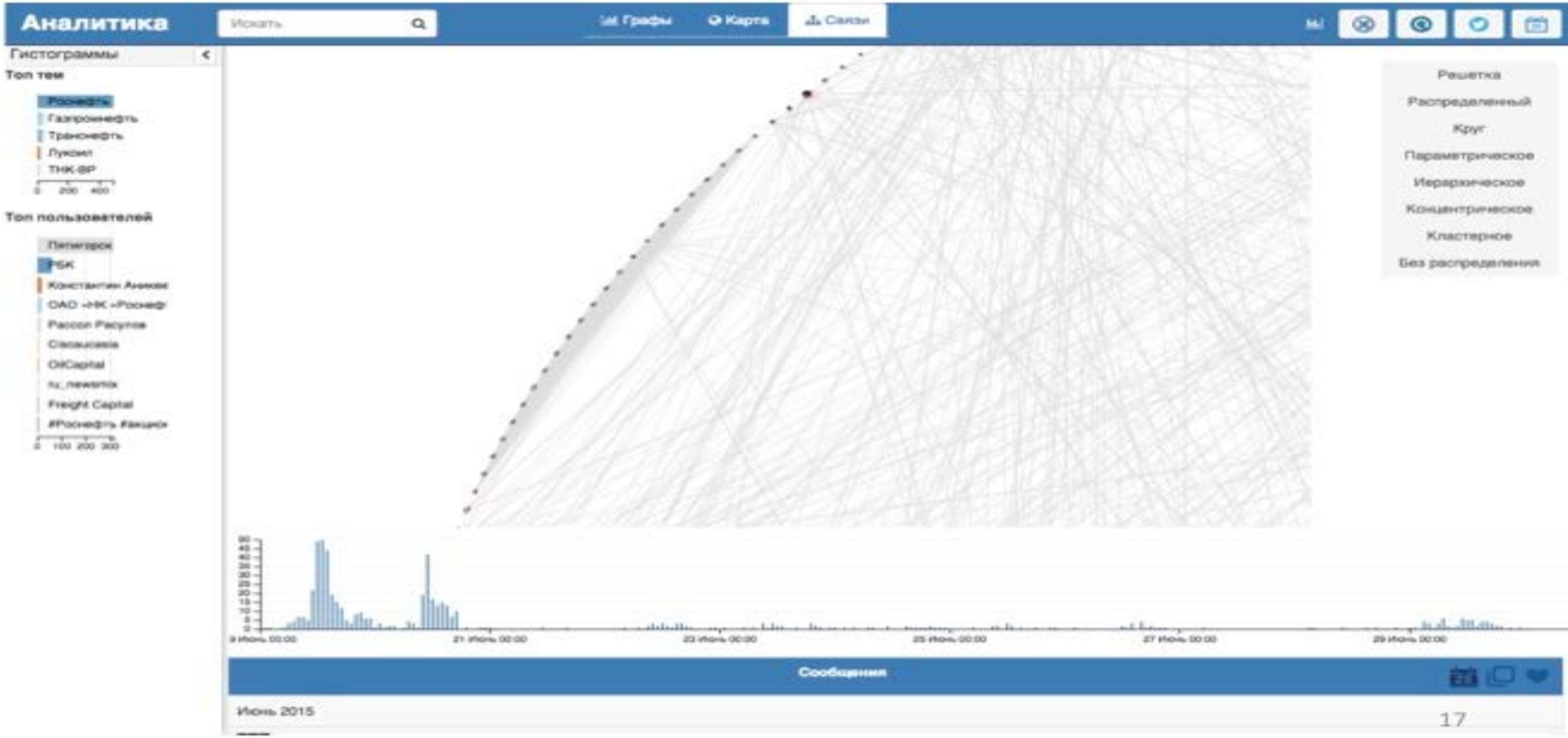


AVALANCHE

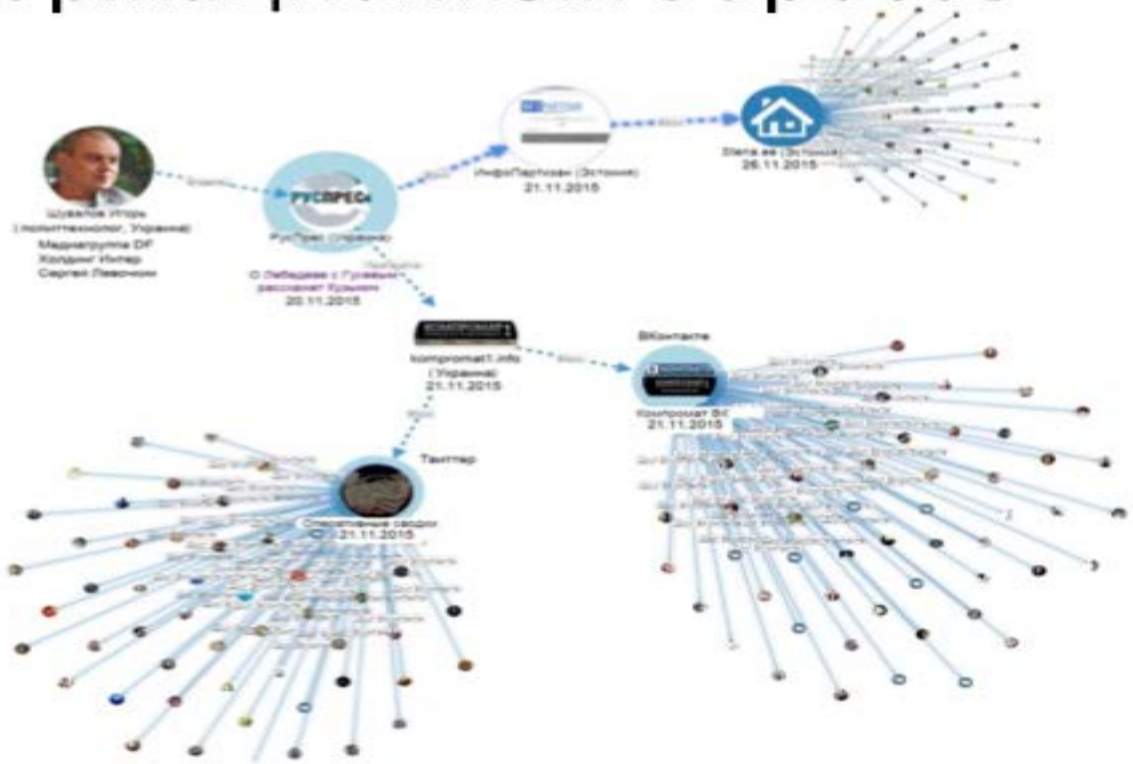
Контроль распространения информации



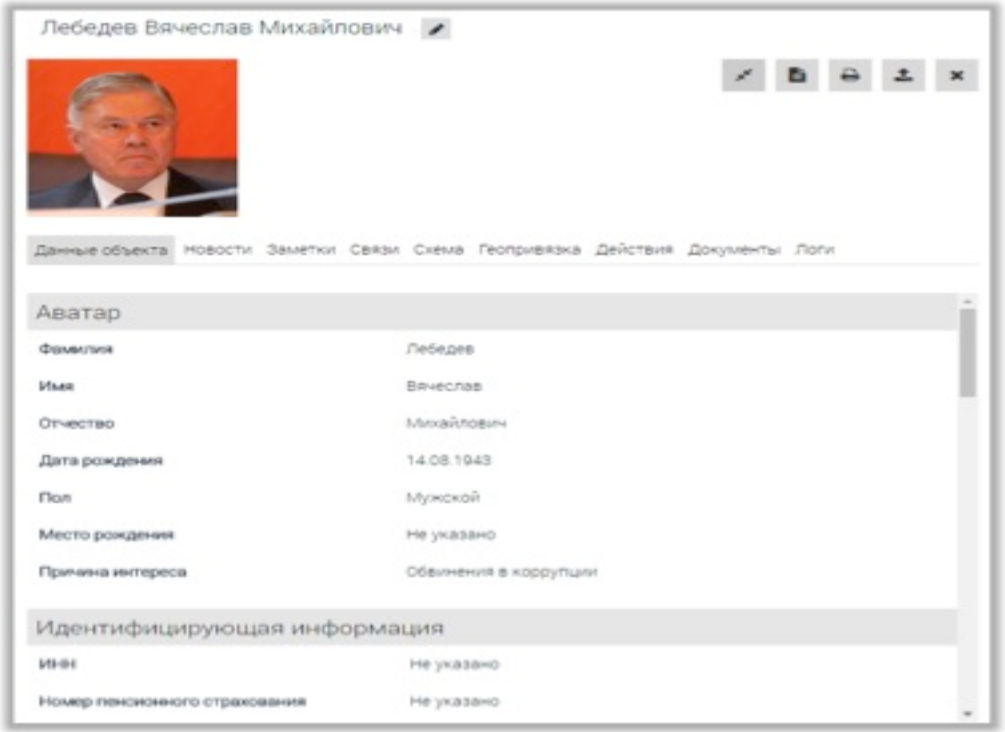
Автоматическое выявление ботов



Анализ источников информационных вбросов



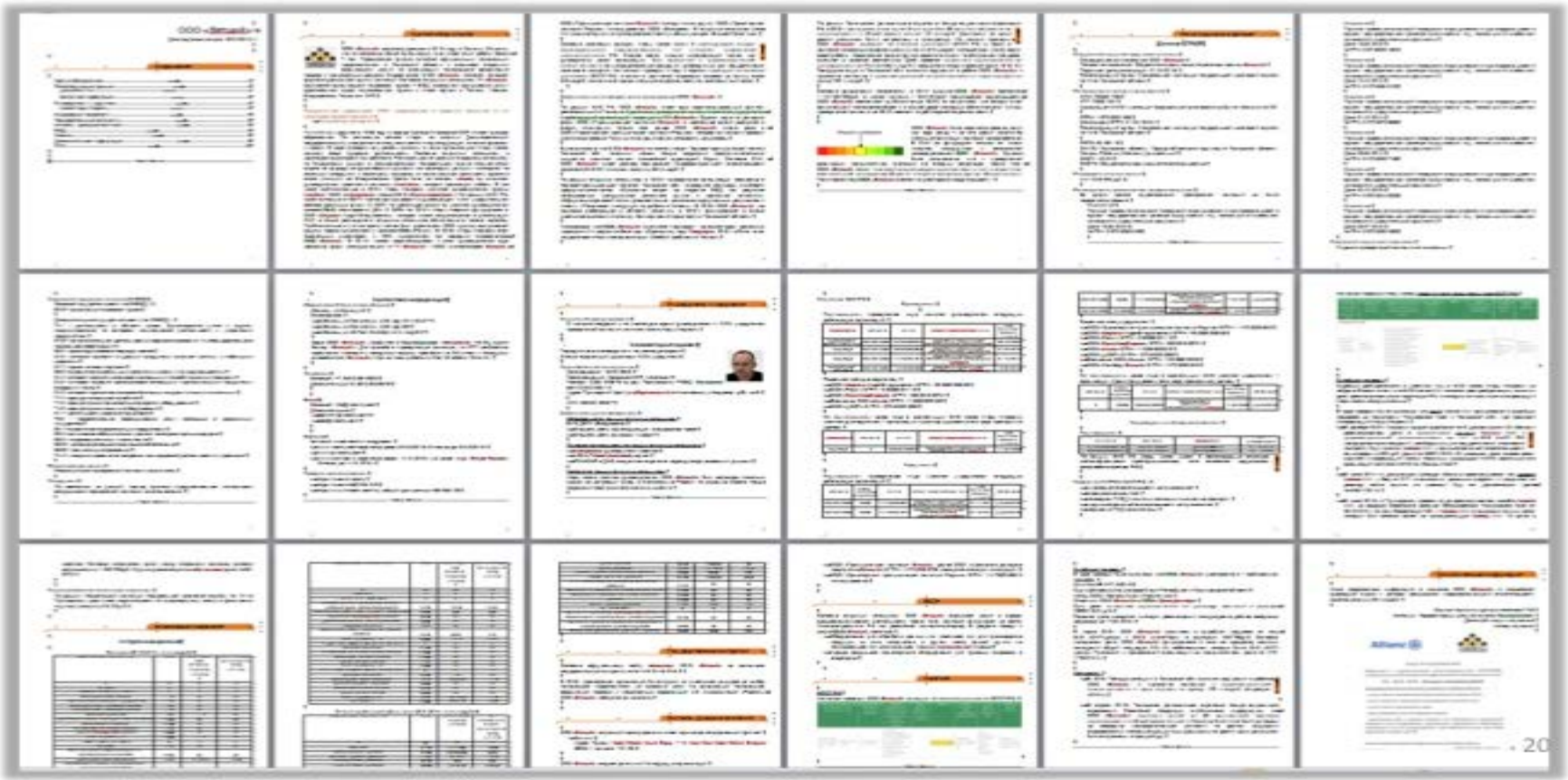
Ведение досье на объекты интереса



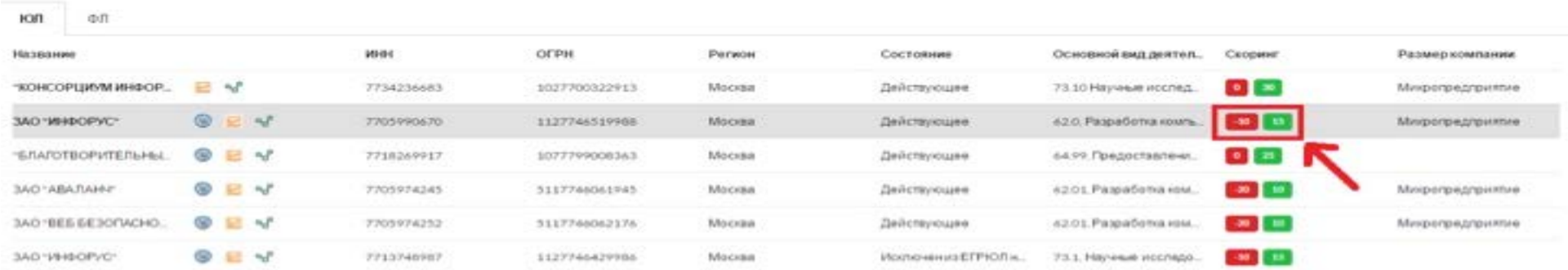
- Персона
- Компания
- Адрес
- Телефон
- Аккаунт
- Адрес e-mail
- Ip-адрес
- Автомобиль
- Номер счета
- и т.д.

AVALANCHE

Автоматическое построение отчетов и справок



Автоматическая проверка контрагентов

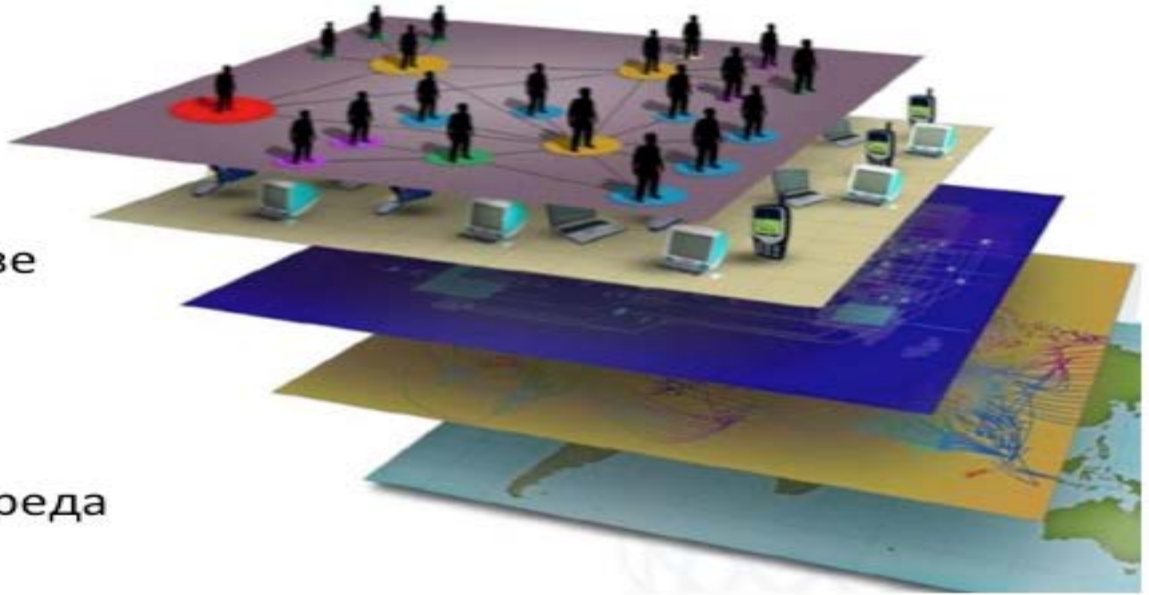


ЮЛ ФЛ

Название	ИНН	ОГРН	Регион	Состояние	Основной вид деятел...	Скоринг	Размер компании
"КОНСОРЦИУМ ИНФОР...	7734236683	1027700322913	Москва	Действующее	73.10 Научные исслед...	0 30	Микропредприятие
ЗАО "ИНФОРУС"	7705990670	1127746519988	Москва	Действующее	62.0, Разработка комп...	-50 53	Микропредприятие
"БЛАГОТВОРИТЕЛЬНЫ...	7718269917	1077799008363	Москва	Действующее	64.99, Предоставлени...	0 21	
ЗАО "АВАЛАНЧ"	7705974245	5117746061945	Москва	Действующее	62.01, Разработка ком...	-20 10	Микропредприятие
ЗАО "ВЕБ БЕЗОПАСНО...	7705974252	5117746062176	Москва	Действующее	62.01, Разработка ком...	-20 10	Микропредприятие
ЗАО "ИНФОРУС"	7713746987	1127746429986	Москва	Исключение из ЕГРЮЛ н...	73.1, Научные исследо...	-50 53	

Возможность авто-ассоциирования данных из различных баз

- Люди
- Идентичность в киберпространстве
- Информация
- Физическая инфраструктура
- Географическая среда



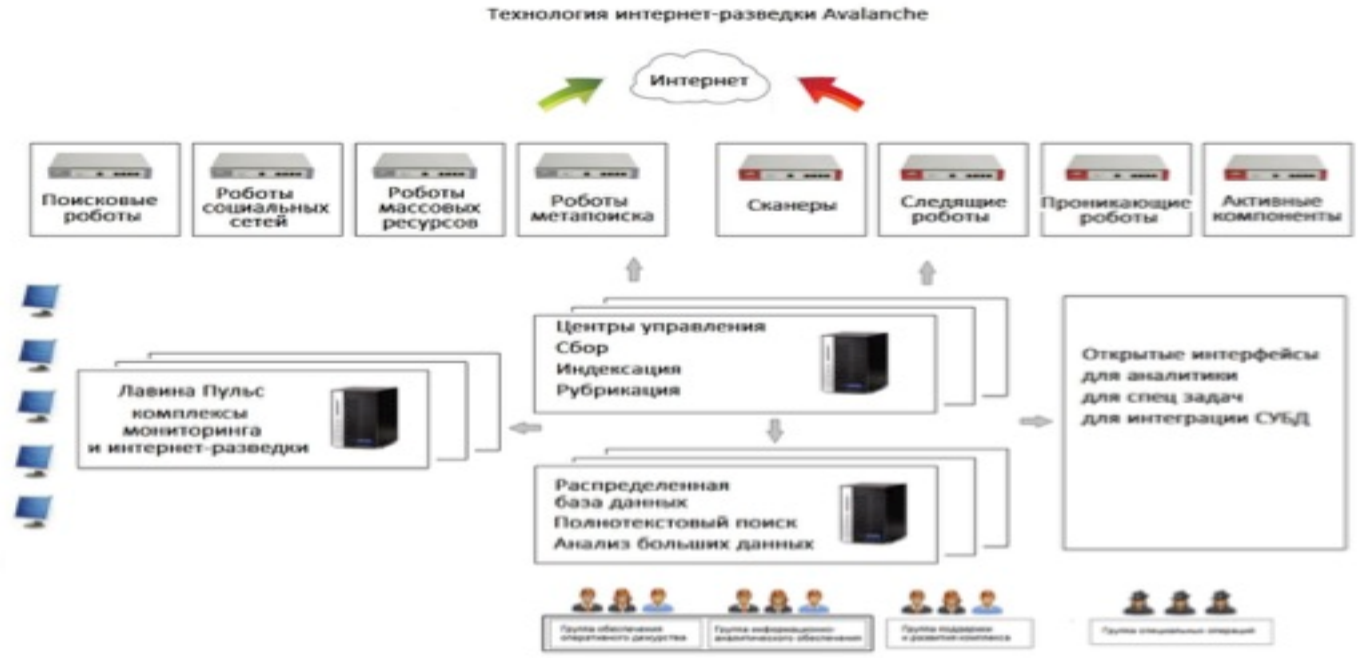
Базы данных за последние 15 лет

Пример проверки компании:

Ген. директор неоднократно судим за невозврат кредитов,

Прошлое учредительницы не соответствует официальной биографии

Технология интернет-разведки



- Более 20 типов роботов, более 60 типов сканеров
- Масштабируемый кластер управления
- Распределенная база данных
- Только открытый код и отсутствие рисков санкций
- Встроенные механизмы работы с большими данными

Система контроля защищенности веб-ресурсов

- Сканеры общей защищенности
- Сканеры утечек служебной и гос тайны
- Сканеры анализа конфигурации (18 шт.)
- Сканеры уязвимостей (27 шт.)
- Сканеры слабой аутентификации
- Сканеры комплексной проверки (3 шт.)
- Сканеры поиска стороннего кода
- Сканеры поиска внутренних документов

Пример: утечки конфиденциальной информации, служебной тайны и персональных данных

Открытое акционерное общество

«ВАРЬЕГАННЕФТЕГАЗ»

(ОАО «Варьеганнефтегаз»)

ПРОТОКОЛ № 9

Заседания Закупочной комиссии

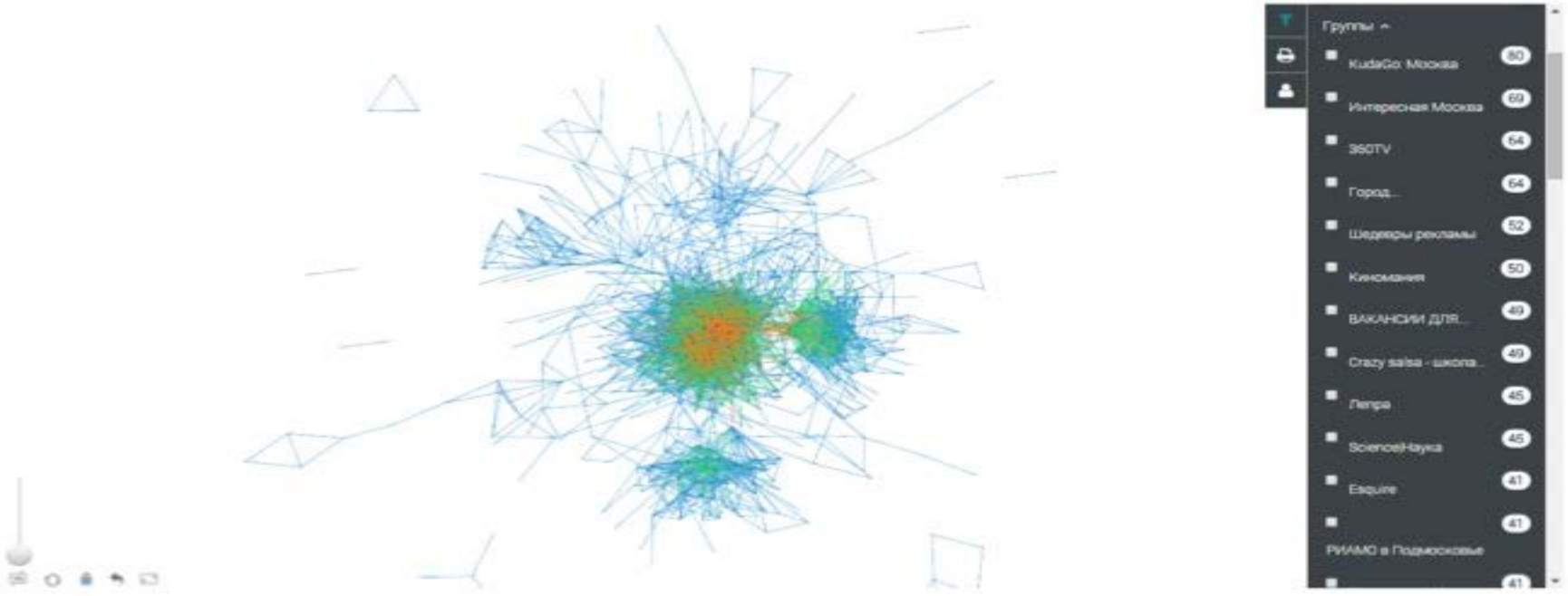
УТВЕРЖДАЮ

Доверенность № 41

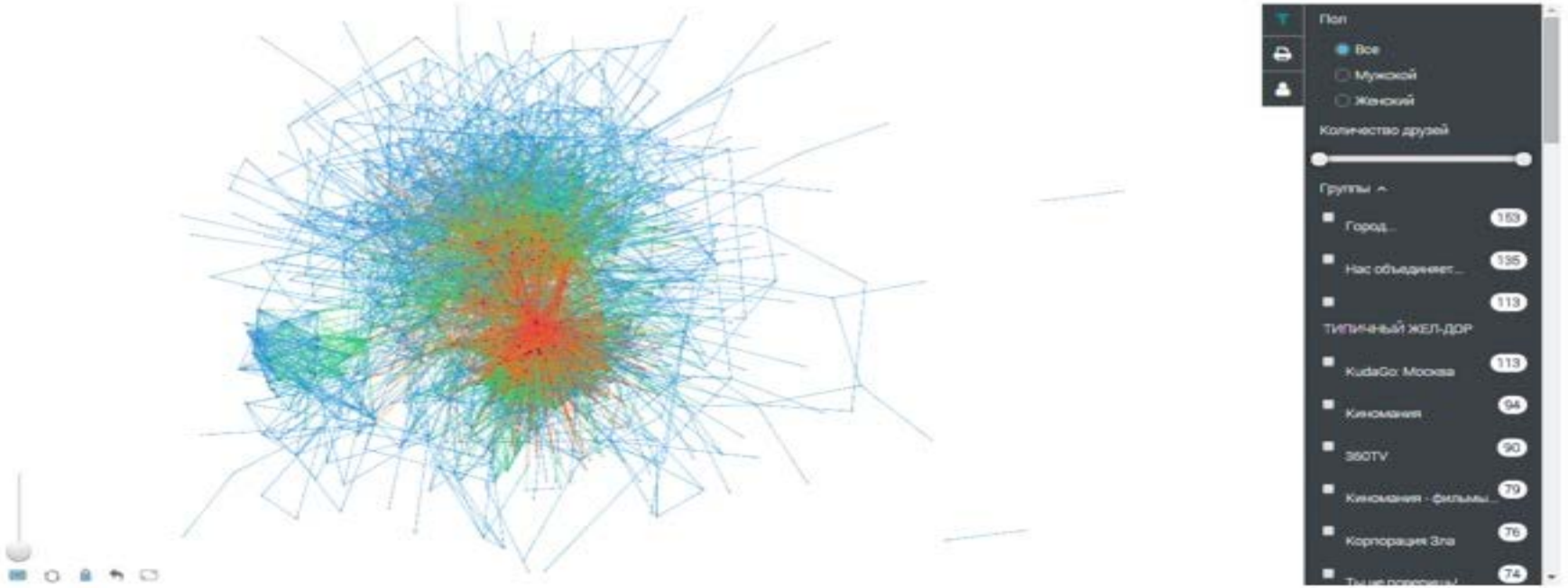
Конфиденциально. Только для служебного пользования.

http://zakupki.rosneft.ru/files/zakup/45799/2013-11/70803/prot/protokol_no_28_ot_23_10_2013.pdf
http://zakupki.rosneft.ru/files/zakup/45799/2013-11/72719/prot/protokol_no_29_ot_25.10.2013.pdf
http://zakupki.rosneft.ru/files/zakup/45799/2013-11/73698/prot/protokol_no_32_9_ot_06_11_2013.pdf
http://zakupki.rosneft.ru/files/zakup/45799/2013-11/71876/prot/protokol_zk_no30.pdf
http://zakupki.rosneft.ru/files/zakup/45799/2013-08/59005/prot/protokol_no_9_ot_31.07.2013.pdf
http://zakupki.rosneft.ru/files/zakup/202/2013-07/58527/docs/dogovor.pdf

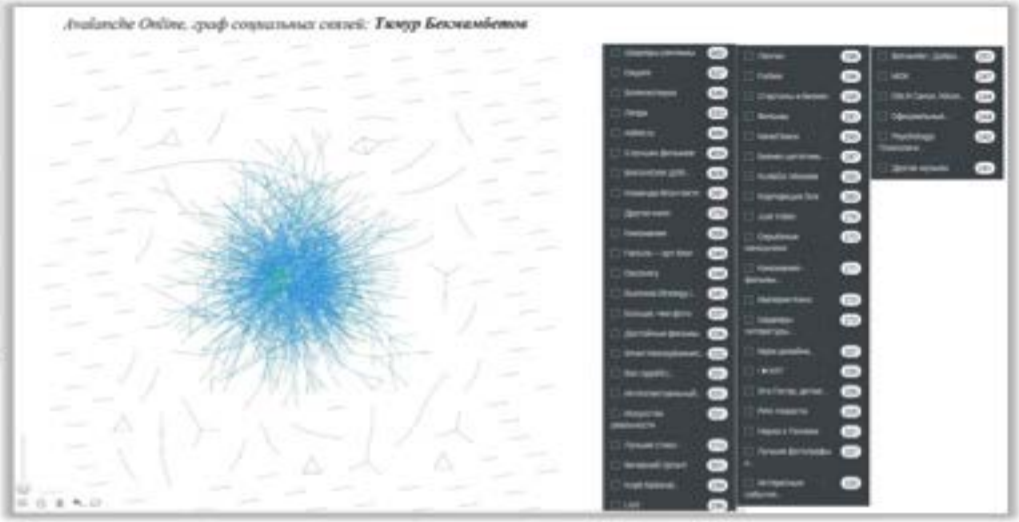
Построение социальных портретов
Пример: журналист

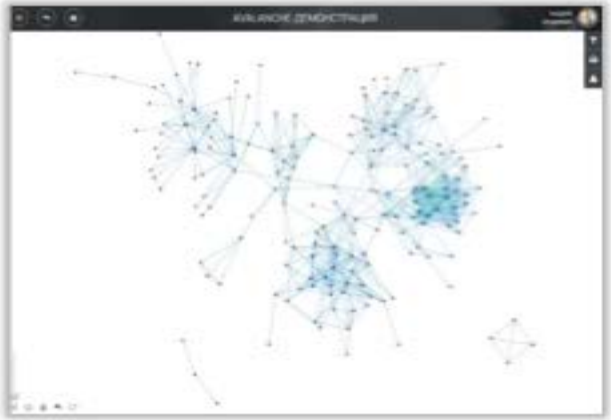


Социальный портрет - политик

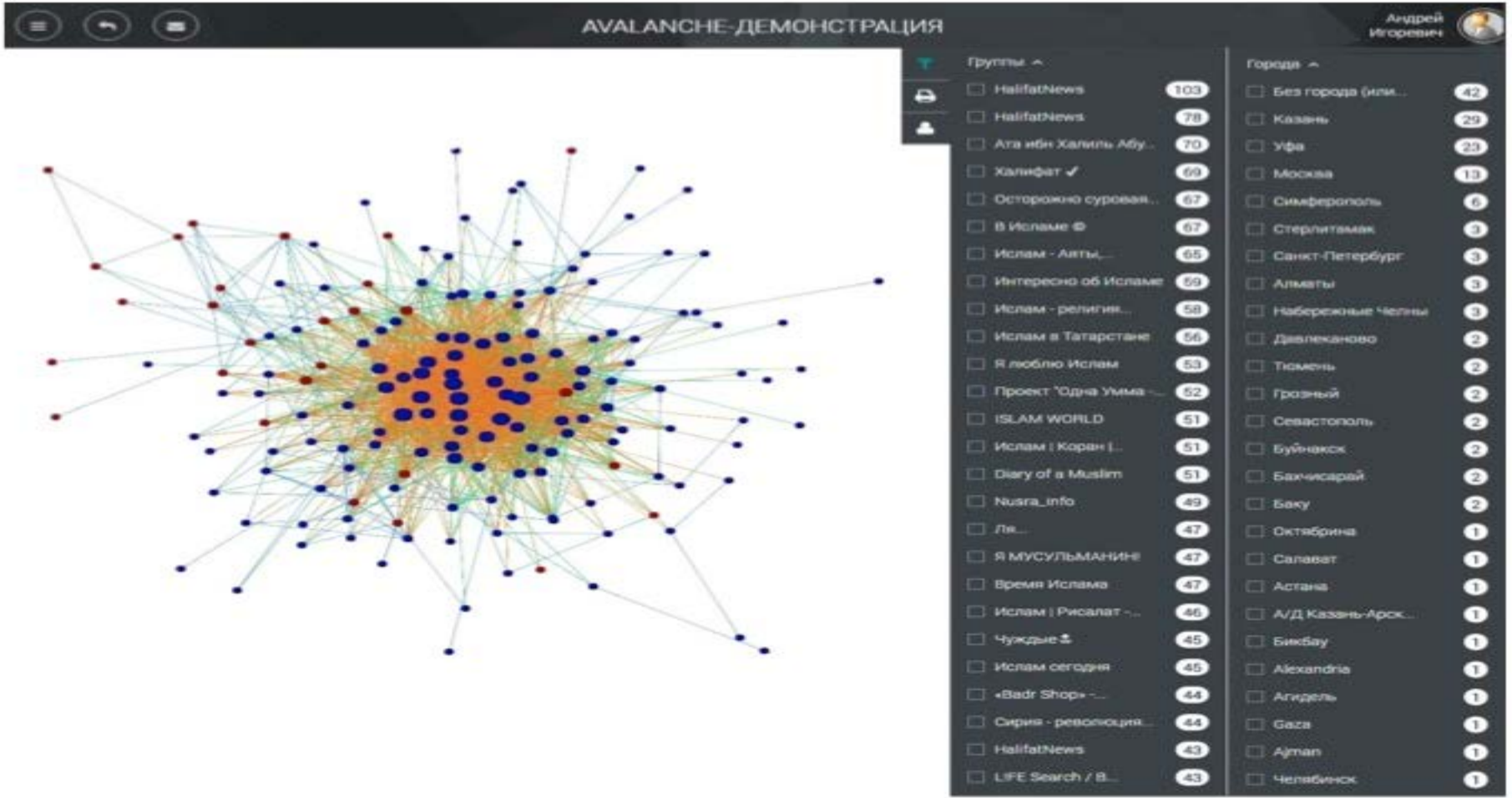


Социальный портрет – блогер

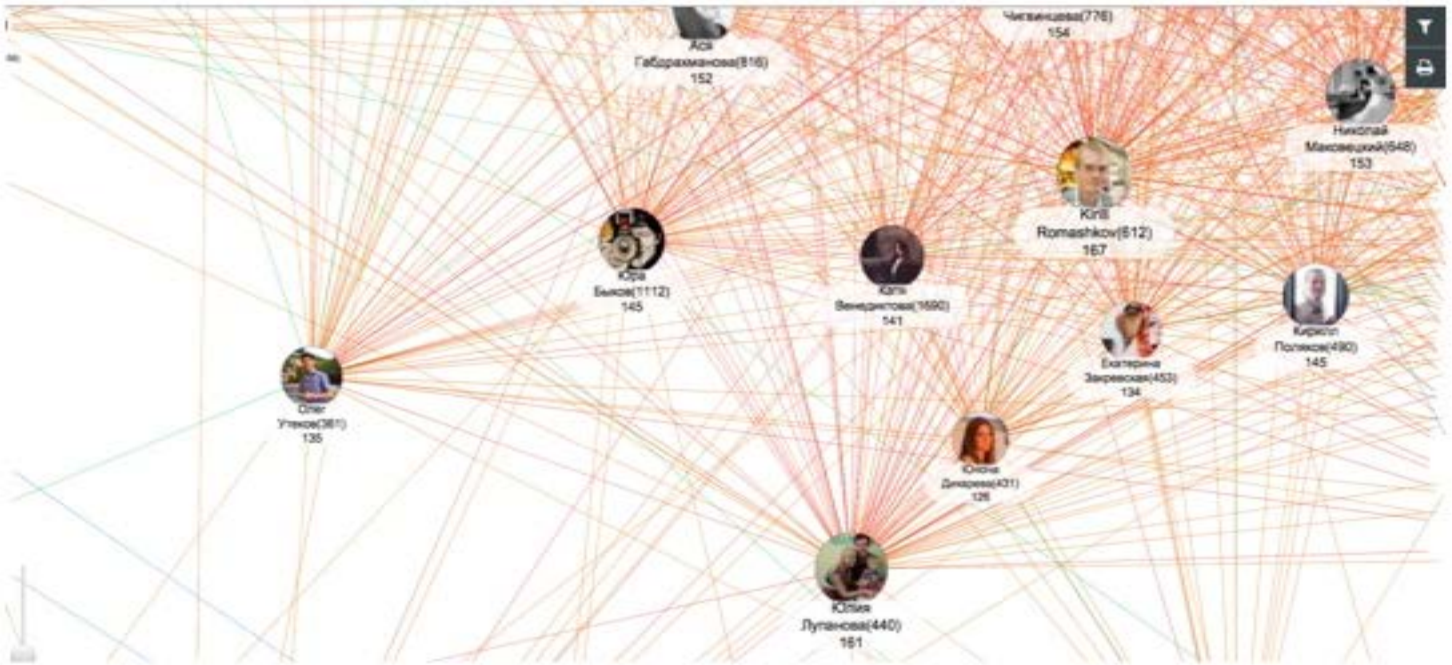




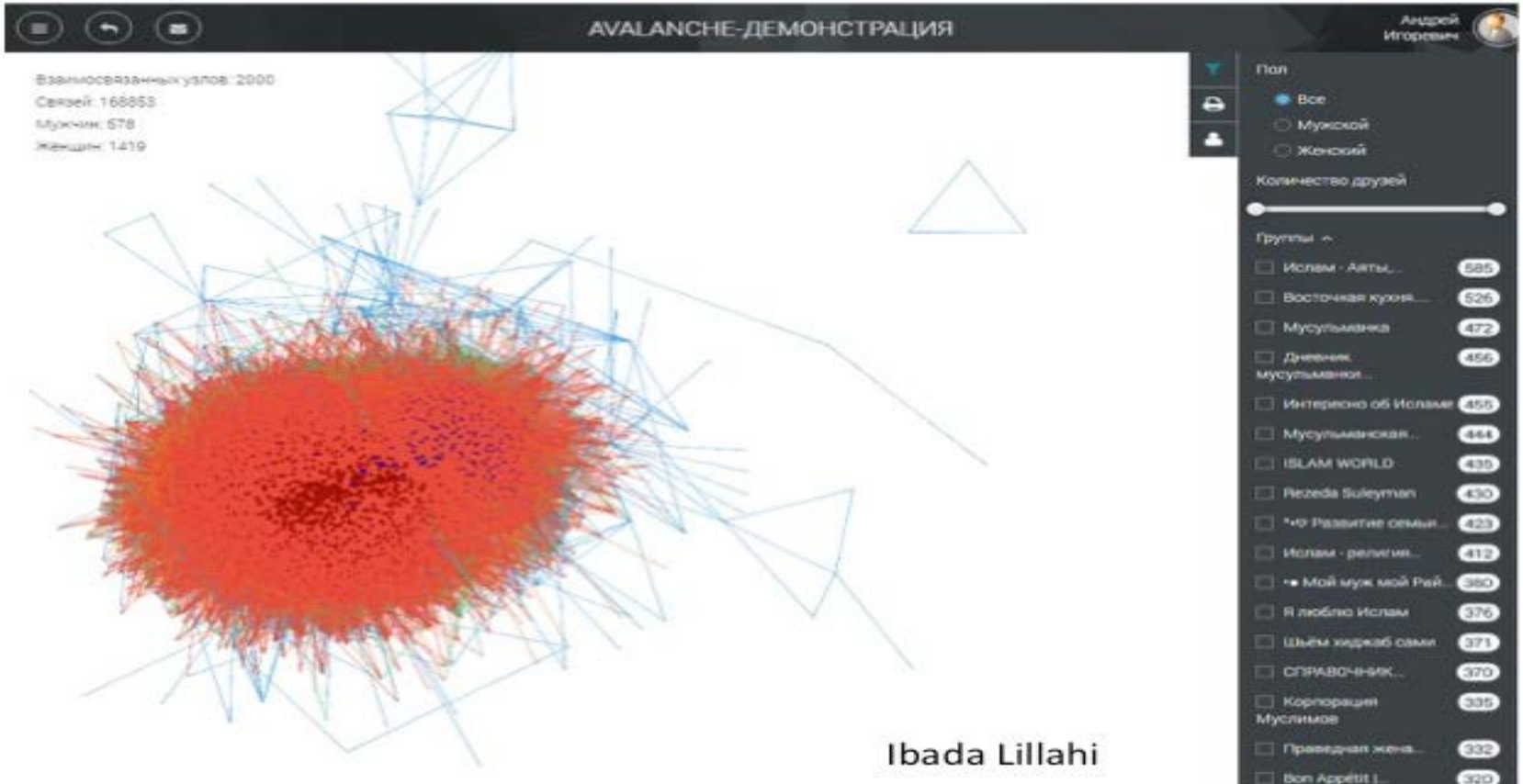
Экстремистская группировка



Детализированный анализ



Социальный портрет – вербовщица



Краткие результаты тестирования информационно-поисковой системы «Лавина Пульс»

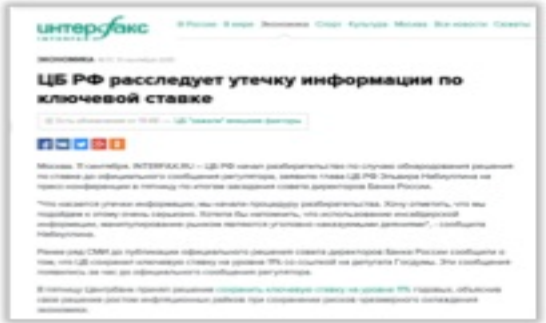
Лавина Пульс – система контроля оперативной обстановки в Сети

Система Лавина Пульс объединяет в себе
расширенные возможности интернет-поиска
(на основе собственного семейства поисковых роботов)
и средства автоматизированного ведения досье
с возможностями интеллектуальной аналитической обработки больших данных (Big Data)
и выявления актуальных угроз в сети Интернет и социальных сетях (слухи о предстоящем банкротстве банков, компромат и т.п.), которые могут привести к возникновению репутационных рисков и проблемам с устойчивостью участников банковского сектора.

Преимущества системы Лавина Пульс

1. Обнаружение угроз на ранних стадиях

- Пример: Утечка информации в Банке России (сентябрь 2015)
- Одной из наиболее громких тем обсуждения в СМИ стала утечка информации об изменении ключевой ставки рефинансирования Банком России в сентябре 2015 года. Ряд СМИ опубликовал информацию об изменении ставки рефинансирования до официального решения Центробанка, что в значительной степени повлияло на ход торгов на финансовых рынках.
- Система Лавина Пульс позволила моментально отслеживать распространение информации в СМИ и реагировать на соответствующие публикации максимально оперативно, на ранней стадии.



Преимущества системы Лавина Пульс

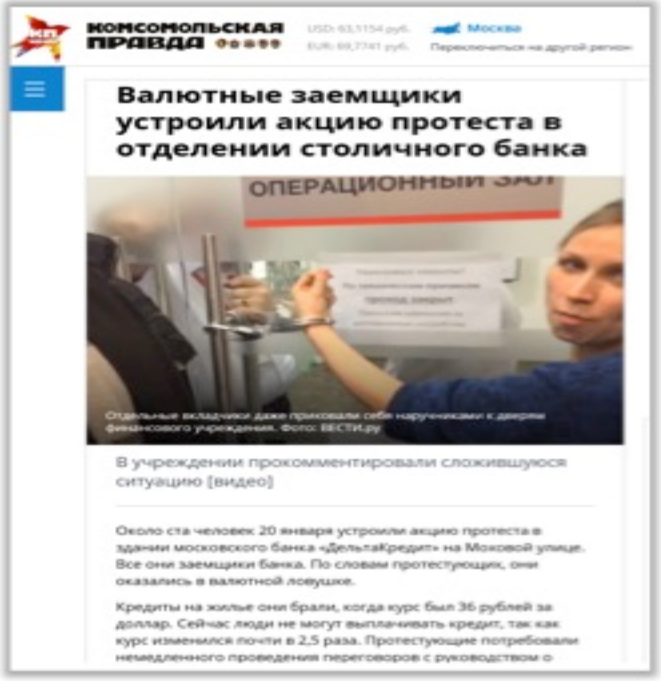
1. Обнаружение угроз на ранних стадиях

- Пример: Акции протеста клиентов «Байкал-банка»
- Система Лавина Пульс следит за информационным фоном вокруг проблемных банков и на ранних стадиях оповещает о возможных проблемах, в том числе реакции жителей на его закрытие, а также предоставляет информацию по поведению вкладчиков.

Преимущества системы Лавина Пульс

2. Раннее обнаружение резонансных тем.

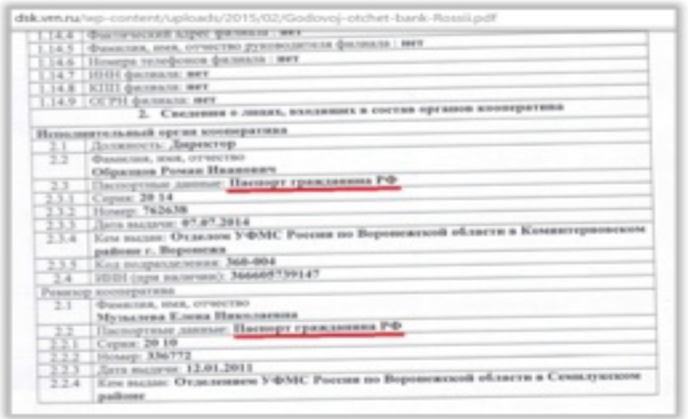
- Пример: Акции протеста валютных заемщиков (20.01.2016)
- Изначально, после ослабления курса рубля, активность валютных заемщиков началась в социальных сетях, затем – разовые выступления, и только после этого волна была подхвачена федеральными и региональными СМИ.
- Система Лавина Пульс позволила идентифицировать угрозу еще на уровне социальных сетей и региональных СМИ, задолго до того, как история получила федеральное освещение.



Преимущества системы Лавина Пульс

3. Обнаружение утечек внутренней и конфиденциальной информации, персональных данных и др. с выявлением первоисточника утечки.

- Специализированные роботы системы Лавина Пульс автоматически обнаруживают утечки секретной, конфиденциальной и внутренней информации, а также персональных данных и коммерческой тайны
- Пример: разглашение персональных данных в документе «Годовой отчет Банк России» ДНК «Доступное жилье»


dnk.vrn.ru/wp-content/uploads/2015/02/Godovoj-otchet-bank-Rossii.pdf

1.14.4	Фактический адрес филиала: нет
1.14.5	Фамилия, имя, отчество руководителя филиала: нет
1.14.6	Номера телефонов филиала: нет
1.14.7	ИНН филиала: нет
1.14.8	КПП филиала: нет
1.14.9	ОГРН филиала: нет
2.	Сведения о лицах, входящих в состав органов кооператива
Исполнительный орган кооператива	
2.1	Должность: Директор
2.2	Фамилия, имя, отчество: Образцов Роман Иванович
2.3	Паспортные данные: Паспорт гражданина РФ
2.3.1	Серия: 20 14
2.3.2	Номер: 762638
2.3.3	Дата выдачи: 07.07.2014
2.3.4	Кем выдан: Отделом УФМС России по Воронежской области в Коминтерновском районе г. Воронежа
2.3.5	Код подразделения: 360-004
2.4	ИНН (при наличии): 366605739147
Ревизор кооператива	
2.1	Фамилия, имя, отчество: Музыкина Елена Николаевна
2.2	Паспортные данные: Паспорт гражданина РФ
2.2.1	Серия: 20 10
2.2.2	Номер: 336772
2.2.3	Дата выдачи: 12.01.2011
2.2.4	Кем выдан: Отделением УФМС России по Воронежской области в Семилукском районе

Преимущества системы Лавина Пульс

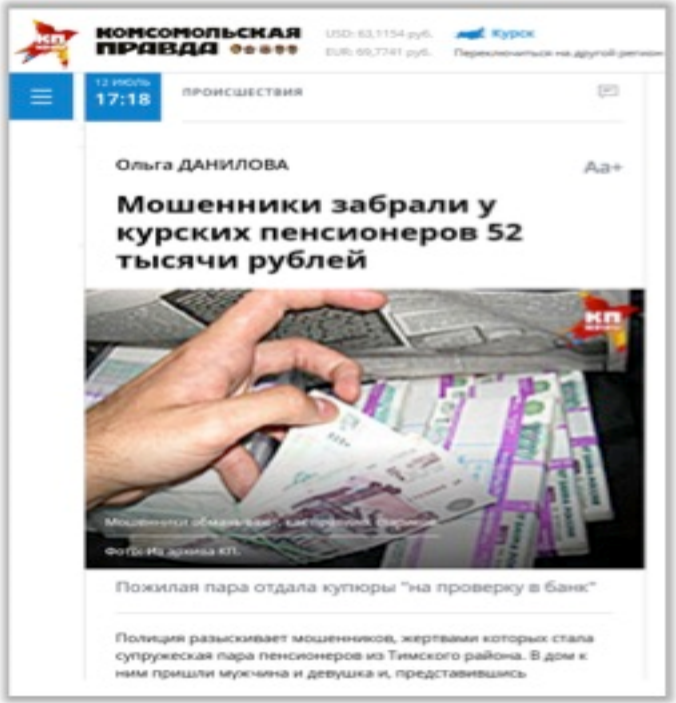
4. Анализ путей распространения информации

- Пример: информационная атака на руководство Верховного суда РФ (сентябрь-октябрь 2015)
- Система **Лавина Пульс** позволила не только мгновенно получать информацию о новостных вбросах, но и отследить динамику информационных сообщений вплоть до источника.

Преимущества системы Лавина Пульс

5. Выявление признаков противоправной деятельности в сети

- Пример: в июне 2016 г в Курске мошенники под предлогом подготовки денежной реформы похитили сбережения у нескольких пенсионеров
- Система Лавина Пульс зафиксировала появление и распространение мошеннической схемы задолго до официального пресс-релиза МВД



Преимущества системы Лавина Пульс

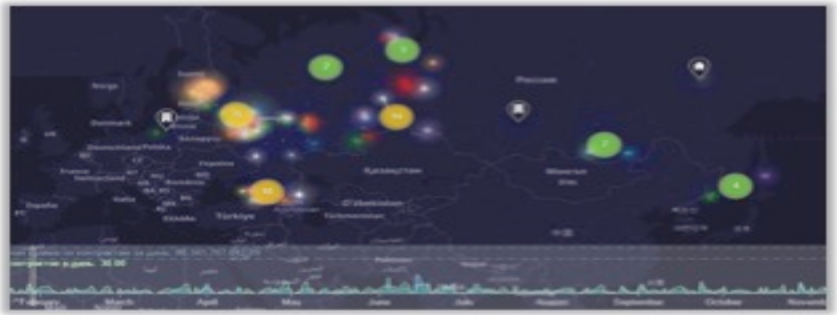
6. Сбор досье на объекты интереса

- Система **Лавина Пульс** позволяет формировать справки и пополнять досье на объекты интереса – организации и персоны
- Сбор информации происходит как из баз данных, так и из различных интернет-источников, включая социальные сети
- Система также строит «социальные портреты» сетевой активности интересующих персон

Преимущества системы Лавина Пульс

7. Тепловые карты общей обстановки

- Система Лавина Пульс позволяет строить «тепловые карты» активности в социальных сетях по заданным темам
- Пример: в декабре 2014 года по России массово распространялись слухи о проблемах со счетами и картами Сбербанка
- Система Лавина Пульс помогла Сбербанку взять ситуацию под контроль



Преимущества системы Лавина Пульс

8. Сканеры защищенности

- В состав **Лавина Пульс** входит семейство сканеров защищенности, которые постоянно анализируют стойкость заданных интернет-ресурсов к различным видам хакерских атак
- В системе более 60 сканеров
- *Пример: результаты сканирования портала Альфа-банка*

Сайт: alfabank.ru

16.01.2015 20:53:56 16.01.2015 10:04:00

обнаружены критические проблемы и уязвимости

Сайт: alfabank.ru

Дата исследования: **2015-01-16 10:40:02**
Статус: обнаружены критические проблемы и уязвимости
Найдены:

Служебные разделы
Время обнаружения: 2015-01-15 15:24:53

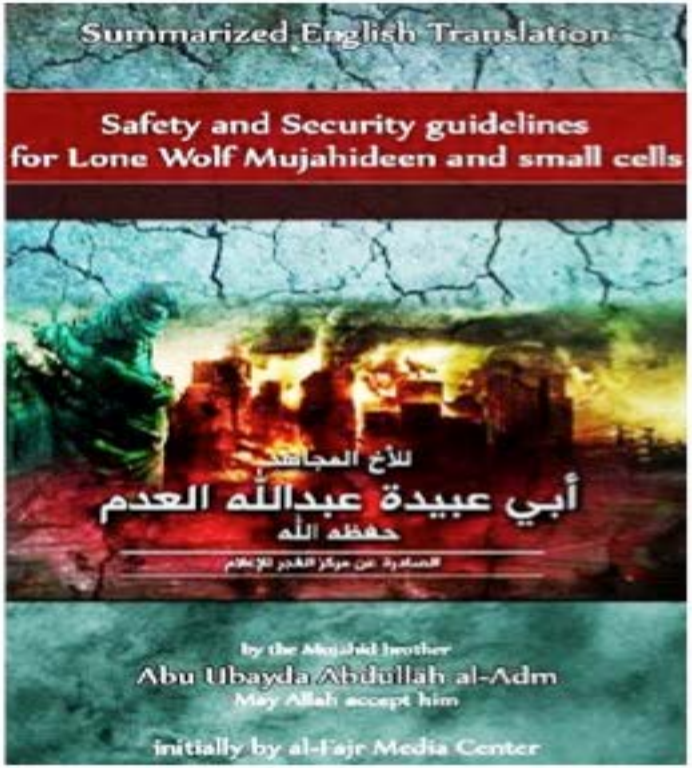
Служебные разделы
с открытым доступом:
/sitemap.xml
/restricted/
/adm/
/i/
/security/
/p/
/docs/
доступ закрыт:
/wholesale-login.php
/ai-bolit.php
/adminhome.php
/admin.php
/.htpasswd
/adminka.php

Выводы и рекомендации

По результатам проведённого тестирования системы «Лавина Пульс» установлено следующее:

1. Все функции системы **Лавина Пульс**, заявленные в эксплуатационной документации и проверенные в ходе тестирования полностью реализованы.
2. Система **Лавина Пульс** в ходе тестирования зарекомендовала себя как инструмент выполнения информационно-аналитической работы и может быть рекомендована к использованию в Банке России

Пример работы в «сером» интернете: Методички террористов по бескомпроматной работе



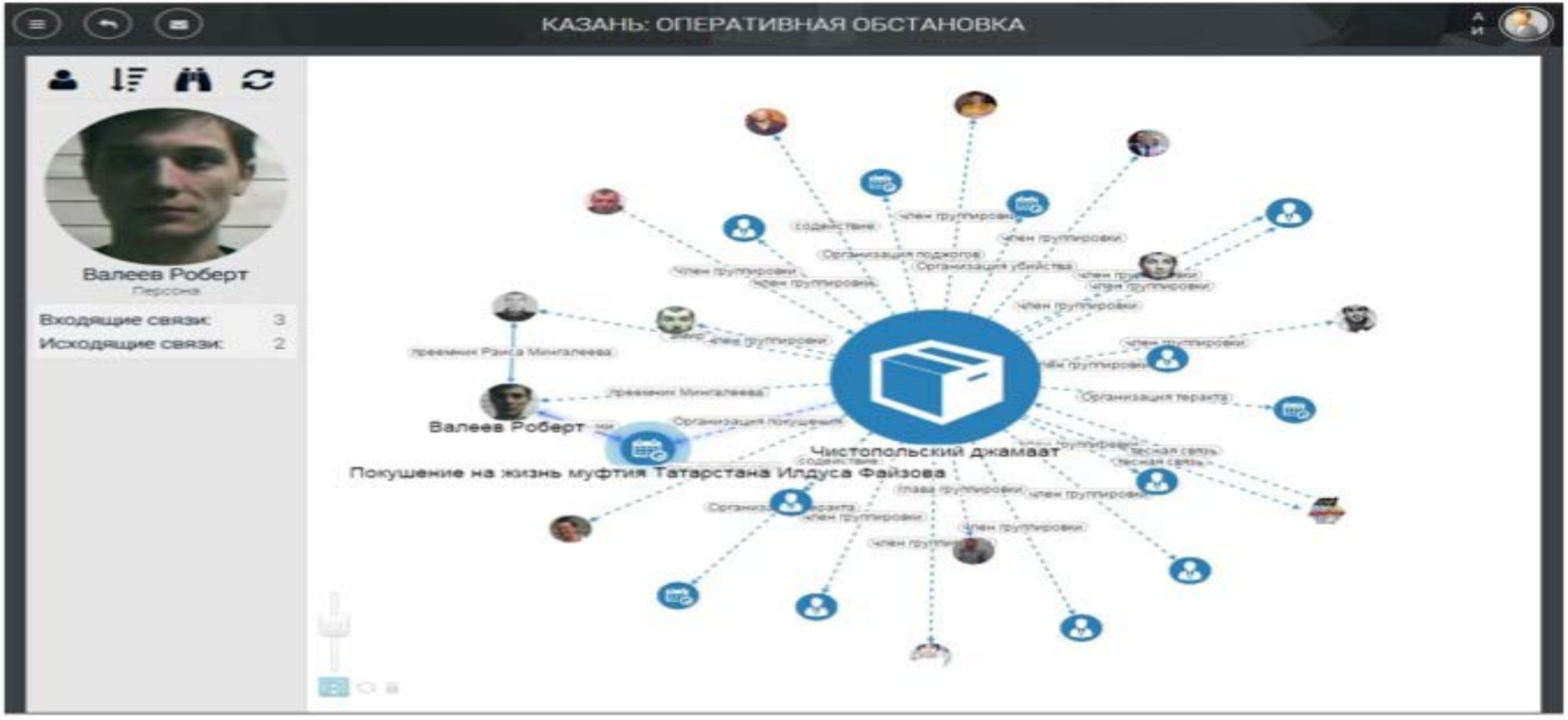
Пример: контроль оперативной обстановки

Казань, чемпионат мира по водным видам спорта, 2015

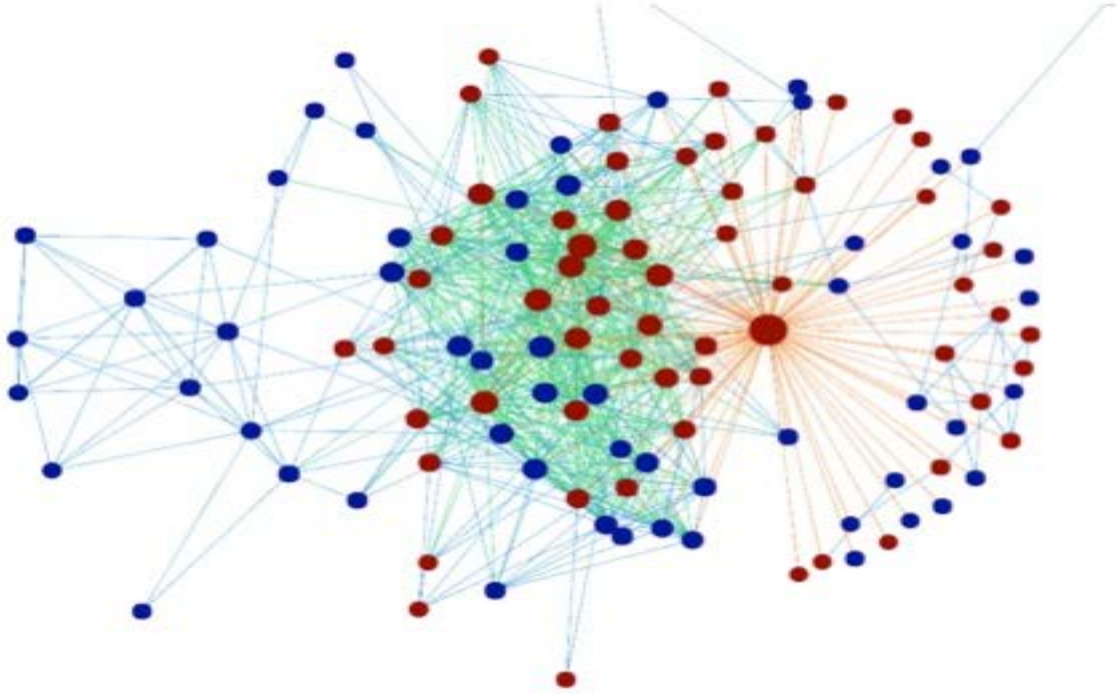
FINA WORLD CHAMPIONSHIPS
KAZAN
RUSSIA 2015

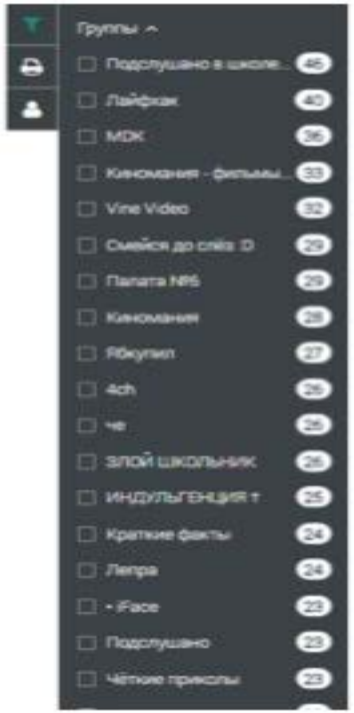
- Общая обстановка
- Освещение ЧМ, критика
- Митинги, выступления
- Радикалы, оппозиция
- Межконфессиональные
- Межнациональные
- Правонарушения
- Радикальный ислам
- Критика полиции

Анализ связей остатков группировки «Чистопольский джамаат»

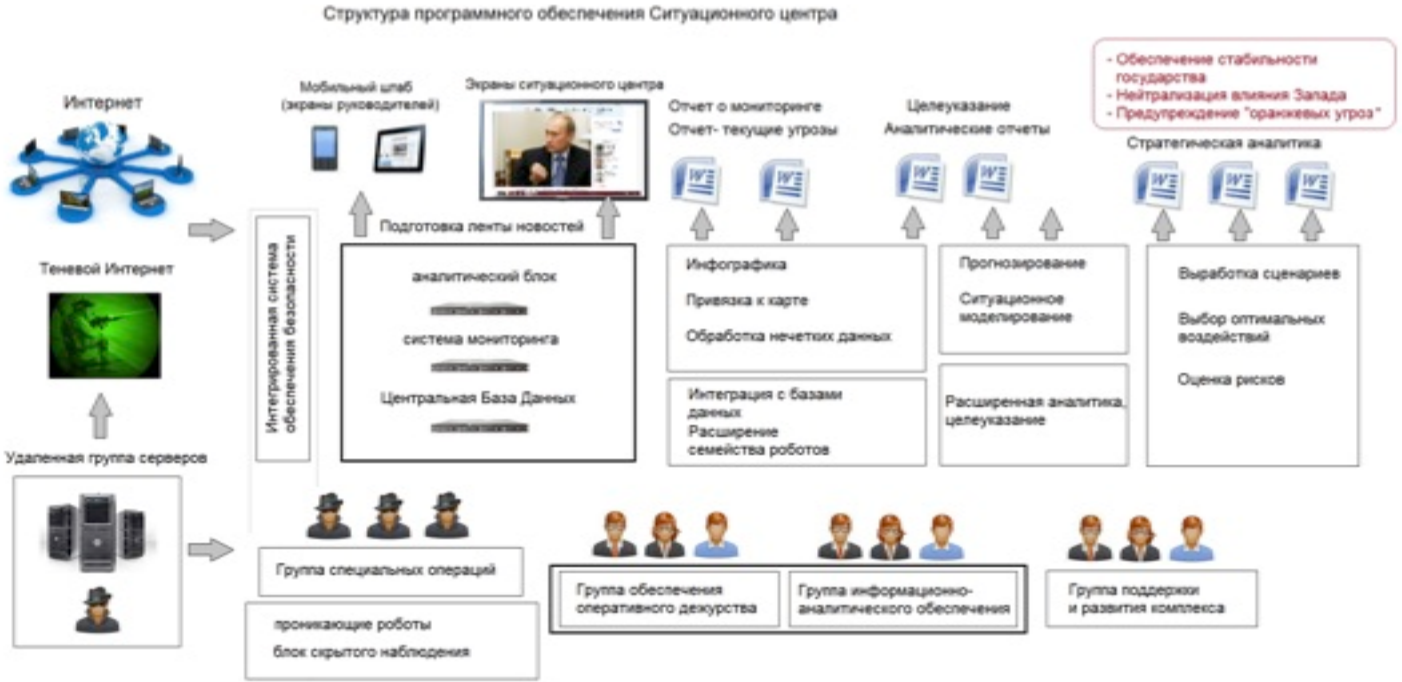


Социальный портрет - подросток





Комплекс Avalanche – основа построения современных ситуационных центров

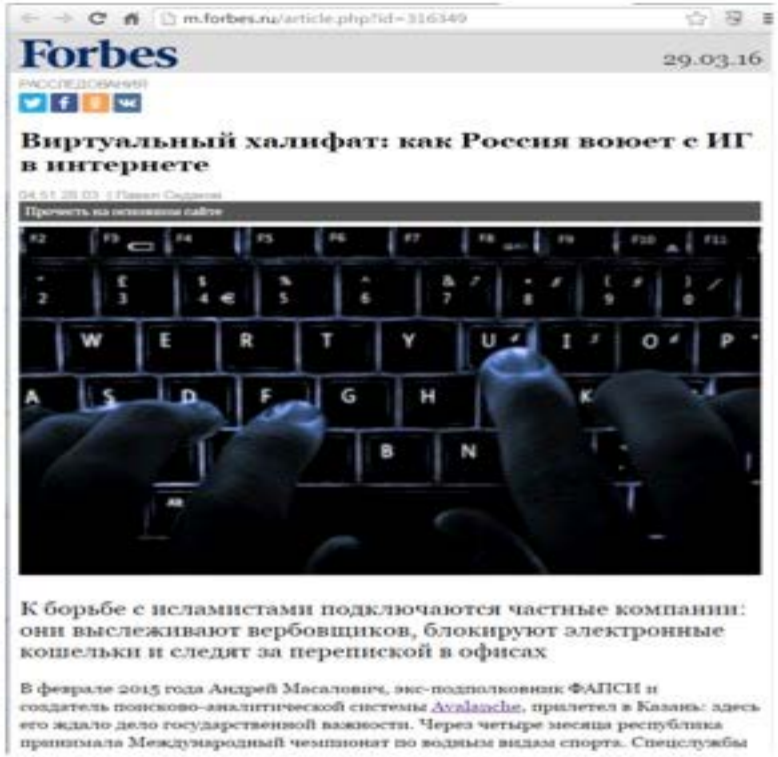


Преимущества технологии Avalanche:

Обучение пользователей

- Учебный курс «**Конкурентная разведка в Интернете**» - 2 дня
- Учебный курс «**Информационная безопасность в Интернете**» – 3 дня
- Учебный курс «**Технологии информационного противоборства в Интернете**» – 2 дня

О поисковой технологии Avalanche: Forbes Russia N2, 2015 и др.



Спасибо за внимание ☺

Масалович Андрей Игоревич

- E-mail: am@inforus.biz
- Phone: +7 (964) 577-2012