



# Каз'Хак'Стан

# Kaz'Hack'Stan

Алматы  
5 ОКТЯБРЯ  
2018

Ежегодная практическая конференция  
по вопросам информационной безопасности

conference



# Остаться невидимкой

Андрей Масалович

Andrei Masalovich

Live smart, live longer

[am@avl.team](mailto:am@avl.team)

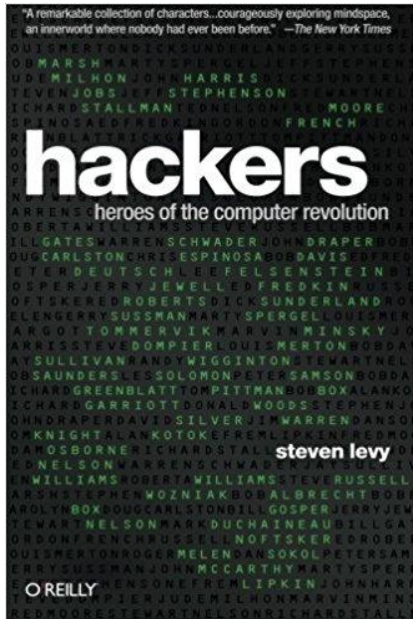
# Hackers. Evolution

## Хакеры. Эволюция

Романтики

Преступники

Спецназ  
информационной  
войны



Heroes



Cyber Crime



Cyber Army

# Bachosens: Highly-skilled petty cyber criminal with lofty ambitions targeting large organizations



Rdata results for ANY/2a01:4f8:120:8355::

Returned 19 RRs in 0.11 seconds.

akb.md.	AAAA	2a01:4f8:120:8355::1
www.akb.md.	AAAA	2a01:4f8:120:8355::1
static.akb.md.	AAAA	2a01:4f8:120:8355::1
akkumulator.md.	AAAA	2a01:4f8:120:8355::1
www.akkumulator.md.	AAAA	2a01:4f8:120:8355::1
xxhost.ru.	AAAA	2a01:4f8:120:8355::1
www.xxhost.ru.	AAAA	2a01:4f8:120:8355::1
ddns.su.	AAAA	2a01:4f8:120:8355::1
bbxapp.com.	AAAA	2a01:4f8:120:8355::1
www.bbxapp.com.	AAAA	2a01:4f8:120:8355::1
ip2name.com.	AAAA	2a01:4f8:120:8355::1
ip2name.net.	AAAA	2a01:4f8:120:8355::1
xn--ilaj.net.	AAAA	2a01:4f8:120:8355::1
lastmd.org.	AAAA	2a01:4f8:120:8355::1
www.lastmd.org.	AAAA	2a01:4f8:120:8355::1
oyy.name.	AAAA	2a01:4f8:120:8355::1
mail.oyy.name.	AAAA	2a01:4f8:120:8355::1
noip.name.	AAAA	2a01:4f8:120:8355::1
xn--ilaj.name.	AAAA	2a01:4f8:120:8355::1

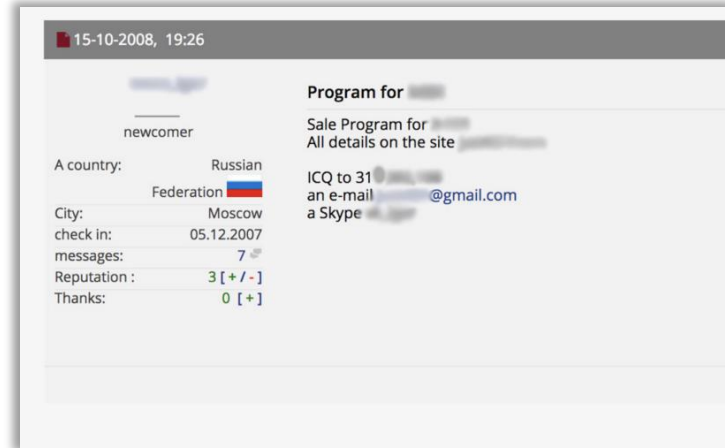


- Сложное заказное malware
- Целевой фишинг
- Эфемерные AES-ключи
- IPv6, DGA,DDNS
- Связь через DNS, ICMP, HTTP

- Исходный код на VirusTotal
- Распространяется с играми
- Кейлоггер без обфускации
- Менее 20 доменов в год
- Имя домена в коде

# Internet Intelligence

Если использовать методы интернет-разведки...



- Игорь С\*\*\*\*\*
- Тирасполь
- Телефон: \* \*\*\* \*\* \* \*\* \*
- E-mail: \*\*\*\*\*@gmail.com

# Мы – дети в мире умных вещей

## Военные – дети с гранатой



- Высокоточное оружие
- Умное оружие
- Автономное летальное оружие
- Сетецентрическая война

# Honeypots

A **honeypot** is a decoy computer system for trapping hackers or tracking unconventional or new hacking methods.

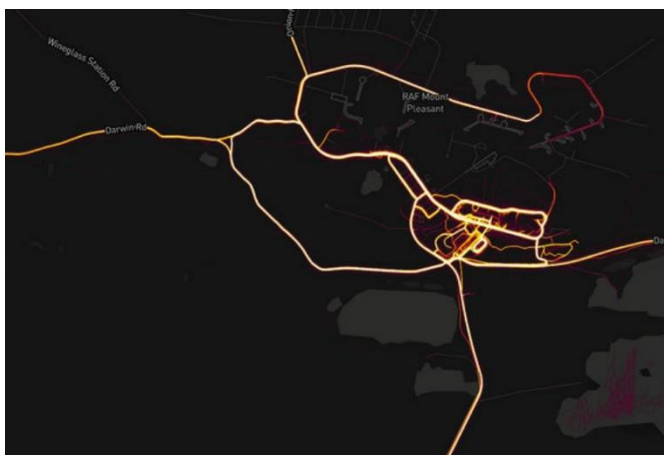
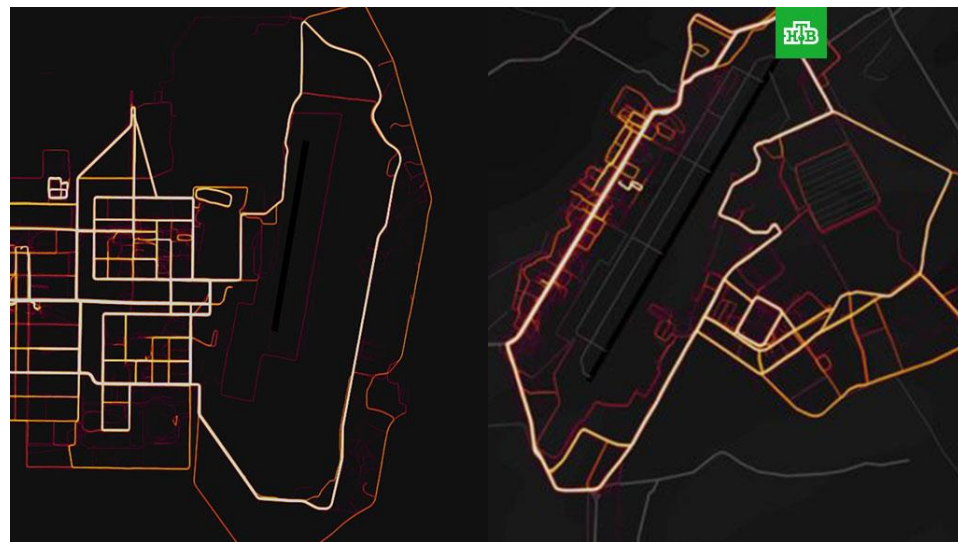


Кто первым клюнул на приманку?

- Министерство обороны одной из стран СНГ
- Антивирусная компания
- Спецслужба одной из стран СНГ

# Fitness app Strava lights up staff at military bases

## Фитнес-трекер Strava выдал расположение военных баз США



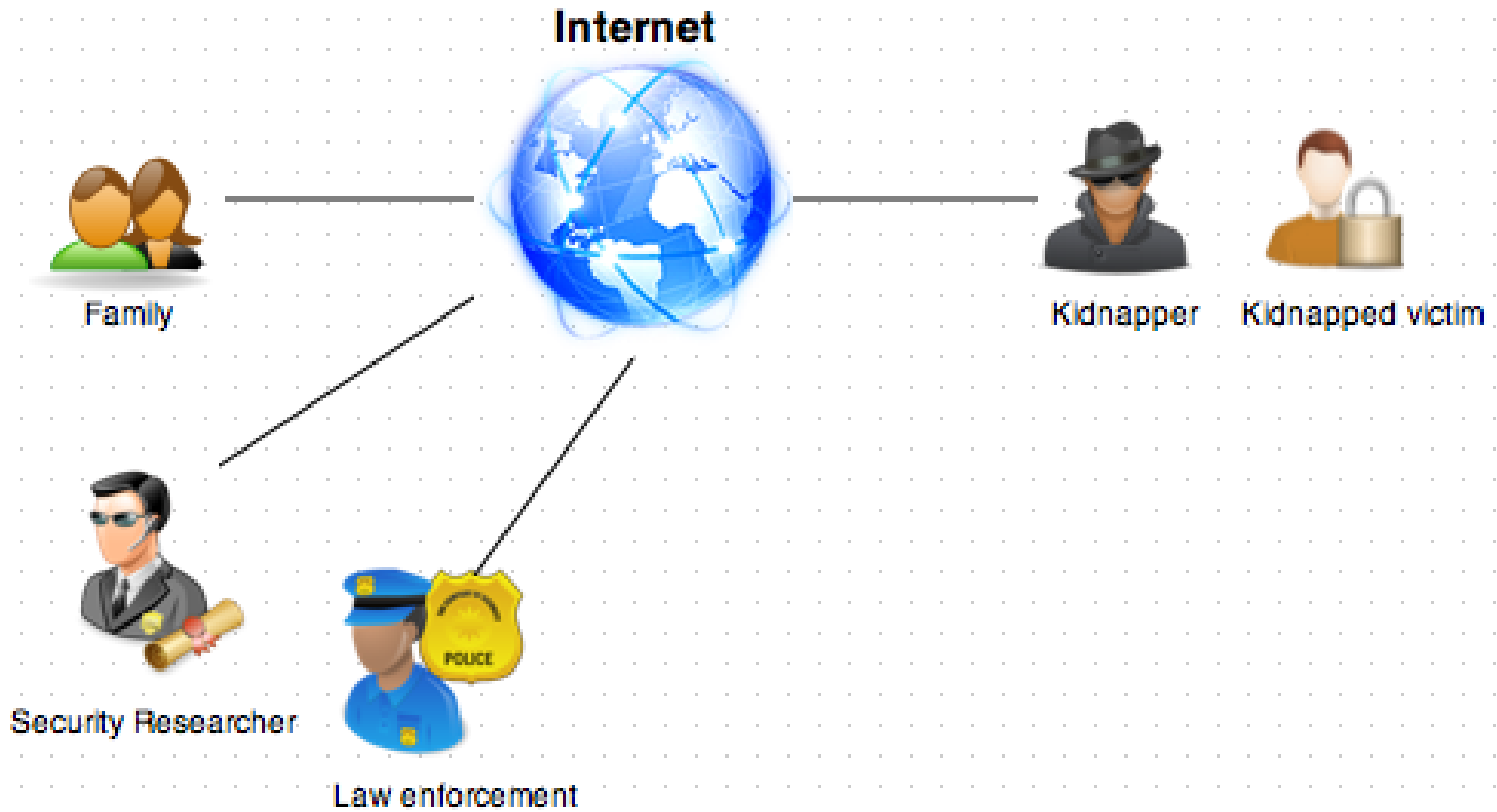
*Working off the IP address, U.S. investigators identified Guccifer 2.0...*

Скрывайте IP. Всегда.





# «Адресные ловушки»



# Что значит: «Не оставлять следов?»

- Безуликовость
- Недостаточность доказательной базы
- Скрытие присутствия
- Маскировка
- Размывание цели
- Ложный след
- ...
- Легенда прикрытия

# Digital Forensics

**Digital forensics** (sometimes known as **digital forensic science**) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.

**Форензика** (компьютерная криминалистика, расследование киберпреступлений) — прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств



Source: Rocky Mountain

# Прячем данные

- Безвозвратное уничтожение
- Невидимые разделы
- TrueCrypt
- Криптоконтейнеры
- Стеганография
- «Двойное дно»

# Digital Footprint Наш цифровой след



Новости



Интернет



Бизнес



Финансы



Недвижимость



Биография



Документы



Семья



Аккаунты



Привычки



Местоположение



Гаджеты



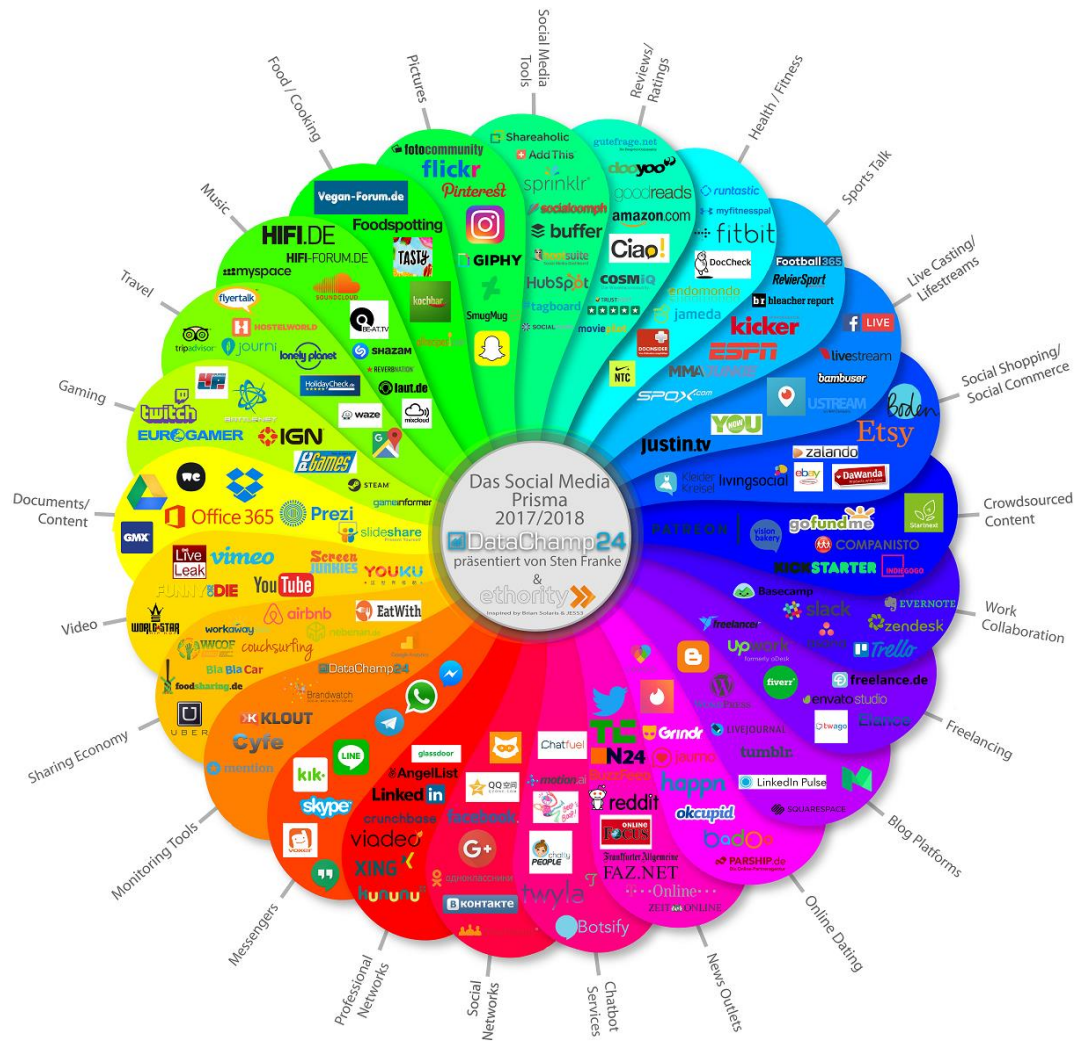
Социальные сети



Проблемы с законом

# OSINT (Open Source Intelligence)

- Разведка по открытым источникам



# Using OSINT...



# Источник утечек личной информации – базы удаленных страниц в соцсетях

Собрано более **174 161 000** фотографий

Мы собираем частные картинки ВКонтакте

Перед вами сайт, который содержит большую базу фотографий ВКонтакте, недоступных большинству пользователей. Введите ссылку на страничку любого человека и узнайте, есть ли он в Скотобаза.

Мы постоянно добавляем новые картинки, поэтому если сегодня ничего не было найдено – завтра оно может оказаться у нас. Также мы любим рассматривать все ваши вопросы и пожелания через электронную почту.

[reasonpolice@skotobaza.org](mailto:reasonpolice@skotobaza.org) @GermarSkotobaza Случайные фото NSFW

Поделиться Лайкнуть Твитнуть Плюснуть



Скотобаза

22615856

Среди друзей Гарина Вадима, в Скотобаза найдены следующие:

Александра Марина Юля Ника Мила Катерина

Валерий

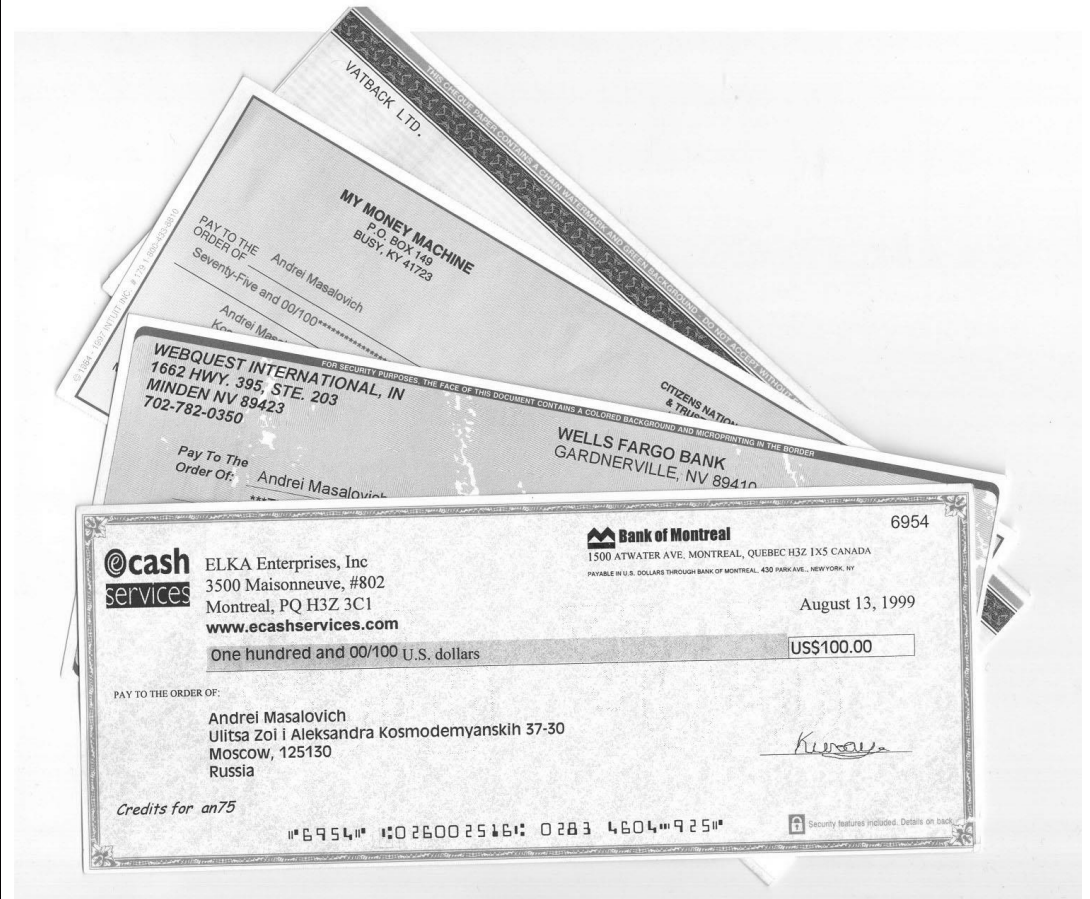
[reasonpolice@skotobaza.org](mailto:reasonpolice@skotobaza.org) [Помогите сайту](#)

1 078 226 53 4-30





# The Hacker



# “Skin”. Кража цифровой личности



Улов на [vk.com/docs](https://vk.com/docs)

# Выйти из-под видеокамер

Multipeer connectivity framework в iOS7



# APT – Advanced Persistent Threat



- An **advanced persistent threat (APT)** is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity.
- АРТ ( «развитая устойчивая угроза»; также целевая кибератака) — противник, обладающий современным уровнем специальных знаний и значительными ресурсами, которые позволяют ему создавать возможности для достижения целей посредством различных векторов нападения

# Advanced Persistent Threat Groups



## **APT37 (Reaper)**

North Korea

Target sectors: Primarily South Korea – though also Japan, Vietnam and the Middle East

– in various industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive, and healthcare

## **APT28 Tsar Team**

Suspected attribution: Russian government

Target sectors: The Caucasus, particularly Georgia, eastern European countries and militaries, North Atlantic Treaty Organization (NATO) and other European security organizations and defense firms

Associated malware: CHOPSTICK, SOURFACE



## **APT33**

Suspected attribution: Iran  
Target sectors: Aerospace, energy. APT33 has targeted organizations, spanning multiple industries, headquartered in the U.S., Saudi Arabia and South Korea.  
Associated malware: SHAPESHIFT, DROPSHOT, TURNEDUP, NANOCORE, NETWIRE, ALFA Shell

# Using Google Translate

## WannaCry:

- Требования о выкупе были написаны на 28 языках
- На трех языках без перевода
- Родной – китайский, второй - английский

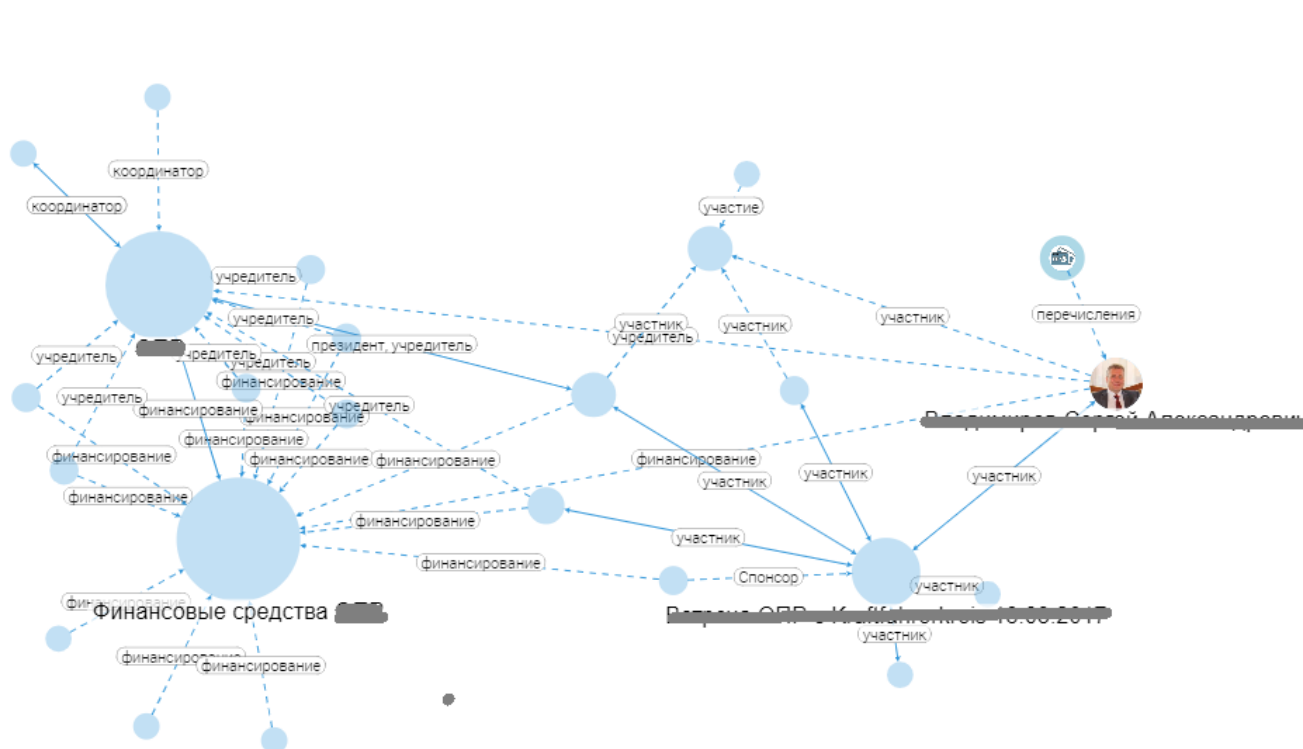


# Анализ графа связей

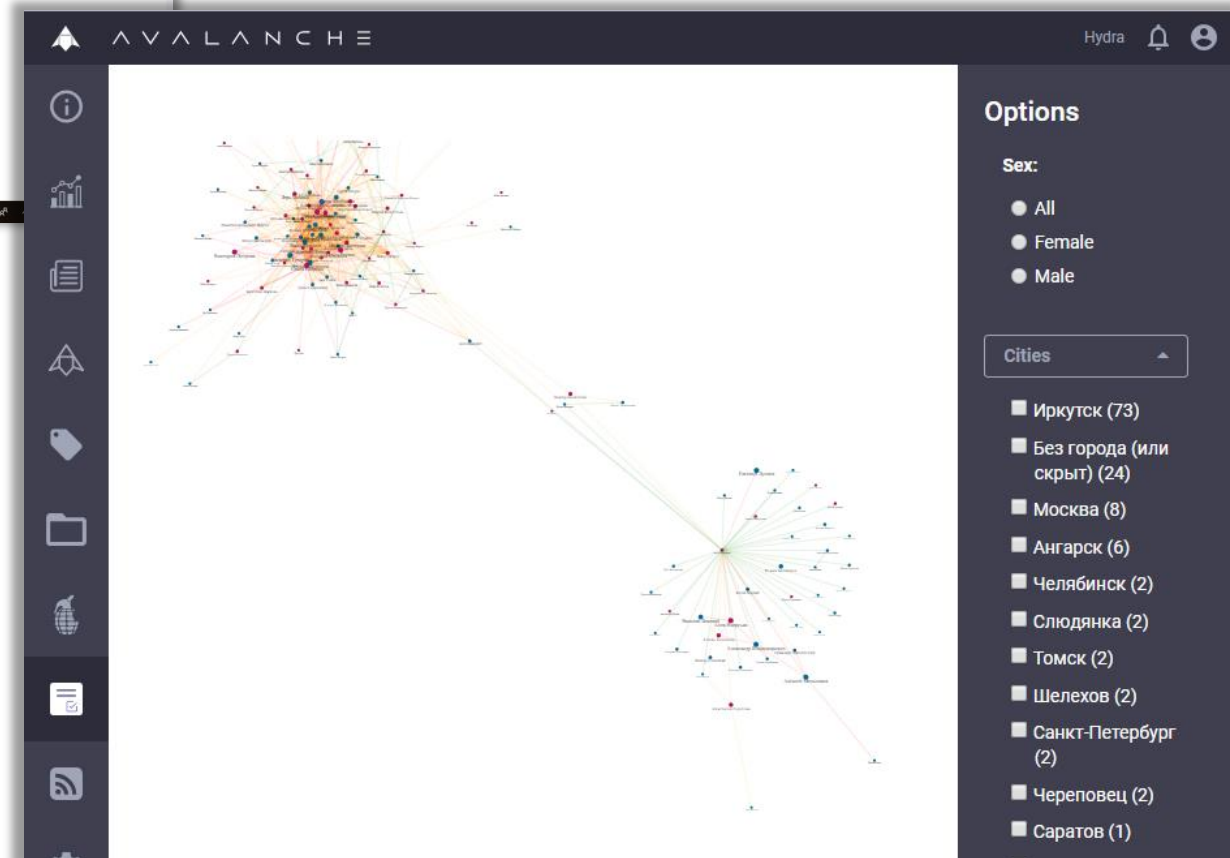
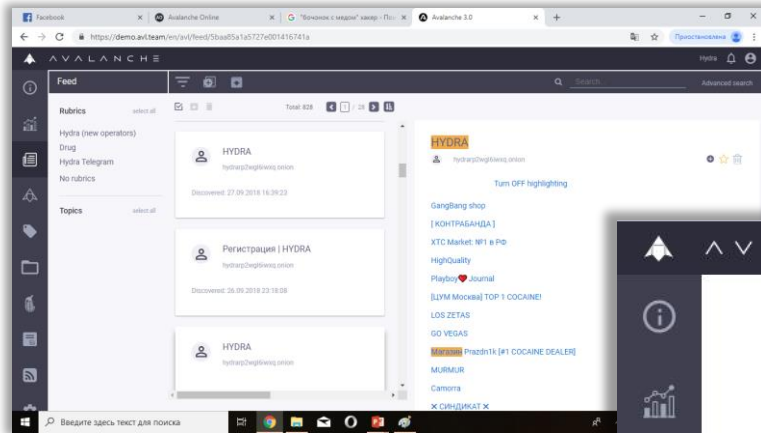
Счет № 6761 0600 0104  
5200 07  
Банковский счёт

Входящие связи 0  
Исходящие связи 1

Таблица связей  
Перейти к -

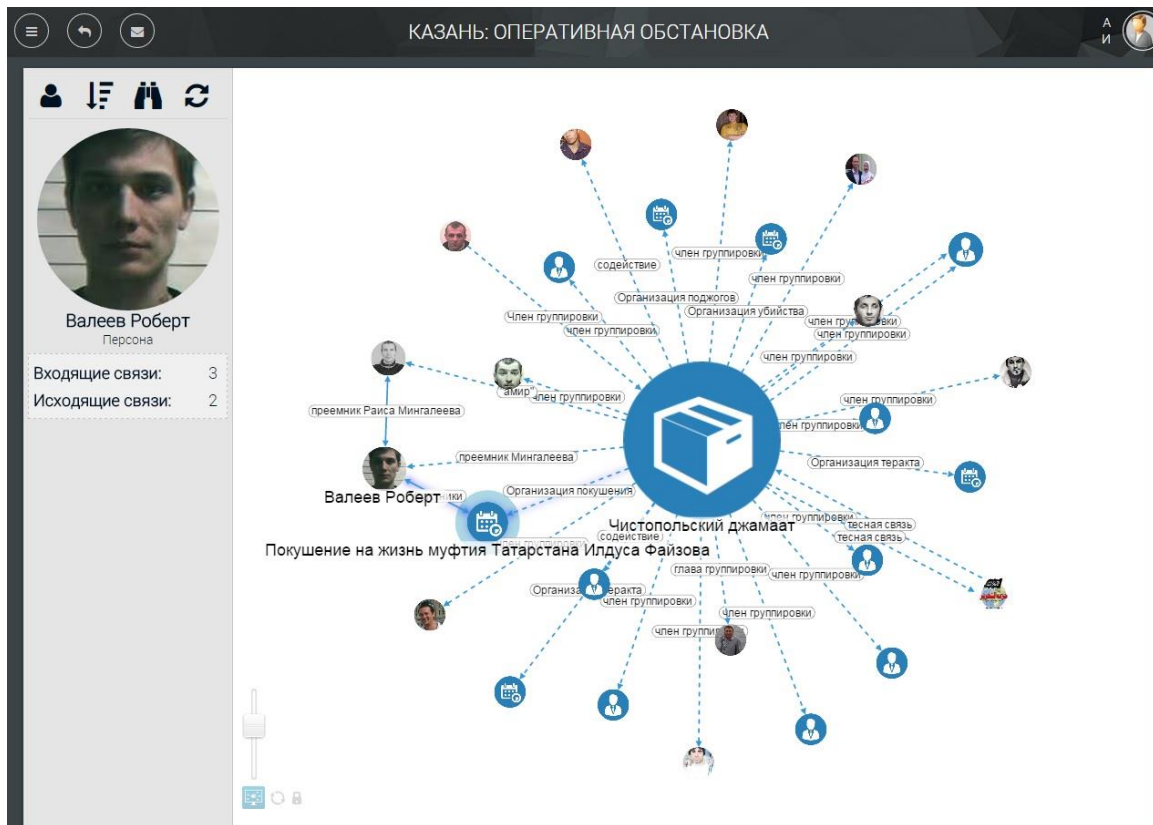


# HYDRA: Outside TOR

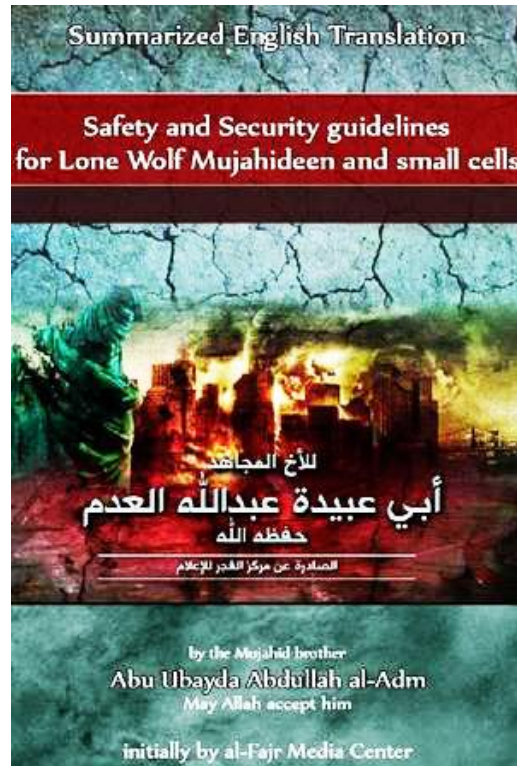




# Анализ связей остатков группировки «Чистопольский джамаат»



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

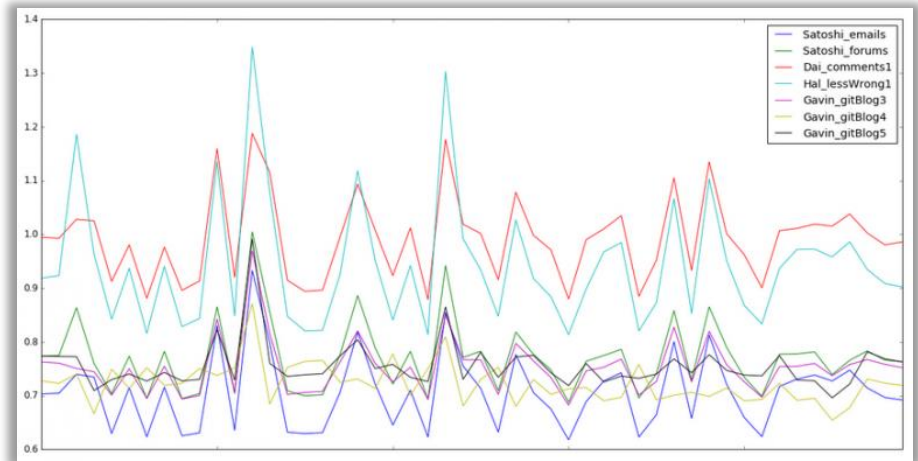


# Stylometry

## Identify Satoshi Nakamoto



- **Stylometry** is the application of the study of linguistic style, usually to written language. Stylometry is often used to attribute authorship to anonymous or disputed documents



Zy Crypto

# ЧТО ДЕЛАТЬ?

- Люди
- Процессы
- Технологии
- Спецназ информационной войны
- Кибероружие

# 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...

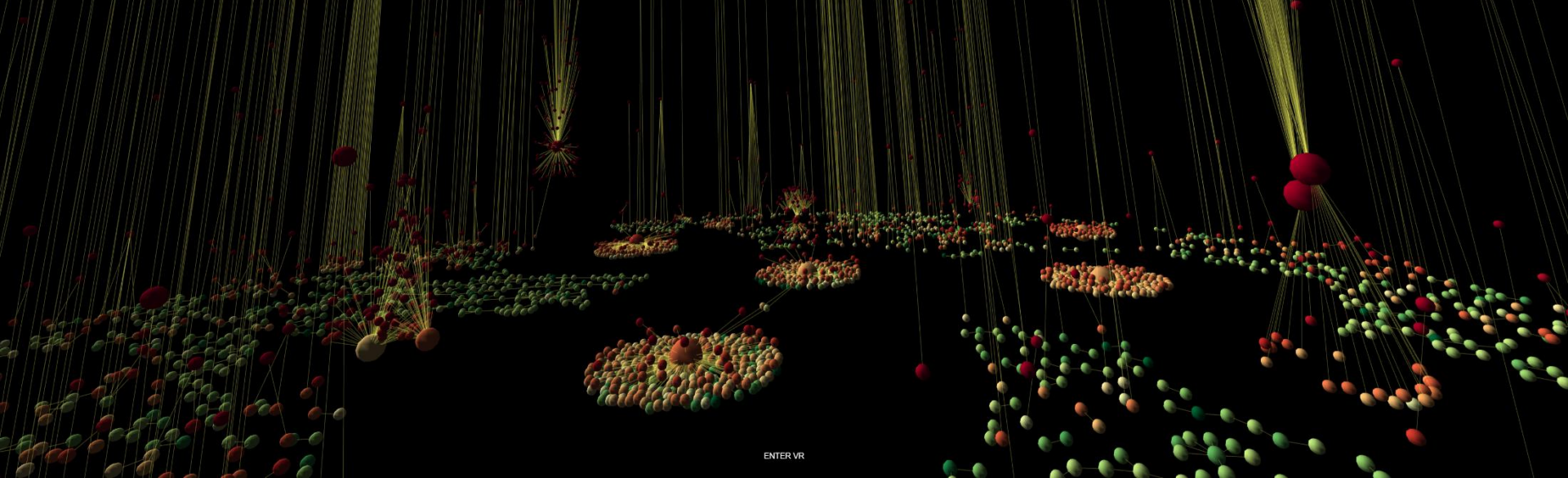
# ТЕХНОЛОГИИ

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



Первый шаг – системы контроля оперативной обстановки

# Step to the Web



ENTER VR

^ V ^ L ^ N C H E



# Аналитические технологии на службе разведывательного сообщества США

Infrastructure				Analytics				Applications			
<b>Hadoop On-Premise</b> cloudera, Hortonworks, MAPR, Pivotal, IBM InfoSphere, bluedata, jethro	<b>Hadoop in the Cloud</b> Amazon, Microsoft Azure, Google Cloud Platform, IBM InfoSphere, CAZENA, altiscale, Quoble, xplenty	<b>Spark</b> databricks, GridGain, TACHYON NEXUS	<b>Cluster Services</b> amazon web services, kubernetes, docker, MESOSPHERE, Core OS, pepperdata, StackIQ	<b>Analyst Platforms</b> Palantir, AYASDI, Quid, enigma, Digital Reasoning, ORBITAL INSIGHTS	<b>Analytics Platforms</b> Microsoft, guAVUS, Datameer, interana	<b>Data Science Platforms</b> context relevant, DataRobot, Alpine, MODE, ADATA, dataiku, tonian, DOMINO, sense, yhat, ALGORITHMIA	<b>Visualization</b> Tableau, Roambi, GOMDATA, Olik, CHARTIO	<b>Sales &amp; Marketing</b> RADIUS, Gainsight, bloomreach, Zeta, livefyre, Kahuna, Lattice, SAILTHRU, persado, infer, sense, AVISO, ACTIONIQ, QUANTIFIND, JEN GAGIO	<b>Customer Service</b> MEDALLIA, ATENSTY, CLARABRIDGE, STELLAService, NGDATA, Preact, DigitalGenius, appurri, fuse:machines	<b>Human Capital</b> gild, Connectifier, textic, entelo, hiQ	<b>Legal</b> RAVEL, JUDICATA, Everlaw, Brevia, PREMOTION
<b>NoSQL Databases</b> Amazon DynamoDB, Google Cloud Platform, Microsoft Azure, ORACLE, mongoDB, DATASTAX, Couchbase, SequoiaDB, redislabs, influxdata	<b>NewSQL Databases</b> SAP HANA, Clustring, Pivotal, memsql, paradigm4, NUODB, MariaDB, VOLTD, CIUDATA, deepdb, Trafalgar, Cockroach LABS	<b>BI Platforms</b> Power BI, Amazon, Domo, Wave Analytics, GoodData, platforma, looker, atscale, QlikView, Qlik Sense, Qlik Nxt	<b>Statistical Computing</b> SAS, SPSS, MATLAB	<b>Log Analytics</b> Splunk, sumologic, kibana, cloud physics, loggly	<b>Social Analytics</b> Netbase, DataSift, tracx, bitly, synthosio, bottlen, simple reach	<b>Ad Optimization</b> MediaMath, Integral, OpenX, Adgortrivers, Livelihood, DataXu, Cppier, TAPAD, rocketfuel, theTradeDesk, Livelihood, distillery	<b>Security</b> Cylance, CounterTack, cybereason, ThreatMetrix, Recorded Future, Fortscale, sifscience, Keybase, feedzai, SICNIFYD	<b>Vertical AI Applications</b> Facebook, Clara, KASIST, lumina			
<b>Graph Databases</b> neo4j, OrientDB, InfoGraph	<b>MPP Databases</b> TERADATA, VERTICA, NETEZZA, Kognitio, dremio	<b>Cloud EDW</b> Amazon web services, Google Cloud Platform, Microsoft Azure, Pivotal, snowflake, WATERLINE, InfoWorks	<b>Data Transformation</b> Alteryx, TRIFACTA, tamr, StreamSets, Alation	<b>Data Integration</b> Informatica, MuleSoft, snapLogic, BedrockData	<b>Real-Time</b> METAMARKETS, confluent, DATA TORRENT, dataArtisans	<b>Machine Learning</b> Azure Machine Learning, H2O, SKY TREE, rapidminer, DATA SWIM, deepsense, VISENZE, predictionIO, slowflash	<b>Speech &amp; NLP</b> NarrativeScience, api.ai, NUANCE, Grindspace, semantic machines, cortico, MindMeid, IDIBON, YSCOPE	<b>Horizontal AI</b> IBM Watson, Cortana, sentiment, VIV, nora, Numenta, MetaMind, clarifai	<b>Publisher Tools</b> Outbrain, mixpanel, Chartbeat, yieldbot, Yieldmo	<b>Govt/ Regulation</b> Socrata, OPENGOV, EN FiscalNote, PREDPOL, mark43, OpenDataSoft	<b>Finance</b> Affirm, LendingClub, OnDeck, Kreditech, finance, LendUp, Kabbage, tidemark, Fafy, INSIKT, UORA, Dataminr, Lendio, KENSHC, AIIDYA, ISENTIUM, Quantopian, sentiment
<b>Management / Monitoring</b> New Relic, illumio, APPDYNAMICS, Amazon web services, actifio, Numerify, splunk, DATA DOG, TROCANO, Anodot	<b>Security</b> TANIUM, illumio, CODE42, DataGravity, CipherCloud, VECTRA, sqrrl, BlueTalon	<b>Storage</b> Amazon web services, Google Cloud Platform, Microsoft Azure, panasas, nimblestorage, Qumulo	<b>App Dev</b> Apigee, CASK, Typesafe, CONCURRENT	<b>Crowd-sourcing</b> Amazon Mechanical Turk, CrowdFlower, WorkFusion	<b>Search</b> HP, ELASTIC, Lucidworks, MAANA, swiftype, Algolia, SINEQUA	<b>Data Services</b> LIQ, OPERA, Mu Sigma, DATA SCIENCE, DATA VALUES, kaggle, datacscope, DataKind	<b>For Business Analysts</b> ClearStory, CIRRO, import IO	<b>SMB / Commerce</b> Google Analytics, OrigamiLogic, AMPLITUDE, RJMetrics, sumAll, granify, Airtable, retention, custora	<b>Publisher Tools</b> Outbrain, mixpanel, Chartbeat, yieldbot, Yieldmo	<b>Govt/ Regulation</b> Socrata, OPENGOV, EN FiscalNote, PREDPOL, mark43, OpenDataSoft	<b>Finance</b> Affirm, LendingClub, OnDeck, Kreditech, finance, LendUp, Kabbage, tidemark, Fafy, INSIKT, UORA, Dataminr, Lendio, KENSHC, AIIDYA, ISENTIUM, Quantopian, sentiment
<b>Cross-Infrastructure/Analytics</b> Amazon web services, Google, Microsoft, IBM, SAP, SAS, HP, Autodesk, vmware, talend, TIBCO, TERADATA, ORACLE, NetApp											
<b>Framework</b> Hadoop, YARN, Spark, Mesos, TEZ, Flink, CDAP	<b>Query / Data Flow</b> SLAMDATA, DRILL, Google Cloud Dataflow	<b>Data Access</b> HBASE, accumulo, mongoDB, kafka, CouchDB, riak, OPEN TSDB, nifi	<b>Coordination</b> talend, Apache Ambari	<b>Real-Time</b> STORM, Spark, APEX, Flink, TACHYON, druid	<b>Stat Tools</b> Scala, NumPy, SciPy	<b>Machine Learning</b> mlilb, Aerolve, Caffe, SINGA, MADlib, CNTK, TensorFlow, WEKA, FeatureFu, DIMSUM, jupyter, DL4J	<b>Search</b> Elasticsearch, Solr, Lucene	<b>Security</b> Apache Ranger, Visualization, Zepalin			
<b>Data Sources &amp; APIs</b>											
<b>Health</b> Apple, JAWBONE, GARMIN, Withings, fitbit, VALIDIC, relatmo, kinsa, Human API	<b>IOT</b> UPTAKE, ThingWorx, helium, samsara, AUGURY, estimize	<b>Financial &amp; Economic Data</b> Bloomberg, DOW JONES, Y DLEE, PREMISE, S&P CAPITAL IQ, Quandl, xignite, CB INSIGHTS, mattermark, estimize, FLAID	<b>Air / Space / Sea</b> PLANET LABS, WINDWARD, spire, CRUISE, SKYCATCH, Airware, DroneDeploy	<b>Location/People/Entities</b> GARMIN, foursquare, InsideView, esri, STREETLINE, CARTO DB, factual, PlaceIQ, Crimon Hexagon, placemeter, BASIS, Sense	<b>Other</b> qualtrics, panjiva, DATA.GOV	<b>Incubators &amp; Schools</b> GA, DataCamp, INSIGHT, DataElite, METIS, The Data Incubator					

# Дополнительная информация



A screenshot of the Forbes magazine website. The main article is titled "Разведка сетью: как система Avalanche помогает спецслужбам и бизнесу". The author is identified as "Павел Седяков". The article includes a photo of a man with a beard and a hand on his chin. The text discusses the "Avalanche" system and its use by intelligence agencies and businesses. On the right side, there are several promotional banners, including one for "ПРОВЕРЬТЕ, ЕСТЬ ЛИ У ВАС ПРИКЛЮЧЕН" and another for "200 БОГАТЕЙШИХ БИЗНЕСМЕНОВ РОССИИ".

# Спасибо за внимание 😊

## Questions?



Masalovich Andrei  
Масалович Андрей Игоревич  
Специалист по связям с реальностью  
+7 (964) 577-2012  
[am@avl.team](mailto:am@avl.team)

[iam.ru/tipaguru.htm](http://iam.ru/tipaguru.htm)