


# Остаться невидимкой

Андрей Масалович

Andrei Masalovich

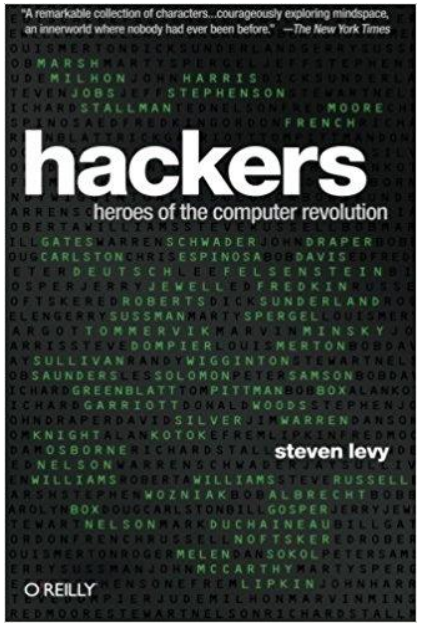
am@avl.team

Live smart, live longer

# Hackers. Evolution

# Хакеры. Эволюция

Романтики




Heroes

Преступники


Cyber Crime

Спецназ информационной войны

Cyber Army

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



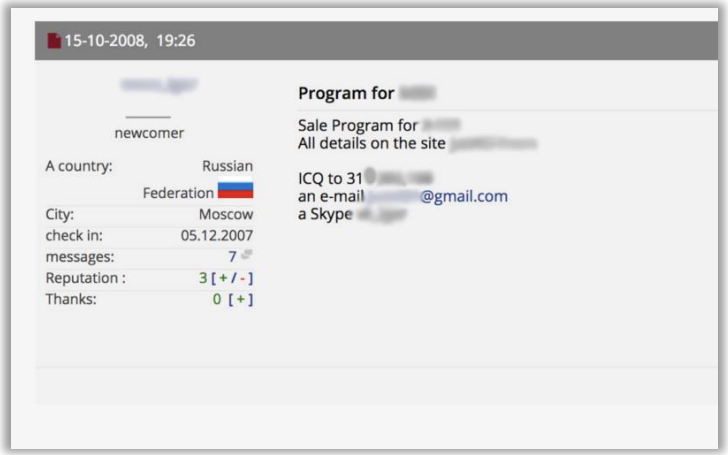

- Сложное заказное malware
- Целевой фишинг
- Эфемерные AES-ключи
- IPv6, DGA,DDNS
- Связь через DNS, ICMP, HTTP

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

https://www.symantec.com/connect/blogs/bachosens-highly-skilled-petty-cyber-criminal-lofty-ambitions-targeting-large-organizations

# Internet Intelligence

Если использовать методы интернет-разведки…

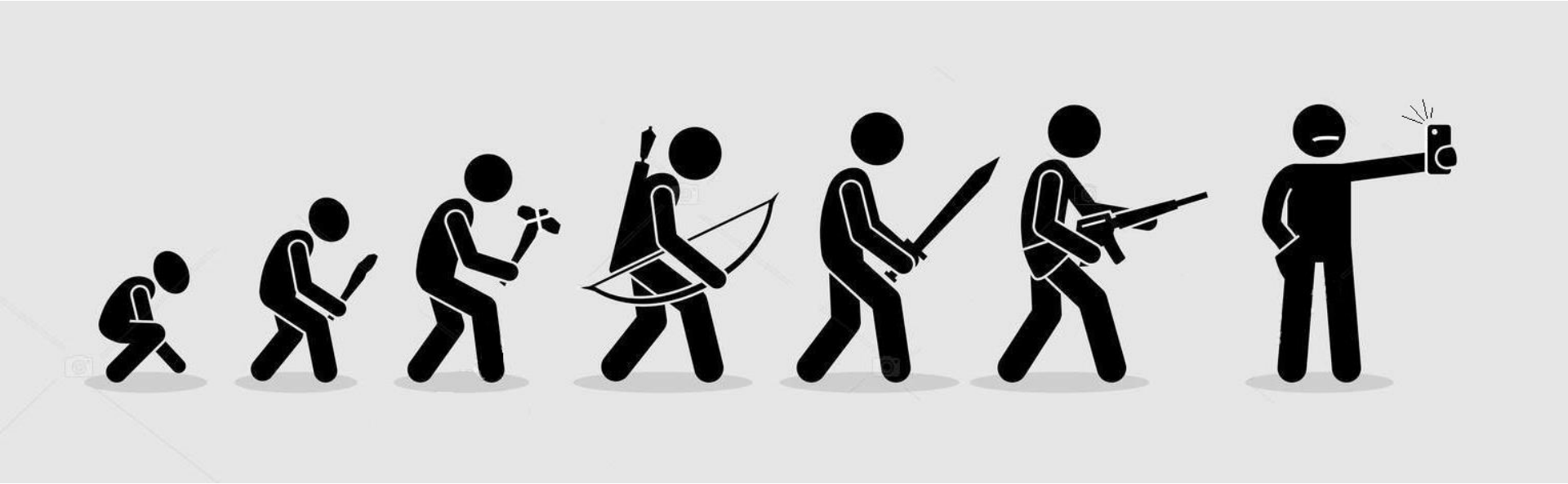



- Игорь С*****
- Тирасполь
- Телефон: * *** *** ****
- E-mail: ******@gmail.com

https://motherboard.vice.com/en_us/article/zmbj7y/lone-wolf-criminal-hacker-gets-doxed-thanks-to-series-of-dumb-mistakes

# 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?

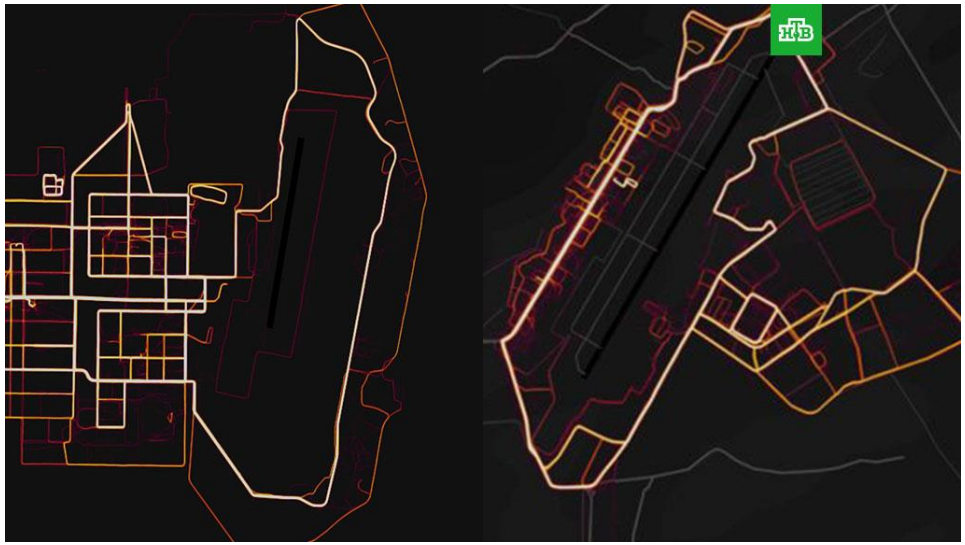
- Министерство обороны одной из стран СНГ
- Антивирусная компания
- Спецслужба одной из стран СНГ

http://cryptoworld.su/kak-vychislit-xakera/

# Fitness app Strava lights up staff at military bases

# Фитнес-трекер Strava

## выдал расположение военных баз США

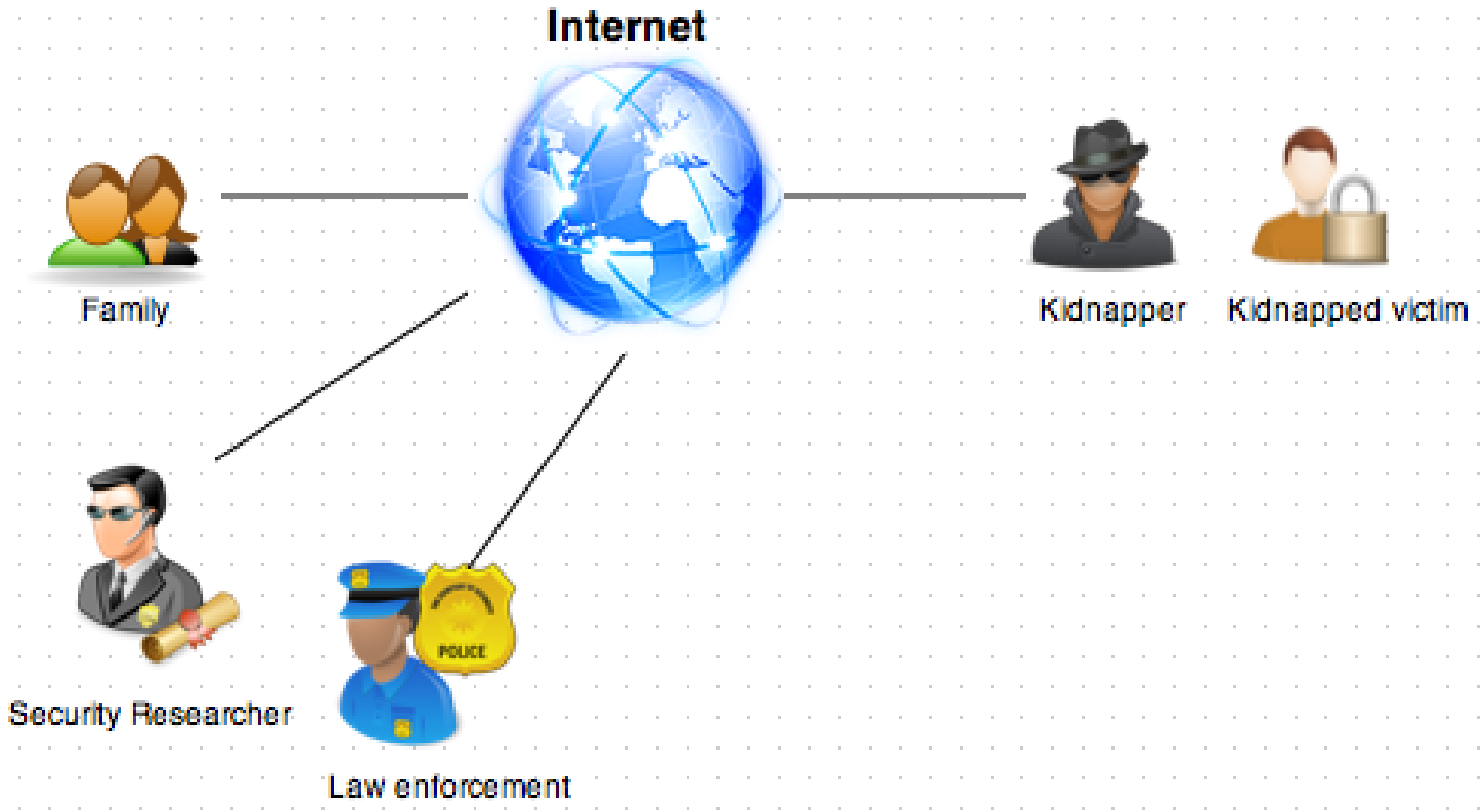
https://www.bbc.com/news/technology-42853072

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

Скрывайте IP. Всегда.

https://www.thedailybeast.com/exclusive-lone-dnc-hacker-guccifer-20-slipped-up

# «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

# Прячем данные

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

# Digital Footprint Наш цифровой след

Новости

Интернет

Бизнес

Финансы

Недвижимость

Биография

Документы

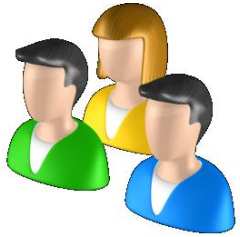
Семья


Аккаунты

Привычки

Местоположение

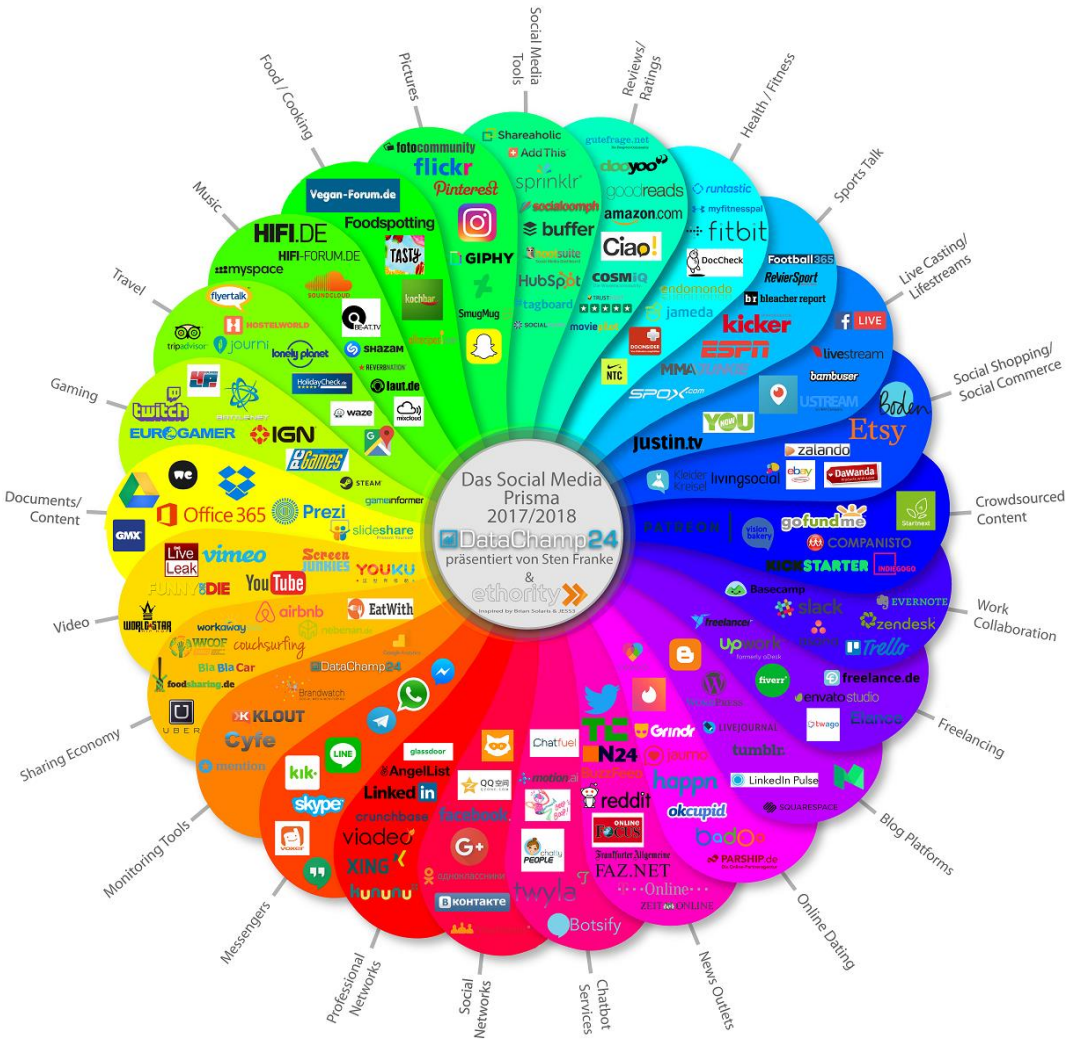
Гаджеты



Социальные сети

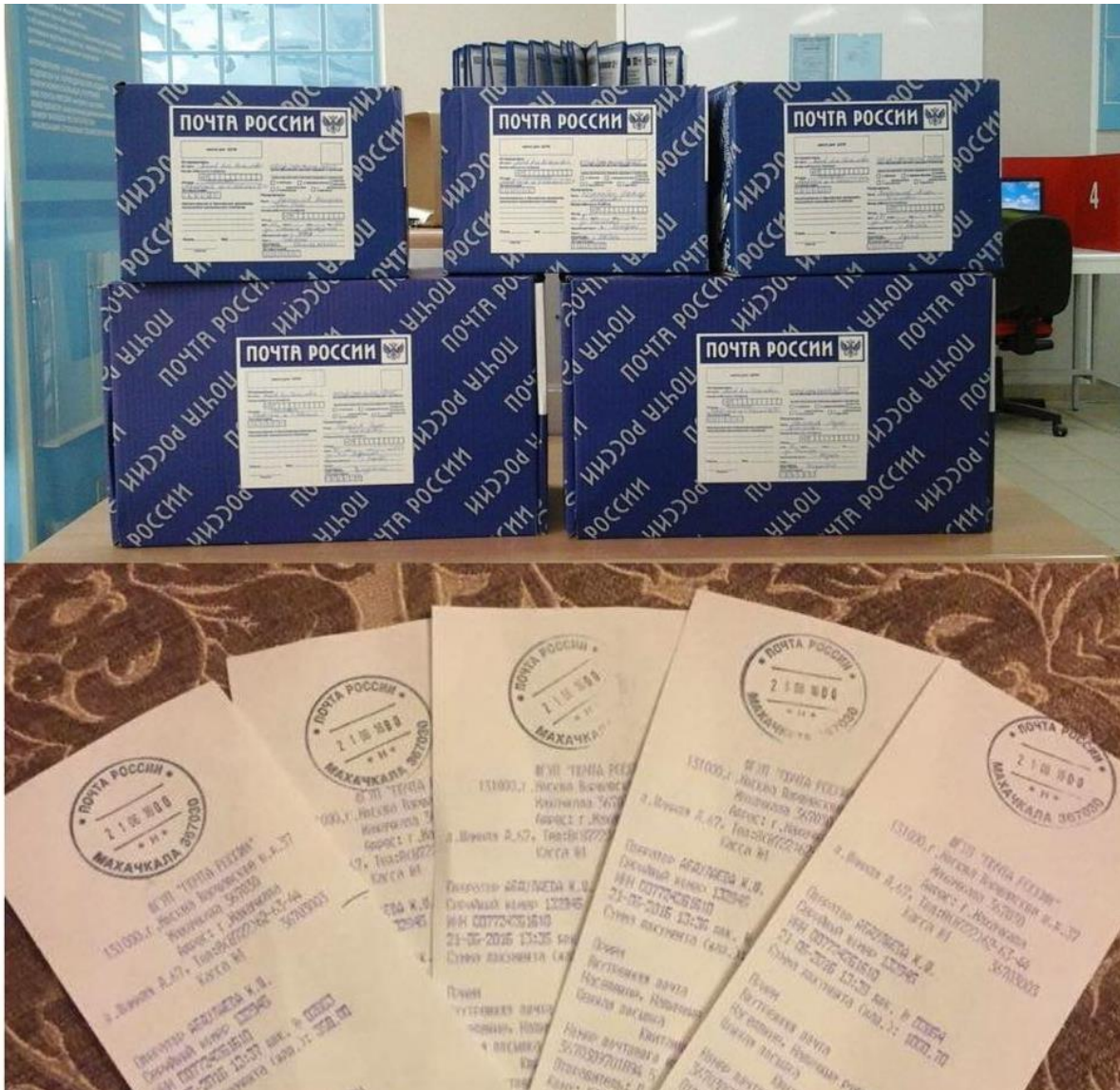
Проблемы с законом

# OSINT (Open Source Intelligence)
# - Разведка по открытым источникам

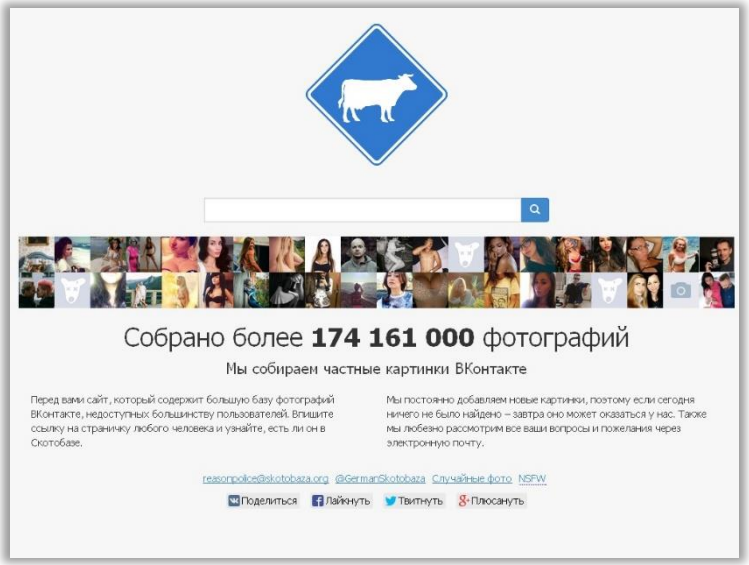


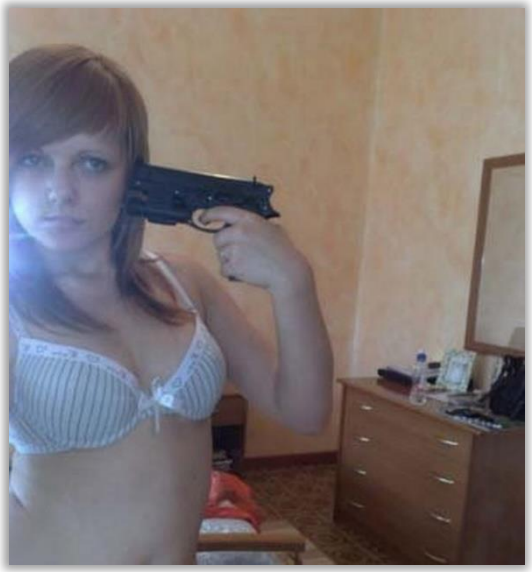
# Using OSINT…

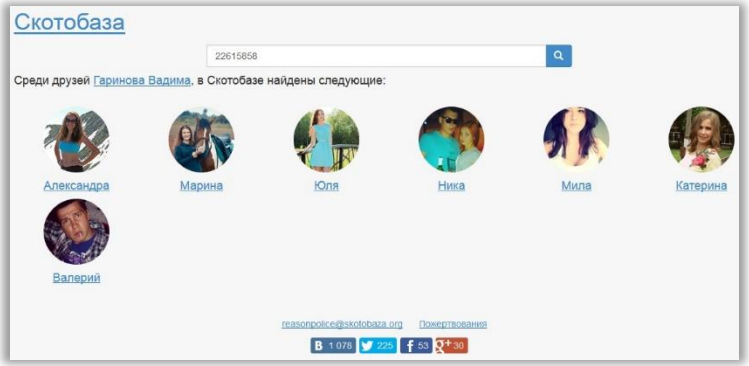

Мюриды и мюридки
Использование
5469 6000 1351 1316
Использование
Фонд ИбнКасир


ПОЧТА РОССИИ
МАХАЧКАЛА

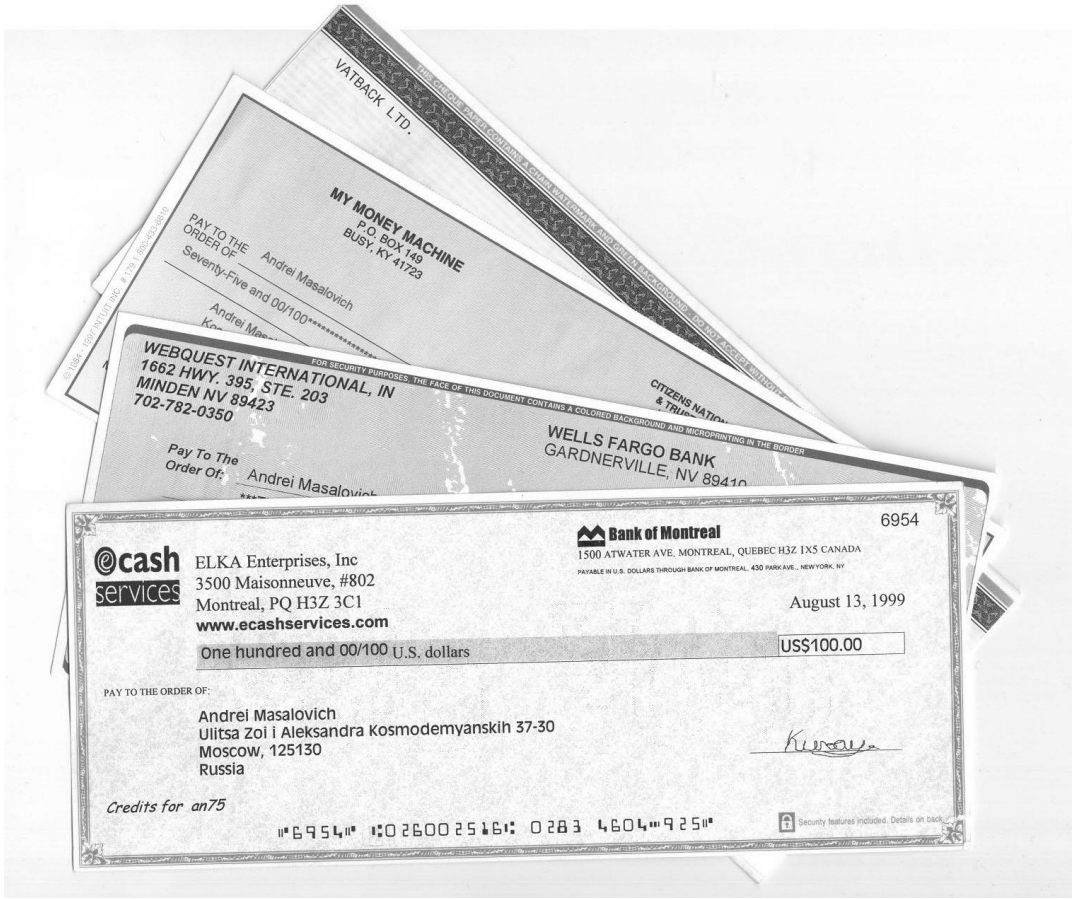
# Источник утечек личной информации – базы удаленных страниц в соцсетях






# The Hacker


VATBACK LTD.
MY MONEY MACHINE
P.O. BOX 149
BUSY, KY 41723
PAY TO THE ORDER OF
Andrei Masalovich
Seventy-Five and 00/100
WEBQUEST INTERNATIONAL, IN
1662 HWY. 395, STE. 203
MINDEN NV 89423
702-782-0350
Pay To The Order Of:
Andrei Masalovich
WELLS FARGO BANK
GARDNERVILLE, NV 89410
6954
ecash services
ELKA Enterprises, Inc
3500 Maisonneuve, #802
Montreal, PQ H3Z 3C1
www.ecashservices.com
Bank of Montreal
1500 ATWATER AVE, MONTREAL, QUEBEC H3Z 1X5 CANADA
August 13, 1999
One hundred and 00/100 U.S. dollars
US$100.00
PAY TO THE ORDER OF:
Andrei Masalovich
Ulitsa Zoi i Aleksandra Kosmodemyanskih 37-30
Moscow, 125130
Russia
Credits for an75

# “Skin”. Кража цифровой личности


Улов на 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.
- APT ( «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 alware: SHAPESHIFT, DROPSHOT, TURNEDUP, NANOCORE, NETWIRE, ALFA Shell

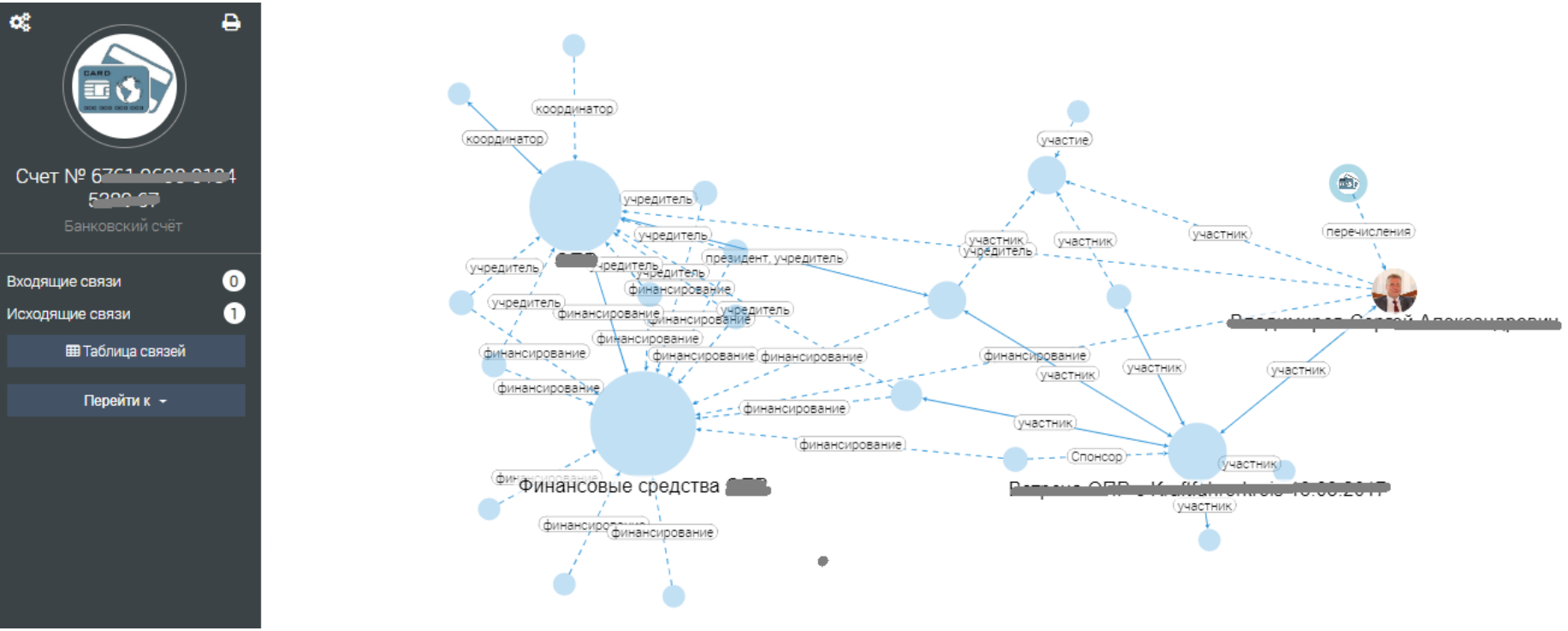
https://www.fireeye.com/current-threats/apt-groups.html

# Using Google Translate

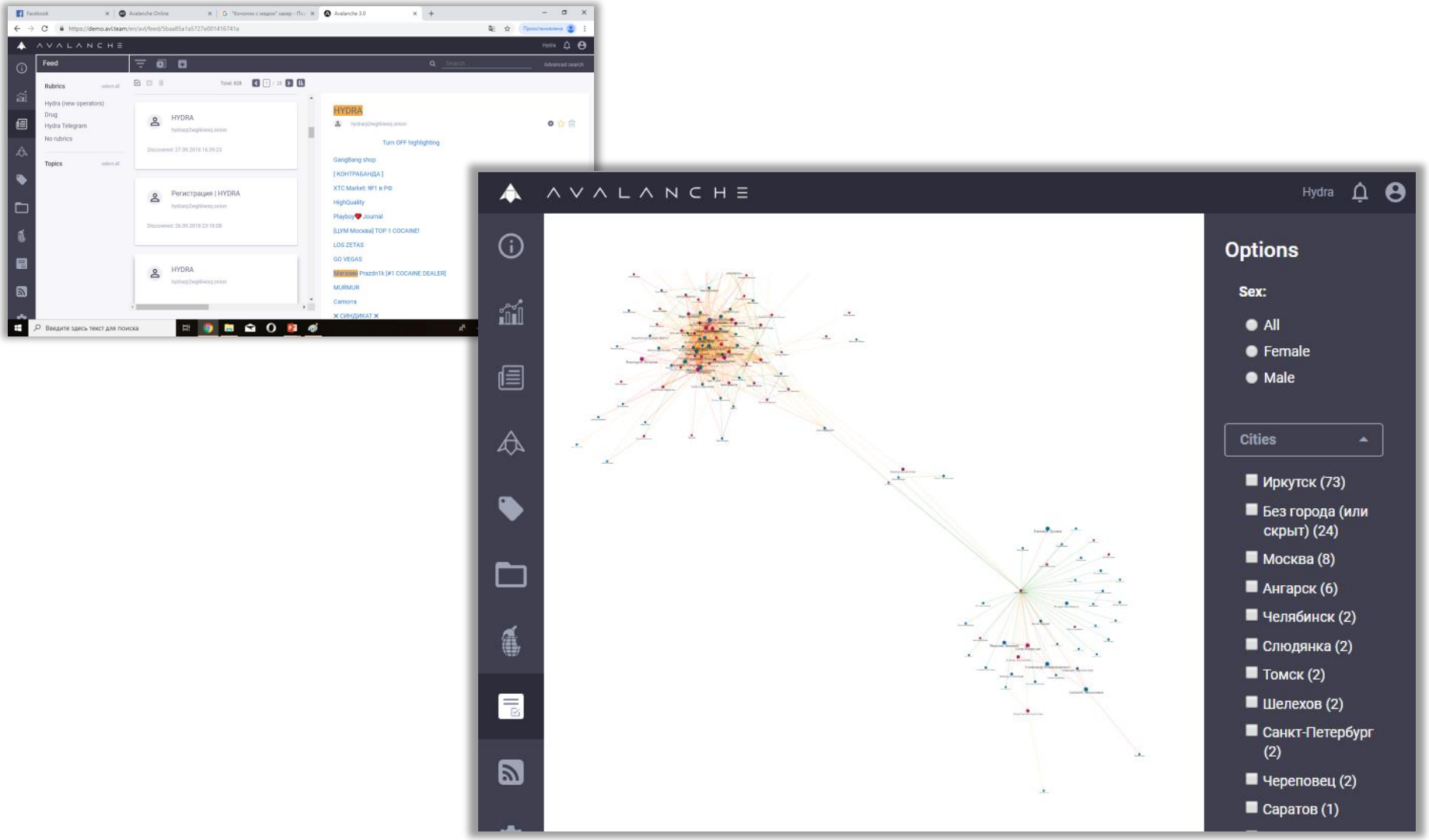
## WannaCry:

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

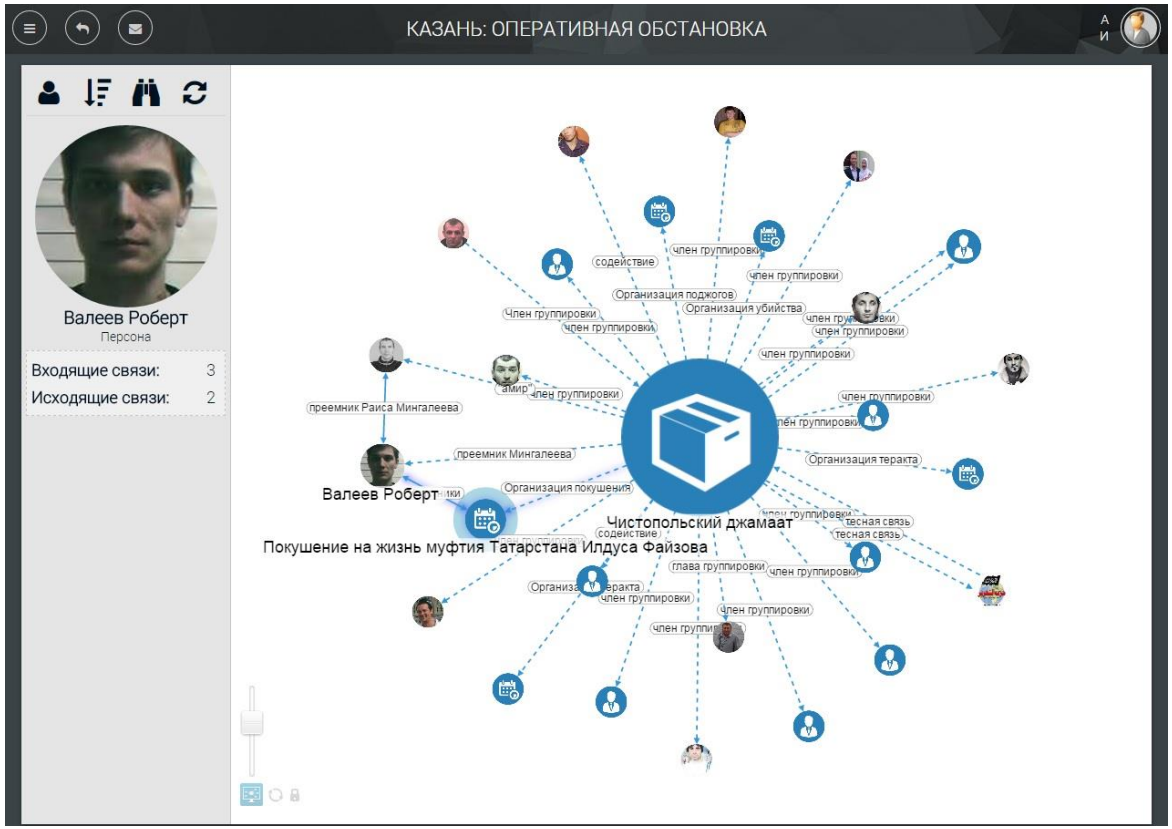
# Анализ графа связей



# HYDRA: Outside TOR



# Анализ связей остатков группировки «Чистопольский джамаат»

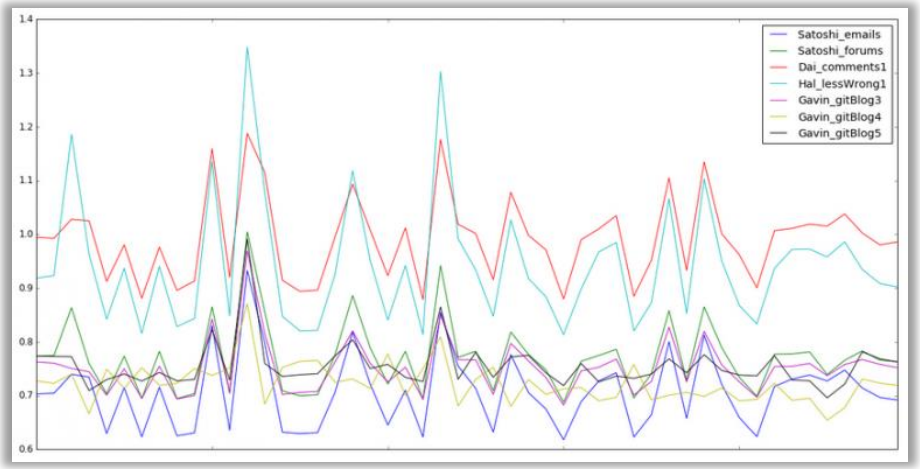


# Пример работы в «сером» интернете: Методички террористов по бескомпроматной работе

# 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

**Source:** hello-crypto.ru/resurs-**zy-crypto**-utverzhdaet-chto-vyichislil-realnogo-satoshi-nakamoto/

# 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

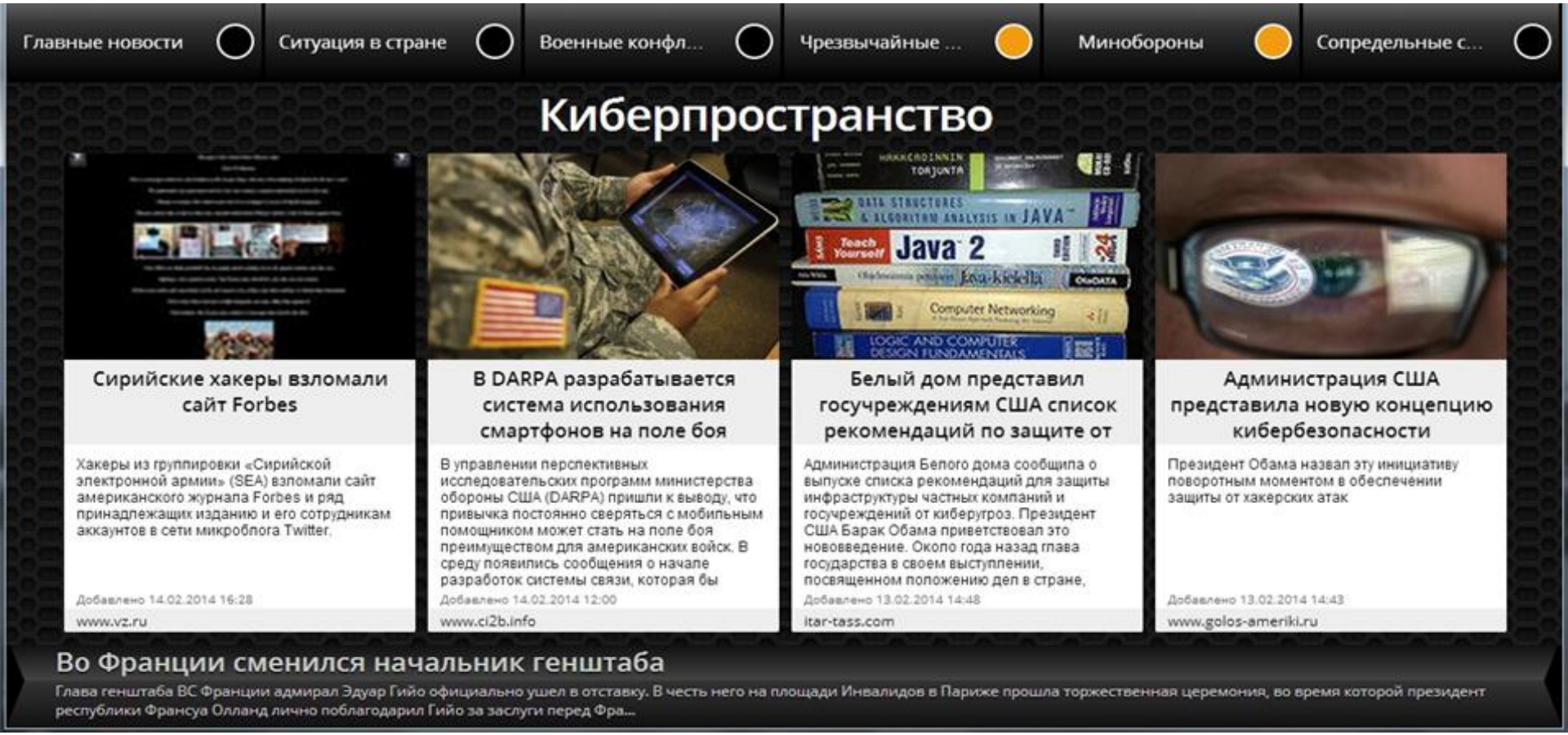
**Первый шаг – ЭКСПРЕСС-КУРСЫ**

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

***Основам безопасности можно научить за один день***

# ПРОЦЕССЫ

## Контроль обстановки в киберпространстве



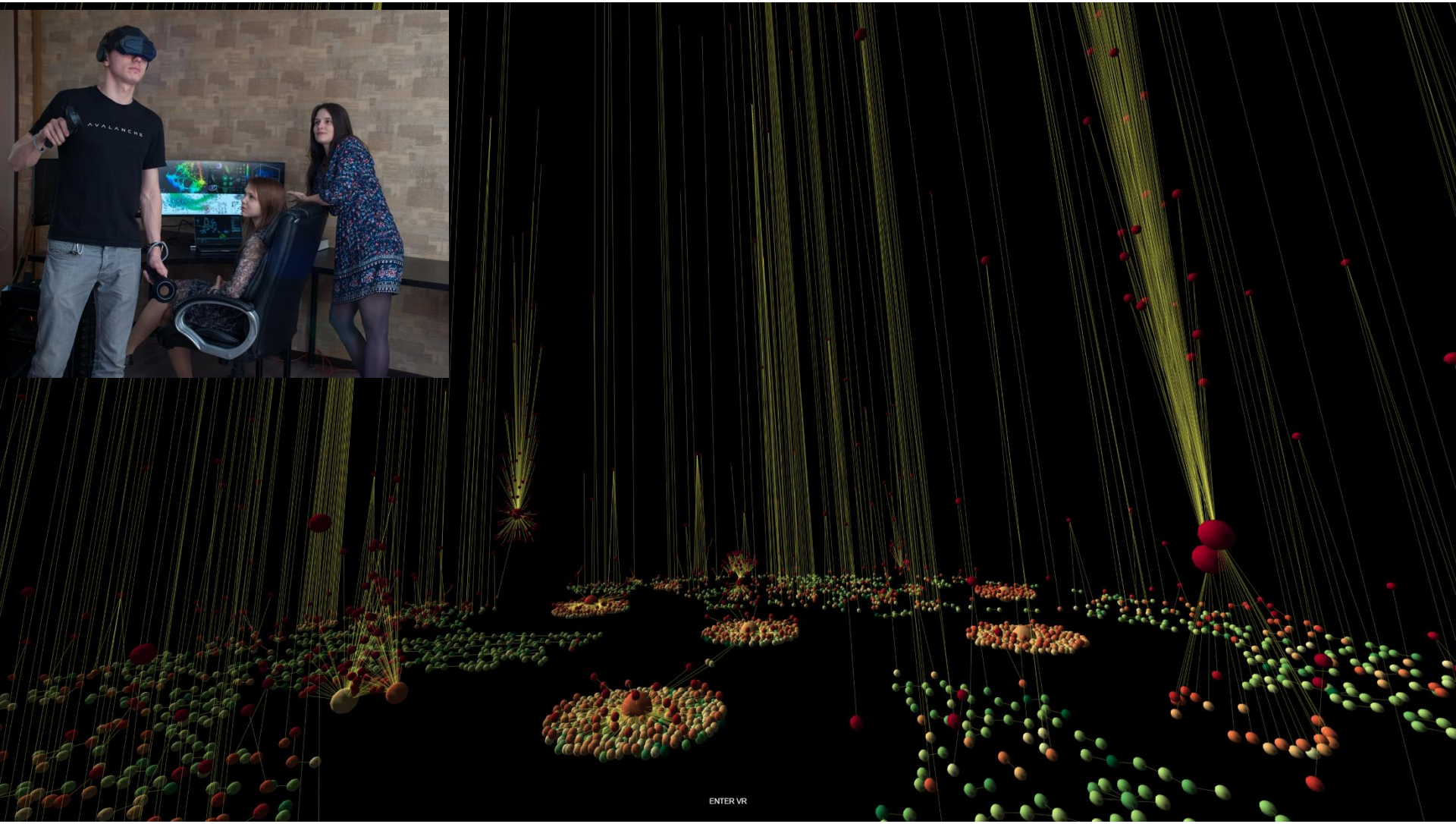

AVALANCHE

# ТЕХНОЛОГИИ

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

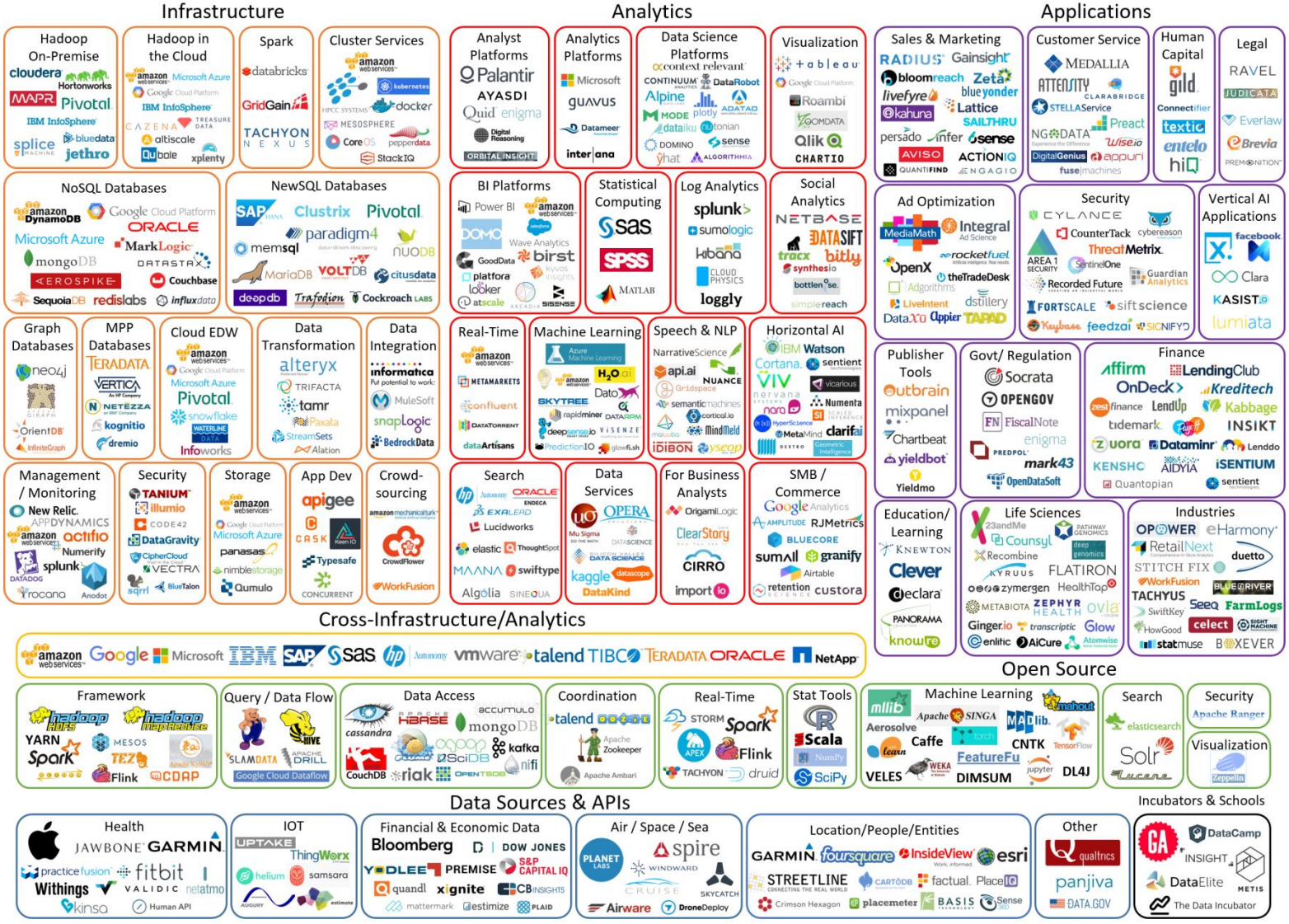
Первый шаг – системы контроля оперативной обстановки

# Step to the Web




AVALANCHE

# Аналитические технологии на службе разведывательного сообщества США



# Дополнительная информация


# Спасибо за внимание ☺

Questions?


Masalovich Andrei

Масалович Андрей Игоревич

Специалист по связям с реальностью

+7 (964) 577-2012

am@avl.team


iam.ru/tipaguru.htm