



**АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ**

# Как искать и находить в Даркнете

**Андрей Масалович**



ЦЕНТР ДОПОЛНИТЕЛЬНОГО  
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ



ЦЕНТР КОМПЕТЕНЦИЙ ПО ЦИФРОВОМУ  
РАЗВИТИЮ И КИБЕРБЕЗОПАСНОСТИ



ОРГАНИЗАТОР МЕЖДУНАРОДНЫХ И  
РОССИЙСКИХ КОНФЕРЕНЦИЙ И ФОРУМОВ



СМОТРИ В БУДУЩЕЕ. ИНВЕСТИРУЙ В ЗНАНИЯ.

# АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ



**Даркнет**, или "**теневой интернет**" сегодня - это средоточие всех видов противоправной деятельности, торговли наркотиками и оружием, экстремистской и террористической активности, координации всевозможных мятежей и бунтов и т.д.

Кроме того, это царство криптовалют и теневых финансовых расчетов.

Сохраняя иллюзию анонимности для своих участников., Даркнет набирает популярность и сегодня стал реальной головной болью для правоохранителей и специальных служб разных стран.

Давайте разберемся, как устроен Даркнет внутри, как он функционирует, и действительно ли он анонимен, а его участники неуязвимы.

**В ходе вебинара будут рассмотрены следующие вопросы:**

- Как устроен Даркнет. TOR как основа Даркнета
- Программное обеспечение для анонимных коммуникаций
- Безопасность анонимных почтовых служб и мессенджеров
- Альтернативные средства коммуникации и их безопасность
- Безопасность криптокошельков и транзакций в Даркнете
- Возможности специальных служб и частных разведок в Даркнете



СМОТРИ В БУДУЩЕЕ. ИНВЕСТИРУЙ В ЗНАНИЯ.

# АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

**Даркнет** - (англ. DarkNet, также известен как «Скрытая сеть», «Темный интернет», «Тёмная сеть», «Теневая сеть», «Тёмный веб») — скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов.

Не следует путать с **Глубоким интернетом (DeepWeb)** — множеством веб-страниц Всемирной паутины, не индексируемых поисковыми системами.

Анонимная сеть представляет собой систему не связанных между собой виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде. Даркнет отличается от других распределённых одноранговых сетей, так как файлообмен происходит анонимно (поскольку IP-адреса недоступны публично), и, следовательно, пользователи могут общаться без особых опасений и государственного вмешательства[3].

Термин «даркнет» первоначально появился в 1970-х годах и в целях безопасности использовался для обозначения сетей, изолированных от ARPANET, которая впоследствии эволюционировала в Интернет. Даркнеты могли получать данные от ARPANET, но их адреса не появлялись в списках сетей и не отвечали на запросы извне.



# Даркнет выходит из сумрака

## 2002 - The Darknet and the Future of Content Distribution

<http://am.news/worlds/darknet.pdf>

### The Darknet and the Future of Content Distribution

Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman

Microsoft Corporation<sup>1</sup>

#### Abstract

We investigate the *darknet* – a collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing networks. Examples of darknets are peer-to-peer file sharing, CD and DVD copying, and key or password sharing on email and newsgroups. The last few years have seen vast increases in the darknet's aggregate bandwidth, reliability, usability, size of shared library, and availability of search engines. In this paper we categorize and analyze existing and future darknets, from both the technical and legal perspectives. We speculate that there will be short-term impediments to the effectiveness of the darknet as a distribution mechanism, but ultimately the darknet-genie will not be put back into the bottle. In view of this hypothesis, we examine the relevance of content protection and content distribution architectures.

#### 1 Introduction

People have always copied things. In the past, most items of value were physical objects. Patent law and economies of scale meant that small scale copying of physical objects was usually uneconomic, and large-scale copying (if it infringed) was stoppable using policemen and courts. Today, things of value are increasingly less tangible: often they are just bits and bytes or can be accurately represented as bits and bytes. The widespread deployment of packet-switched networks and the huge advances in computers and codec-technologies has made it feasible (and indeed attractive) to deliver such digital works over the Internet. This presents great opportunities and great challenges. The opportunity is low-cost delivery of personalized, desirable high-quality content. The challenge is that such content can be distributed illegally. Copyright law governs the legality of copying and distribution of such valuable data, but copyright protection is increasingly strained in a world of programmable computers and high-speed networks.

For example, consider the staggering burst of creativity by authors of computer programs that are designed to share audio files. This was first popularized by Napster, but today several popular applications and services offer similar capabilities. CD-writers have become mainstream, and DVD-writers may well follow suit. Hence, even in the absence of network connectivity, the opportunity for low-cost, large-scale file sharing exists.

##### 1.1 The Darknet

Throughout this paper, we will call the shared items (e.g. software programs, songs, movies, books, etc.) *objects*. The persons who copy objects will be called *users* of the darknet, and the computers used to share objects will be called *hosts*.

The idea of the darknet is based upon three assumptions:

<sup>1</sup> Statements in this paper represent the opinions of the authors and not necessarily the position of Microsoft Corporation.

The small-worlds darknet continues to exist. However, a number of technological advances have given rise to new forms of the darknet that have superseded the small-worlds for some object types (e.g. audio).

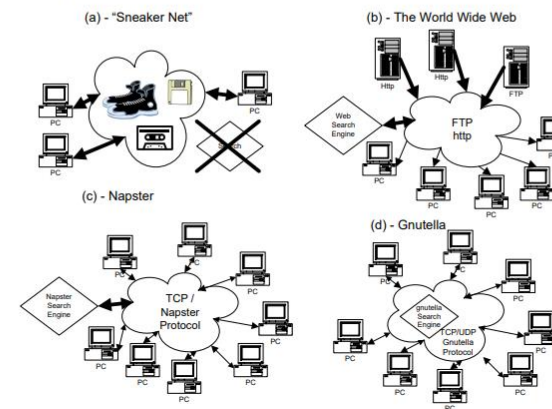


Figure 1: Historical evolution of the Darknet. We highlight the location of the search engine (if present) and the effective bandwidth (thicker lines represent higher bandwidth). Network latencies are not shown, but are much longer for the sneaker net than for the IP-based networks.

#### 2.2 Central Internet Servers

By 1998, a new form of the darknet began to emerge from technological advances in several areas. The Internet had become mainstream, and as such its protocols and infrastructure could now be relied upon by anyone seeking to connect users with a centralized service or with each other. The continuing fall in the price of storage together with advances in compression technology had also crossed the threshold at which storing large numbers of audio files was no longer an obstacle to mainstream users. Additionally, the power of computers had crossed the point at which they could be used as rendering devices for multimedia content. Finally, "CD ripping" became a trivial method for content injection.

The first embodiments of this new darknet were central internet servers with large collections of MP3 audio files. A fundamental change that came with these servers was the use of a new distribution network: The Internet displaced the sneaker net – at least for audio content. This solved several problems of the old darknet. First, latency was reduced drastically.

Secondly, and more importantly, discovery of objects became much easier because of simple and powerful search mechanisms – most importantly the general-purpose world-wide-web search engine. The local view of the small world was replaced by a global view of the entire collection accessible by all users. The main characteristic of this form of the darknet was centralized storage and search – a simple architecture that mirrored mainstream internet servers.

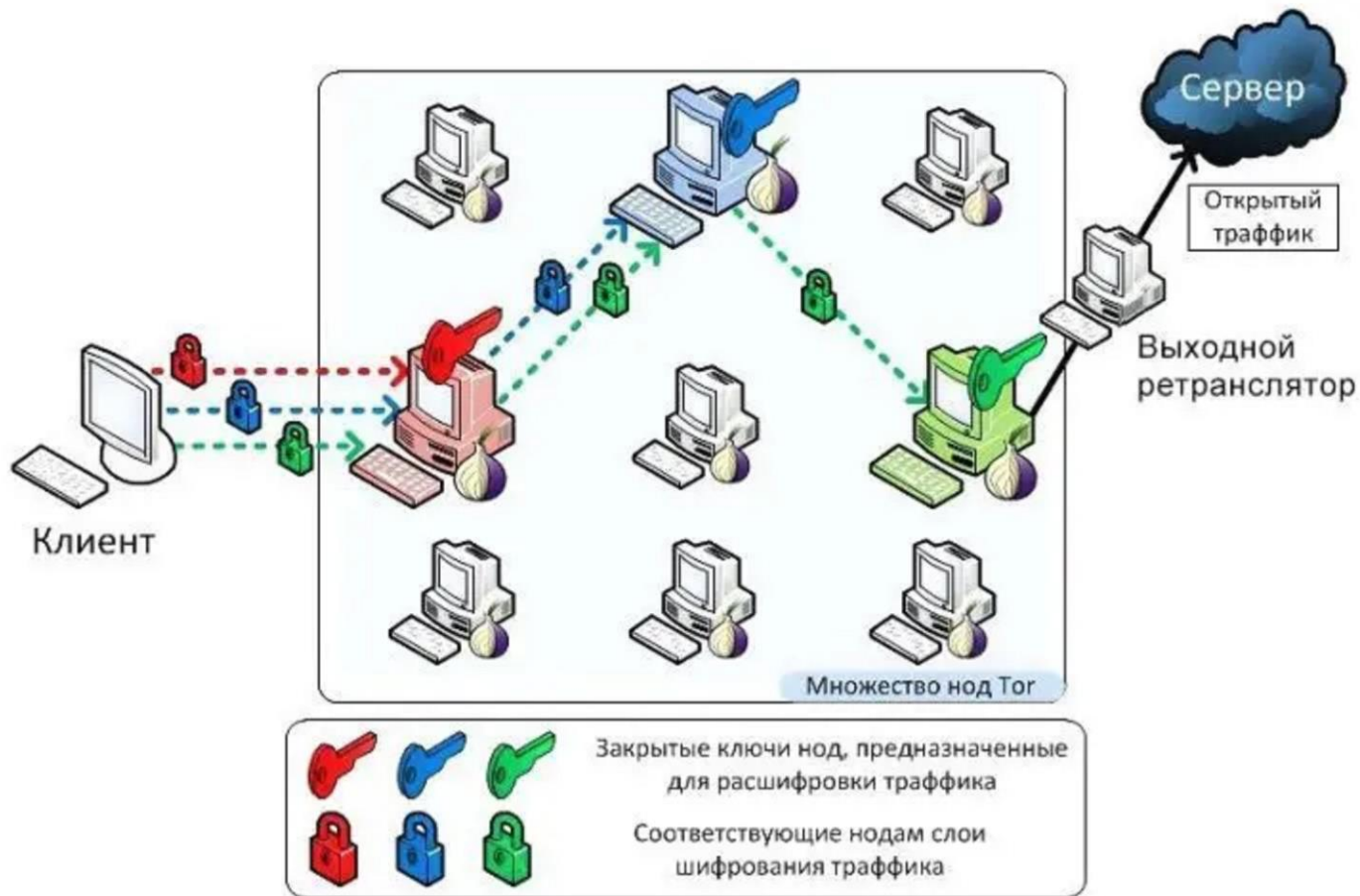


# Интернет сегодня



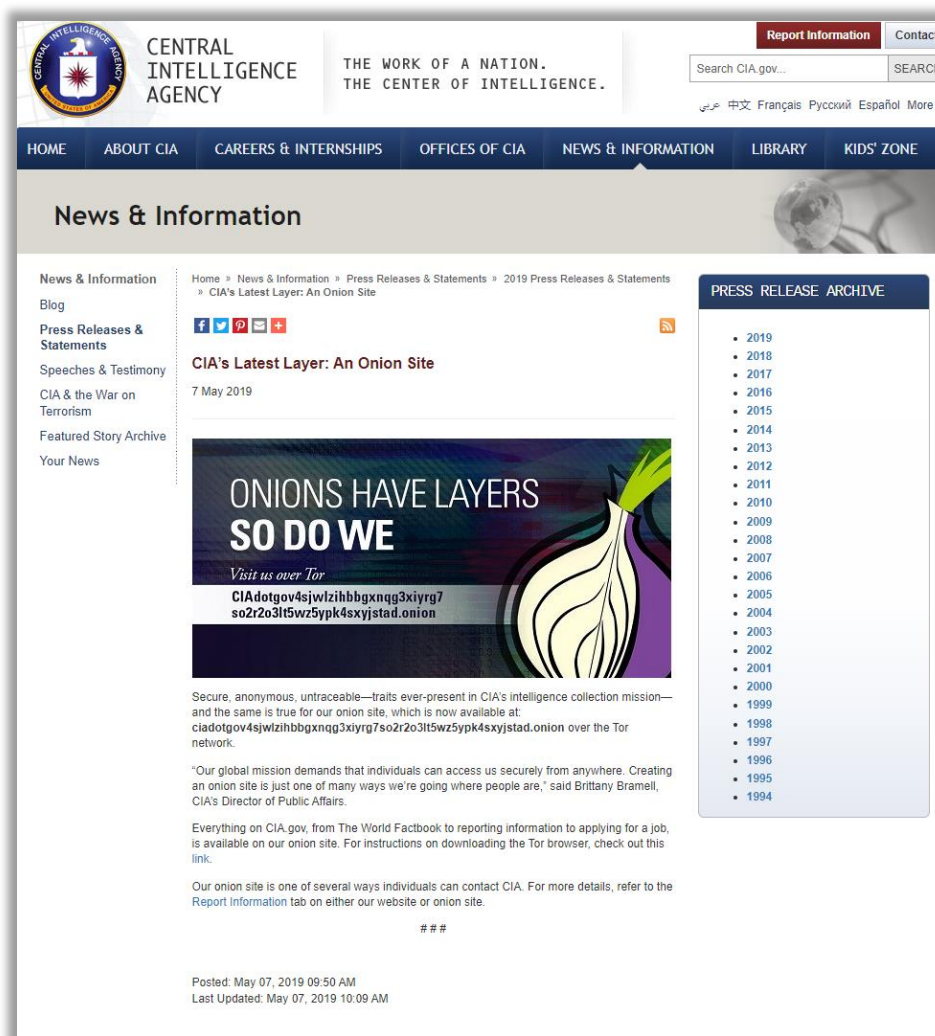
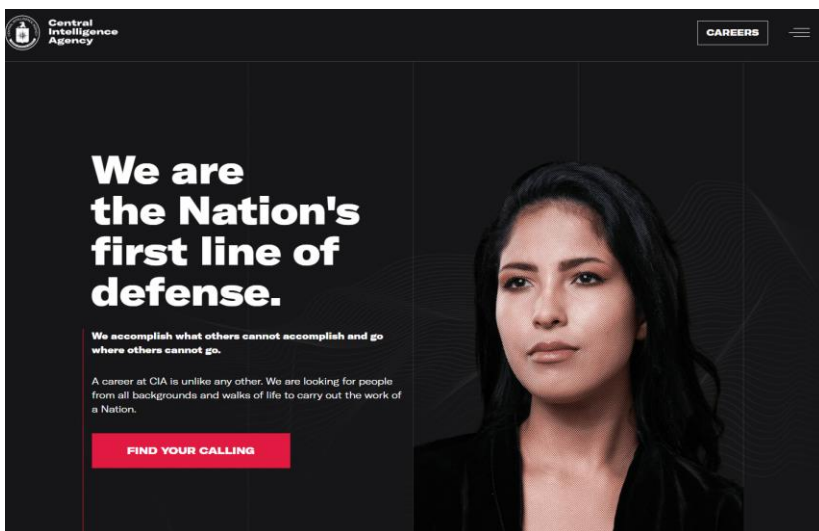


# TOR – The Onion Router (TorProject, 2002) изначально – FreeHaven, «Свободная гавань»





# Все в TOR – даже ЦРУ ;-)





СМОТРИ В БУДУЩЕЕ. ИНВЕСТИРУЙ В ЗНАНИЯ.

# АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

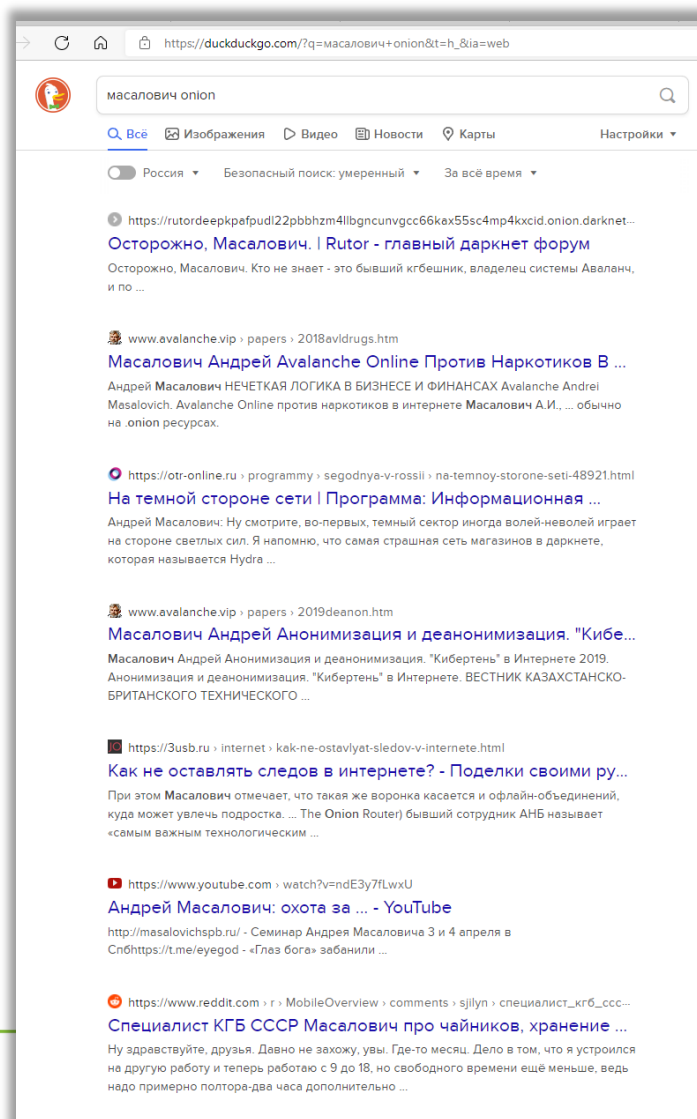
TOR – 1995, “FreeHaven”, Центр высокопроизводительных вычислительных систем Исследовательской лаборатории Военно-морских сил США (NRL)





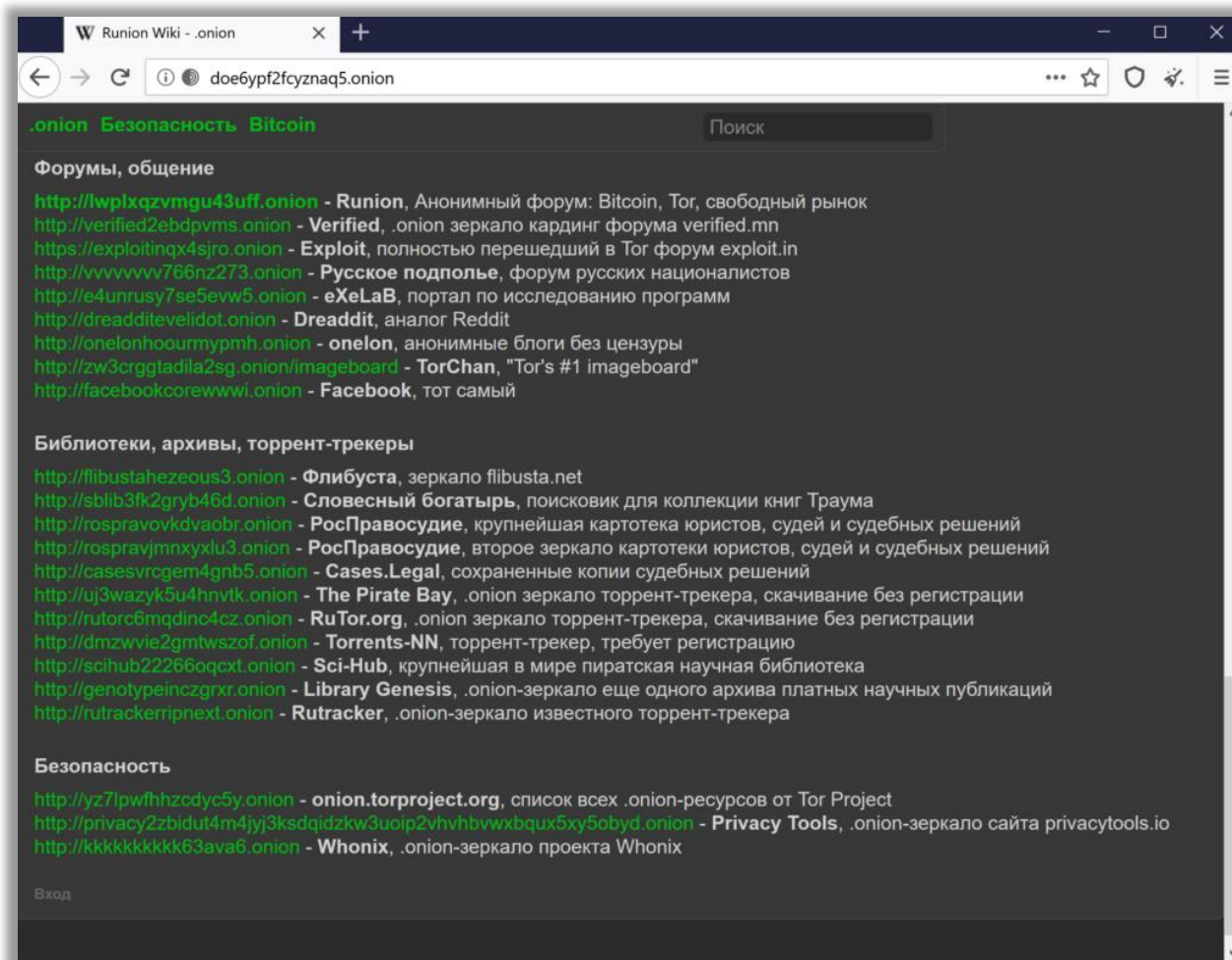
# Поиск в TOR: [duckduckgo.com](https://duckduckgo.com) (с 2008)

- без «пузырей фильтров» и не шпионит





# Каталог русскоязычных ресурсов **Runion Wiki** (<http://doe6ypf2fcyznaq5.onion>)

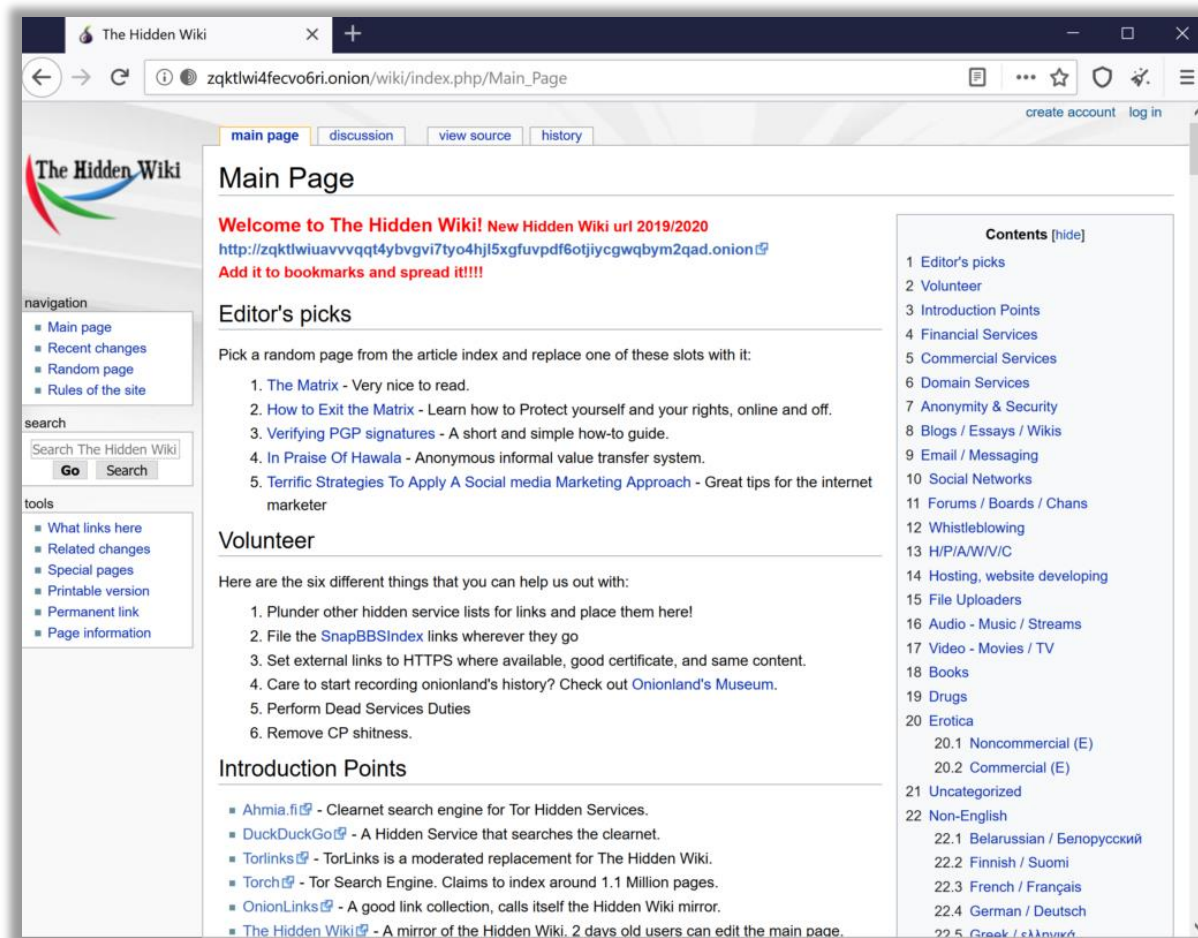




# Самый большой каталог Даркнета

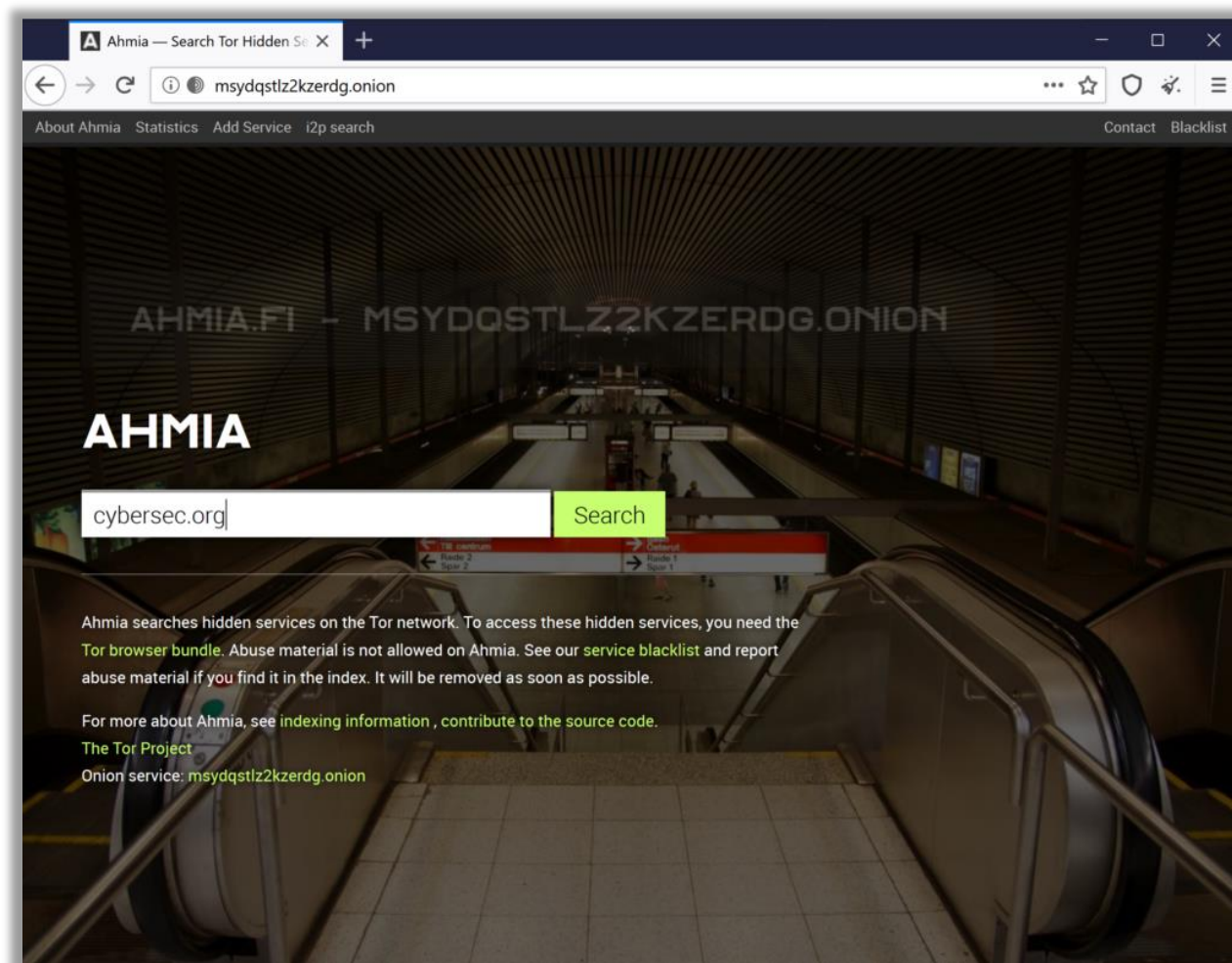
## The Uncensored Hidden Wiki

([http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main\\_Page](http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page))



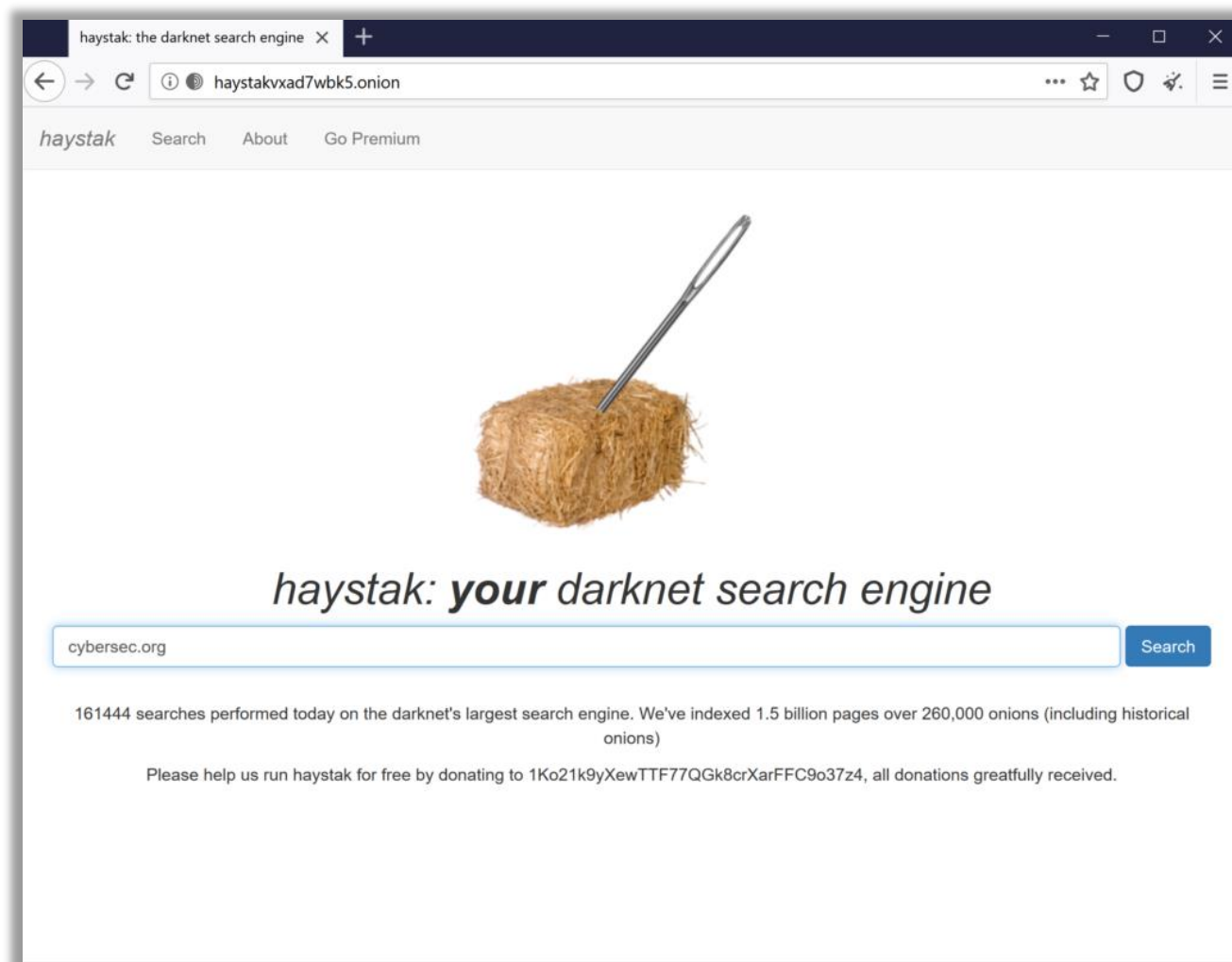


# Один из лучших поисковиков Даркнета Ahmia (<http://msydstlz2kzerdg.onion>)



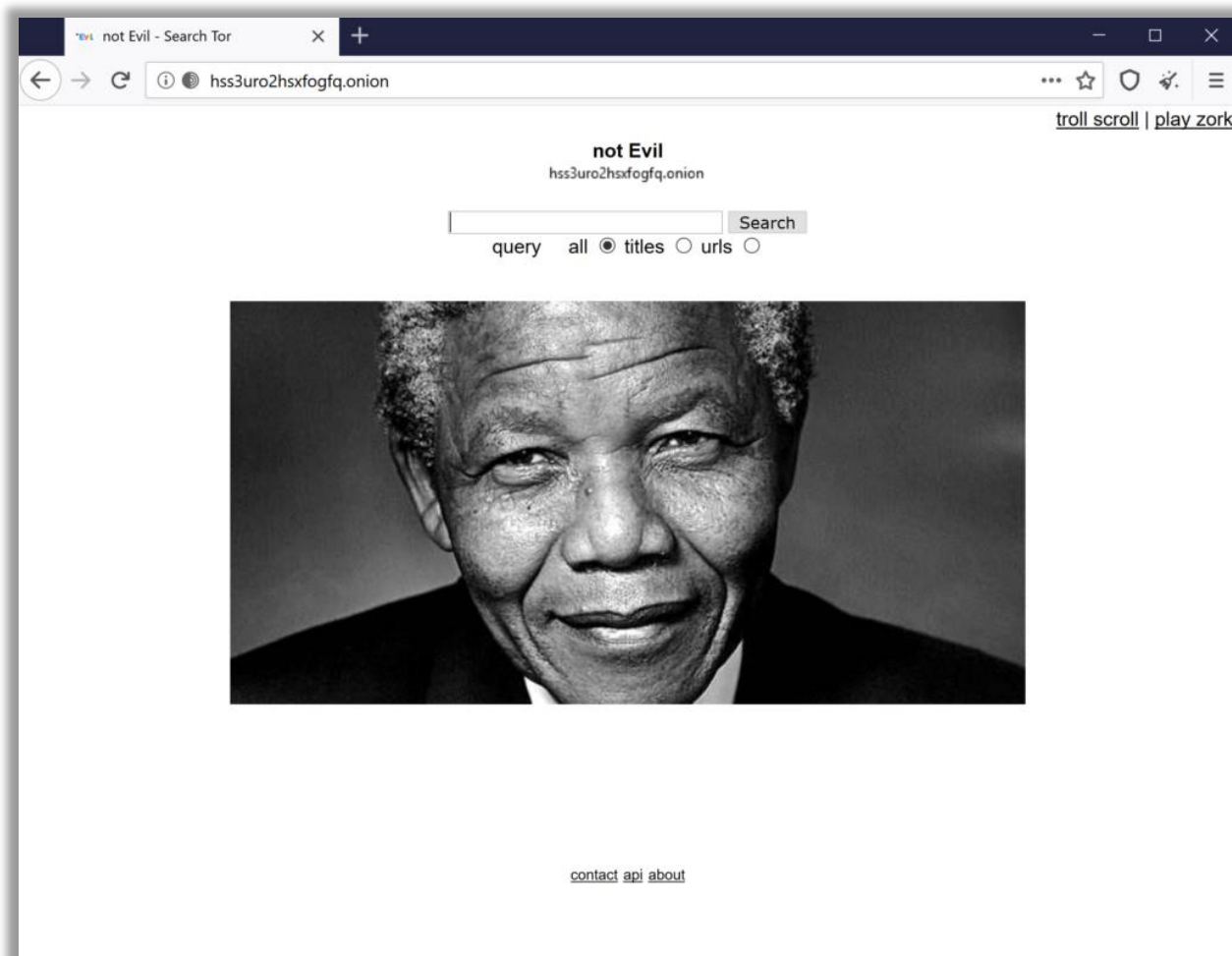


# Сравнительно новый, с амбициями на охват HayStack (<http://haystakvxad7wbk5.onion>)






Хорошая релевантность, около 3М ссылок  
Not Evil (<http://hss3uro2hsxfogfq.onion>)





# Поиск и анонимность в duckduckgo



## Андрей Масалович

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР «ЛАВИНА ПУЛЬС»

### О докладчике

Генеральный директор компании «Лавина Пульс». Руководитель ряда успешных проектов по аналитическому оснащению банков, финансово-промышленных групп, крупных торговых сетей, государственных организаций. Автор многочисленных публикаций. Провел семинары по проблемам поиска и анализа данных в ряде университетов России и США. Провел более 700 авторских семинаров по конкурентной разведке в интернете. Автор поисковой технологии Avalanche. Кандидат физико-математических наук, лауреат стипендии РАН «Выдающийся ученый России», подполковник ФАПСИ в отставке.


**15 МАЯ 17:00 - 18:00** Зал «Селигер» Хотят пойти: 143

**ТЕХНИЧЕСКИЙ ДОКЛАД** Язык доклада: Русский

**УМНЫЕ ЖИВУТ ДОЛЬШЕ. Технологии разума в современном кибероружии**

Докладчик: Андрей Масалович

Материалы: [Видео](#) [Презентация](#)



масалович onion

Россия Безопасный поиск: умеренный За всё время

<https://rutordeepkpfudl22pbhzm4lbgncunvgcc66kx55sc4mp4kxcid.onion.darknet...>  
**Осторожно, Масалович. | Rutor - главный даркнет форум**  
Осторожно, Масалович. Кто не знает - это бывший кГБешник, владелец системы Аваланч, и по ...

[www.avalanche.vip/papers/2018avidrugs.htm](http://www.avalanche.vip/papers/2018avidrugs.htm)  
**Масалович Андрей Avalanche Online Против Наркотики В ...**  
Андрей Масалович НЕЧЕТКАЯ ЛОГИКА В БИЗНЕСЕ И ФИНАНСАХ Avalanche Andrei Masalovich. Avalanche Online против наркотиков в интернете Масалович А.И., ... обычно на .onion ресурсах.

<https://otr-online.ru/programmy/segodnye-v-rossii/na-temnoy-storone-seti-48921.html>  
**На темной стороне сети | Программа: Информационная ...**  
Андрей Масалович: Ну смотрите, во-первых, темный сектор иногда волей-неволей играет на стороне светлых сил. Я напомню, что самая страшная сеть магазинов в даркнете, которая называется Hydra ...

[www.avalanche.vip/papers/2019deanon.htm](http://www.avalanche.vip/papers/2019deanon.htm)  
**Масалович Андрей Анонимизация и деанонимизация. "Кибе...**  
Масалович Андрей Анонимизация и деанонимизация. "Кибертепы" в Интернете 2019. Анонимизация и деанонимизация. "Кибертепы" в Интернете. ВЕСТНИК КАЗАХСТАНСКО-БРИТАНСКОГО ТЕХНИЧЕСКОГО ...

<https://3usb.ru/internet/kak-ne-ostavlyat-sledov-v-internete.html>  
**Как не оставлять следов в интернете? - Поделки своими ру...**  
При этом Масалович отмечает, что такая же воронка касается и офлайн-объединений, куда может увлечь подростка. ... The Onion Router) бывший сотрудник АНБ называет «самым важным технологическим ...

<https://www.youtube.com/watch?v=ndE3y7LwxU>  
**Андрей Масалович: охота за ... - YouTube**  
<http://masalovichspb.ru/> - Семинар Андрея Масаловича 3 и 4 апреля в Спб<https://t.me/eyeegod> - «Глаз бога» забанили ...

[https://www.reddit.com/r/MobileOverview/comments/sjilyn/специалист\\_кГБ\\_ссср...](https://www.reddit.com/r/MobileOverview/comments/sjilyn/специалист_кГБ_ссср...)  
**Специалист КГБ СССР Масалович про чайников, хранение ...**  
Ну здравствуйте, друзья. Давно не захожу, увя. Где-то месяц. Дело в том, что я устроился на другую работу и теперь работаю с 9 до 18, но свободного времени еще меньше, ведь надо примерно полтора-два часа дополнительно ...



## Осторожно, Масалович.

Кто не знает - это бывший кГБешник, владелец системы Аваланч, и по совместительству имеет отношение к администрированию кремлеботов в интернете. Некоторые источники называют его главным по ботам в стране. Также сидит на этом форуме и активно его мониторит. Имея внешность забавного старичка, тем не менее является опасным персонажем, из недавно появившихся в инфо поле русского интернета. После получения медийности на ЛюдиПро, начал активно продвигать кремлёвскую повестку, работая по системе 60 на 40. Бывших кГБешников, как говорится, не бывает. Обладает навыками вербовщика, что хорошо прослеживается в его речи.



# Как ломали TOR – 2012, 2014, 2016, 2019...

## Исследователи взломали Tor и передали данные ФБР

Сотрудники Университета Карнеги-Меллон в США взломали сеть Tor и передали [ФБР](#) информацию о пользователях. Об этом сообщает [Motherboard](#).

После многомесячной атаки на Tor в 2014 году, исследователи обнаружили уязвимость, которая позволила ее взломать. Атаки были частью исследовательского проекта [министерства обороны](#), о котором известно из материалов уголовного дела в отношении администраторов площадки Silk Road 2.0 Брайана Кинга.

Представители ФБР потребовали у сотрудников университета данные о некоторых преступниках, после чего им предоставили реальные IP-адреса. Представители ФБР утверждают, что все уязвимости были устранены.

Ранее Tor удалось собрать более \$200 тыс. пожертвований и разработку новых инструментов обеспечения анонимности.

18:01, 1 декабря 2016 Интернет и СМИ

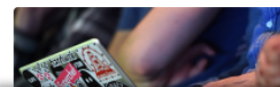
## Найден способ взломать Tor-браузер

Администрация Tor Project предупредила пользователей о возможном взломе анонимной сети из-за критической ошибки Mozilla Firefox, на основе которого разработан защищенный браузер. Об этом в четверг, 1 декабря, сообщает 9to5mac.

«Каждому, кто пользуется Tor и хочет сохранить свою анонимность, рекомендуется обновить браузер сразу после обнаружения критической ошибки Firefox».

Отмечается, что ошибка позволяет злоумышленникам раскрыть личность любого юзера Tor.

По словам представителей Mozilla, хакеры уже использовали эту уязвимость на Windows, но угроза нарушения анонимности всех платформ.



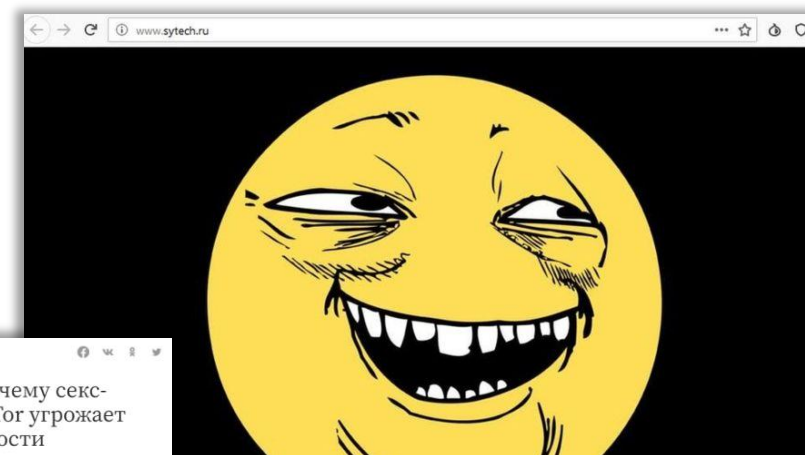
00:04, 14 июня 2016 Интернет и СМИ

## Все хакеры делают это Почему секс-скандал с разработчиком Tor угрожает всем любителям анонимности



Фото: Internet Chronicle

В начале июня руководство анонимной сети Tor отказалось от сотрудничества с легендой хакерского сообщества Джейкобом Эпплбаумом из-за анонимных обвинений в сексуальных домогательствах. Интимная жизнь одного из самых известных в мире специалистов по безопасности и раньше вызывала немало вопросов, но на этот раз в Tor посчитали, что секс-скандал серьезно ударит по репутации проекта. Сам Джейкоб отрицает все обвинения и утверждает, что против него ведется спланированная кампания. «Лента.ру» вспомнила подробности биографии Эпплбаума и выяснила, как его уход скажется на работе анонимной сети.





СМОТРИ В БУДУЩЕЕ. ИНВЕСТИРУЙ В ЗНАНИЯ.

# АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Анонимность, псевдонимность,  
зона нулевого доверия



Девичьи дневники:

- Не залетела в 14
- Не залетела в 15
- Не залетела в 16
- ...



# Анонимный герой снимает китайский флаг (Гонконг)





Чшоу Ишуань:  
«Хе-хе, угадайте, кто это делает»

14億中國人齊心緝拿  
辱國旗港獨暴徒 周頌軒





# David Bukowski

## - Quantum Stresser, DDoS и пицца



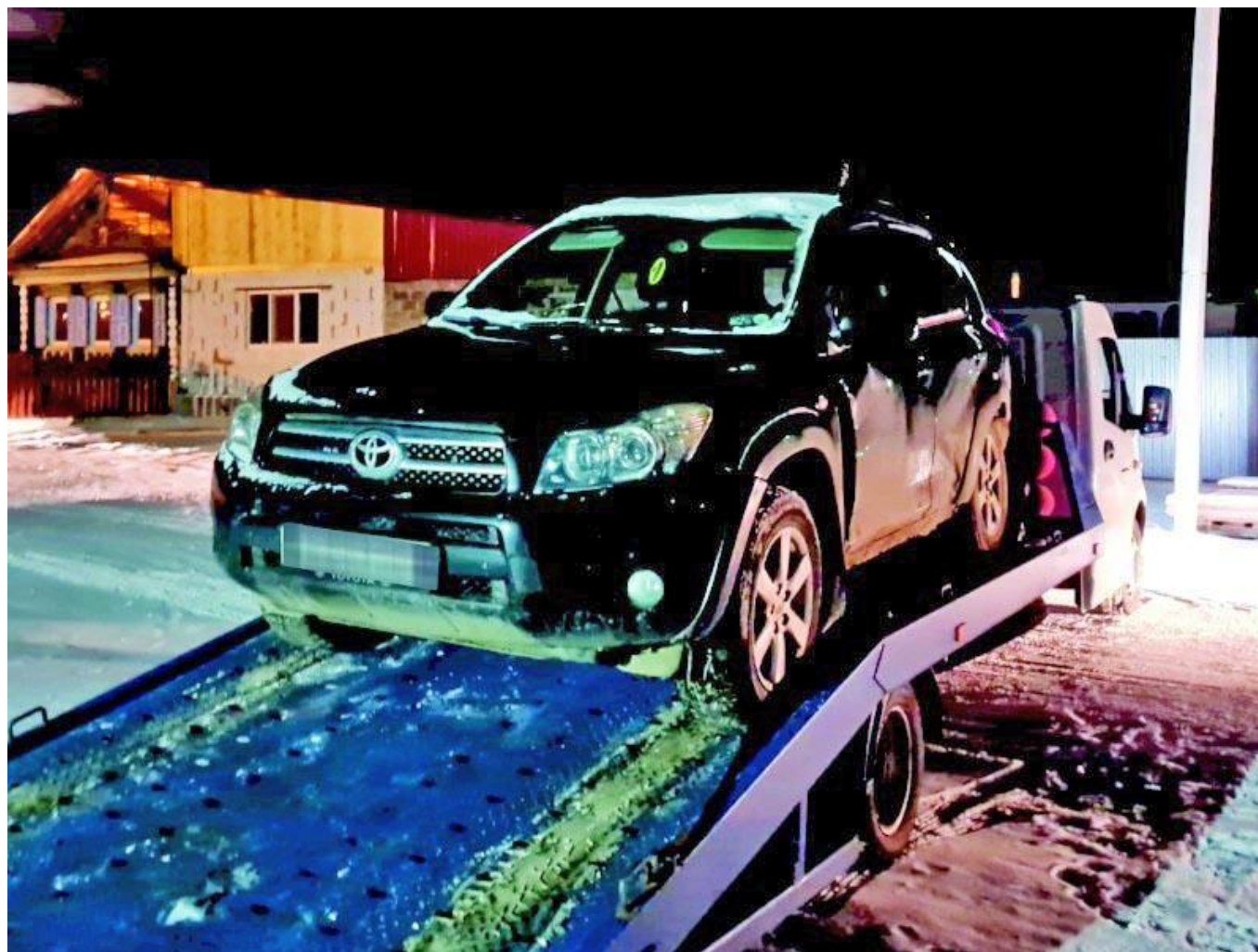


# Социальная активность как основа для расследования





# Источник утечек – наши ошибки и слабости

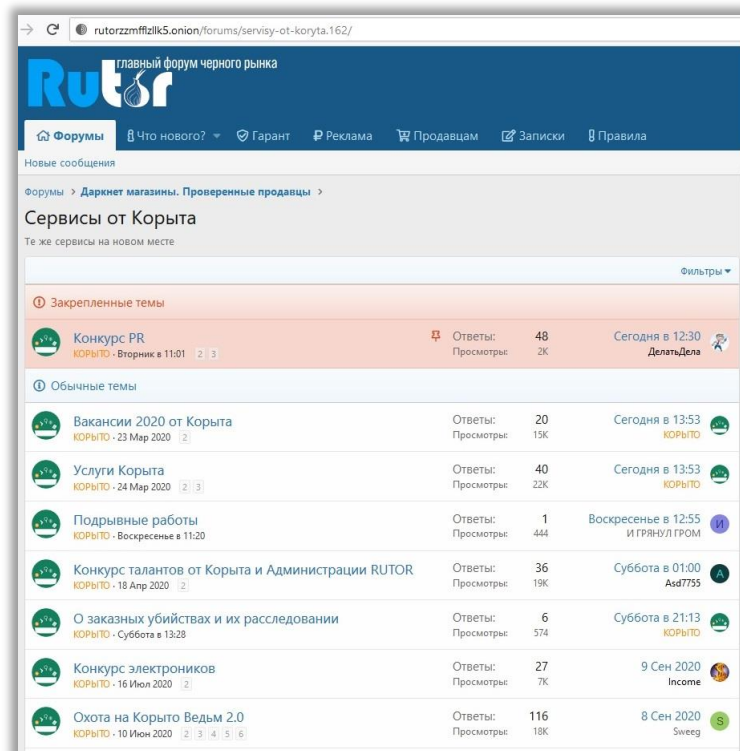
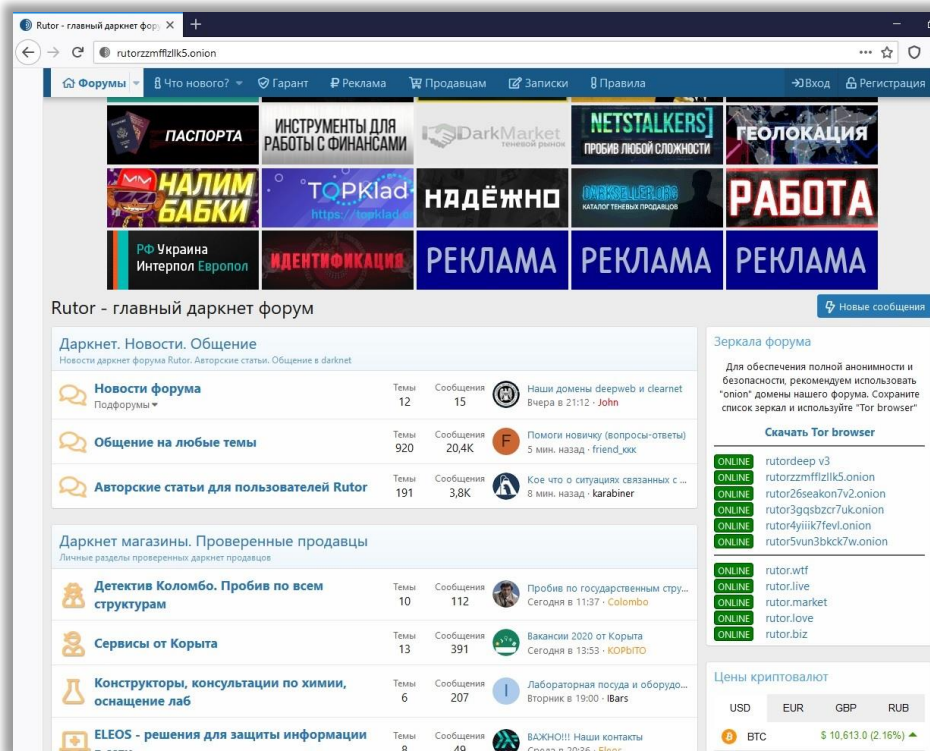




СМОТРИ В БУДУЩЕЕ. ИНВЕСТИРУЙ В ЗНАНИЯ.

# АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

## RUTOR - главный форум российского Даркнета






СМОТРИ В БУДУЩЕЕ. ИНВЕСТИРУЙ В ЗНАНИЯ.

# АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

## Корыто – услуги: взрывы, убийства...



**КОРЫТО**  
В деле с 2016 года  
Проверенный сервис

Сообщения: 133  
Реакции: 524

Воскресенье в 11:20

Бывает такое, что неожиданно требуется прорубить скалы для прокладки новой автомагистрали или железнодорожной ветки. Или иногда снос самовольных построек по указу Собянина нужно произвести очень оперативно. Где взять подрывников для выполнения столь интересных заданий? Правильно, вы уже пришли по адресу!

Итак, сервисы от Корыта предлагают ряд фокусов:

1. Превращение автомобиля в лом металла
2. Превращение отличных стейков в фарш

Сразу скажу что данные услуги не нацелены на совершение террористических актов и минирование школ, детсадов и прочего не рассматривается, строго одна акция на 1-2 целей. По ценам опять же скажу - не дешево (как часто у меня бывает), только еще умноженное на 2-3, поскольку дела такие интересуют очень сильно [людей в форме](#).

Пример работы можете посмотреть [тут](#). Любителям сока "добрый" смотреть не рекомендуется.


Контакты для заказов как всегда в моей подписи.

Jabber: [kopbitoxmpp.jp](mailto:kopbitoxmpp.jp)  
TLG шоппорта: @MSK\_SPB\_KZN  
Публичный PGP-ключ

MisterSmith47, Macanap, Dragon States и 2 других

Подписчики

7 дней 14 дней 30 дней 60 дней 90 дней ... часы дни недели месяцы



Подписчики

26 Jun 3 Jul 10 Jul 17 Jul 24 Jul 31 Jul 7 Aug 14 Aug 21 Aug 28 Aug 4 Sep 11 Sep 24 Sep



СМОТРИ В БУДУЩЕЕ. ИНВЕСТИРУЙ В ЗНАНИЯ.

# АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

КОРЫТО - После проведения  
оперативных мероприятий...

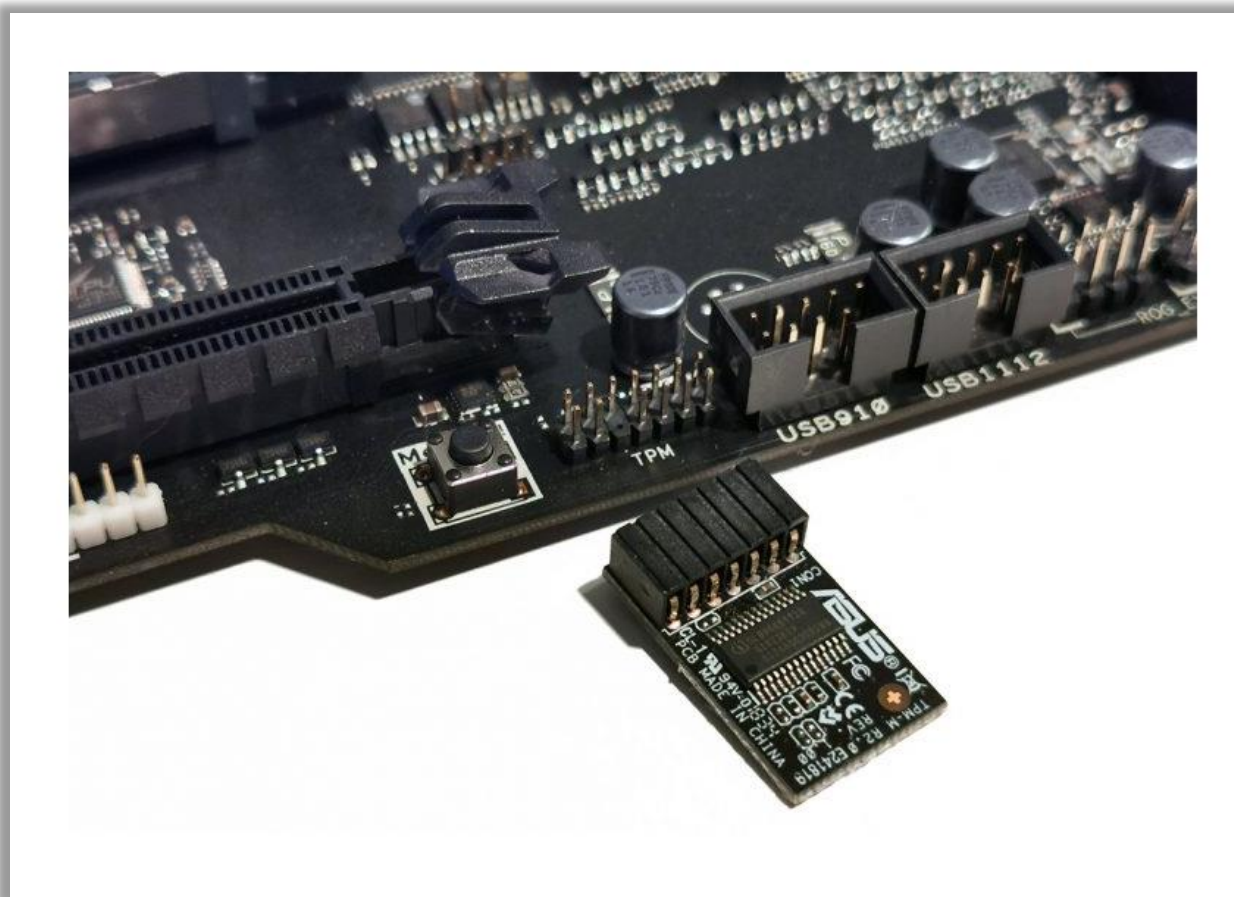




СМОТРИ В БУДУЩЕЕ. ИНВЕСТИРУЙ В ЗНАНИЯ.

# АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

## Знакомьтесь: TPM





СМОТРИ В БУДУЩЕЕ. ИНВЕСТИРУЙ В ЗНАНИЯ.

# АКАДЕМИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

## Анонимность криптокошельков

### Транзакции

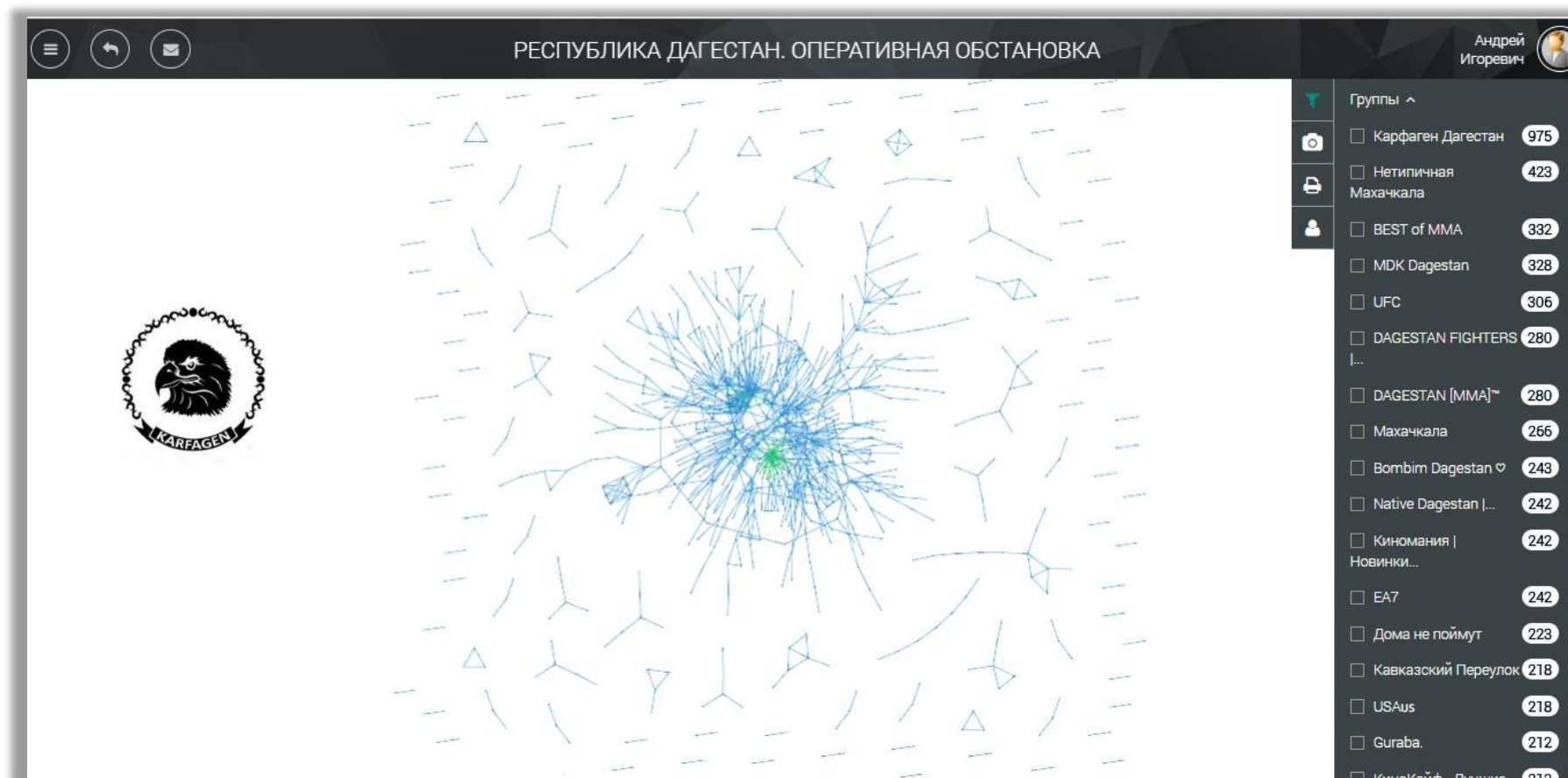
1 2 3 4 5 Следующие +10

Хэш	3047eb0b8d1b3cf89aca01d13f405324d04...	2019-12-02 17:12
	3GeMfo3bEzeuHB8p... 10.00000000 BTC	3BZT8ZvCS8H9dZPm4j... 1.02990000 BTC
	3KKf2jSa2rPB41bmgH5... 0.09954690 BTC	3QwV1m6ttYfsKeyZ6Pb... 0.14987000 BTC
	33EF1pU2MDGYM3N53... 0.00118819 BTC	1PSLgcCu1A1ZzsRr6tX... 0.05072000 BTC
	34MixVhZGpdk9G9Fj2... 0.00184643 BTC	13Je1ECP9bmmwXGs4... 3.49358039 BTC
	3AYxM6Vi2B7JsDm6D... 0.20399570 BTC	18xpKrX1h9cRLzfmBxR... 0.05050000 BTC
	3NtcCL5vKx81TW5mpu... 0.01250424 BTC	3QzYvaRFY6bakFBW4... 0.02914000 BTC
	33odgBapiucvyBgxDrX... 0.12306868 BTC	34Z1hqfeoRh1iBdvqbPh... 0.07060000 BTC
	3EwxcuSsHZcWa976W... 0.01250129 BTC	1LxjE29E9Gi9udZYQ4k... 0.23218000 BTC
	37dtNL8V34z4dPLvp3... 0.01000000 BTC	3CkczugtALRrskCo5uq... 0.25000000 BTC
	3LduCgBKY4anNF12e6... 0.04500000 BTC	1GggxnmYrcqFVxXwym... 0.12039531 BTC
		Загрузить больше выходов ... (2 осталось)
Комиссия	0.00032472 BTC (8.781 sat/B - 4.516 sat/WU - 3698 bytes)	-10.00000000 BTC

# Анализ активности в социальных сетях: Муфтият Дагестана

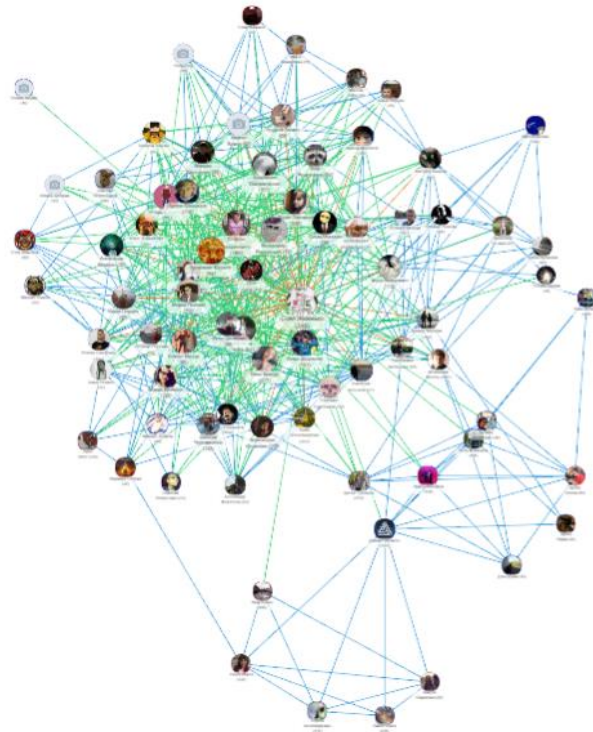


# Вайнахское молодежное движение (Карфаген) в социальных сетях - Дагестан





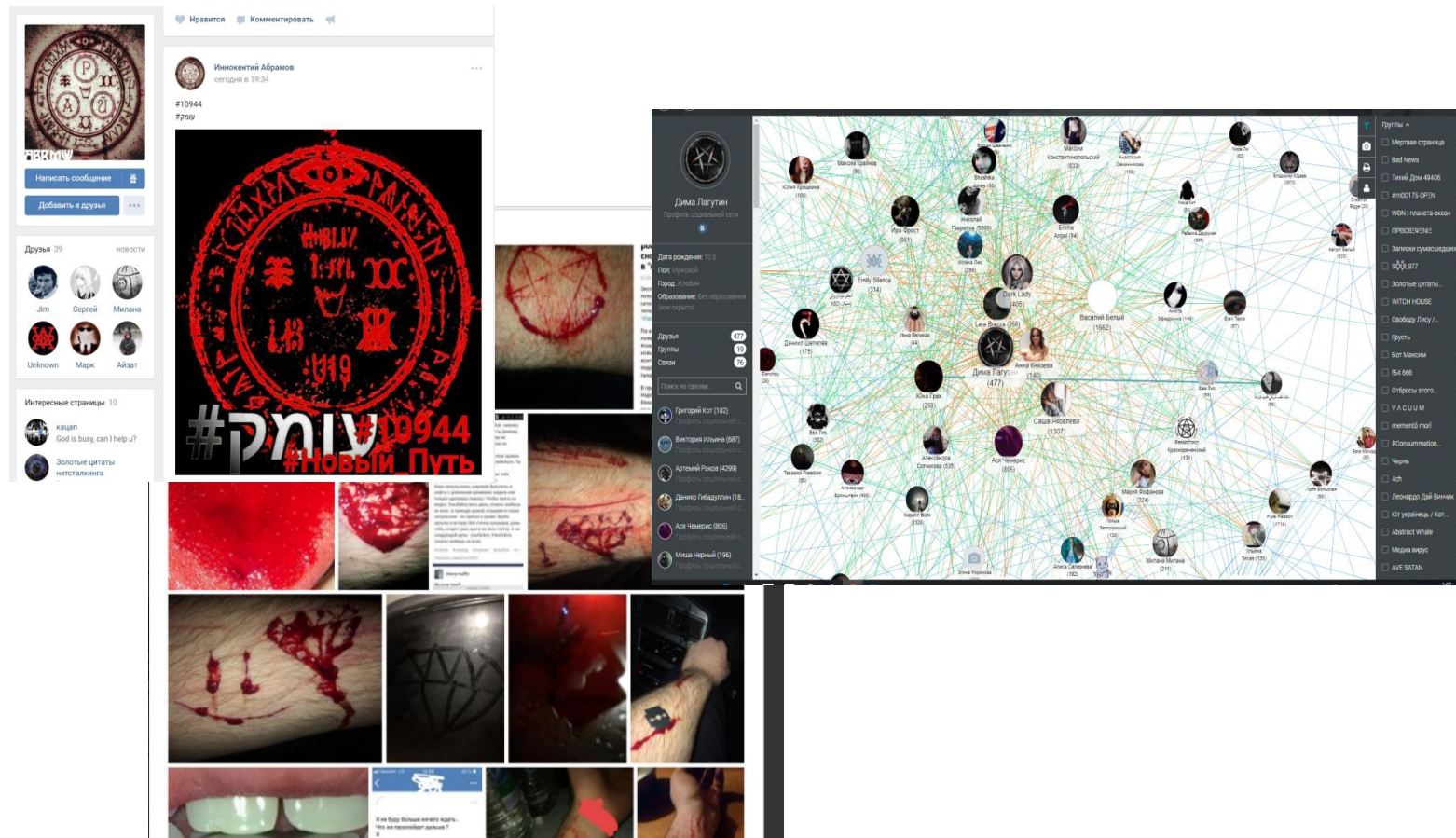
# Анализ связей: города, группы, интересы



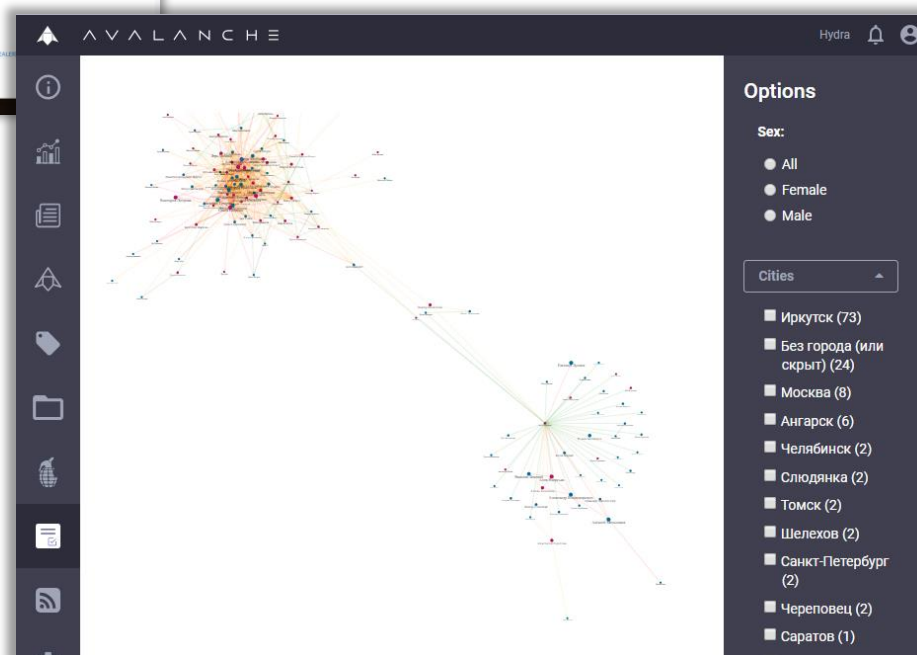
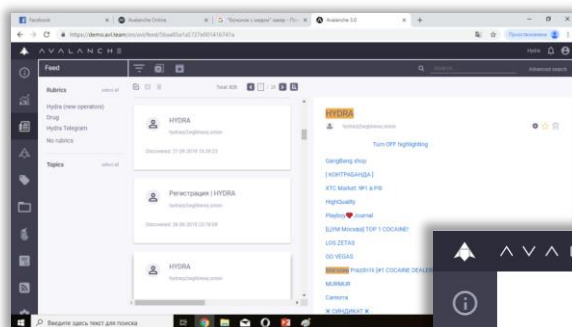
Города ^	
<input type="checkbox"/> Москва	57
<input type="checkbox"/> Без города (или...	34
<input type="checkbox"/> Бологое	1
<input type="checkbox"/> Санкт-Петербург	1
<input type="checkbox"/> Новороссийск	1
<input type="checkbox"/> Днепропетровск...	1
Образование ^	
<input type="checkbox"/> Без образования...	87
<input type="checkbox"/> МГУ	3
<input type="checkbox"/> НИУ ВШЭ (ГУ-ВШЭ)	1
<input type="checkbox"/> МПГУ (бывш. МГПИ...	1
<input type="checkbox"/> МИОО (бывш. МИПКРО)	1
<input type="checkbox"/> МГТУ им. Н. Э....	1

Группы ^	
<input type="checkbox"/> Смейся до слёз :D	21
<input type="checkbox"/> ПРИКОЛЫ   Смеяка	20
<input type="checkbox"/> Сигнал	16
<input type="checkbox"/> Кладовая комиксов	15
<input type="checkbox"/> Лайфхак	15
<input type="checkbox"/> Улыбнуло :D	13
<input type="checkbox"/> Бот Максим	13
<input type="checkbox"/> Чёрный юмор	12
<input type="checkbox"/> Весёлый гусь	12
<input type="checkbox"/> Книга Рекордов	12
<input type="checkbox"/> Палата №6	12
<input type="checkbox"/> Новая Музыка 2018  ...	12
<input type="checkbox"/> Собака оборжака	11
<input type="checkbox"/> Арт Бот	11
<input type="checkbox"/> Книга рекордов	11
<input type="checkbox"/> Филиал сообщений от...	11
<input type="checkbox"/> Овсянка, сэр!	11

# Пример: суицидные группы подростков «Синий кит», «Красная сова»



# Работа в «сером» и «черном» интернете (TOR и др)



# СПАСИБО ЗА ВНИМАНИЕ!

## Ваши вопросы

### КОНТАКТЫ:



+7 (495) 120-04-02



[ais@infosystem.ru](mailto:ais@infosystem.ru)



[www.infosystems.ru](http://www.infosystems.ru)  
[www.vipforum.ru](http://www.vipforum.ru)  
[www.moreais.ru](http://www.moreais.ru)