

OSINT

Разведка на основе открытых источников
информации



Daria Shcherbatyuk

aka

Pandora Lewandowski

aka

the_eternal_insomnia



Reconnaissance?
Open Source Intelligence?
Competitive Intelligence?
Threat Intelligence?

OSINT



MASINT



TECHINT



FININT



HUMINT



SIGINT



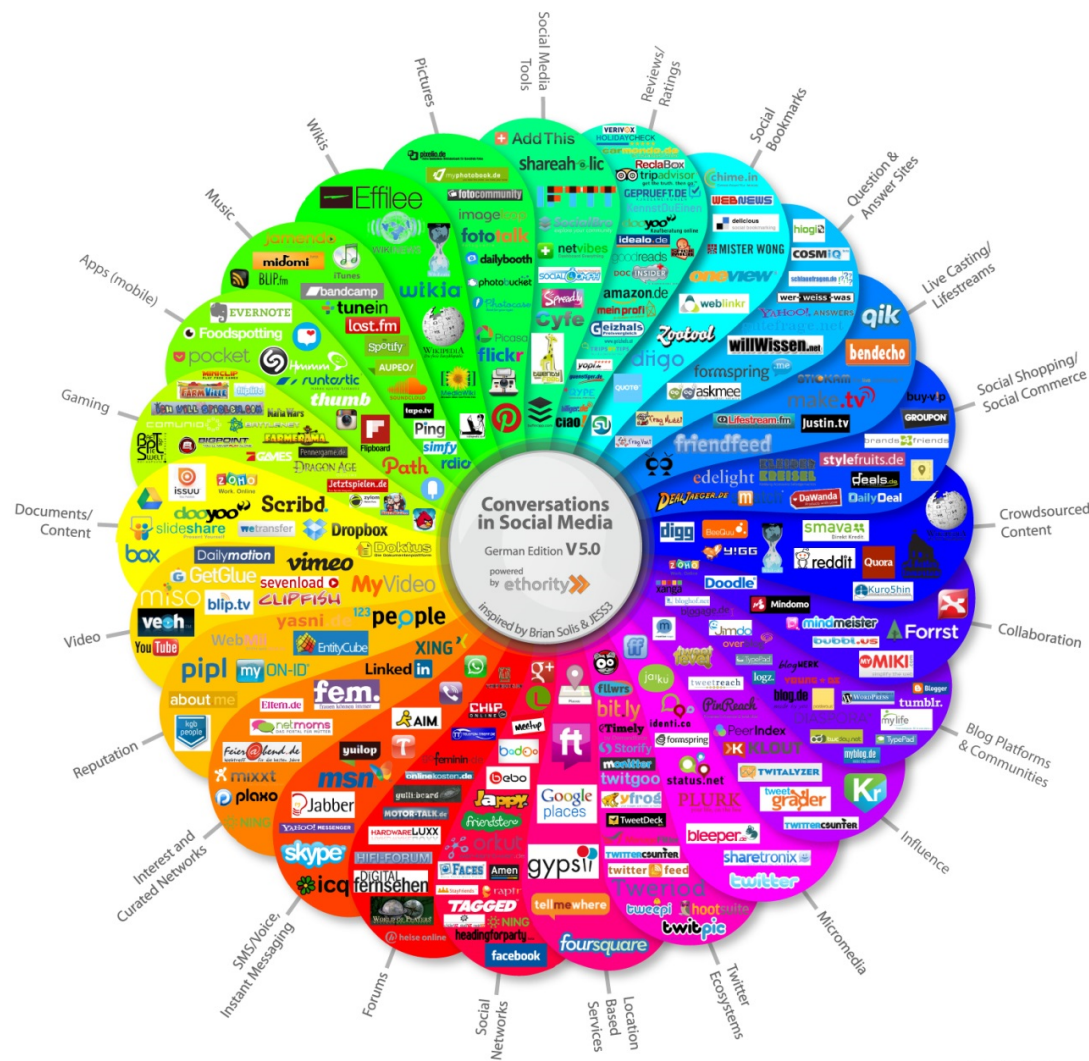
GEOINT/IMINT

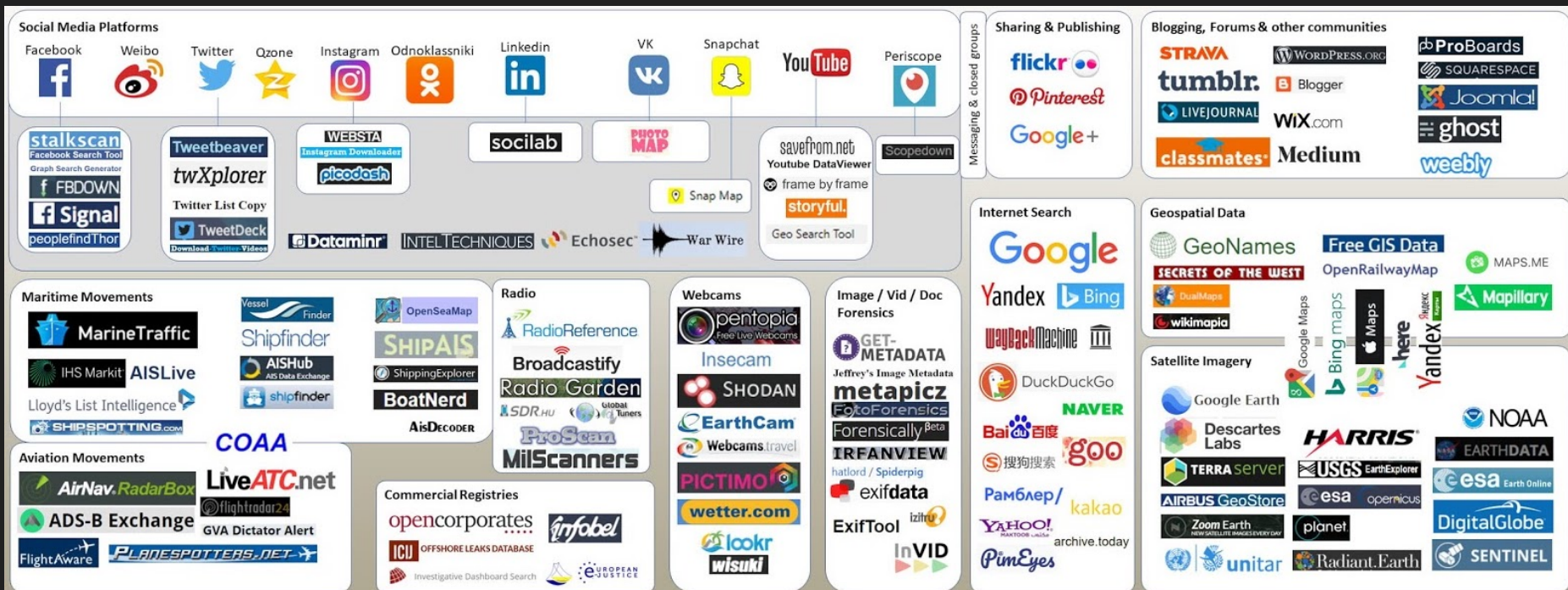


COMINT



Открытые источники





ТЫСЯЧИ ИХ...



OPEN SOURCE INTELLIGENCE TOOLS AND RESOURCES HANDBOOK

Social Media Tools: VKontakte

Tool	Link
Дезертир	http://vk.com/app3046467
Barkov.net	http://vk.barkov.net
Find Face	http://findface.ru
Report Tree	http://dcpu.ru/vk_repost_tree.php
Social Stats	http://socialstats.ru
SnRadar	http://snradar.azurewebsites.net
Spotlight	http://spotlight.svezet.ru
Target Hunter	https://targethunter.net
Target Log	http://targetolog.com
VK5	http://vk5.city4me.com
VK Community Search	http://vk.com/communities
VK Parser	http://vkparser.ru
VK People Search	http://vk.com/people
VK to RSS Appspot	http://vk-to-rss.appspot.com
vMetaDate	https://gist.github.com/cryptolok/8a023875b47e20bc5e64ba8e27294261

325

Устройство интернета

Vk?

Wikileaks?

The Hidden Wiki?

Freenet?

Torch?



Coursera?

4chan?

i2p?

The Pirate Bay?

Wikipedia?

Поисковые системы

Общего назначения

Google

Яндекс

yahoo!

Baidu 百度



DuckDuckGo

Специального назначения



SHODAN



Censys



TinEye

МАМОТ

Метапоисковые системы

Metabot.ru

info.com

zapmeta

izito

Crawler-based
search engine

Web directories

Meta search

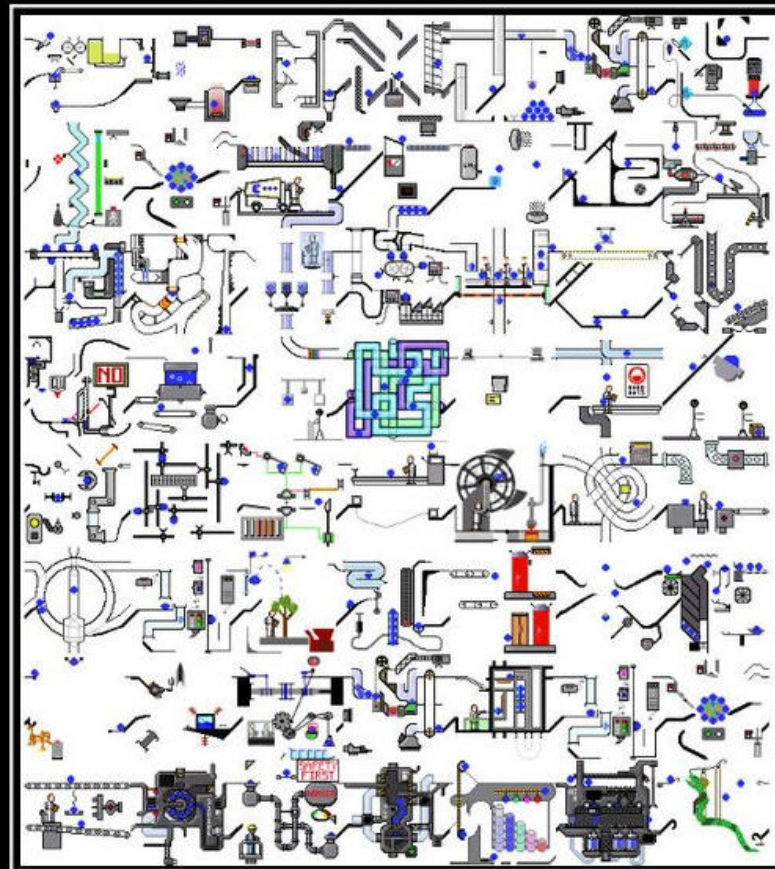


Схема работы

Поисковой системы



Операторы поиска Google (2018)

«google»	define:	inurl:	movie:
OR	cache:	allinurl:	in
AND	filetype:	intext:	source:
-	ext:	allintext:	—
*	site:	AROUND(N):	
()	related:	weather:	
\$ €	intitle:	stocks:	
@ #	allintitle:	map:	

Операторы поиска Google (2018)

Частично рабочие

#..#

inanchor:

allinanchor:

blogurl:

loc:

location:

Сломанные

+

~

inpostauthor:

allinpostauthor:

link:

id: info:

daterange:

phonebook:

Google Dorks



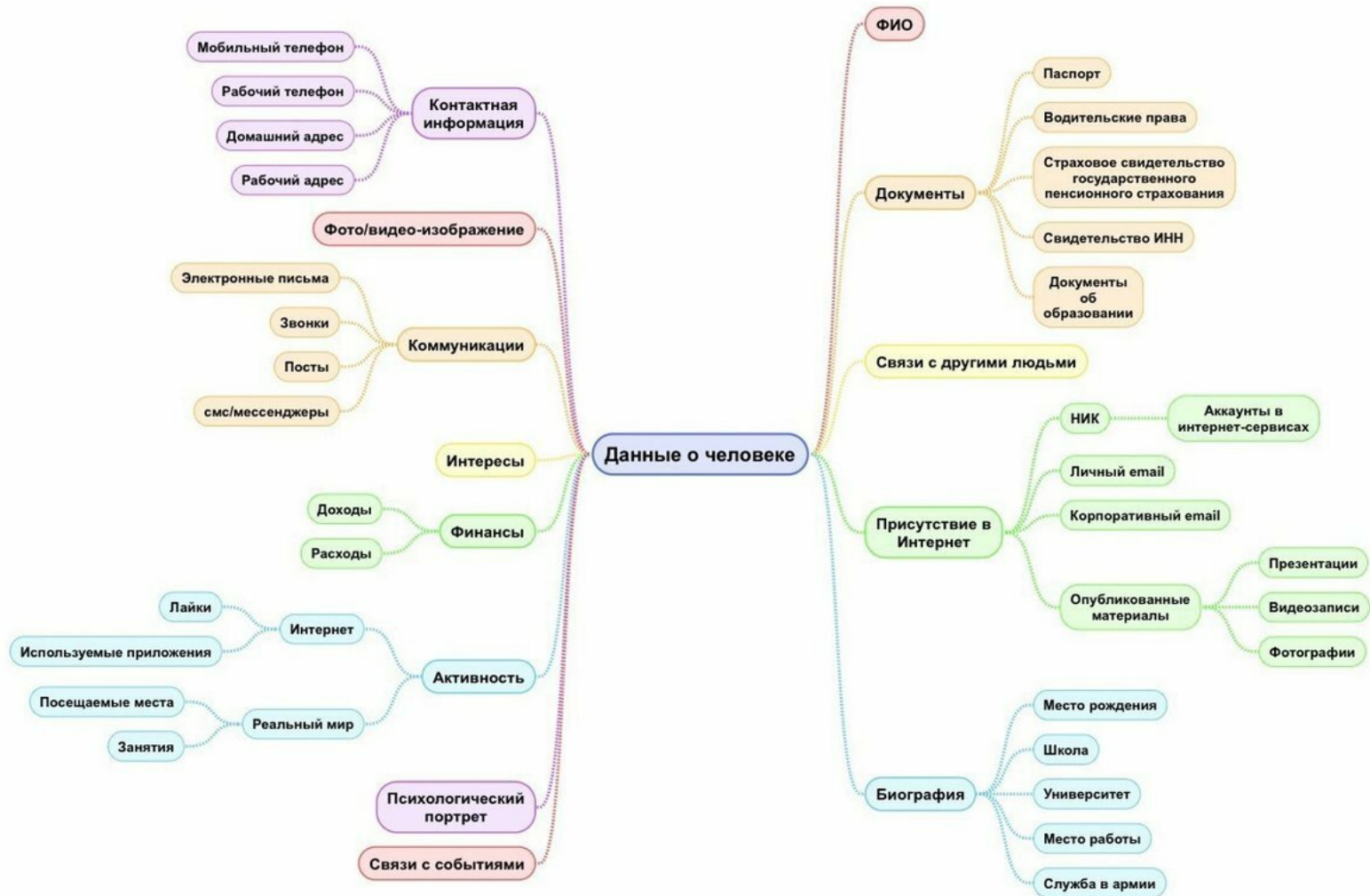
intitle:"Index of" secret

ext:pwd (administrators |
users | lamers | service)

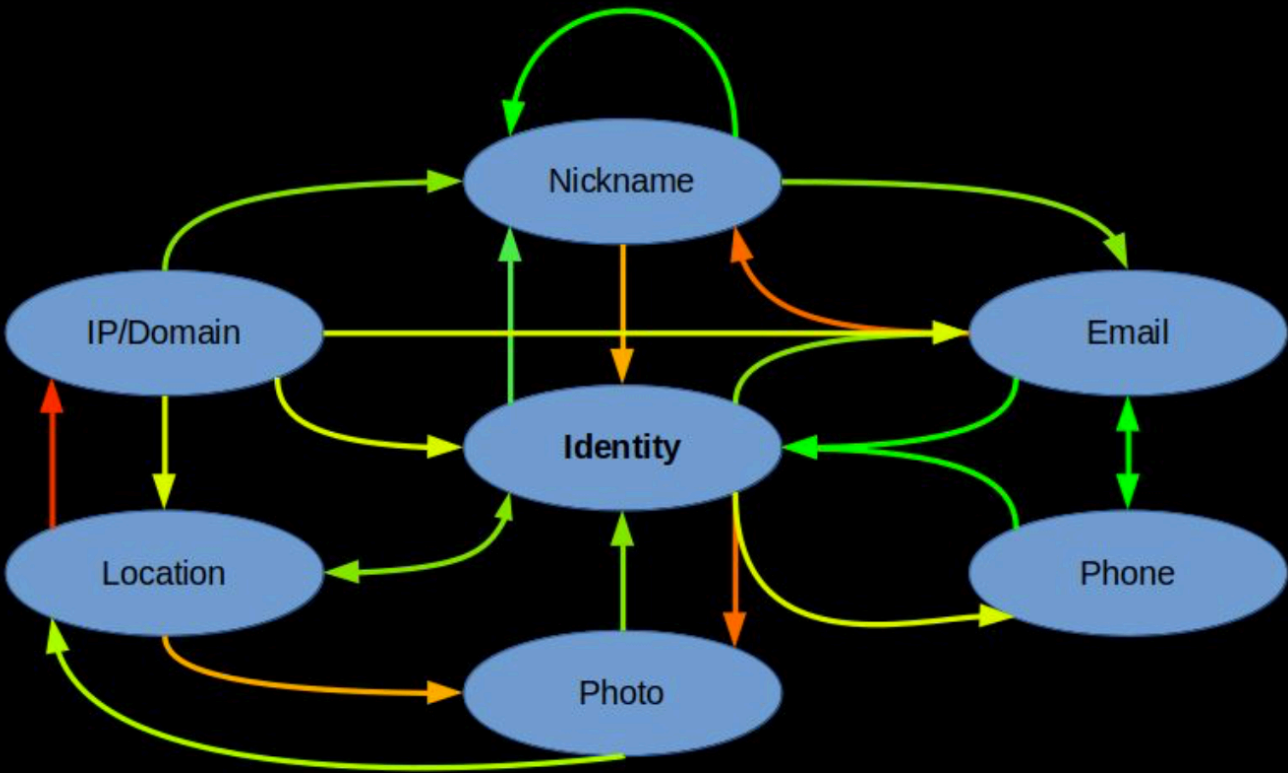
inurl:wp-config
-intext:wp-config
"DB_PASSWORD"

Цифровой след,
цифровая тень,
цифровой отпечаток,
digital footprint





Градации точности и
эффективности, от
НИЗКИХ до ВЫСОКИХ



instantusername.com

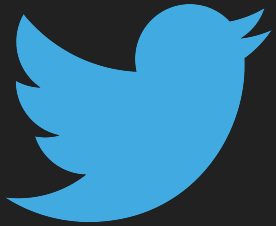
Namech_k

suip.biz

Username

 Facebook	 YouTube	 Twitter	 Instagram	 Blogger	 Reddit	 Ebay	 Wordpress	 Pinterest	 Yelp	 Slack	 Github
 Basecamp	 Tumblr	 Flickr	 Pandora	 ProductHunt	 Steam	 MySpace	 Foursquare	 OkCupid	 Vimeo	 Etsy	 SoundCloud
 BitBucket	 CashMe	 DailyMotion	 About.me	 Disqus	 Medium	 Behance	 Photobucket	 Coderwall	 Fanpop	 deviantART	 Good Reads
 Instructables	 Keybase	 Kongregate	 LiveJournal	 Mix	 AngelList	 last.fm	 Slideshare	 Tripit	 PayPal	 Dribbble	 Imgur
 Tracky	 Flipboard	 Vk	 Kik	 Codecademy	 Roblox	 Gravatar	 Trip	 Pastebin	 blip.fm	 Wikipedia	 Ello

Социальные сети





vk.barkov.net

vk.watch

[snradar](https://snradar.com)

vk5.city4me.com

[220vk](https://220vk.com)

vk.com/vk_groups_bot



insta-stories.ru

[www.instagram.com/
example/?__a=1](https://www.instagram.com/example/?__a=1)

Мессенджеры





search.buzz.im

lyzem.com

[@usinfobot](#)

[@SangMataInfo_bot](#)

Другие сервисы



dis.cool



FindMySnap



@get_kontakt_bot

snapdex.com

Github, GitLab, Bitbucket

```
Merge: 84fa6be 6a26afa  
Author: John Hammond <johnhammond010@gmail.com>  
Date: Sat Jun 8 11:56:59 2019 -0400
```

```
Merge pull request #4 from Prodicode/patch-1
```

```
Added Steganography Online
```

```
commit 84fa6be948d608889bc3636248cffa3a3baaa578  
Merge: d3d50b4 f500f15  
Author: John Hammond <johnhammond010@gmail.com>  
Date: Sat Jun 8 11:56:41 2019 -0400
```

```
Merge pull request #6 from Abemarkar23/patch-1
```

```
added a website for cryptography
```


Почты



emailrep.io

mostwantedhf.info

email2phonenumber

@last4mailbot

searchmy.bio

Утечки

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?

@Smart_SearchBot

@mailsearchbot

@shi_ver_bot

@info_baza_bot

leakedsource.ru

Восстановление доступа

 Сброс пароля

Русский ▾

Найдите свою учётную запись в Твиттере

Укажите адрес электронной почты, номер телефона или имя пользователя.

Поиск



Не удается войти?

Введите имя пользователя или электронный адрес, и мы отправим вам ссылку для восстановления доступа к аккаунту.

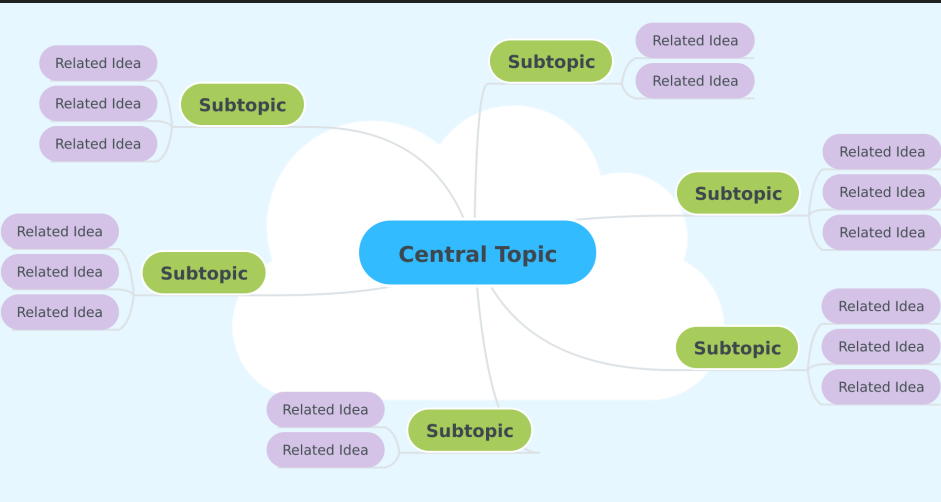
Электронный адрес, телефон или имя пользователя
the_eternal_insomnia

Отправить ссылку на вход

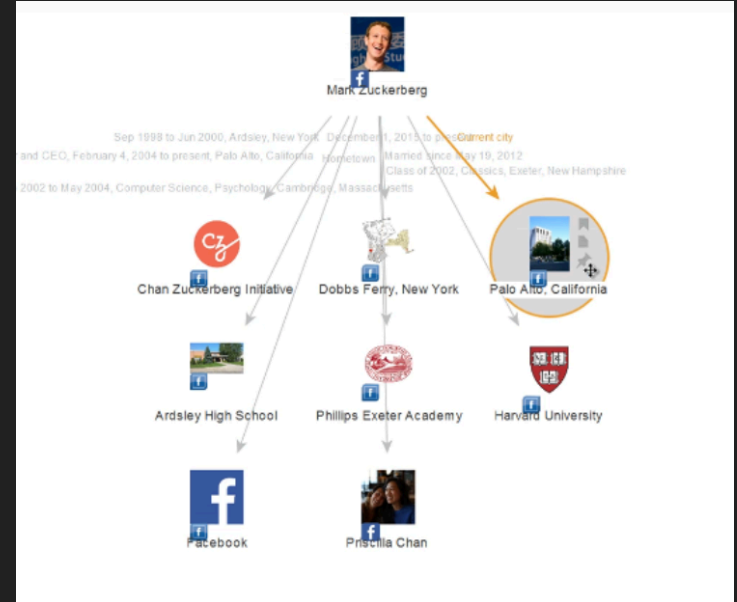
или

Создать новый аккаунт

Систематизация информации

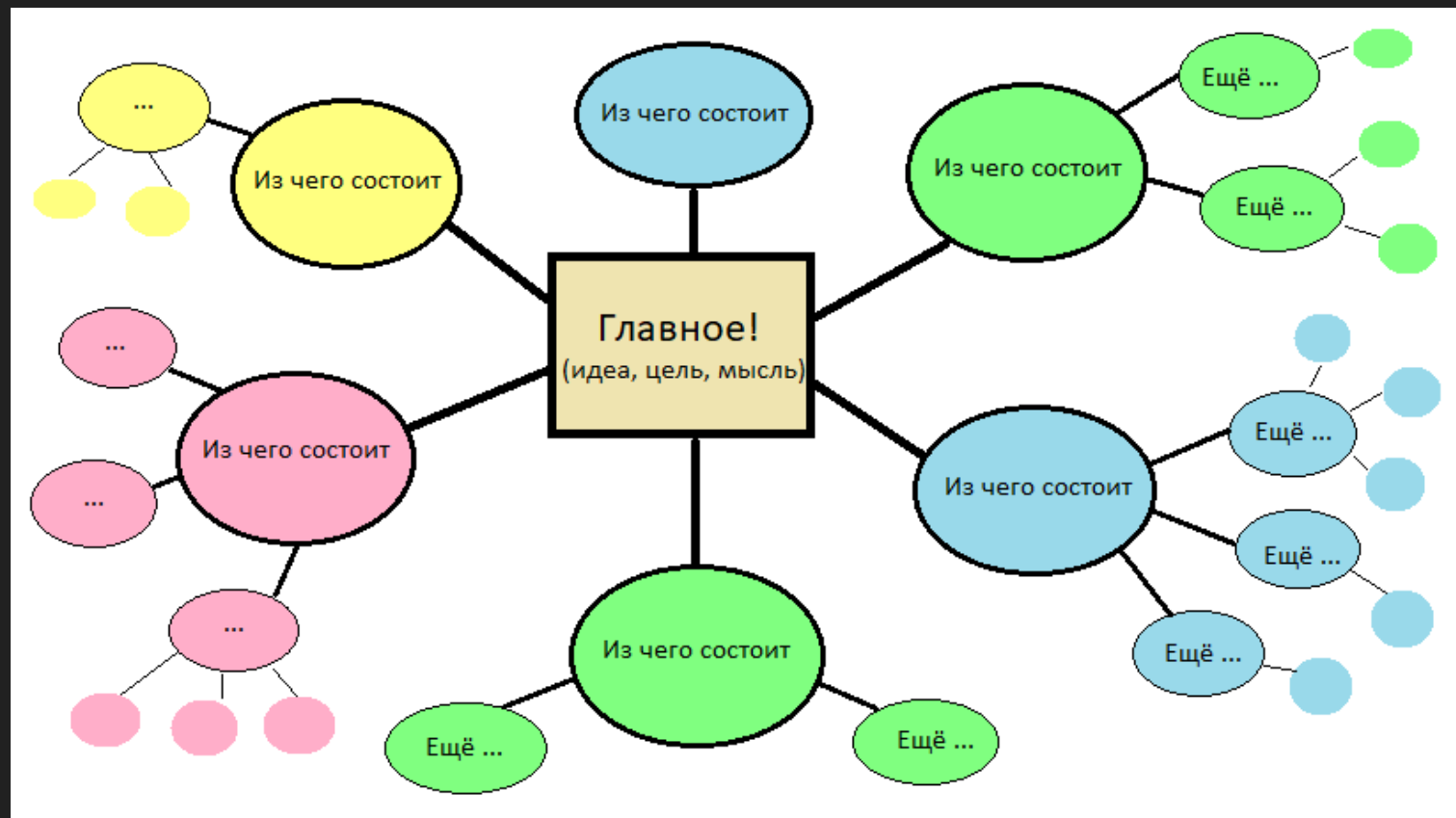


MindMap

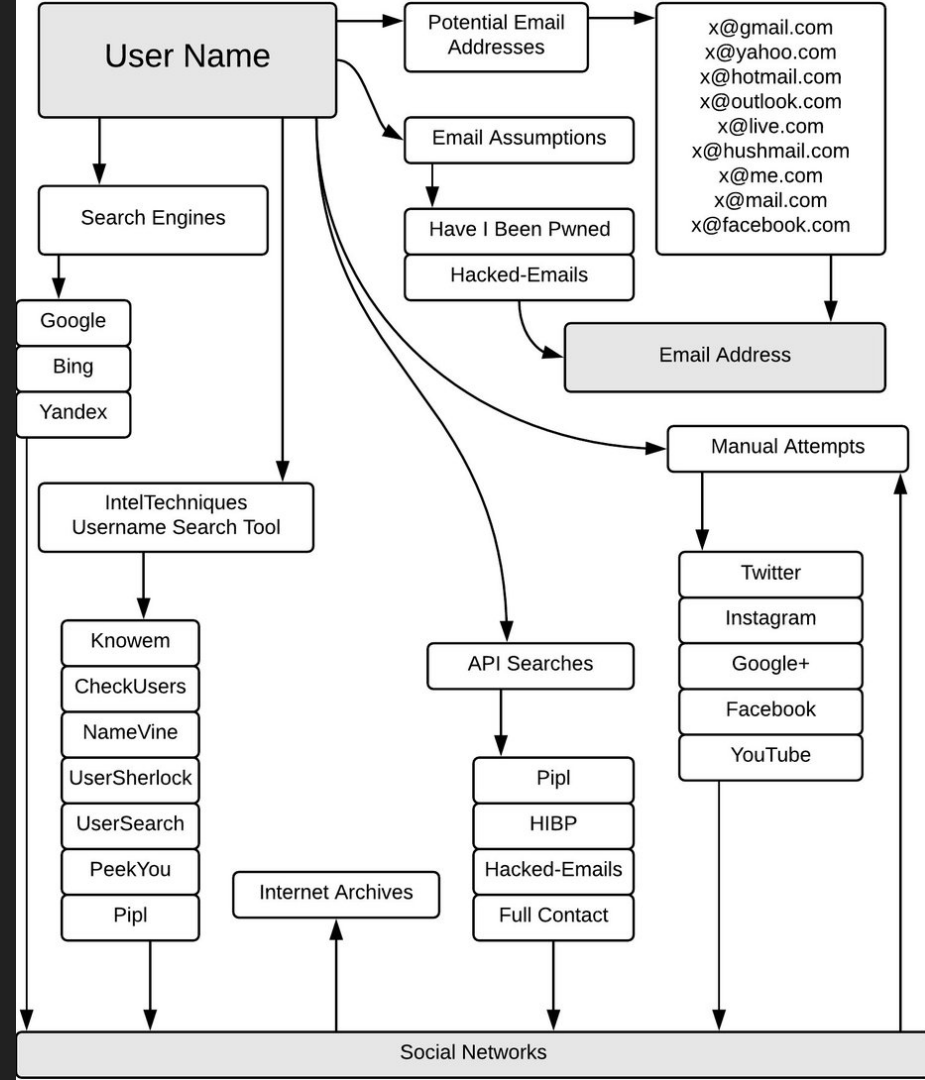
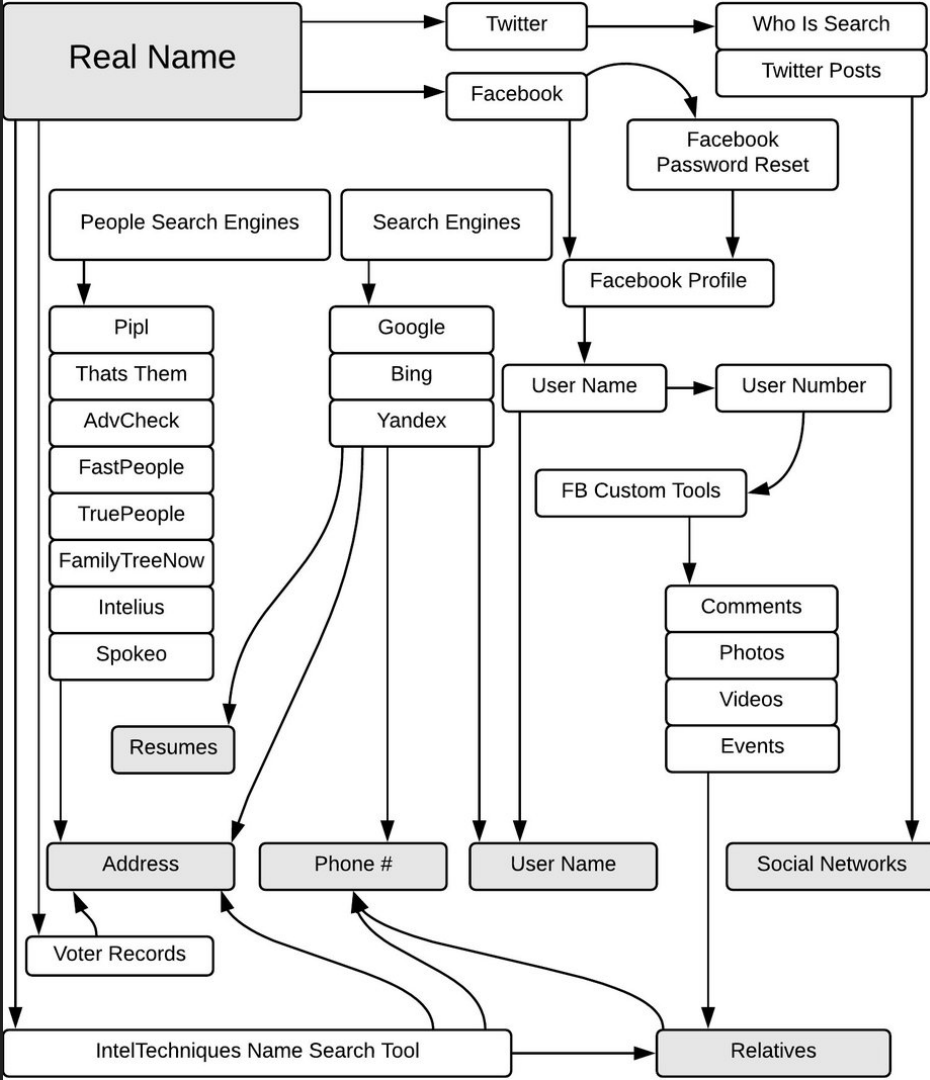


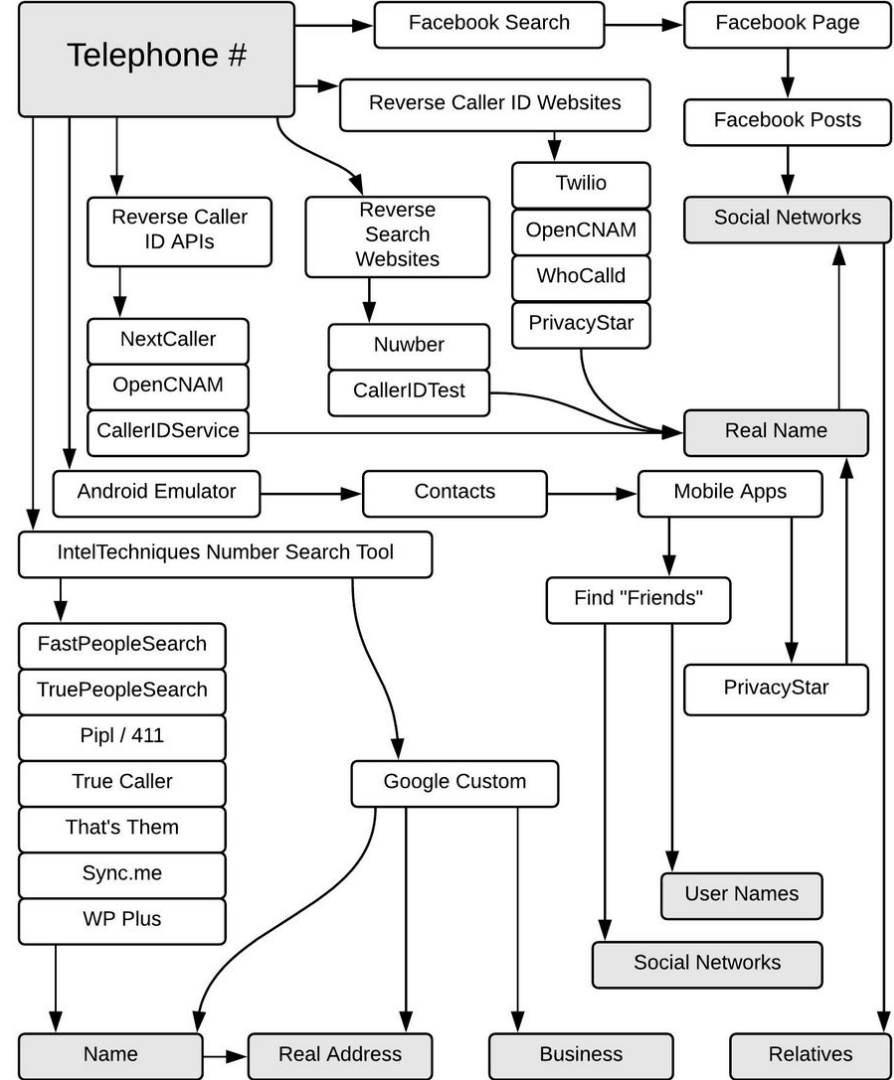
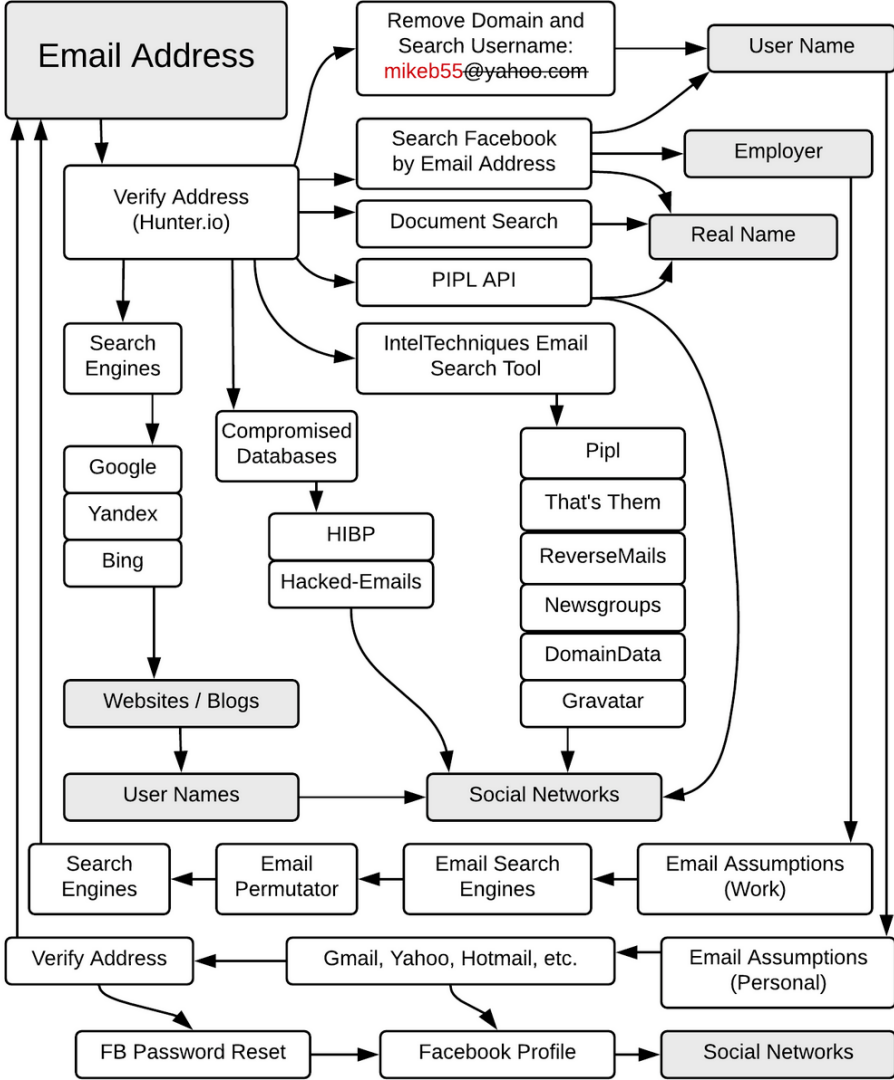
Graph

MindMap



Шаблоны поиска





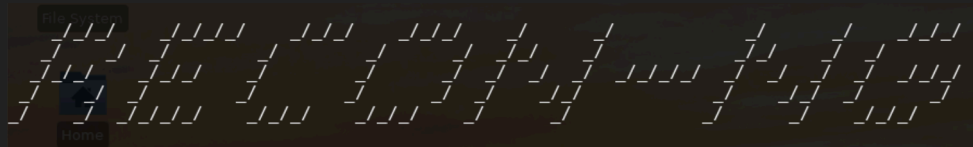
УТИЛИТЫ

OSINT Framework

 **MALTEGO**

lampyre 

DataSploit 



 **Palantir**

Больше как заметка.

Было задание, условное задание найти информацию о случайном человеке, зная его ник допустим.

И собрать информацию о компании.

Собственно, искать инфу я люблю, но на тот момент что-то лень было, та как не было какой-то цели или особо

Спойлер

Pandora

<https://www.instagram.com/p/a22/1810/41/59e1c5a0ff69.png>

@the_eternal_insomnia Ник

Дополнительная информация, детект по фото, ситилу фото

<https://www.instagram.com/p/1810/10/8960fade6d38.png>

<https://www.instagram.com/p/1810/5d/7eb440cc90e1.png>

https://www.instagram.com/the_eternal_insomnia/

<https://www.instagram.com/p/1810/cc/b5c9168765f8.png>

Любит котиков

<https://www.instagram.com/p/1810/b0/37abf3a2c47f.png>

<https://www.instagram.com/p/1810/64/5ca4921694d0.png>



Гитхаб

Сайт, написание ников, увлечение итд.

<https://github.com/1810/de/f39a14757baa.png>

<https://github.com/1810/e6/4544ef63d988.png>

Гитхаб

Почта: pandora.lewandowski@gmail.ru

<https://github.com/1810/b9/c251e2faf30a.png>

У неё много почт

ВК, твит и гитхаб зареган не на pandora.lewandowski@gmail.ru

<https://github.com/1810/61/184f3ebacad4.png>

Зато на Гите сработало Так: pandora.lewandowski@gmail.COM

<https://github.com/1810/32/521b27cd55c1.png>

<https://github.com/1810/f5/8004a4e3a78e.png>

8-***-***-**-62

<https://github.com/1810/1d/5c5da40562ea.png>

dar*****@yandex.ru

<https://github.com/1810/da/030f592c1bcd.png>

@TheEternalInsomnia

dar????????????????@yandex.ru

Making Everything Easier!

Competitive Intelligence FOR DUMMIES

A Wiley Brand

Learn to:

- Locate, collect, and analyze competitive intelligence
- Use competitive intelligence in your decision-making process
- Stop guessing and start making well-informed business decisions

Jim Underwood

Professor, bestselling author, and consultant to Fortune 500 companies

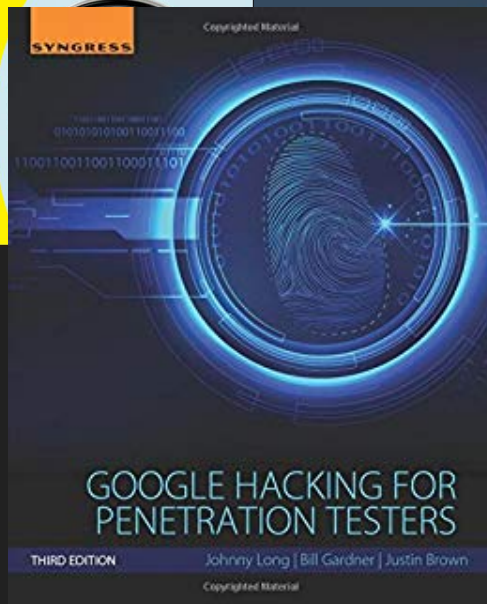
OPEN SOURCE INTELLIGENCE TECHNIQUES

RESOURCES FOR SEARCHING AND ANALYZING ONLINE INFORMATION

SIXTH EDITION



EL BAZZELL



"Most malware and client-side attacks have a social engineering component to deceive the user into letting the bad guys in. You can patch technical vulnerabilities as they evolve, but there is no patch for stupidity, or rather gullibility. Chris will show you how it's done by revealing the social engineering vectors used by today's intruders. His book will help you gain better insight on how to recognize these types of attacks." —Kevin Mitnick, Author, Speaker, and Consultant

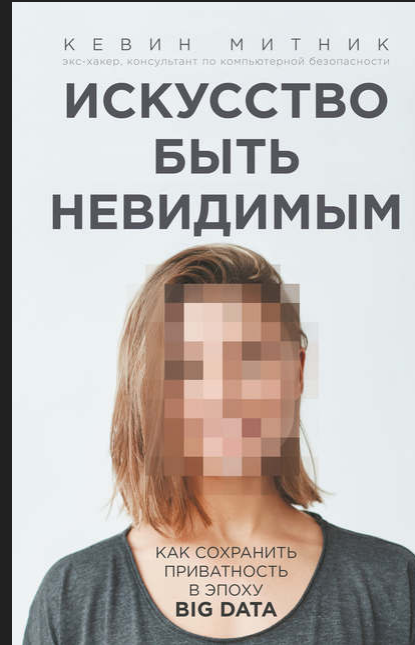
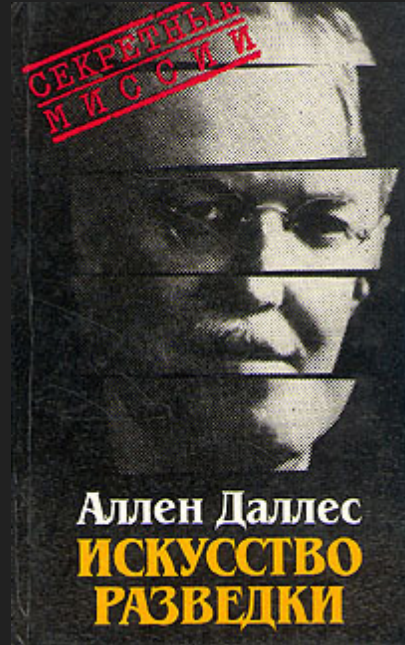
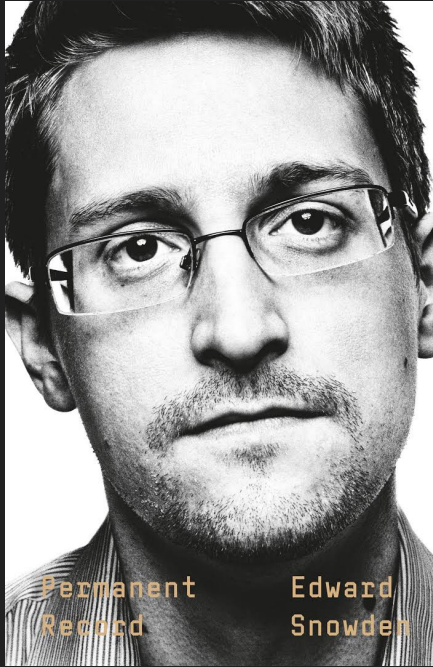
SOCIAL ENGINEERING

The Art of Human Hacking



CHRISTOPHER HADNAGY

FOREWORD BY PAUL WILSON



{18+}

Даниил
Туровский

Вторжение

Краткая
история
русских
хакеров

19.9.21

Вопросы?



Спасибо за внимание!



Pandora Lewandowski

SFTO

@the_eternal_insomnia