

Ломаем на корпоративном уровне

Стекольников Илья

КОЛЁСА | КРЫША | МАРКЕТ

Часто бывает:



Часто бывает:

Защита только сетевого периметра

Часто бывает:

Защита только сетевого периметра

И ТАК
СОЙДЕТ!



Часто бывает:

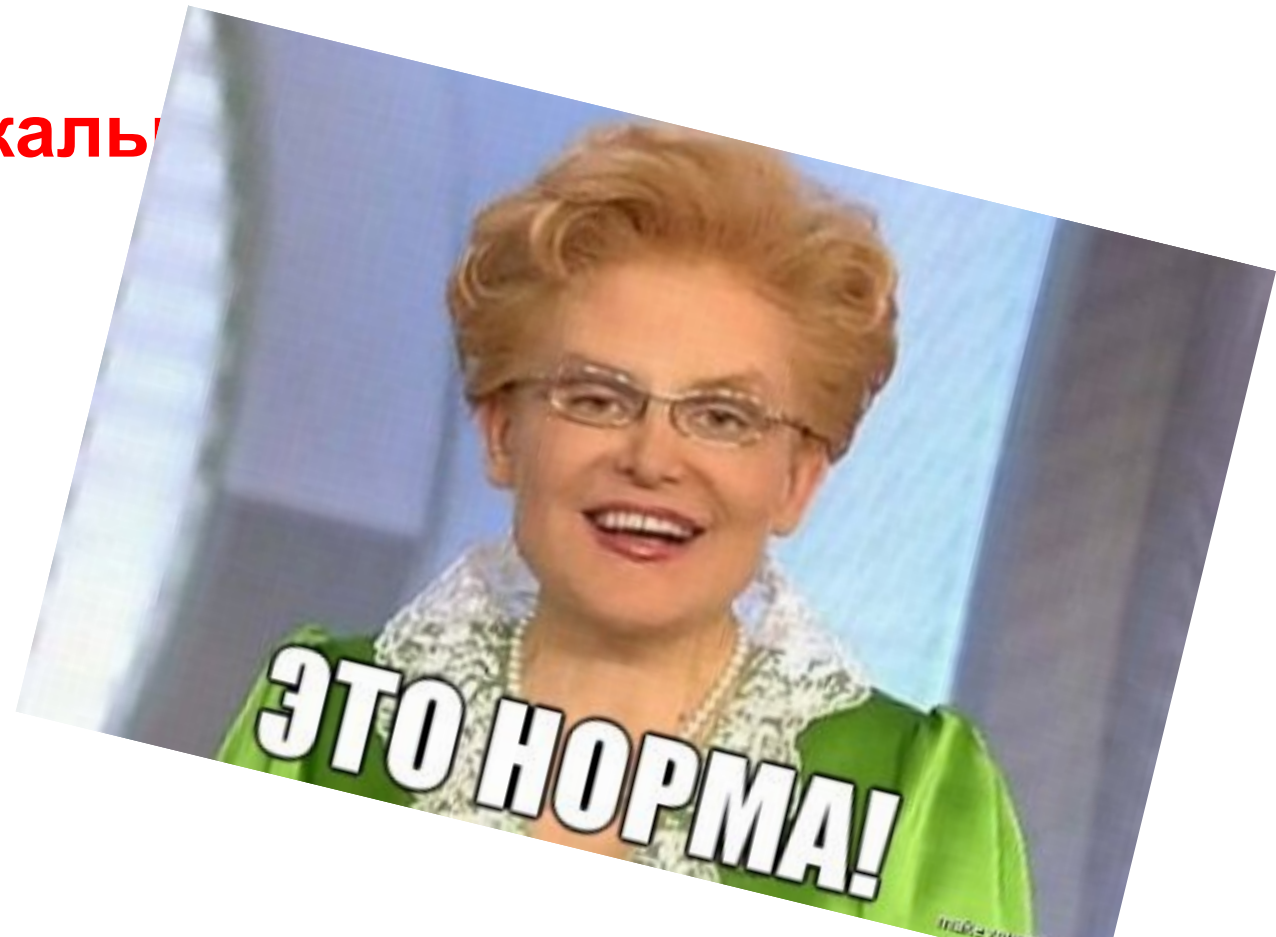
Защита только сетевого периметра

Личные устройства и локальные админы

Часто бывает:

Защита только сетевого периметра

Личные устройства и локаль



Част

За

Ли

Я ДАЖЕ НЕ ЗНАЮ

НОРМА ЭТО ИЛИ НЕТ...

risovach.ru

НОРМА!

Часто бывает:

Защита только сетевого периметра

Личные устройства и локальные админы

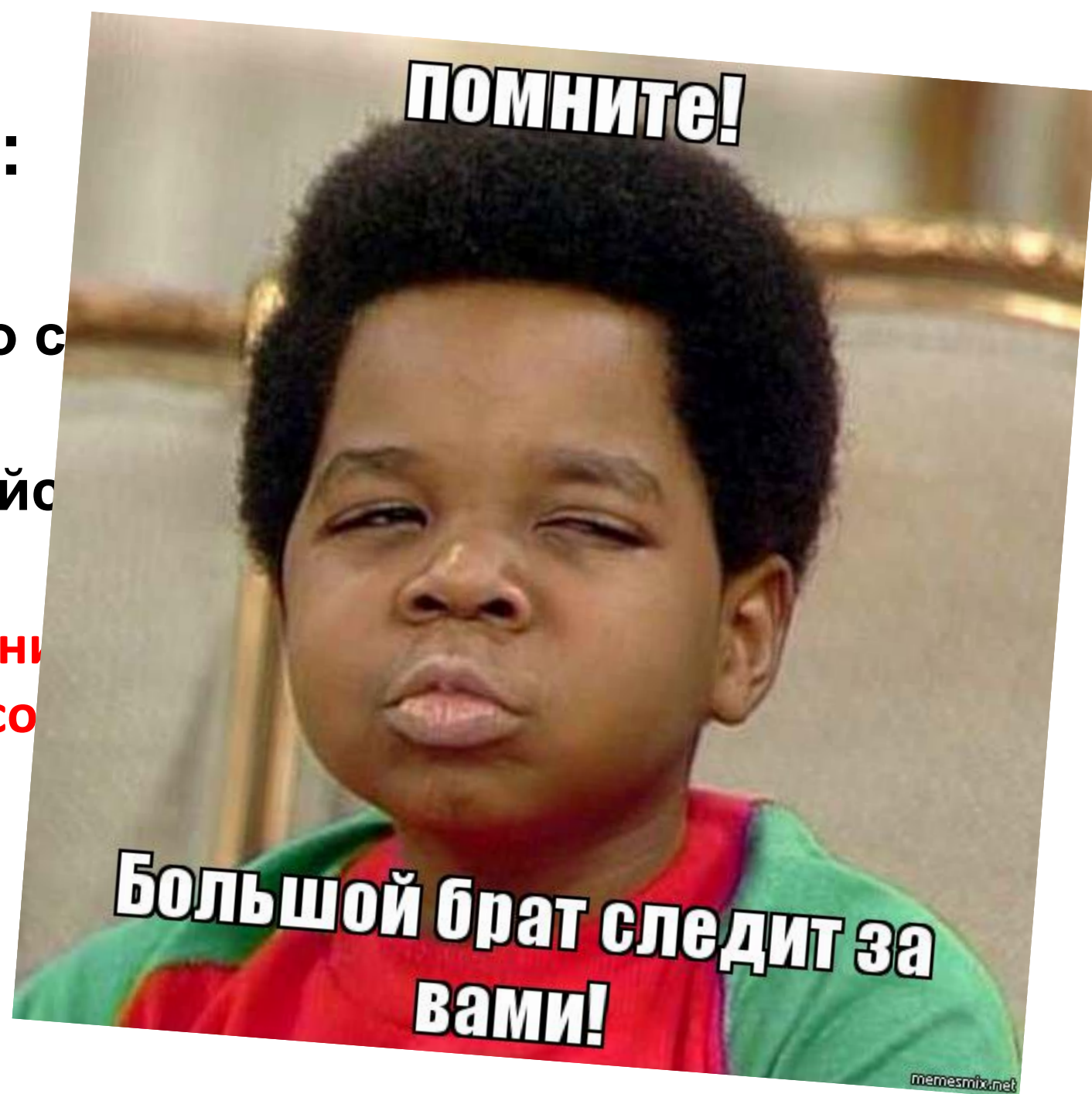
**Открытые источники информации
и сотрудники в социальных сетях**

Часто бывает:

Защита только с

Личные устройс

Открытые источни
и сотрудники в со



Часто бывает:

Защита только сетевого периметра

Личные устройства и локальные админы

**Открытые источники информации
и сотрудники в социальных сетях**

Человеческий фактор

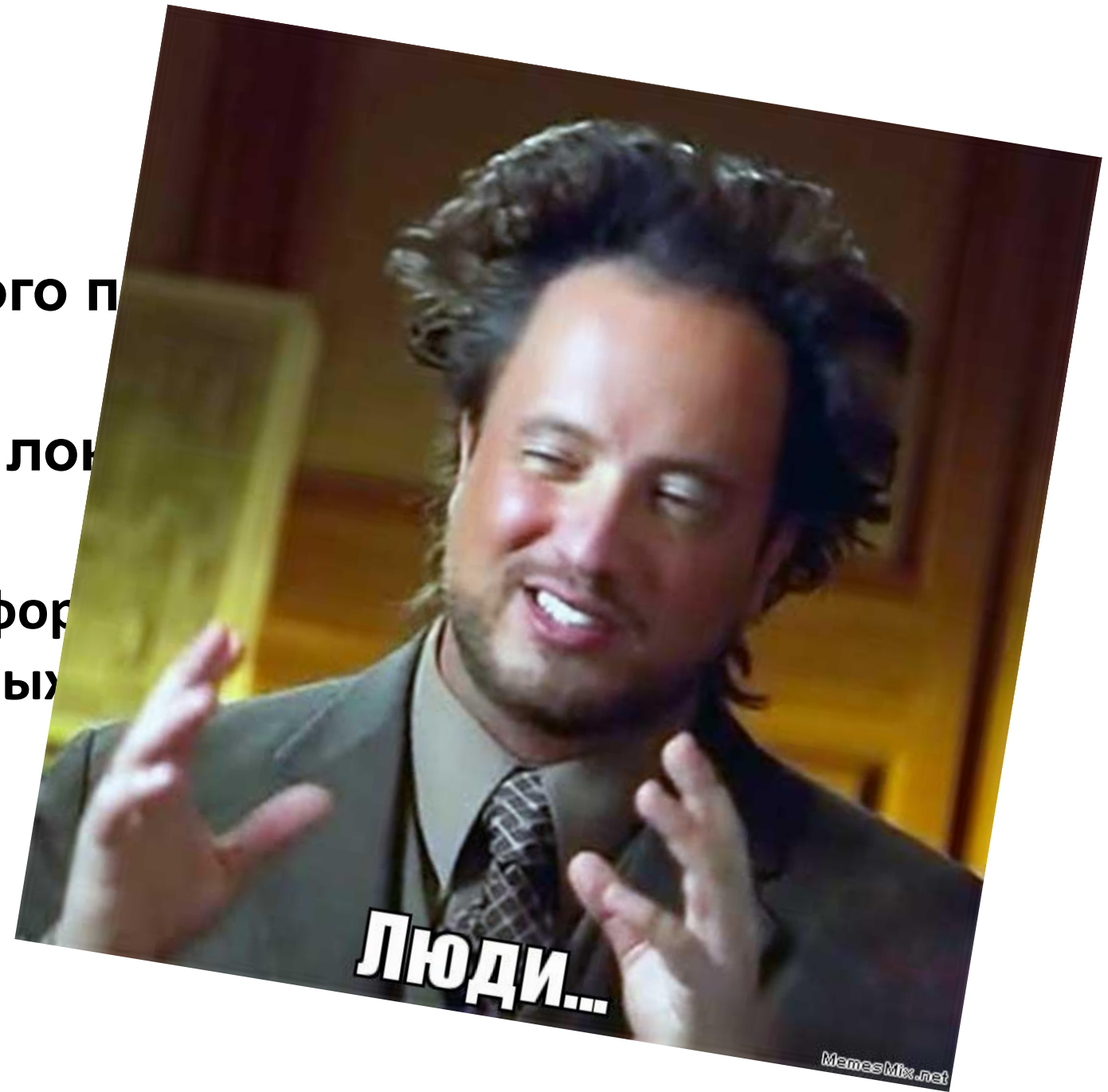
Часто бывает:

Защита только сетевого п

Личные устройства и лок

**Открытые источники инфор
и сотрудники в социальных**

Человеческий фактор



Часто бывает:

Защита только

Личные устройства

**Открытые источники
и сотрудники в соц**

Человеческий факт



**Я чё то
нажала
и всё исчезло**

Операция «Таргетированный фишинг»



Операция «Таргетированный фишинг»

Сбор информации - OSINT



× bash

```
macbook-pro:theHarvester ilya$ python theHarvester.py -d kolesa.kz -b google -l 100
```

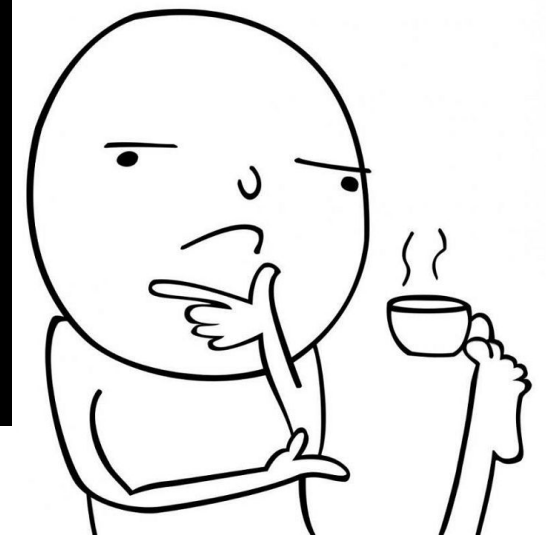
```

*****
*
*
* | | | | _ _ _ ^ ^ _ _ _ _ _ | | _ _ _
* | _ | ' _ \ / _ \ / / / _ ' | ' _ \ \ / / _ \ _ | _ \ / ' _ |
* | | | | | | _ / _ / ( | | | \ \ / _ ^ \ | | _ / |
* \ _ | | | \ _ | \ / \ , _ | | \ \ _ | | ^ \ _ | |
*
* TheHarvester Ver. 2.7.1
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

```

```
[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...
```

```
[+] Emails found:
-----
shirkevich@kolesa.kz
```



```
python theHarvester.py -d kolesa.kz -b google -l 100
```



Найдет любого ВКонтakte!

Инновационный сервис поиска людей по фотографии

Найди одинаковых!

☒ Согласен с [пользовательским соглашением](#)

или скачайте приложения

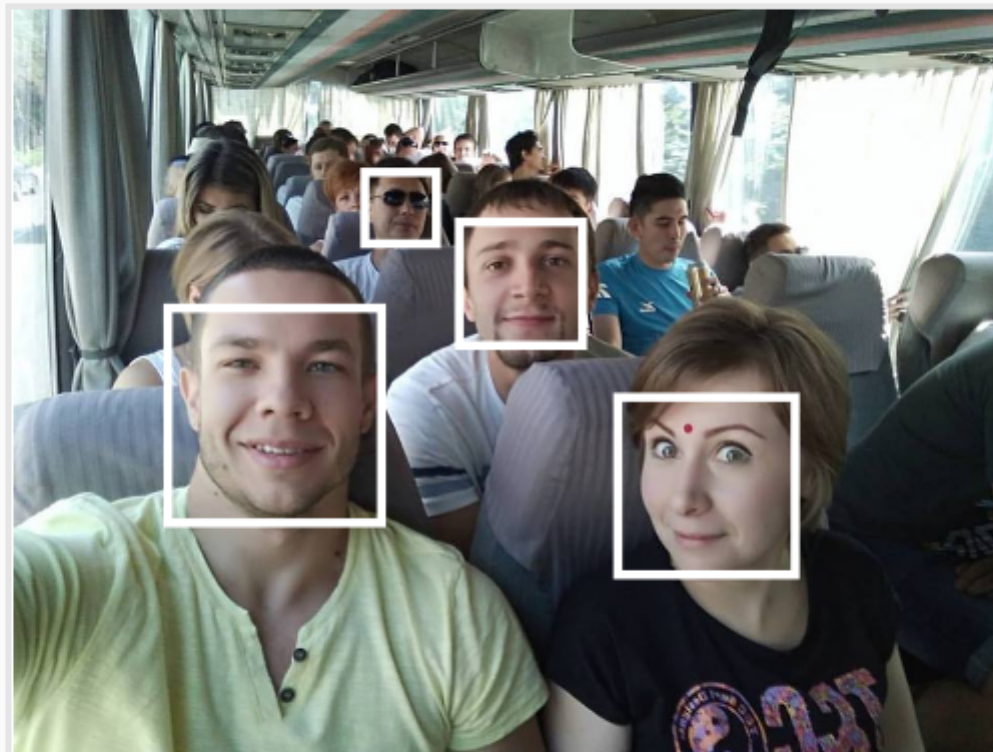


Посмотреть тур по сервису

```
[+] Emails found:  
-----  
shirkevich@kolesa.kz
```



Выберите лицо для поиска



[Загрузить](#) другую фотографию

Максимальный объем фотографии 5 МБ

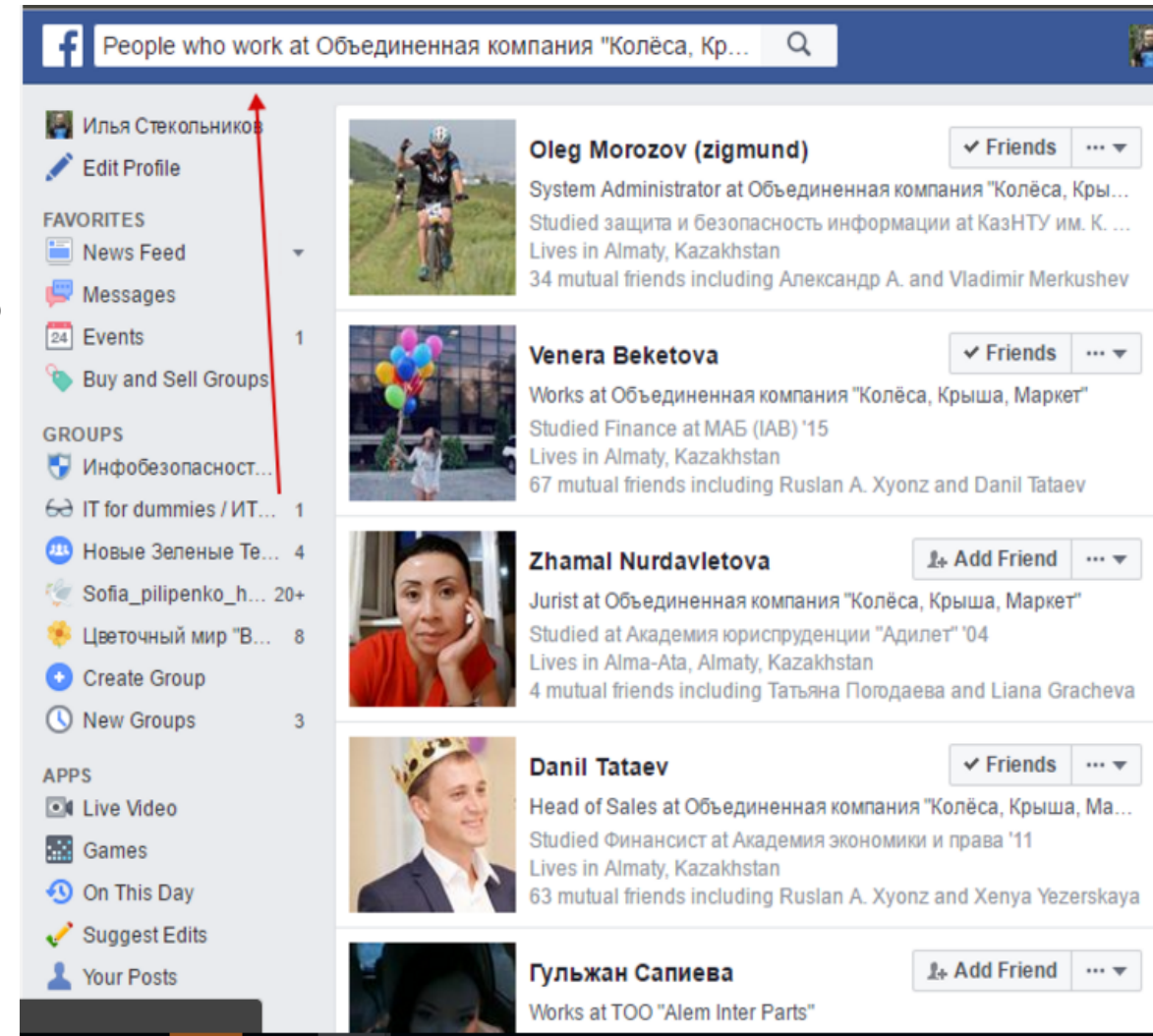
Файлы с расширением JPG, PNG

How does Graph Search work?



Facebook **Graph Search** :

1. People who work at %EMPLOYER%
2. Comments by %USERNAME% from Almaty
3. Posts liked by %USERNAME% at 2017
4. Posts liked by People who work at %EMPLOYER%
5. People who are younger than 50 and older than 40 and work at %EMPLOYER%
6. ...
7. ...
8. ...



Telegram Bot **GeoPhoto**:

<https://t.me/GeoPhotoBot>



Операция «Таргетированный фишинг»

Сбор информации - OSINT

Анализ и подготовка сценария



Показано 3 социальные сети

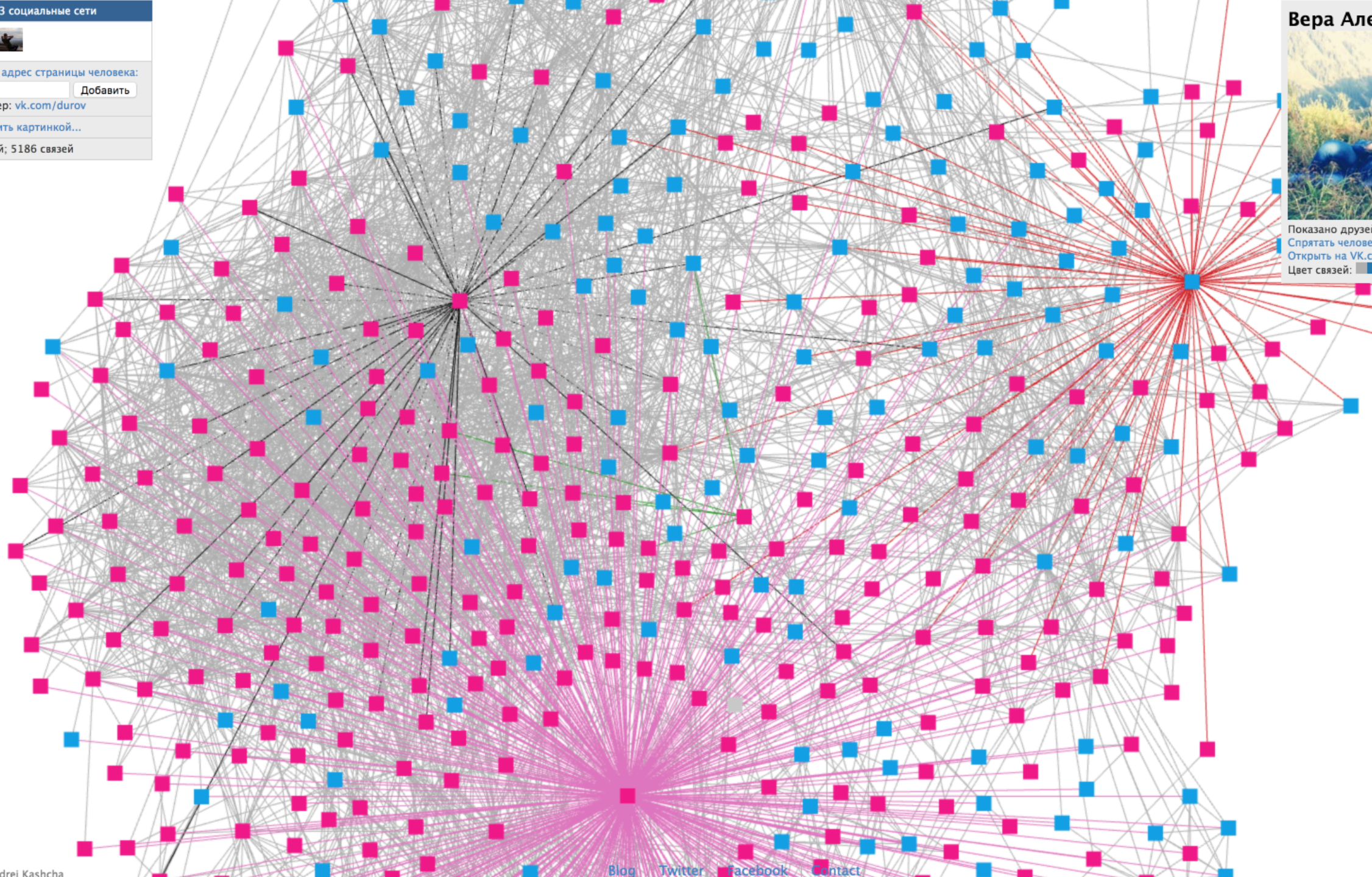


– Введите адрес страницы человека:

Например: [vk.com/durov](#)

[Сохранить картинкой...](#)

710 людей; 5186 связей



Вера Але



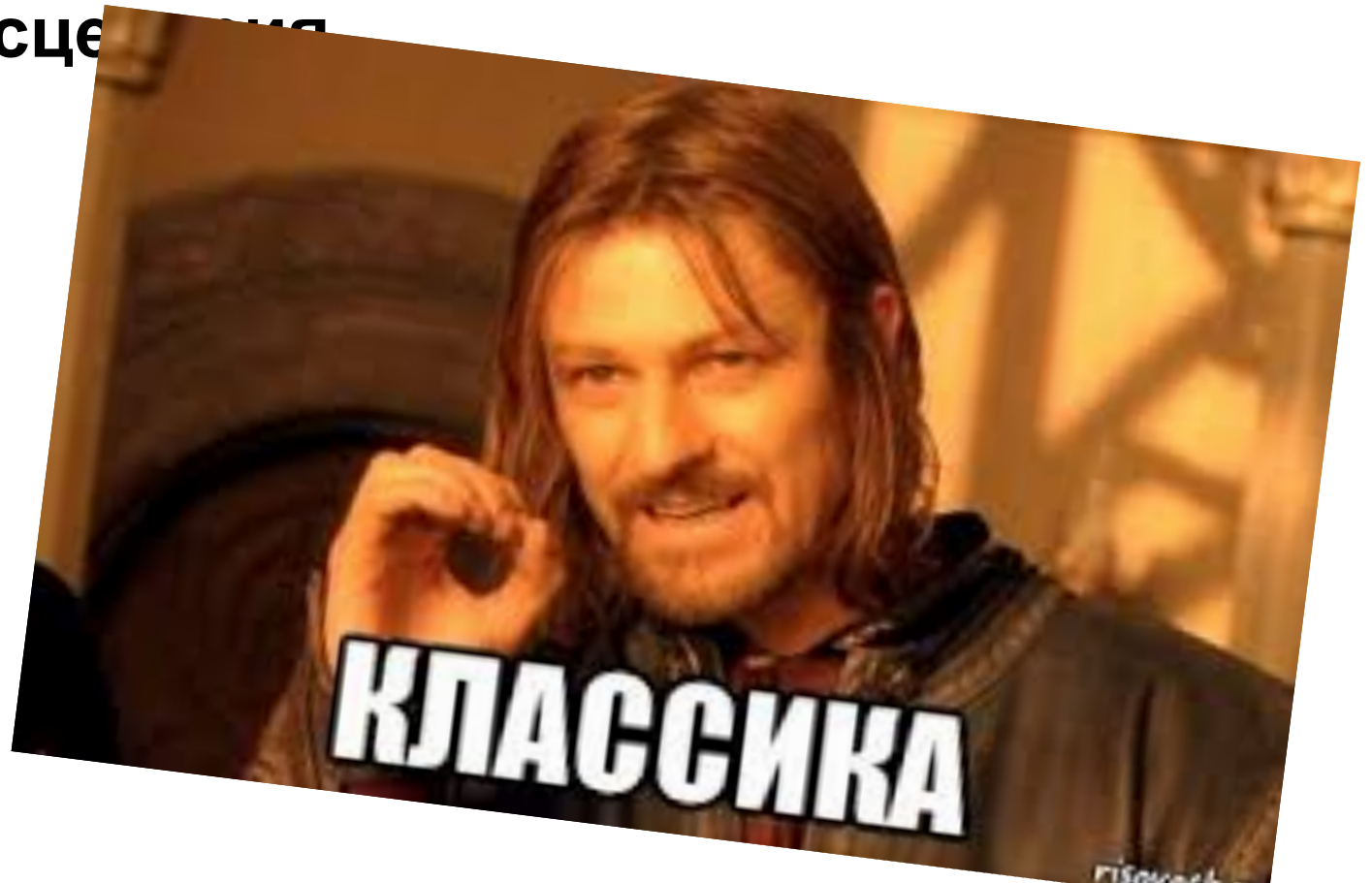
Показано друзей
Спрятать человека
Открыть на VK.com
Цвет связей: ☐ ☐ ☐

Операция «Таргетированный фишинг»

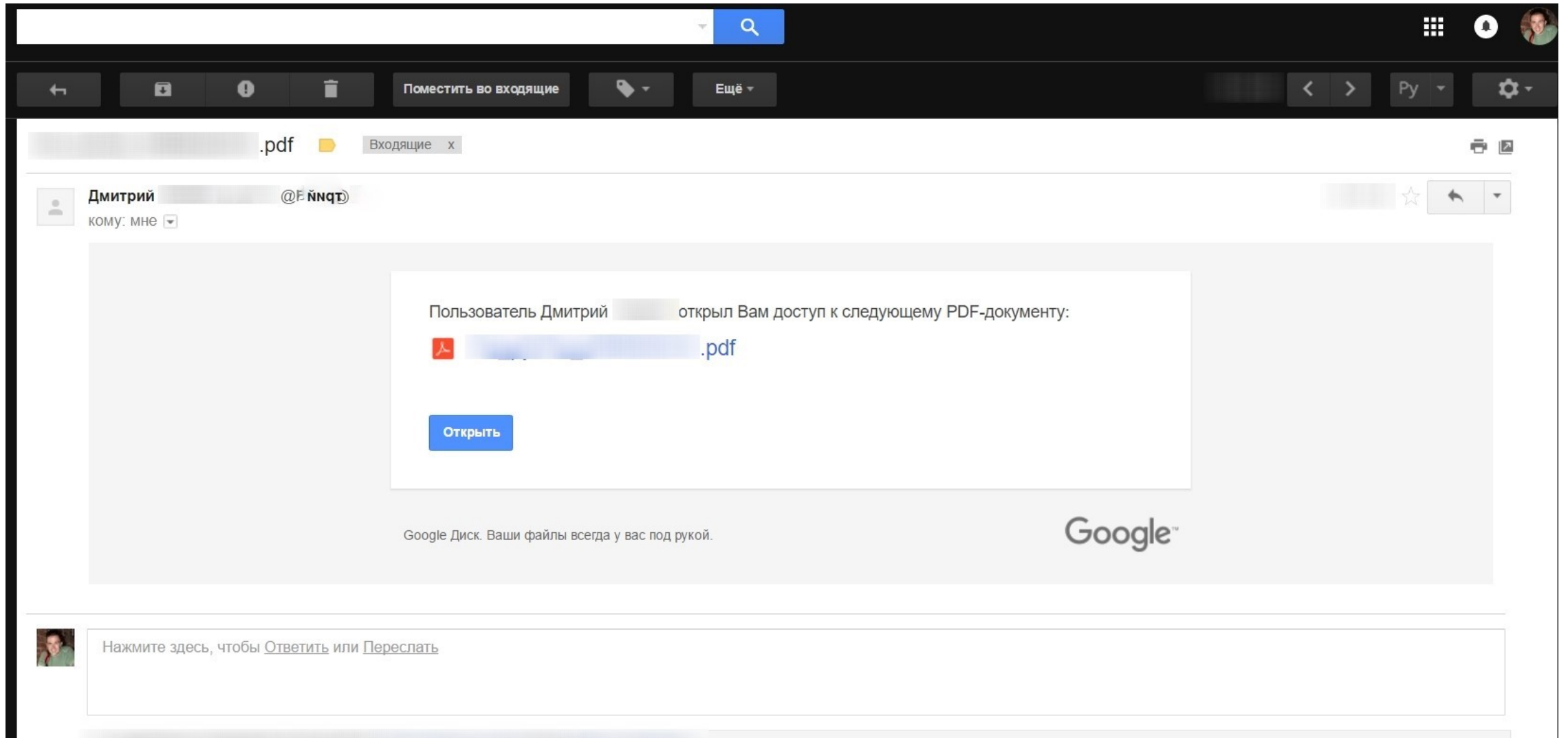
Сбор информации - OSINT

Анализ и подготовка сценария

Реализация



Как было сделано. Пример письма



Как было сделано.



Один аккаунт. Весь мир Google!

Войдите, используя аккаунт Google



stekolnikov@kolesa.kz

Войти

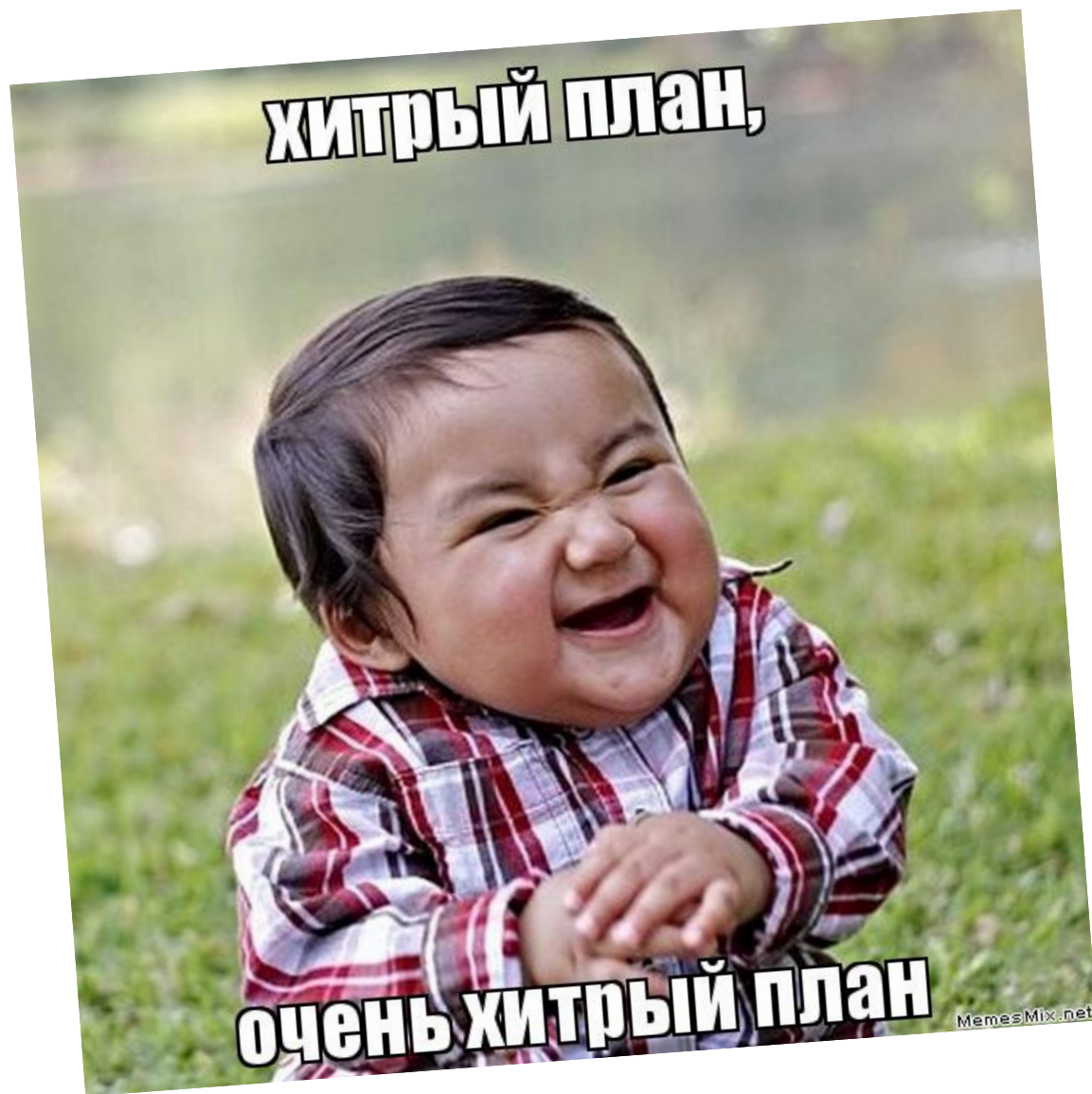
[Нужна помощь?](#)

[Войти в другой аккаунт](#)

Один аккаунт для всех сервисов Google

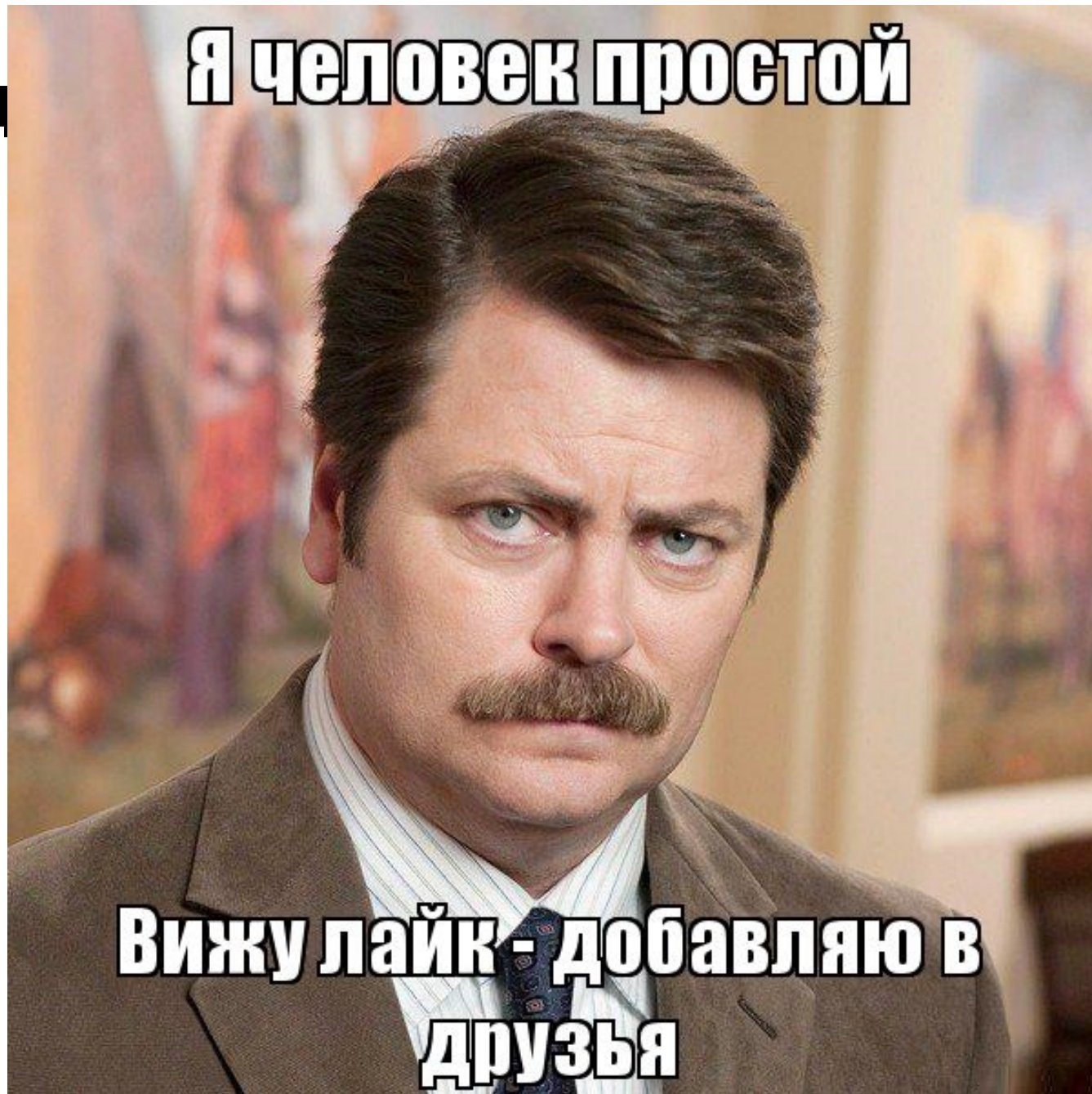


Операция «Фейковый сотрудник»



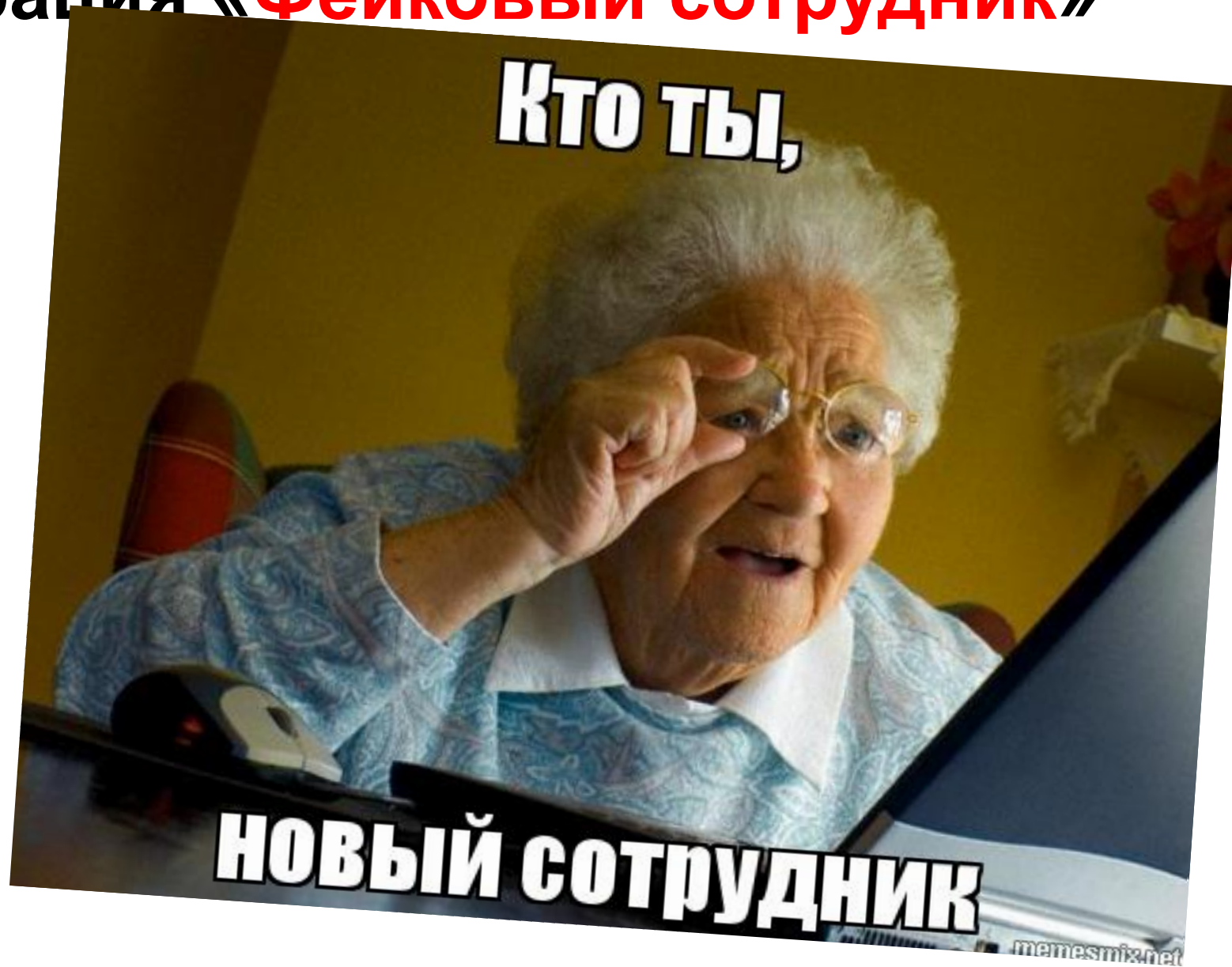
Операц

Я человек простой



**Вижу лайк - добавляю в
друзья**

Операция «**Фейковый сотрудник**»



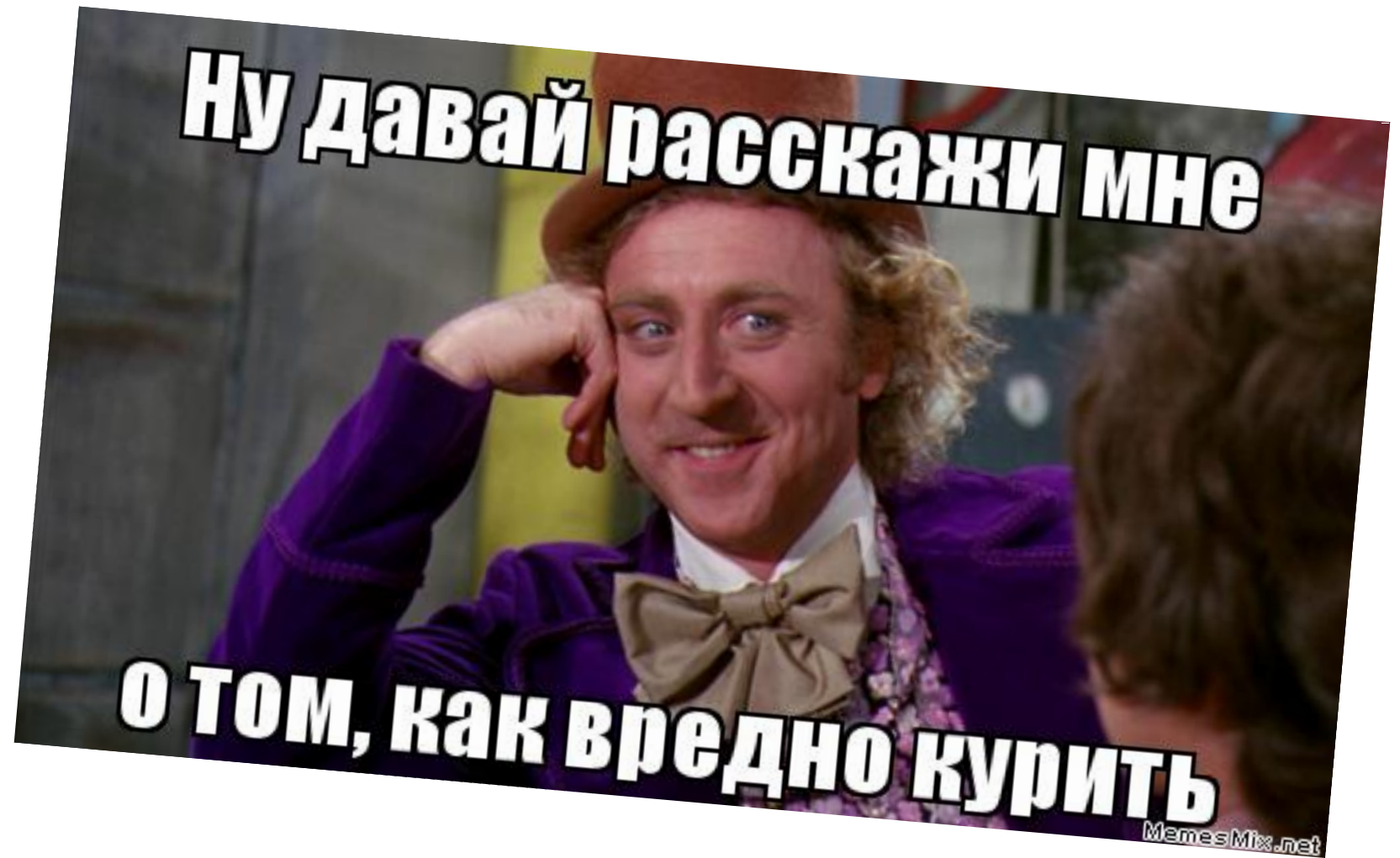
Опер

ДА КАК ТАК-ТО

НЕ МОЖЕТ ТАКОГО БЫТЬ!

risovech.ru

Операция «**Курилка**» или «У нас чужие не ходят»



Операция «Курилка»

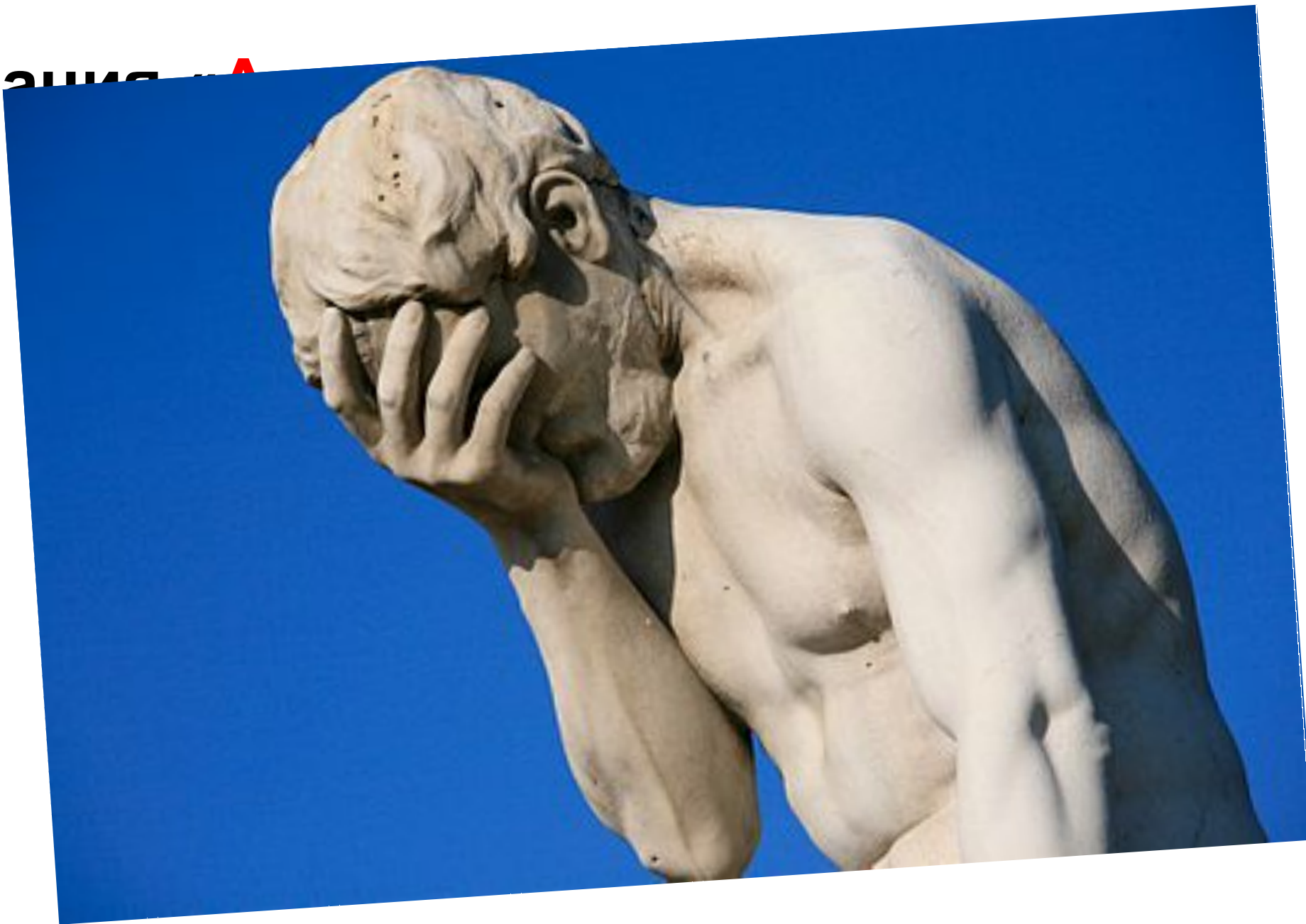


memesmix.net

MemesMix.net

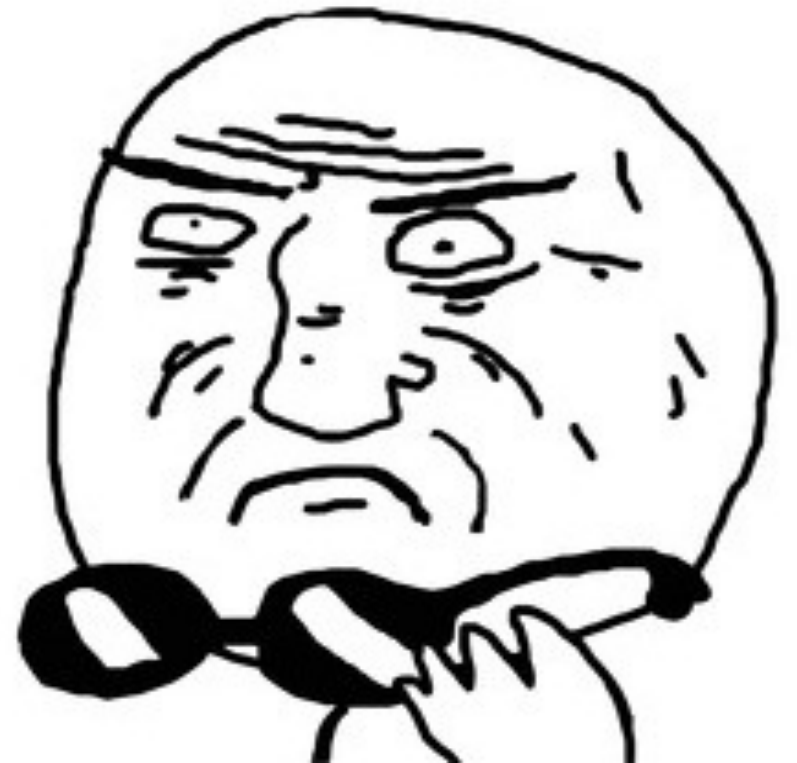
Операция «Аутсорсинг»

Операция ▲



Итого:

- ~ 50% сотрудников ввели учетные данные
- ~ 70% паролей подходили к внутренним системам
- ~ 2-3 недели на реализацию

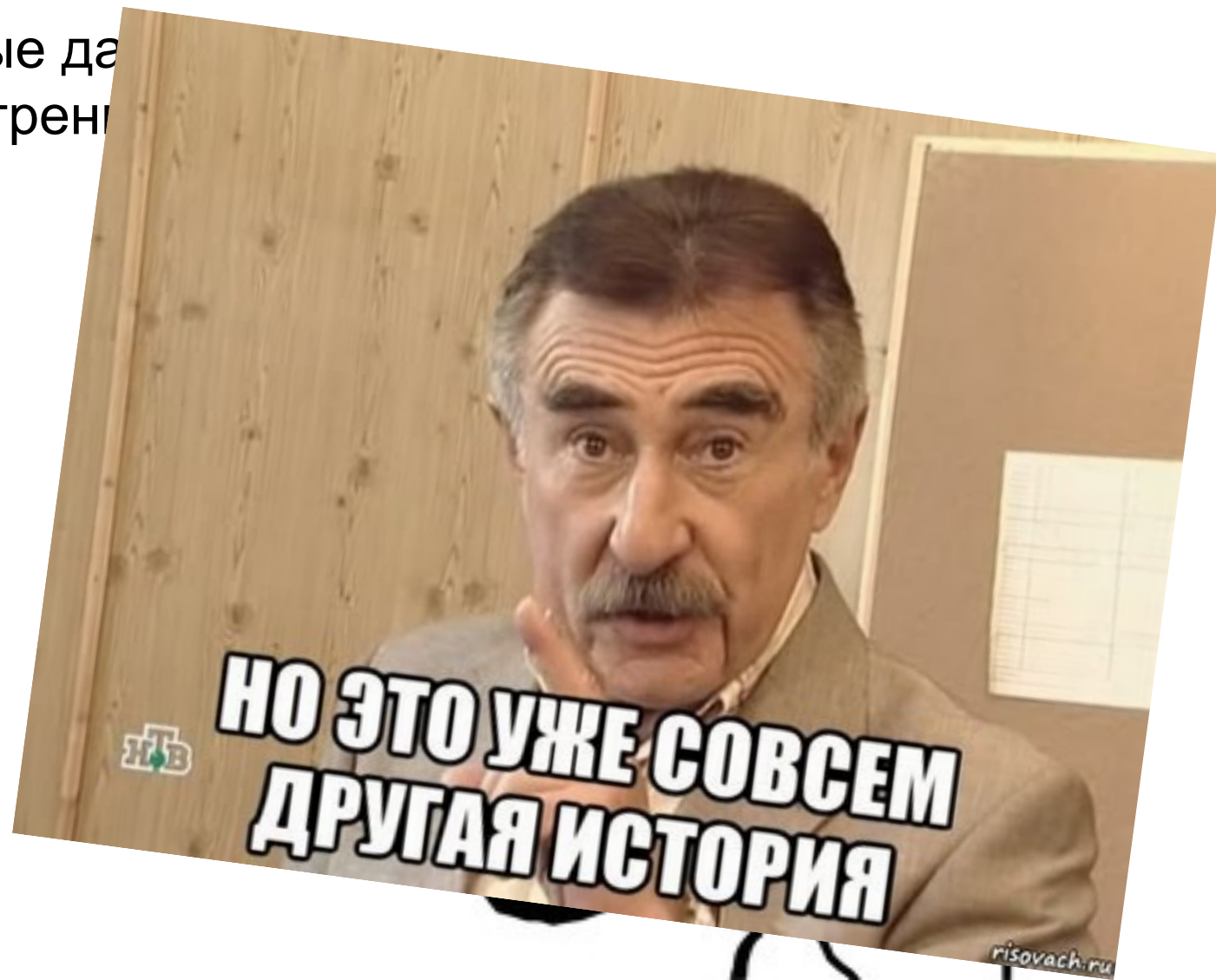


Итого:

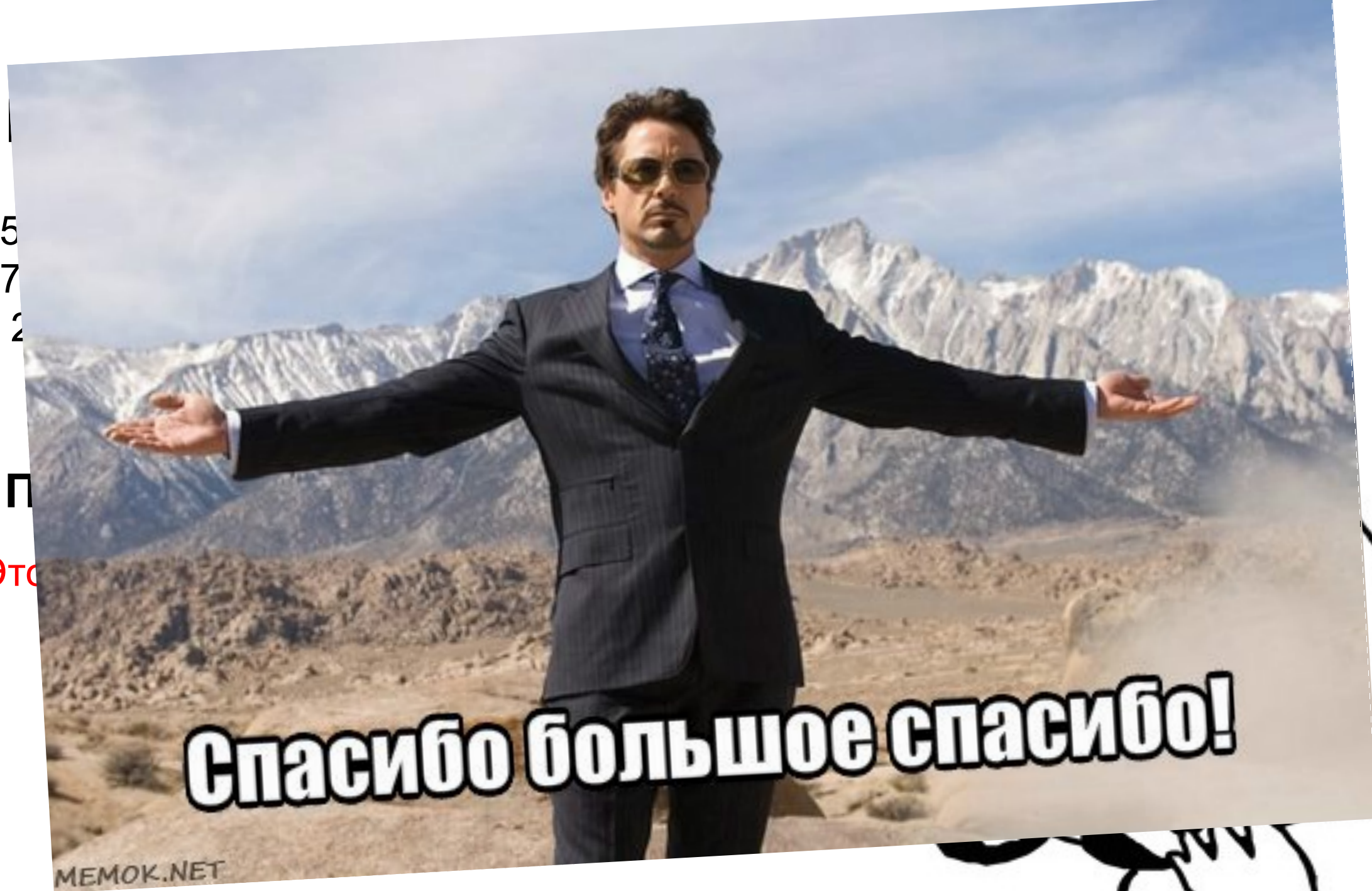
- ~ 50% сотрудников ввели учетные да
- ~ 70% паролей подходили к внутренн
- ~ 2-3 недели на реализацию

P.S.

- Это только вершина айсберга



- ~5
- ~7
- ~2



- Это