



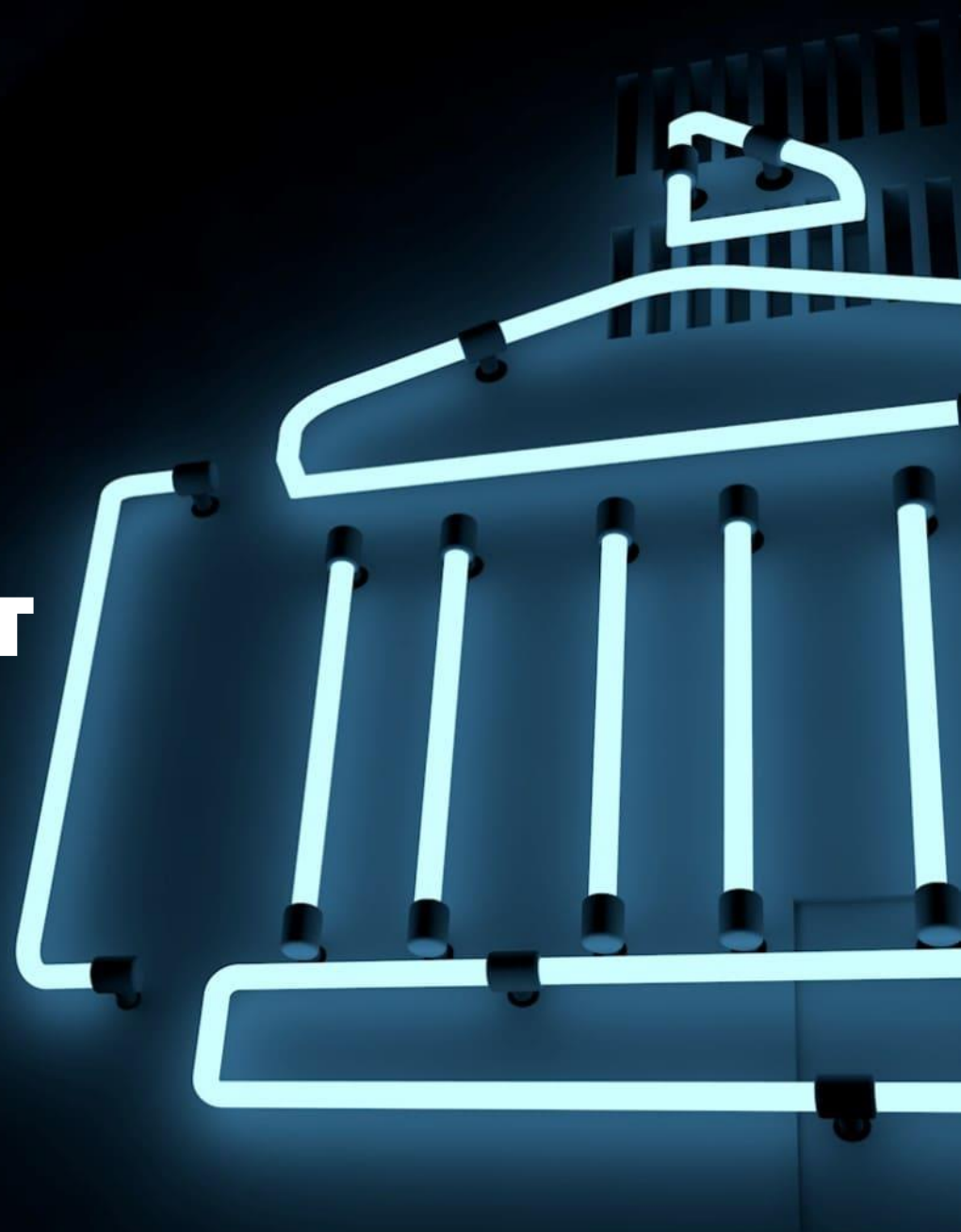
Физический пентест

Почему иногда все-таки стоит смотреть камеры



Корняков Захар

Специалист по тестированию на проникновение, Group-IB



Group-IB – это:



550+

сотрудников
в компании



18 лет

практического опыта



80%

технические
специалисты

Технологии Group-IB
признаны ведущими
аналитическими
агентствами



60+

стран, где мы
работаем



29 лет

средний возраст
сотрудников



1200+

высокотехнологичных
расследований по всему
миру



Официальные партнеры



Европол



Интерпол

Рекомендованный партнер



OSCE



SWIFT

Наши клиенты



Райффайзен
Банк



Сбербанк



АльфаСтрахование



Мегафон



HeadHunter

Дисклеймер

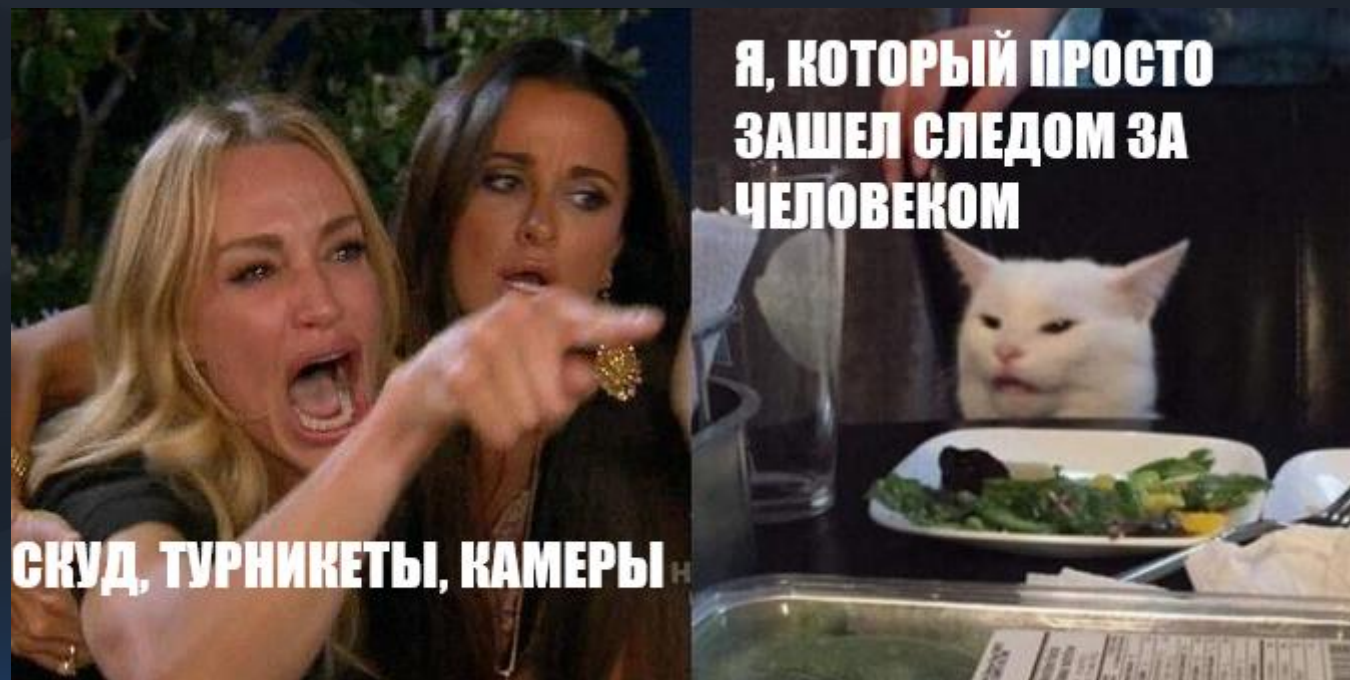
Все найденные совпадения случайны, материалы предоставлены или из личного архива, или из открытых источников и используются лишь для наглядности доклада.

Автор не несет ответственности за последствия от использования материалов из данного доклада. Автор не призывает и не рекомендует производить какие-либо работы по физическому тестированию на проникновение без юридического договора с тестируемой стороной и другие противозаконные действия.

Помните, что в нынешний век цифровых технологий, ваши действия и присутствие не останется без внимания.

О чем будем сегодня говорить

Рассмотрим основные техники, используемые при физическом пентесте для проникновения на территорию объекта, а также из нашей практики расскажем, что работает, а что нет



Основные этапы

В целом можно выделить четыре основных этапа:

- Определение цели
- Разведка
- Подготовка
- Исполнение



Определение цели

Получение цели

Целью физического пентеста может быть:

- Физическое проникновение на объект Заказчика
- Получение доступа во внутреннюю сеть, находясь на территории объекта
- Получение доступа в определенное помещение
- Получение определенного уровня доступа на объекте
- ...

|GROUP|IB|

Разведка

Разведка

- Онлайн
- Оффлайн (on-site)
- Дополнительная онлайн разведка

Онлайн разведка производится до оффлайн разведки в Интернете путем использования Open Source Intelligence – OSINT.

Оффлайн разведка производится непосредственно на объекте.

Дополнительная онлайн разведка производится после разведки на объекте.

Разведка

Онлайн разведка может включать в себя (OSINT):

- Снимки со спутника и панорамы
- Поэтажный план здания
- Разведка по сотрудникам
- Просмотр соцсетей сотрудников/компании
- Просмотр блога компании

Разведка

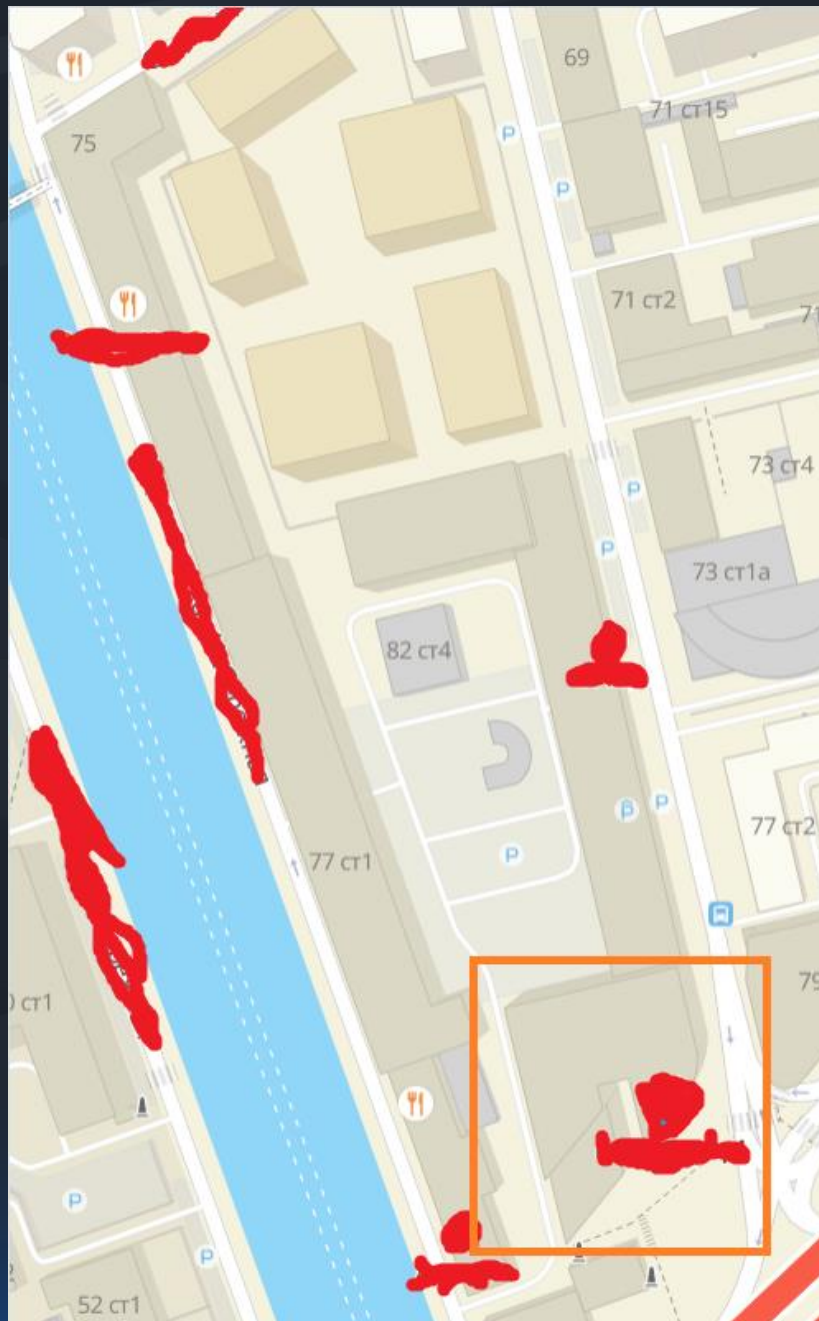
Снимки со спутника

Yandex, Google



Разведка

|GROUP|IB|



Разведка

|GROUP|IB|

Панорамы, фото (Yandex, 2gis)



Разведка

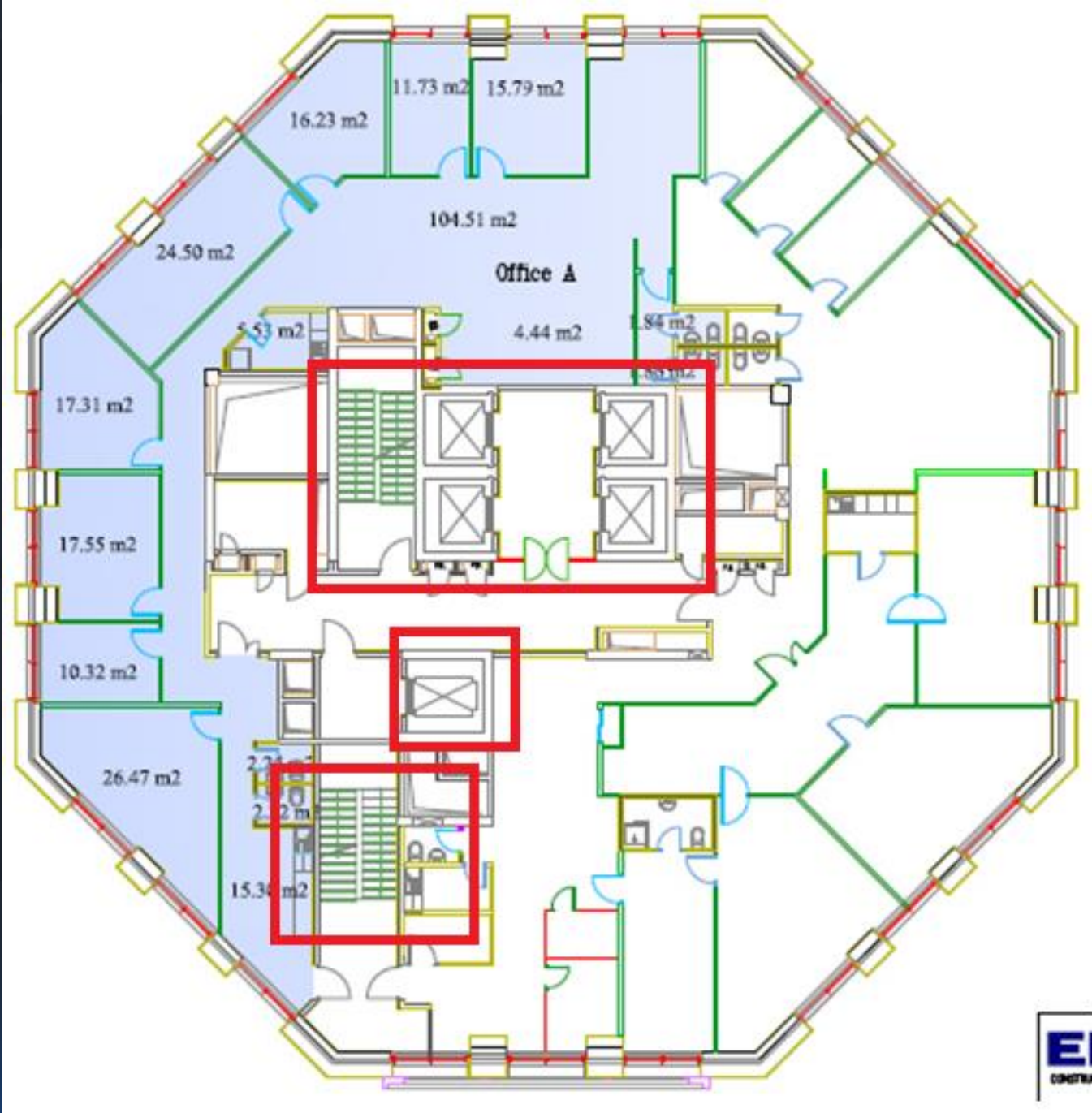
|GROUP|IB|

Панорамы



Разведка

Поэтажный план здания



Разведка

Поэтажный план здания

Google

поэтажный план плаза

Показать все

<https://www.premier-plaza.ru/plans>

Поэтажные планы - Бизнес центр Премьер Плаза. Аренда ...

Поэтажные планы. Главная · О проекте · Свободные площади · Коммерческие условия · Характеристики · Расположение · Фотогалерея · Оставить заявку · Контакты.

<https://omega-plaza-bc.ru/plans>

Москва, улица Ленинская слобода 19. Планы этажей.

ОМЕГА ПЛАЗА - 115280, РФ, Москва, Ленинская Слобода, д.19. Официальный сайт бизнес центра на Автозаводской. **Поэтажные планы.** 1й-5й этаж.

<http://навелецкая-плаза.рф/poetazhnye-plany>

Поэтажные планы - ПАВЕЛЕЦКАЯ ПЛАЗА. Аренда и ...

Поэтажные планы. Планы типовых этажей. Copyright © 2011-2020 All rights reserved. Телефон принадлежит консультанту по сдаче площадей в аренду.

 **Картинки по запросу поэтажный план плаза**

 лотос плаза  омега плаза  development plaza  лахта плаза



Отзыв

Показать все

<http://dpbc.ru/plans>

Поэтажные планы Дежнев Плаза бизнес-центр в Москве

Поэтажные планы г. Москва Бизнес-центр Дежнев Плаза.

<http://rinco-plaza.ru/poetazhnye-plany>

Поэтажные планы - RINCO PLAZA / РИНКО ПЛАЗА. Аренда ...

Поэтажные планы. План 1 этажа. План 2 этажа. План 3 этажа. План 4 этажа. План 5 этажа. План 6 этажа. Copyright © 2011-2020 All rights reserved.



позтажный план плаза



мегафон лотос плаза лотос плаза 2 очередь
ярмарка лотос плаза какие магазины есть в лотос плаза
плаза карта лотос плаза еда

<https://omega-plaza-bc.ru> › plans ▾

Москва, улица Ленинская слобода 19. Планы этажей.

ОМЕГА ПЛАЗА - 115280, РФ, Москва, Ленинская Слобода, д.19. Официальный сайт бизнес центра на Автозаводской. **Позтажные планы.** 1й-5й этаж.

Похожие запросы



мегафон лотос плаза лотос плаза 2 очередь
ярмарка лотос плаза какие магазины есть в лотос плаза
плаза карта лотос плаза еда

<http://dpbc.ru> › plans ▾

Позтажные планы Дежнев Плаза бизнес-центр в Москве

Позтажные планы г. Москва Бизнес-центр Дежнев Плаза.

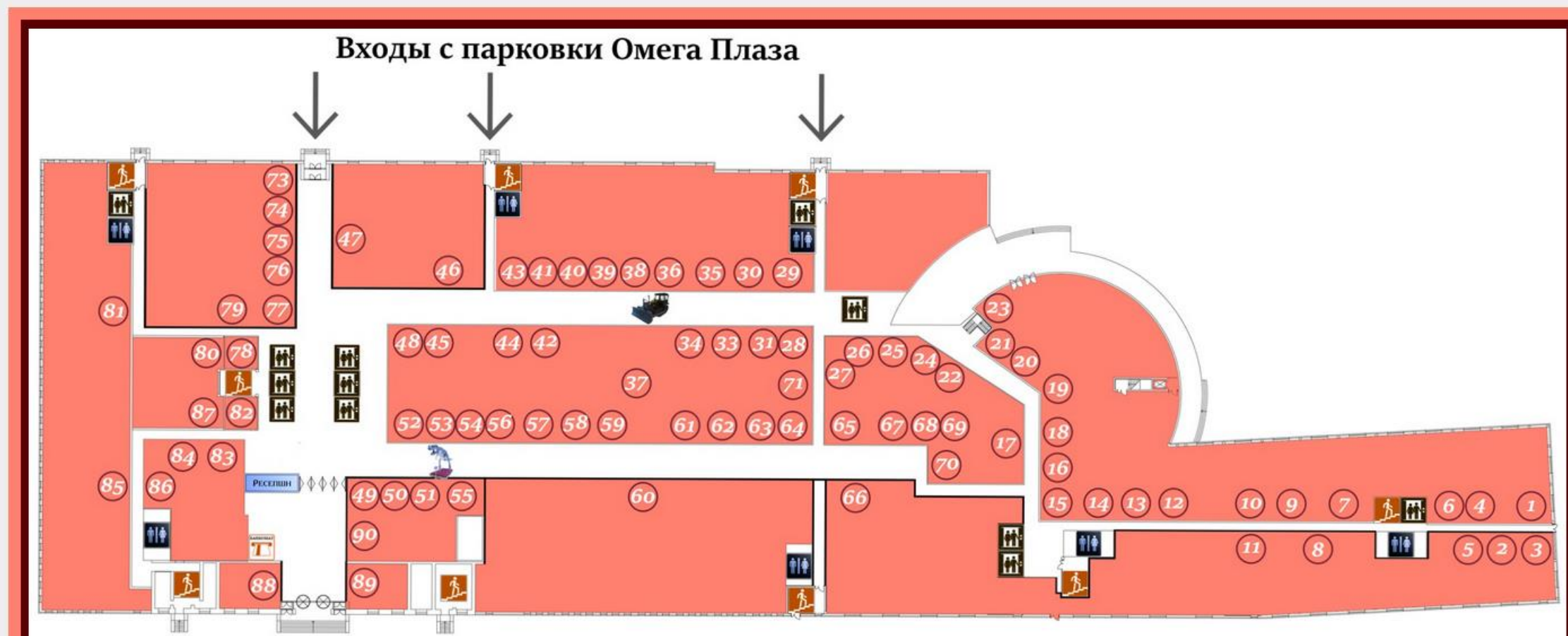
<http://навелецкая-плаза.рф> › poetazhnye-planu ▾

Позтажные планы - ПАВЕЛЕЦКАЯ ПЛАЗА. Аренда и ...

Позтажные планы. Планы типовых этажей. Copyright © 2011-2020 All rights reserved.

Телефон принадлежит консультанту по сдаче площадей в аренду.

План 1-го этажа бизнес-центра "ОМЕГА ПЛАЗА"



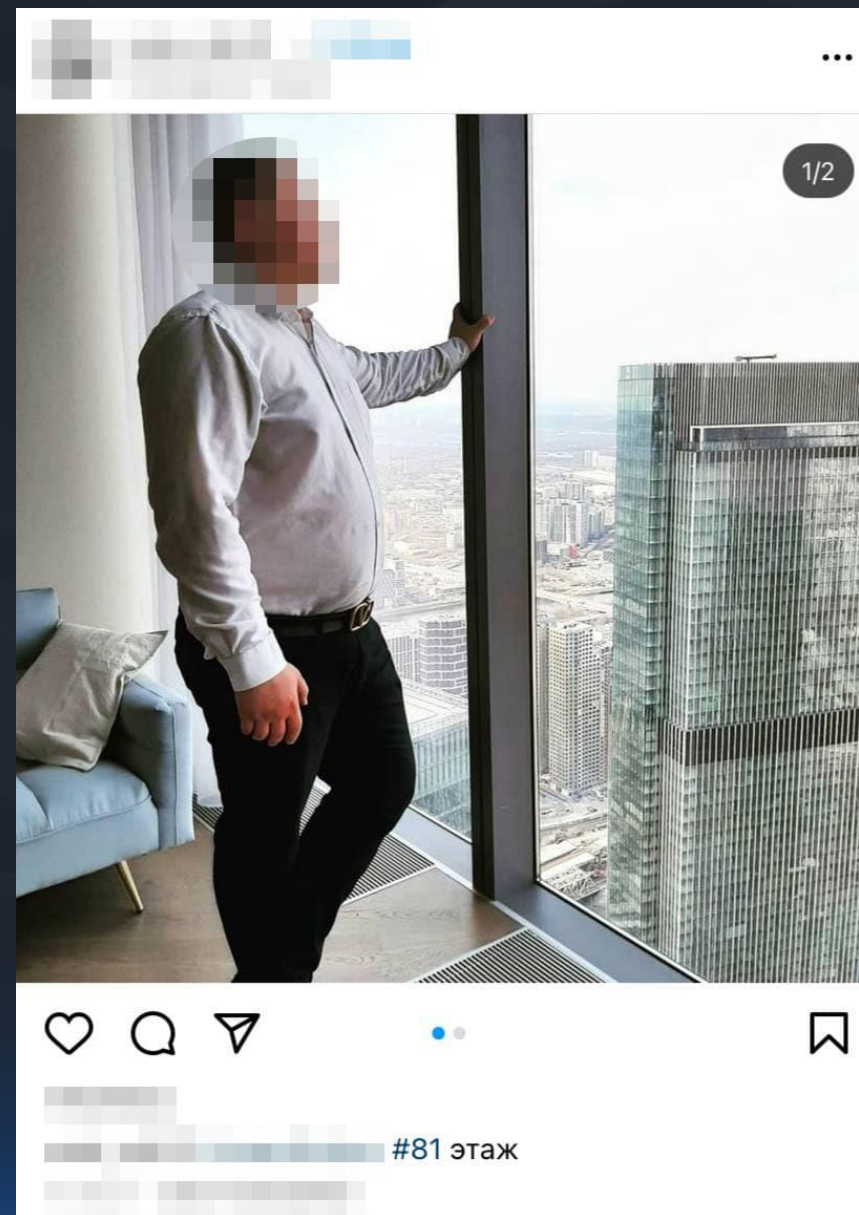
Разведка

Просмотр соцсетей сотрудников/компании

Интерьер/Экстерьер

Пропуска

Униформа



Разведка



Просмотр блога компании

habr.com/ru/company/gazpromneft/blog/450922/

Все потоки Разработка Администрирование Дизайн Менеджмент Маркетинг Научпоп

🔍 👤

командной работы, прозрачности и свободы коммуникации между сотрудниками.

Многим знакомы стандартные системы пропуска в офис, когда необходимо приложить идентификационную карту к считывающему устройству. Сотрудникам этого офиса попасть на рабочее место легче. На входе в офис можно не использовать пропуск благодаря системе EnterFace 3D, которая распознает лица за считанные секунды.



ИНФОРМАЦИЯ

Дата основания	1995
Местоположение	Россия
Сайт	www.gpnbonus.ru
Численность	Неизвестно
Дата регистрации	25 января 2019

БЛОГ НА ХАБРЕ

4 декабря 2020 в 11:11

Про клиентский опыт и оторванность от реальности

👁 3.5К 💬 8 +8

20 сентября 2020 в 09:38

Кайф трекерства в экспансии. Интервью с трекером Дмитрием Безнаскоком

👁 1.9К 💬 2 +2

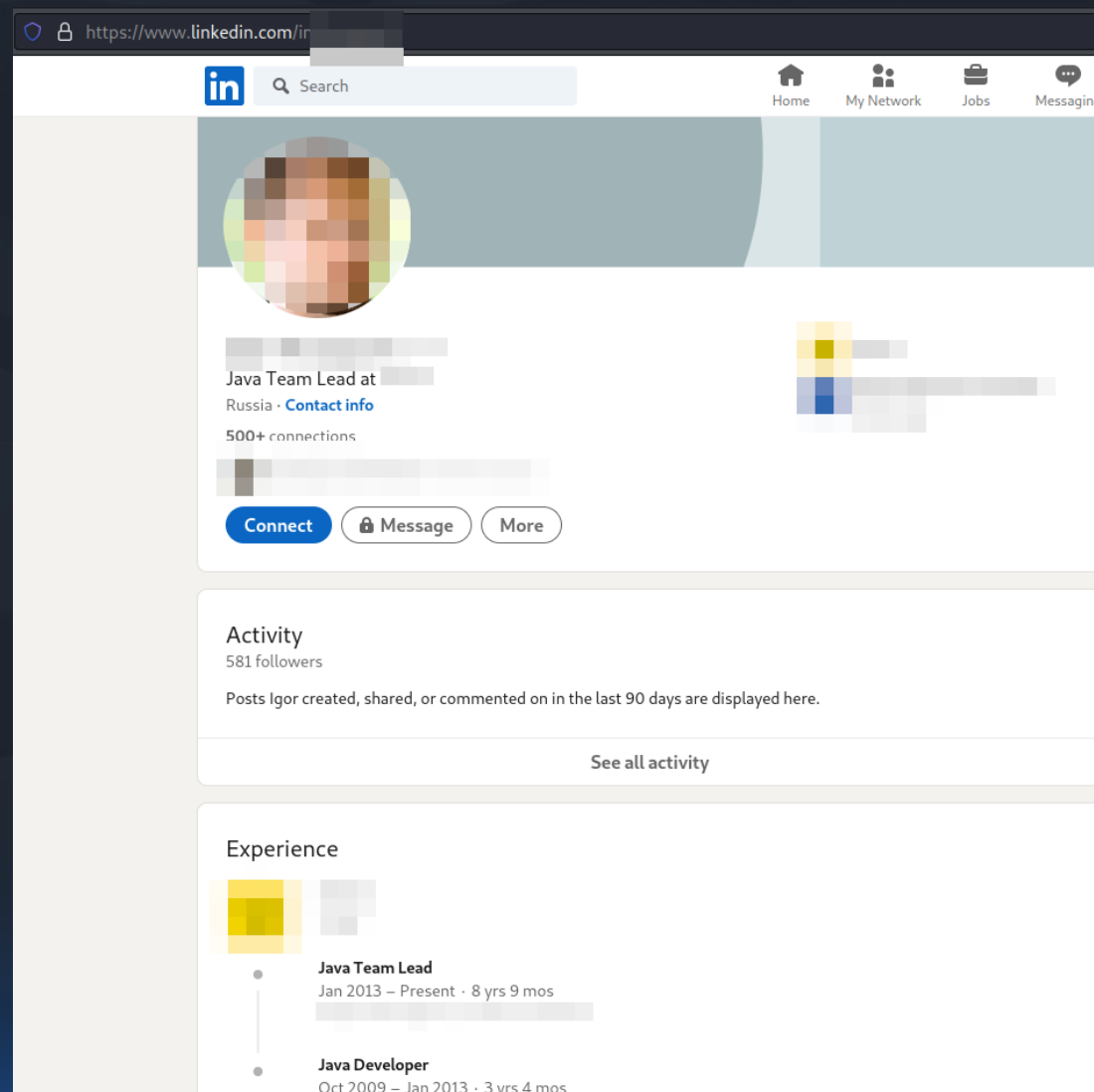
5 августа 2020 в 09:17

Корпоративный архитектор: похож на

Разведка

|GROUP|IB|

Разведка по сотрудникам



The screenshot shows a LinkedIn profile page for a user whose name and profile picture are blurred. The browser address bar at the top shows the URL `https://www.linkedin.com/in/`. The navigation bar includes the LinkedIn logo, a search bar, and links for Home, My Network, Jobs, and Messaging. The profile header displays the user's title, location, and connection count. Below this are buttons for Connect, Message, and More. The Activity section shows the number of followers and a link to view all activity. The Experience section lists two roles: Java Team Lead and Java Developer, each with a duration.

https://www.linkedin.com/in/

in Search Home My Network Jobs Messaging



Java Team Lead at 
Russia · [Contact info](#)
500+ connections

[Connect](#) [Message](#) [More](#)

Activity
581 followers
Posts Igor created, shared, or commented on in the last 90 days are displayed here.
[See all activity](#)

Experience

- 
Java Team Lead
Jan 2013 – Present · 8 yrs 9 mos
- 
Java Developer
Oct 2009 – Jan 2013 · 3 yrs 4 mos

Разведка

Оффлайн разведка может включать в себя:

Human Intelligence:

- Общение с сотрудниками
- Общение с обслуживающим персоналом
- Наблюдение за сотрудниками (униформа, пропуска и т.д.)
- Наблюдение за внутренними процессами

Imagery Intelligence:

- Получение планов этажей
- Разведка прилегающих территорий

Существующие Wi-Fi точки доступа (Signal Intelligence – SIGINT)

Разведка

|GROUP|IB|

Получение информации от сотрудников (также униформа + пропуск)



Разведка

Получение информации от обслуживающего персонала:

- Проблемы
- Отношение охраны
- Работа
- ...



Получение планов этажей



Разведка

|GROUP|IB|

Наблюдение за внутренними процессами



Разведка

|GROUP|IB|

Наблюдение за внутренними процессами



Разведка

|GROUP|IB|

Наблюдение за внутренними процессами



Разведка

|GROUP|IB|

Разведка прилегающих территорий



|GROUP|IB|

Подготовка

Дисклеймер

В данном разделе будут продемонстрированы некоторые инструменты, за использование которых автор не несет ответственности, и не призывает использовать их самостоятельно, без договора с тестируемой стороной. Также автор не рекомендует использовать их в случаях, выходящих за границы проведения работ по задачам работодателя, а также без договора с тестируемой стороной.

Подготовка

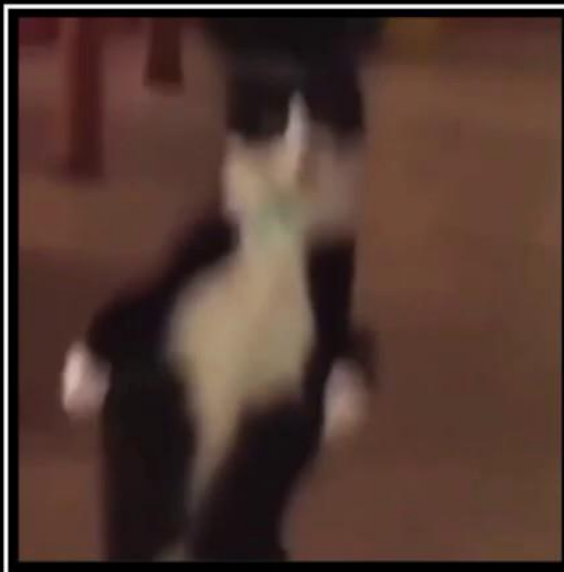
|GROUP|IB|

Формирование сценариев/векторов



Отход

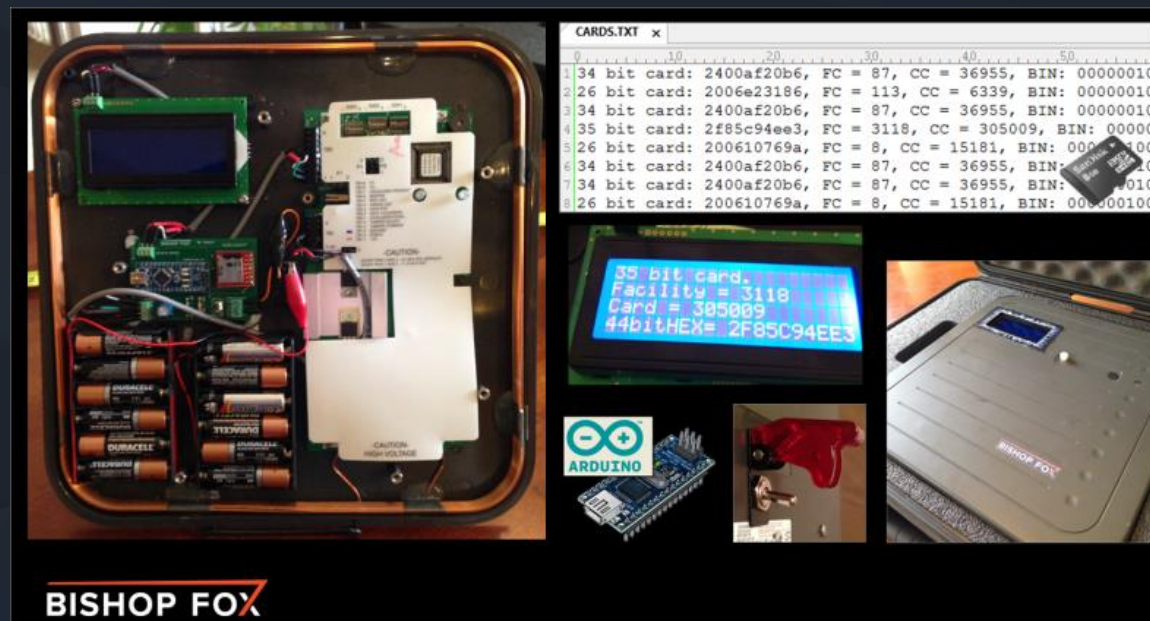
|GROUP|IB|



RUN
NOW!

Подготовка

Инструменты и/или реквизит



Инструменты

|GROUP|IB|





Инструменты

IGROUP LIB





Dewhurst 827 Key

Often used as: Lift Keys, Switch Keys and possibly more...

Suits Locks by the following manufacturers: Dewhurst and possibly more...

Quantity:

 Add to Basket

Ключи

|GROUP|IB|



=



Одежда и реквизит

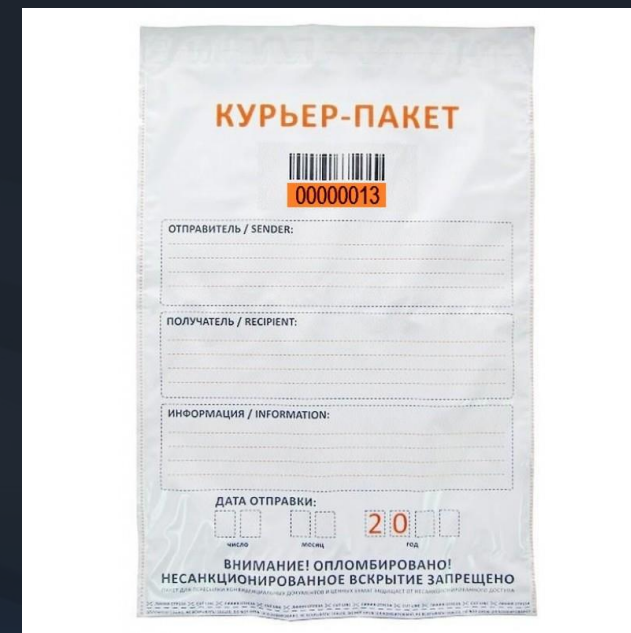
|GROUP|IB|

A big thank you to all our essential workers putting their lives on the line.



Одежда и реквизит

|GROUP|IB|



Пропуска

|GROUP|IB|



Исполнение

Исполнение

Тейлгейтинг (*Tailgating*) – преследование хвоста



Исполнение

|GROUP|IB|

Поддержка связи с командой



Исполнение

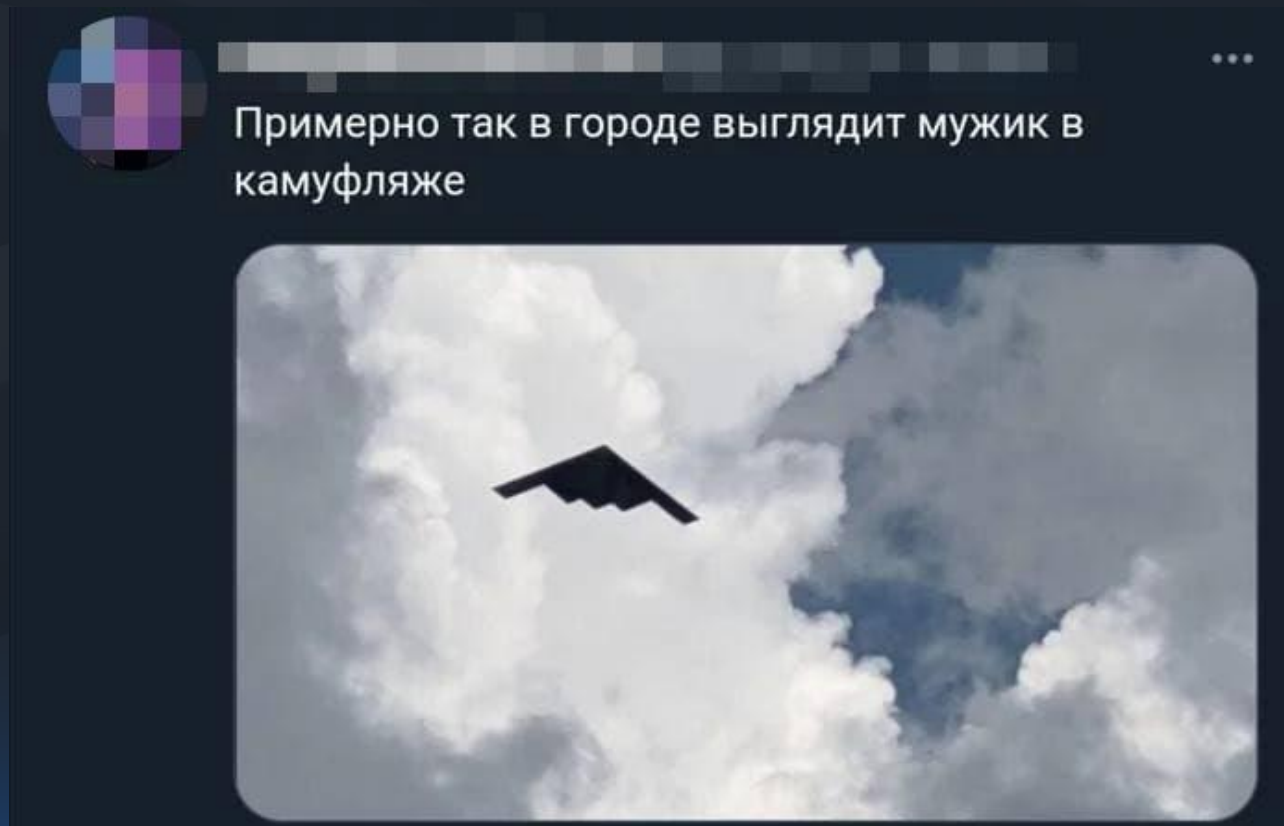
|GROUP|IB|

Детальное знание сценария (и прилегающей территории)



Исполнение

Необходимо учитывать детали сформированного вектора (легенда, время суток для исполнения, необходимое оборудование и т.д.)



Замечания



Замечания

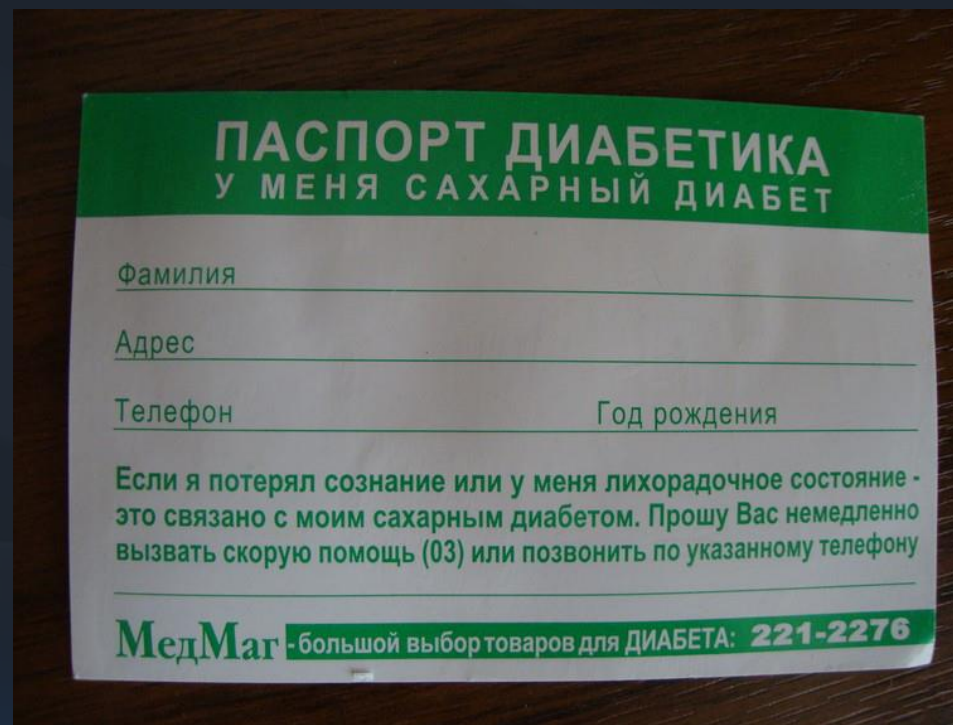
Продолжительное присутствие возле объекта во время разведки



|GROUP|IB|

Funfunffun





Q&A

СТАНЬ ЧАСТЬЮ КОМАНДЫ, КОТОРАЯ ЗАЩИЩАЕТ МИР





Предотвращаем и расследуем киберпреступления с 2003 года



Корняков Захар

Специалист по тестированию на проникновение, Group-IB

www.group-ib.ru

group-ib.ru/blog

info@group-ib.com

+7 495 984 33 64

twitter.com/groupib

facebook.com/groupib

t.me/group_ib

instagram.com/group_ib