# ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Д.Трелевич, Исполнительный директор и научный руководитель ООО «Ти-Жи-Пи-О консалт»



# Обо мне

- Учредитель ООО «Ти-Жи-Пи-О консалт» (основано в 2018 г., зарегистрировано в Москве)
- Работаю в сфере машинного обучения и ИИ с 1980-х
- Опыт в информационной безопасности с начала 1990-х
- Докторская степень по анализу сигналов
- Руководящие должности в IBM, Google, Microsoft, Mail.ru, Тех-Центре Дойче Банке, ТехЛаб S7 и др.

# Кибербезопасность – проблема не новая, но сейчас очень острая.

- В 2023 году[1] ожидается 15,5 млн кибератак.
- Рост числа киберпреступлений только за 2020 год оценивается в 3 трлн. USD.[2]
- В 2020 году конфиденциальные данные 1 300 пострадавших от Ransomeware были размещены в Интернете. В 2021 году замечено почти в 2 раза больше таких инцидентов: были похищены данные 2 435 пострадавших.[3]
- СМБ тоже подвергается таким атакам.
  - *43% кибератак нацелены на средний и малый бизнес.*
  - *При этом 61% игроков в секторе СМБ подвергались кибератаками в течение последних 12 месяцев.*[4]
- Одной из причин ускоренного роста киберпреступности является технологические тренды: к 2022 году к Интернету были подключен уже 1 трлн. устройств; многие из них – датчики «интернета вещей» (IoT)


[1]Данные компании "DDoS-Guard".
[2]Из инвестиционного отчета Росгосстрах Жизнь, 2022 г.
[3]Из отчета «Cyber Threats 2021: A Year in Retrospect», PWC, 2022 г.
[4]https://firewalltimes.com/small-business-cybersecurity-statistics/)

# Проблем с «традиционными» подходами к защите больше, чем эффективной защиты

**403 Access Denied**
You don't have permission to access "http://www.whateversite.com/" on this server.
Reference #18.1234567.1667374347.123456

- Блокировка по геолокации
  - *ВПН*
  - *Где ваши клиенты на самом деле?*
  - *Кто определяет политические границы?*
  - *Прокси (напр. Cloudflare)*
- Скорость отправления запросов
- Блокировка конкретных IP-адресов
  - *Прокси*
  - *Ботнеты*

# Пример проблемы: Двойник Google наносит удар!

- 11 августа 2022 года примерно в середине дня в течение 3 минут на сервер клиента поступили почти 10 500 запросов.
- Самым же странным в этих запросах были параметры отправителя.
  - *User-agent ботов Google, но и…*
  - *IP-адрес соответствовал поисковому серверу Google.*
- Зачем притворяться поисковым ботом Google?
  - *Многие вносят поисковые боты в «белый список».*


ИИ дал возможность отсечь атаку после 10-ого запроса, в то же время не блокируя одновременных запросов поисковой системы на этот или другие сайты.

# Защита без специализированной настройки работает хуже

100% защиты = 0 клиентов

- Недоступные ресурсы отталкивают клиентов

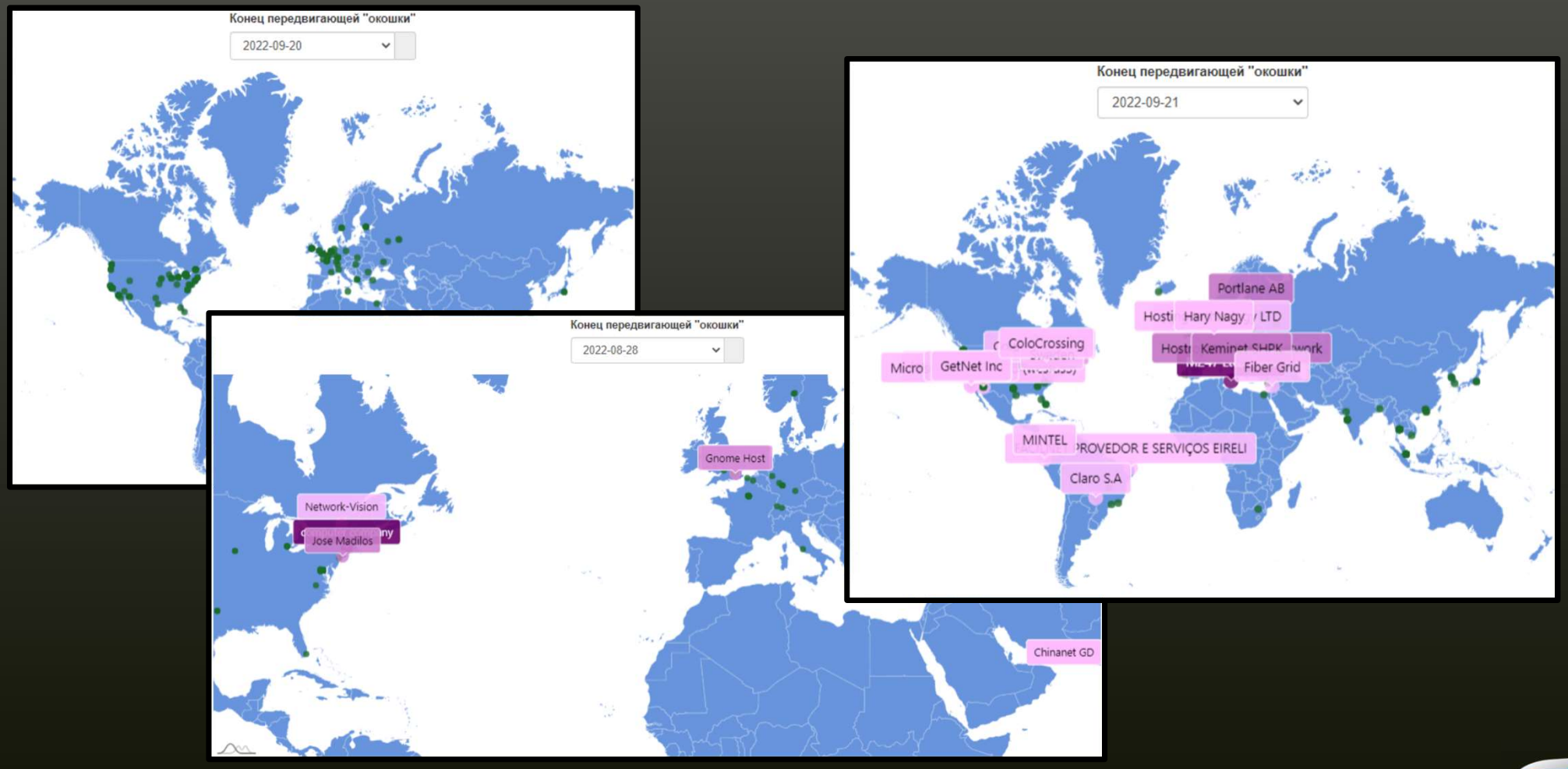
0% защиты = 0 клиентов

- Недоступные ресурсы отталкивают клиентов
- Арендатор облачного сервера платит за серверные ресурсы, даже если не он их использует
- Утечка данных влечет за собой юридическую ответственность
- Взломанный сервер могут использовать для атак третьих лиц, в том числе госорганов

# Примеры: суточная статистика



# Примеры: обнаружение ботнетов



https://felix.techabantu.com

https://tgpo.ru

+7 926 890 68 09

jenya@techabantu.com
d.trelevich@tgpo.ru

@trelewicz

# Спасибо за ваше внимание!