# Лабораторная работа №1\_Отчет.

# Сбор информации, разведка и OSINT

**Все дальнейшие задания выполняются от имени нового пользователя!!!**

|  |  |  |
| --- | --- | --- |
| **Название VM** | **Имя пользователя** | **Сайт и описание компании** |
| **ryskulov** | **ryskulov** | **https://pes.pro/ ПЭС – экспертная строительная компания** |

## ****Упражнение 1. Получение информации о домене/IP с помощью утилиты whois и сервиса whois****

### **Цель**:

понять какую информацию предоставляет утилита whois

**После окончания работы студент должен**

* знать: как работает утилита whois, какие домены и IP-блоки делегируются клиентам
* уметь: получать всю информацию от утилиты whois.

### Задание:

* собрать информацию о домене выбранной компании с помощью команды whois
* собрать информацию о домене выбранной компании с помощью веб-сервиса whois

### Технические инструменты для выполнения работы

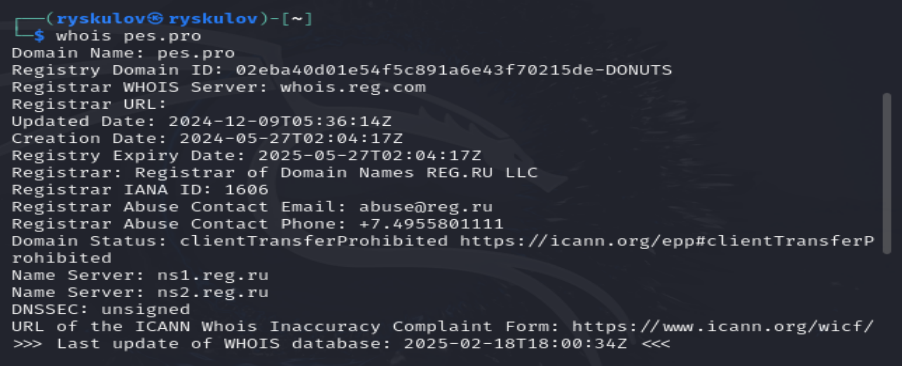
* командная консоль
  + утилита whois
* веб-браузер

### Ссылки

* <https://en.wikipedia.org/wiki/WHOIS>

### ЗАДАНИЕ 1

Получить всю информацию о выбранном домене с помощью команды whois (доказать с помощью снимка экрана). Когда зарегистрировали/изменили домен? Кто владелец домена? Какие отличия между административными, техническими и другими контактами? Объясните.

**Ответ:** 

Домен был зарегистрирован 27.05.2024.

Домен был изменен 09.12.2024

Владелец домена неизвестен

Отличия между административными, техническими и другими контактами:

1. Административный контакт (Admin Contact)

Административный контакт — это лицо или организация, ответственное за управление доменом на административном уровне. Это лицо обычно занимается вопросами управления, изменениями или юридическими аспектами, связанными с доменом.

Задачи административного контакта:

* Управление данными владельца домена.
* Обработка вопросов, связанных с доменом (например, передача прав).
* Получение уведомлений о истечении срока регистрации или проблемах с доменом.

2. Технический контакт (Tech Contact)

Технический контакт — это лицо или организация, отвечающее за техническую поддержку домена. Оно занимается настройками, обслуживанием и решением технических вопросов, связанных с работой домена, серверами и инфраструктурой.

Задачи технического контакта:

* Управление DNS-серверами и другими техническими аспектами.
* Решение проблем с работой сайта, хостингом или серверами.
* Настройка записи доменов и другие вопросы, связанные с серверным обеспечением.

3. Другие контакты

В некоторых случаях могут быть указаны и другие типы контактов:

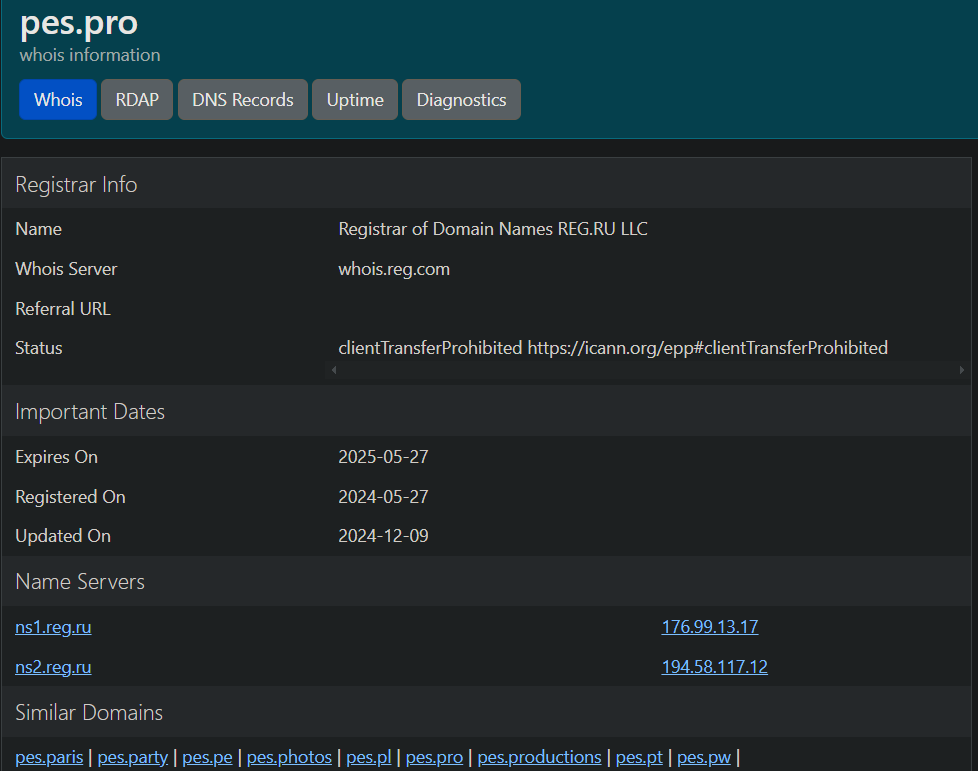
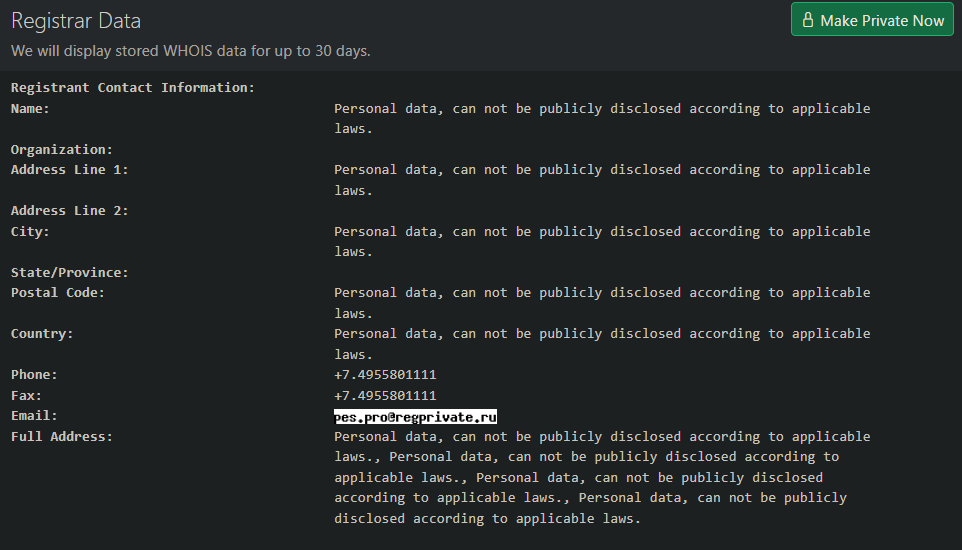
* Контакт для связи с владельцем домена (Registrant Contact) — обычно это основной контакт, который обладает правами на домен.
* Юридический контакт — если домен связан с юридическими вопросами или спорами, могут быть указаны контактные данные юриста.

Отличия и назначение:

* Административный контакт — больше отвечает за управление и юридические вопросы.
* Технический контакт — решает все технические и инфраструктурные задачи, связанные с работой домена.
* Контакт для выставления счетов — следит за финансовыми вопросами, связанными с доменом.
* Прочие контакты — могут быть специфическими для конкретной ситуации, например, для связи с юристами или владельцем.

### ЗАДАНИЕ 2

Получить всю информацию о выбранном домене с помощью веб-службы whois (доказать с помощью снимка экрана).

**Ответ:**  

### ЗАДАНИЕ 3

Есть ли отличия между полученными результатами?

**Ответ:** отличие в Email

### ЗАДАНИЕ 4

Что такое диапазон сети? Кто региональный регистратор? (доказать с помощью скриншотов)

**Ответ:**

Диапазон сети — это диапазон IP-адресов, который может быть использован в конкретной сети, начиная с адреса сети (не используемого для устройств) и заканчивая широковещательным адресом (также не используемым для устройств). Адреса между ними — это те, которые можно присваивать хостам (компьютерам, серверам и т. д.).  


### ЗАДАНИЕ 5

Что такое серверы NS?

**Ответ:**

NS-серверы (или Name Servers, что в переводе с английского означает «Серверы имен») — это серверы, которые отвечают за разрешение доменных имен в IP-адреса. Они являются частью системы доменных имен (DNS) и играют ключевую роль в процессе навигации по интернету.

Основная функция NS-серверов

Когда вы вводите в браузере доменное имя, например, example.com, браузер должен узнать, по какому IP-адресу нужно обратиться для загрузки сайта. Для этого используются NS-серверы.

## ****Упражнение 2. Получить общую информацию о выбранном домене с помощью службы DNS****

### Цель:

Понять основное предназначение DNS

**После окончания работы студент должен**

* знать: как работает DNS, как работают разные типы записей DNS
* уметь: получать всю информацию о доменных записях от DNS.

### Задание:

* получить общие записи DNS (A, AAAA, NS, MX, SPF, PTR) о домене, выбранной компании с помощью команды dig.
* получить общие записи DNS (A, AAAA, NS, MX, SPF, PTR) о домене выбранной компании с помощью веб-сервисов.

### Технические инструменты для выполнения работы

* командная консоль
  + утилита dig
* веб-браузер
  + <https://bgp.he.net/>
  + <https://mxtoolbox.com/>

### Ссылки

* <https://en.wikipedia.org/wiki/Domain_Name_System>
* <https://en.wikipedia.org/wiki/Reverse_DNS_lookup>
* <https://ru.wikipedia.org/wiki/Dig>

### ЗАДАНИЕ 1

Получите всю информацию о выбранном домене с помощью утилиты dig (доказать с помощью снимка экрана). Какие записи доступны (A, AAAA, NS, MX, SPF, PTR)? На что указывают эти записи? Объясните.



**Ответ:** Доступны только записи А.

Запись А связывает доменное имя с IPv4-адресом.

Запись АААА аналогична A-записи, но для IPv6-адресов.

Запись NS указывает на DNS-серверы, отвечающие за зону домена.

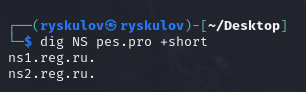
Запись MX определяет серверы, принимающие почту для домена.

Запись SPF - список серверов, которые могут отправлять почту от имени домена.

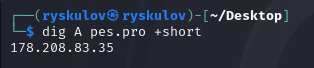
Запись PTR связывает IP-адрес с доменом.

### ЗАДАНИЕ 2

Получить записи PTR для полученных IP-адресов из записей NS/MX/A (не более 5) (доказать с помощью снимка экрана). Есть ли отличия от А записей? Объясните.

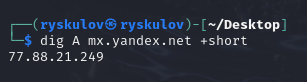






Извлекаем ip-адреса из записей

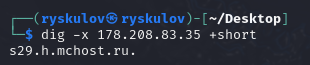


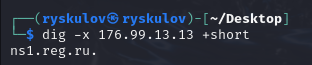


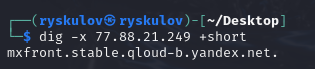
178.208.83.35 – A

176.99.13.13 – NS

77.88.21.249 – MX



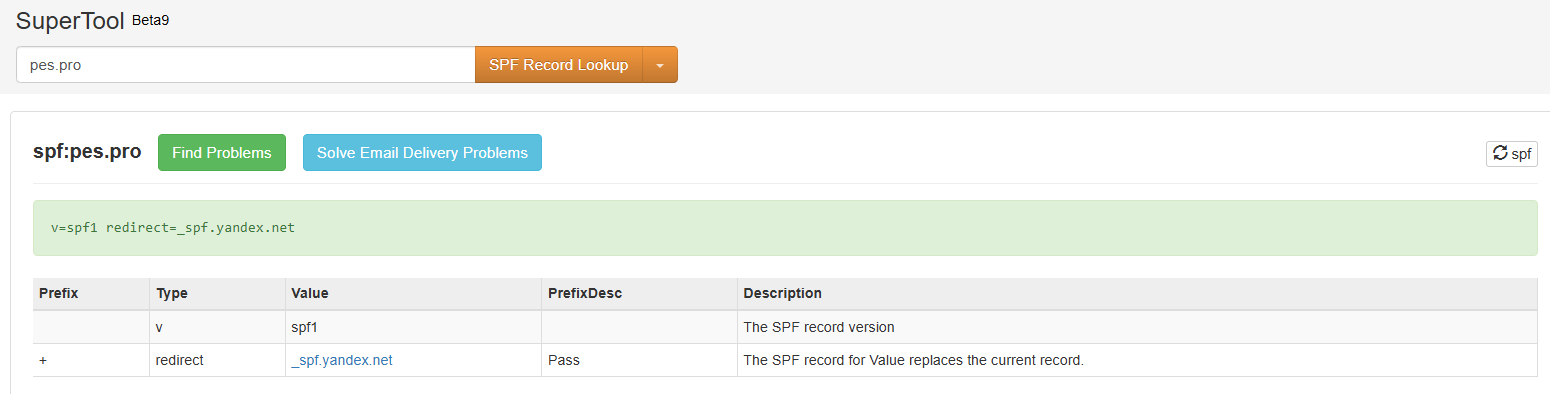




**Ответ:** есть отличие в записи PTR для A записи, т.е. для 178.208.83.35. Это означает, что этот ip-адрес настраивается хостинг-провайдером.

### ЗАДАНИЕ 3

Проверить записи SPF выбранного домена/субдомена с помощью MxToolbox (доказать с помощью снимка экрана)? Объясните результаты.



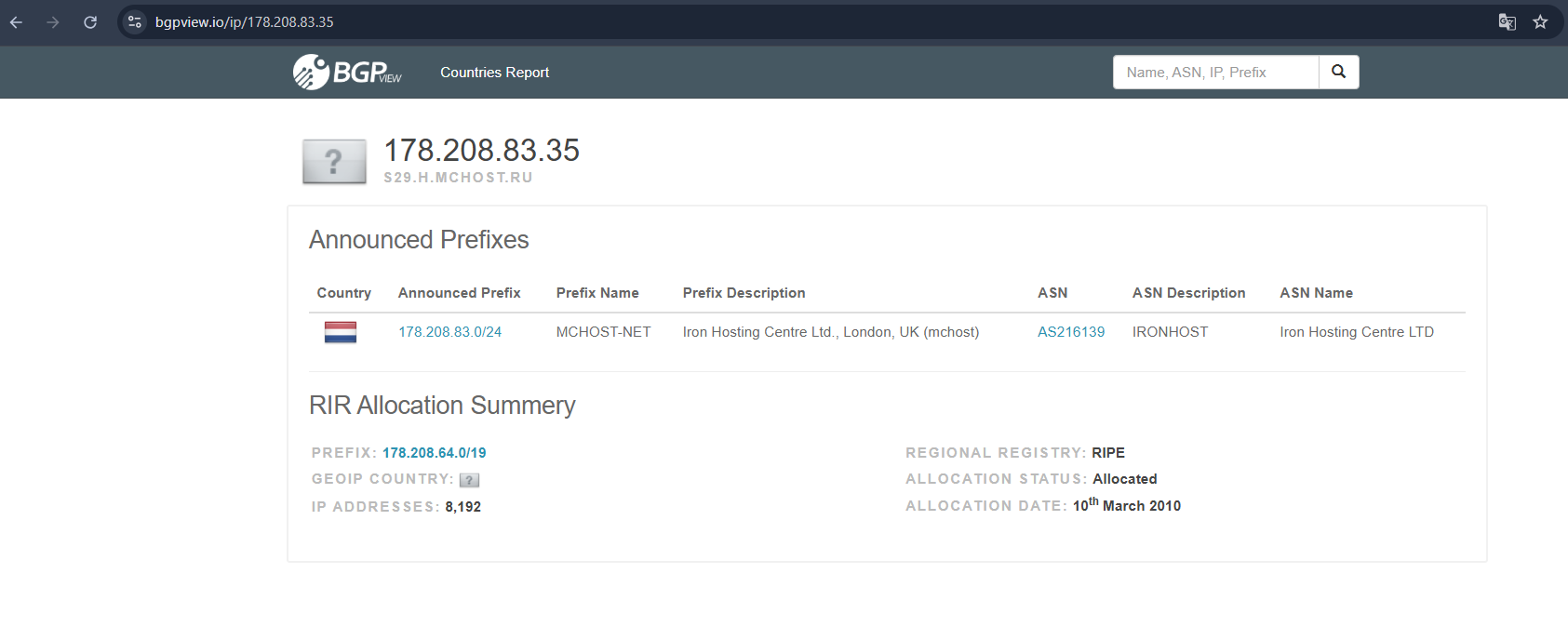
**Ответ:**

v=spf1 redirect=\_spf.yandex.net

Эта SPF запись перенаправляет проверку SPF на SPF запись Яндекса.

### ЗАДАНИЕ 4

Есть ли информация об AS компании? (доказать с помощью скриншотов). Что это значит?



**Ответ:**

Iron Hosting Centre Ltd. – компания, которая владеет ip.

AS216139 – номер автономной системы.

MCHOST-NET – название подсети, зарегистрированное владельцем.

## 

## ****Упражнение 3. Получите общую информацию о целевой AS****

### Цель:

Понять назначение протокола BGP

**После окончания работы студент должен**

* знать: что такое AS, как AS передает трафик
* уметь: получать информацию, связанную с AS (номер, подблоки, соединение, маршруты)

### Задание:

* получить информацию об AS целевой компании с помощью https://bgp.he.net/
* получить изменения в маршрутизации BGP в выбранную AS

### Технические инструменты для выполнения работы

* командная консоль
  + утилита traceroute
* веб-браузер
  + <https://bgp.he.net/>
  + <http://www.routeviews.org/routeviews/>
  + <https://stat.ripe.net/widget/bgplay>

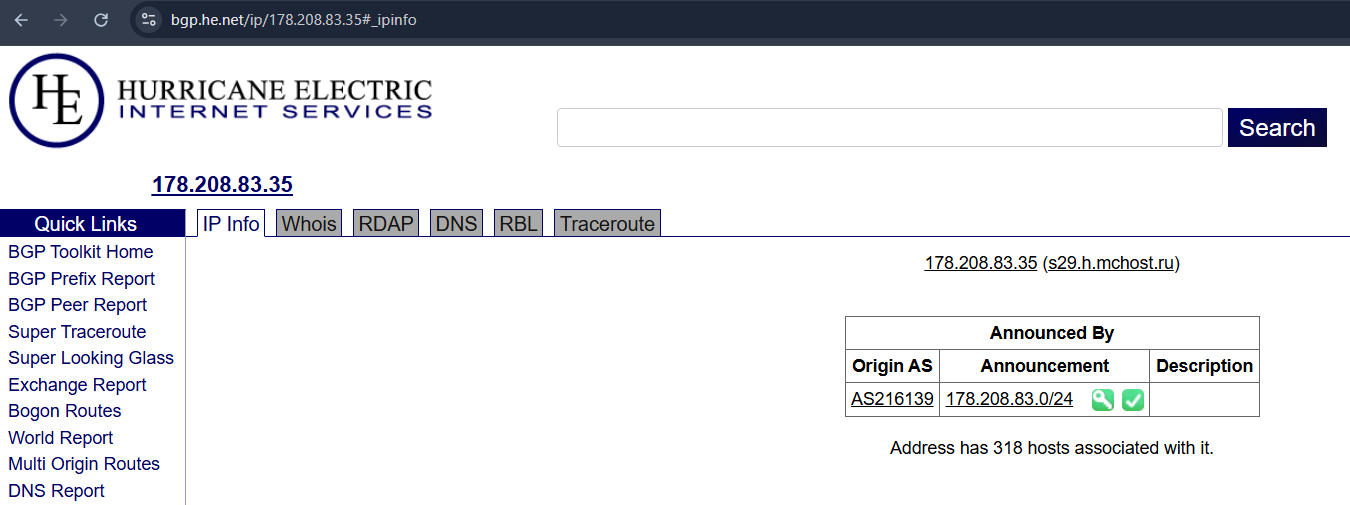
### Ссылки

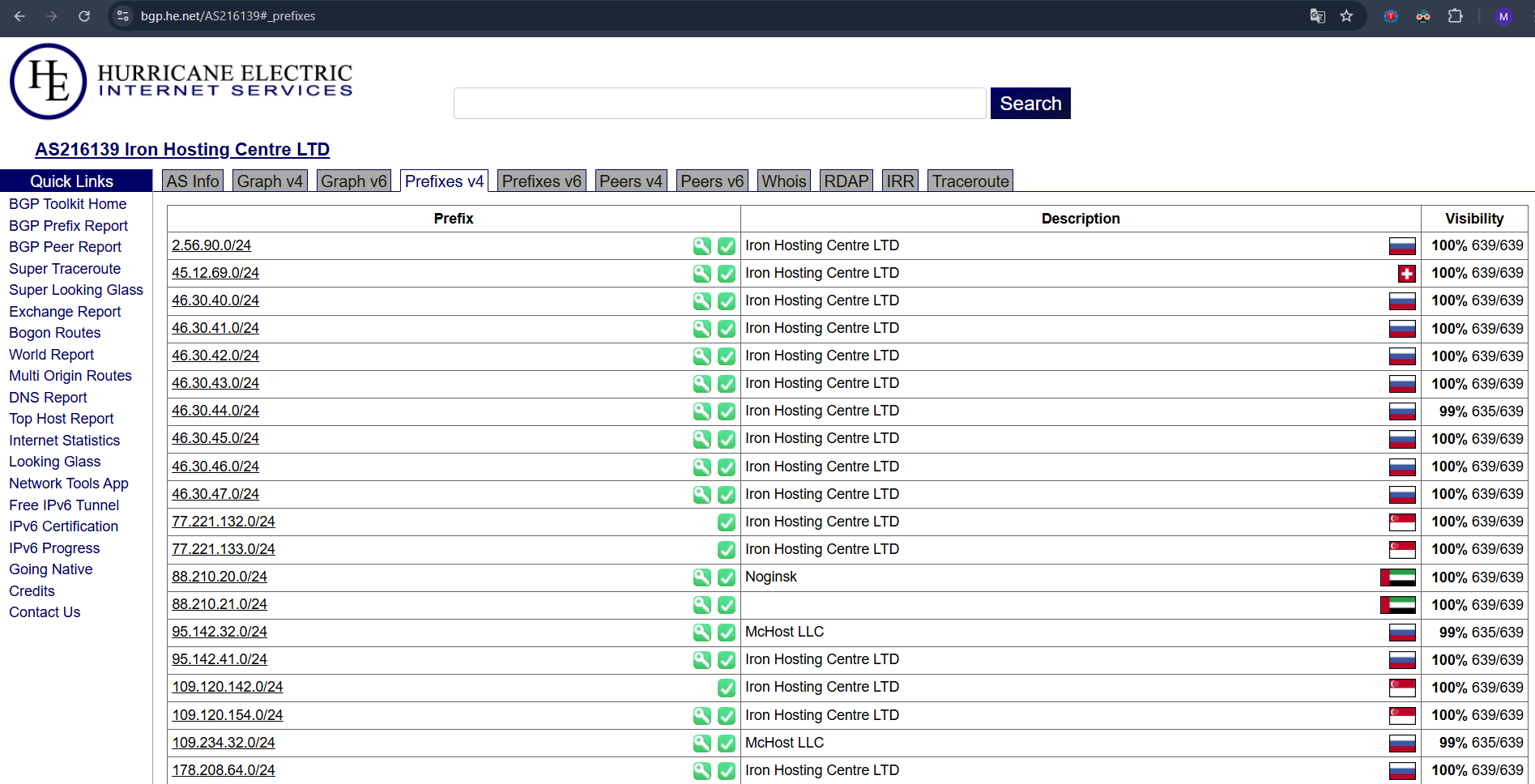
* <https://en.wikipedia.org/wiki/Border_Gateway_Protocol>

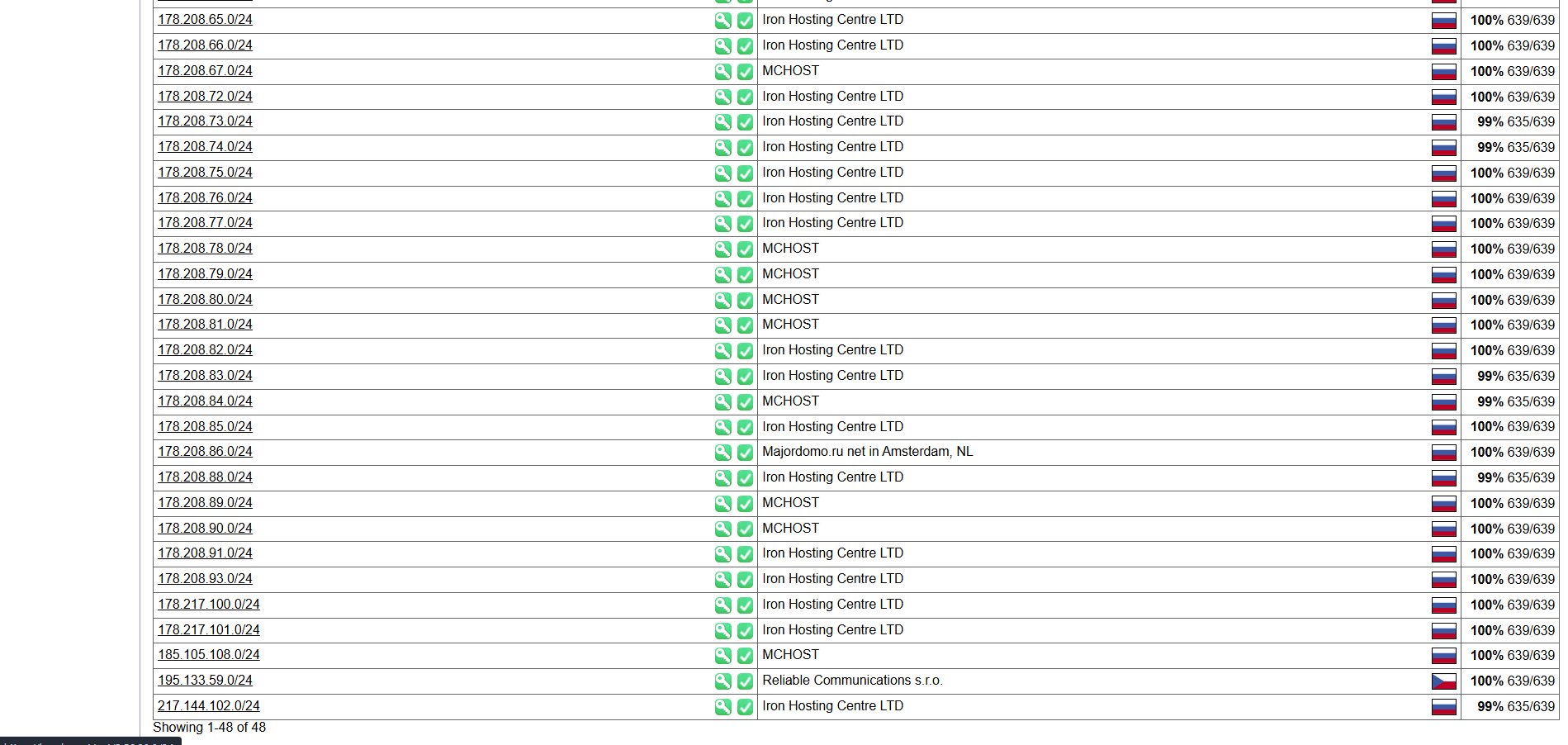
### ЗАДАНИЕ 1

Получить всю информацию об AS с помощью bgp.he.net (доказать с помощью снимка экрана). Что такое номер AS? Какие подблоки делегированы данной AS?









**Ответ:**

ASN — это уникальный номер автономной системы, который идентифицирует сеть провайдера или организации в интернете. Он нужен для управления маршрутизацией трафика между сетями.

Какие подблоки делегированы данной AS – 178.208.83.0/24

### ЗАДАНИЕ 2

Есть какие-то другие AS, которые объявляют тот же подблок? Это верно?

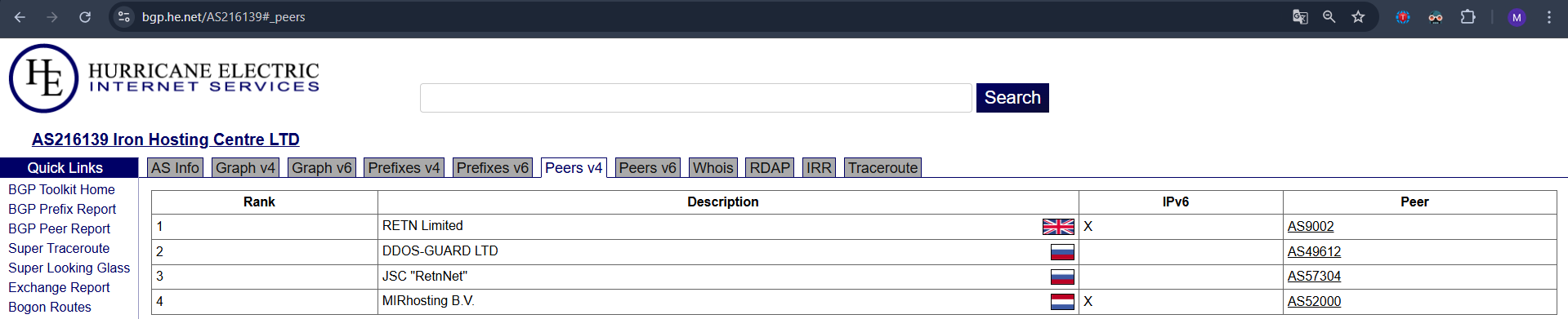


**Ответ:**

Других AS, которые объявляют тот же подблок нет, это верно.

### ЗАДАНИЕ 3

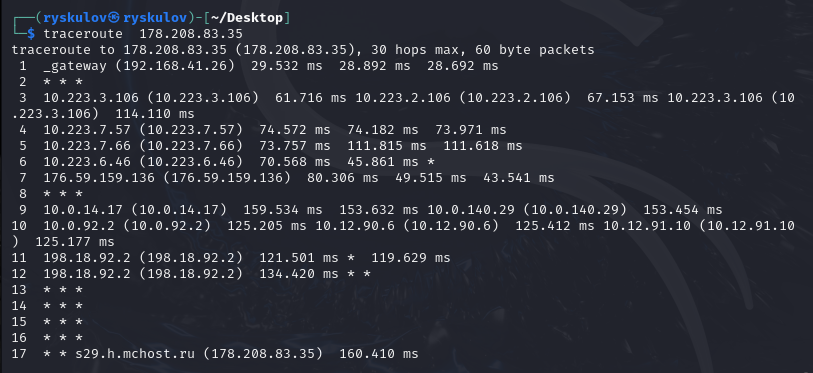
Сколько соединений имеет текущее AS? (доказать с помощью скриншота).

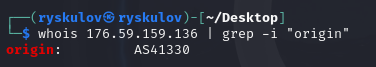


**Ответ:** текущее AS имеет 4 peers. Это соединения, по которым маршрутизируется интернет-трафик.

### ЗАДАНИЕ 4

Каков основной путь между целевой AS и вами? Докажите это с помощью команды traceroute и снимка экрана и результата анализа отношений IP-AS.







**Ответ:**

Построим цепочку на основе вывода traceroute и whois:

Сеть -> AS41330 (T2 Mobile LLC) -> AS216139 (Iron Hosting)

## ****Упражнение 4. OSINT с помощью Shodan****

### Цель:

понять назначение Shodan

**После окончания работы студент должен**

* знать: как работает сервис Shodan

### Задание:

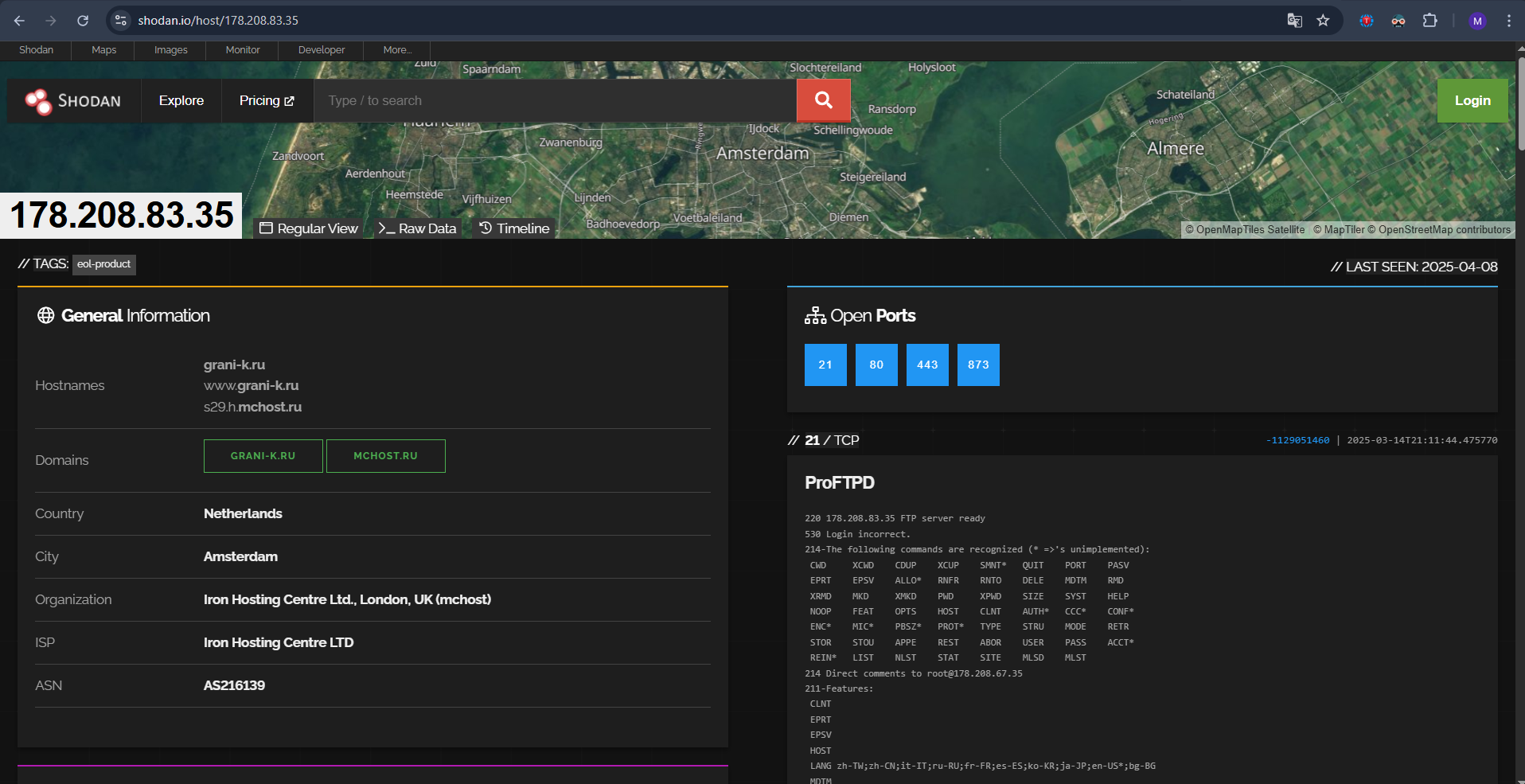
* подтвердить, указать и расширить информацию с предыдущих шагов с помощью сервиса Shodan.

### Технические инструменты для выполнения работы

* веб-браузер
  + <https://www.shodan.io/>

**ЗАДАНИЕ 1**

Какую информацию вы смогли получить из Shodan? (покажите с помощью скриншотов)

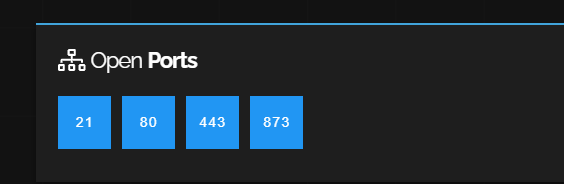


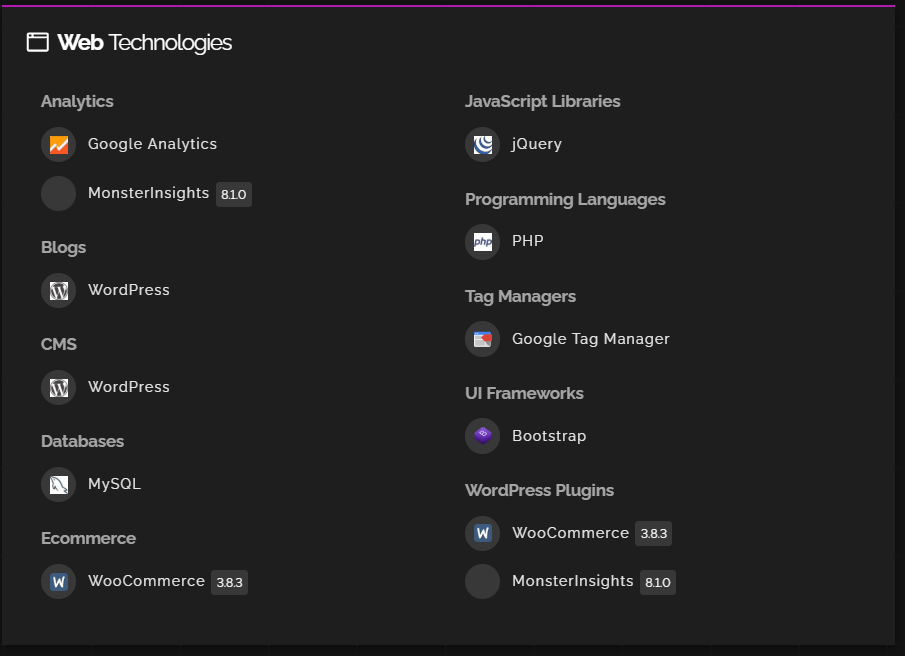
**Ответ:**

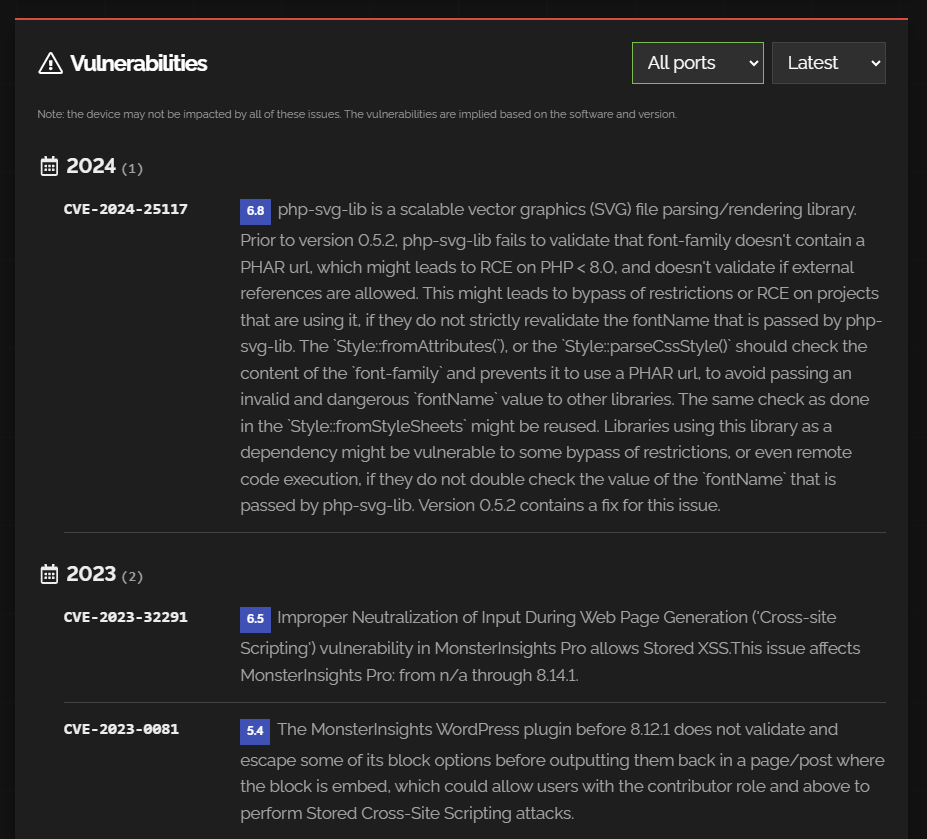
Была получена общая информация о доменах, стране, организации, номере AS.

**ЗАДАНИЕ 2**

Есть ли дополнительная информация об изучаемой цели? (покажите с помощью скриншотов)







**Ответ:**

Есть дополнительная информация об открытых портах, используемых веб технологиях, уязвимостях.

## ****Упражнение 5. Автоматизируйте OSINT с помощью Maltego и FOCA****

### Цель:

понять возможности Maltego и Foca

**После окончания работы студент должен**

* знать: как работает Maltego
* знать: как работает Foca

### Задание:

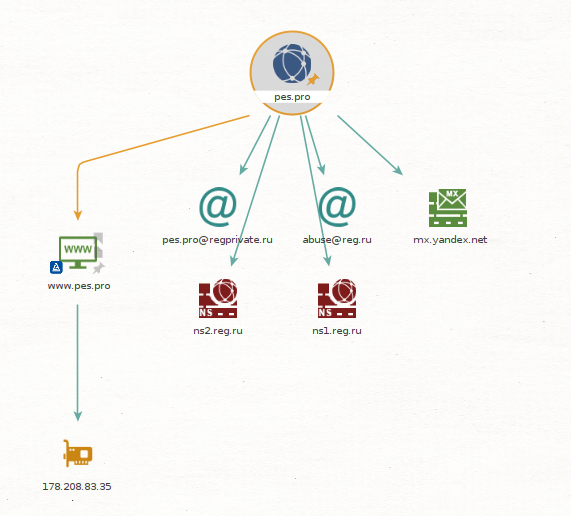
* получить всю информацию из предыдущих шагов используя Maltego

### Технические инструменты для выполнения работы

* + Maltego
  + FOCA

### ЗАДАНИЕ 1

Какую информацию вы смогли получить с помощью Maltego? (доказать с помощью скриншотов)



**Ответ:**

Была получена следующая информация:

Email-адреса

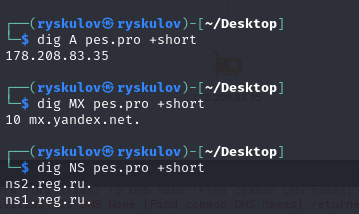
Ip адрес

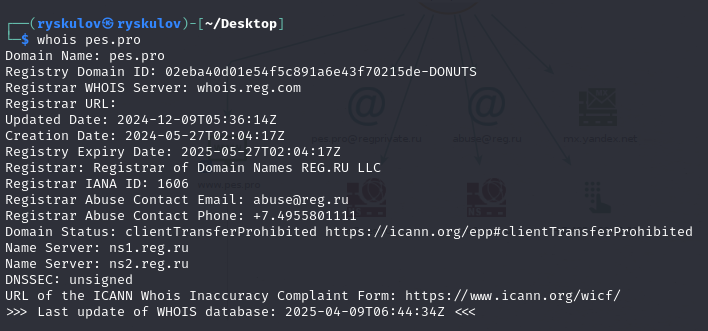
NS записи

MX записи

### ЗАДАНИЕ 2

Есть ли отличия от автоматизированного и ручного сбора данных? (доказать с помощью скриншотов) Объясните.



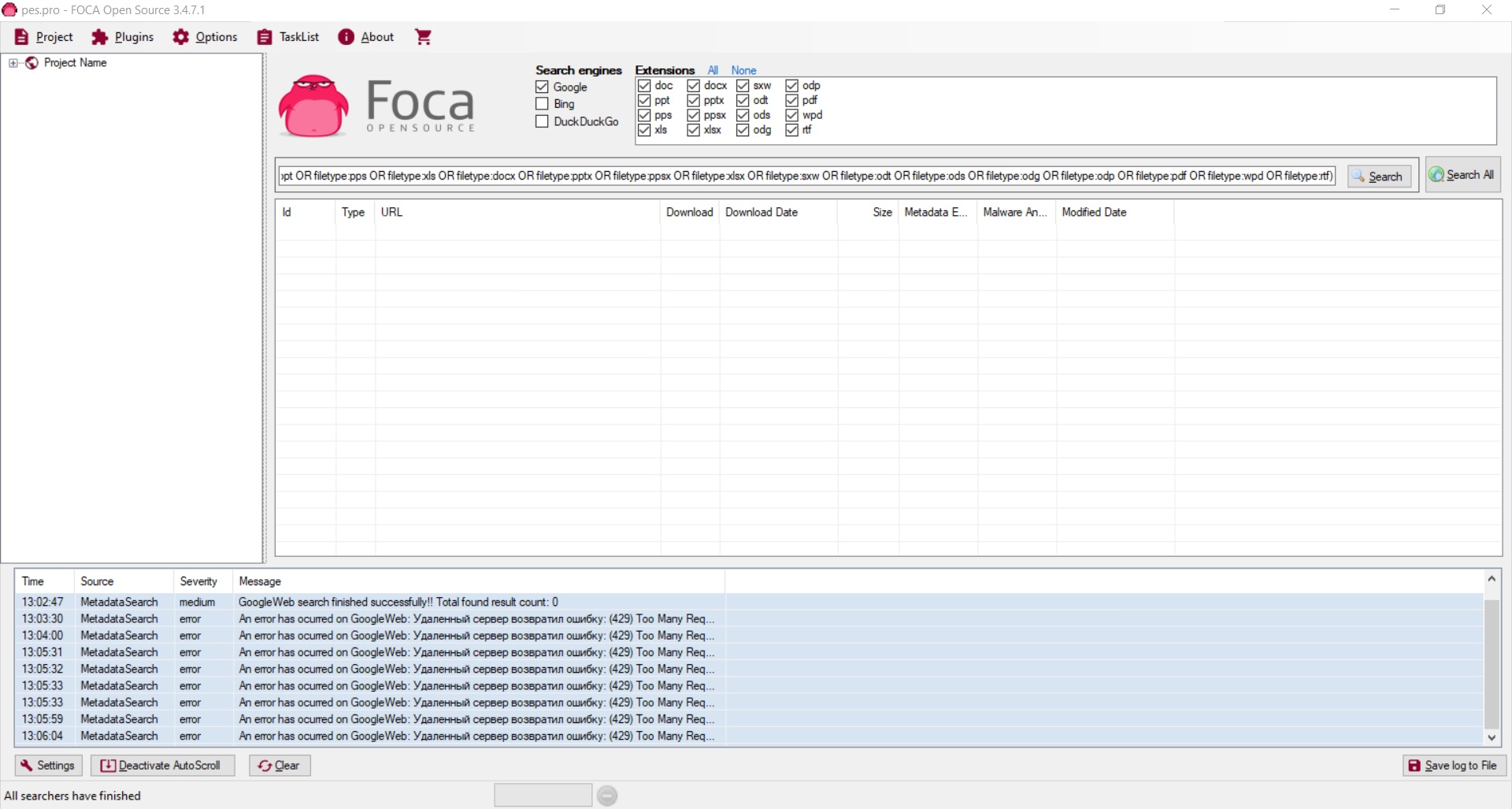


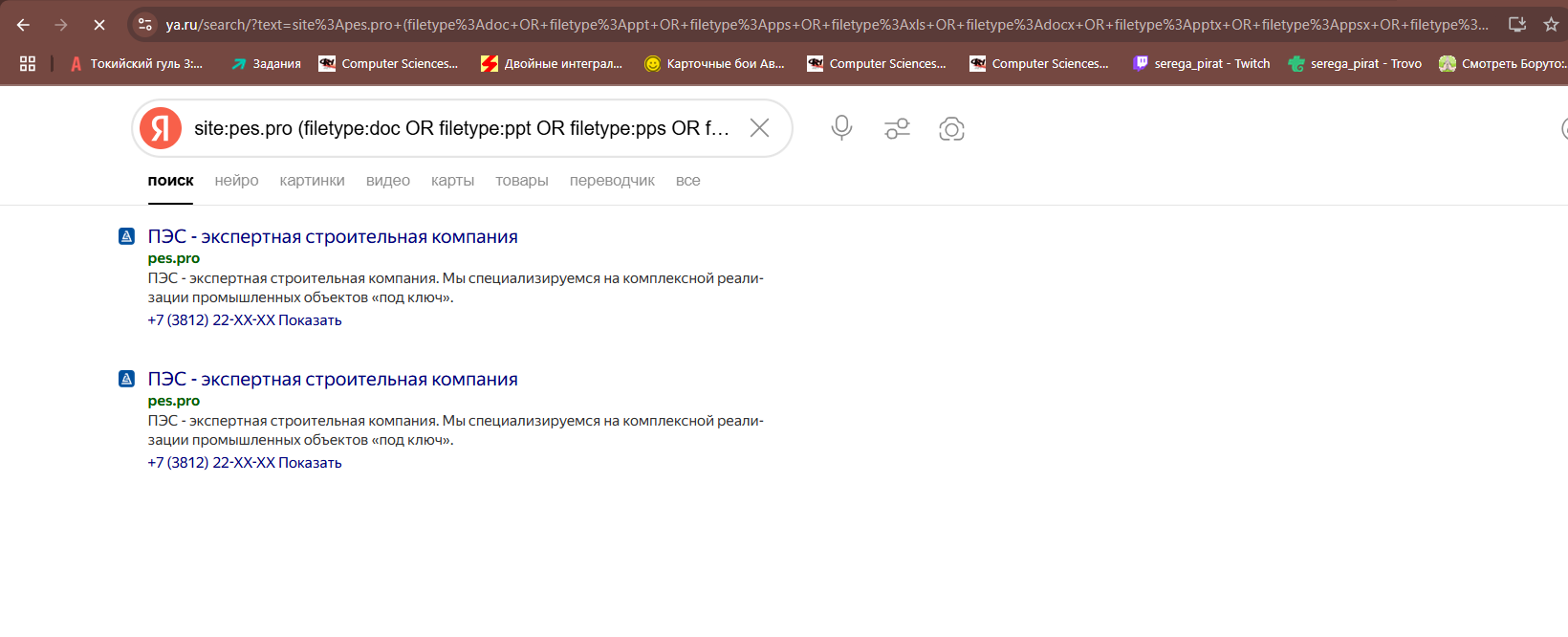
**Ответ:**

Есть отличие в информации об email адресах, при автоматизированном сборе данных есть еще pes.pro@regprivate.ru

### ЗАДАНИЕ 3

Загрузить и извлечь метаданные из файлов, полученных из целевого домена/субдоменов компании с помощью FOCA? (доказать с помощью скриншотов) Объясните.





**Ответ:**

FOCA не вывел никаких данных.

Но при вставке запроса из FOCA вывелся результат выше.

### ЗАДАНИЕ 4

Есть ли какие-либо имена пользователей/электронные письма? (доказать с помощью скриншотов)

**Ответ:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## ****Упражнение 6. Проверка учетных данных с помощью Pastebin и Haveibeenpwned****

### Цель:

Понять для чего предназначены сервисы **Pastebin и Haveibeenpwned**

**После окончания работы студент должен**

* знать: как проверить учетные данные в общедоступных базах данных

### Задание:

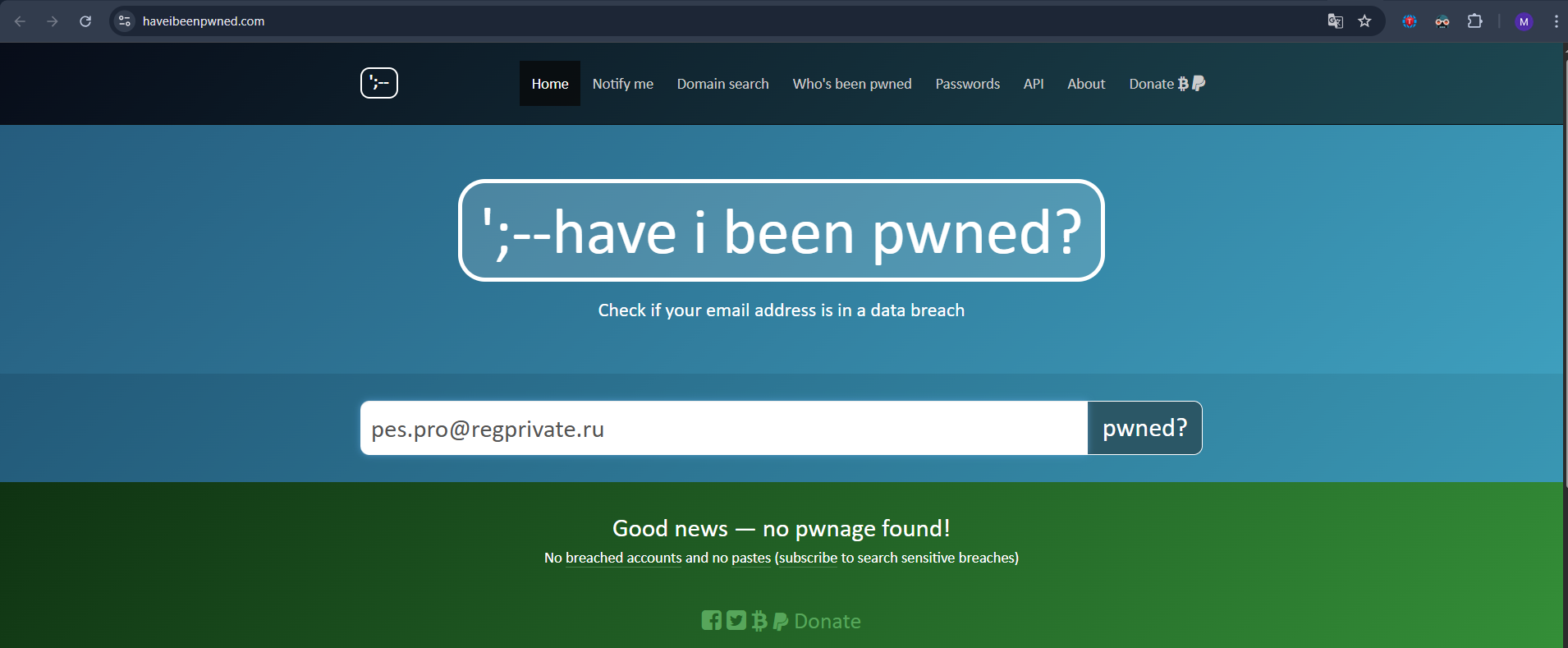
* проверить все учетные данные из предыдущих шагов по предоставленным ресурсам

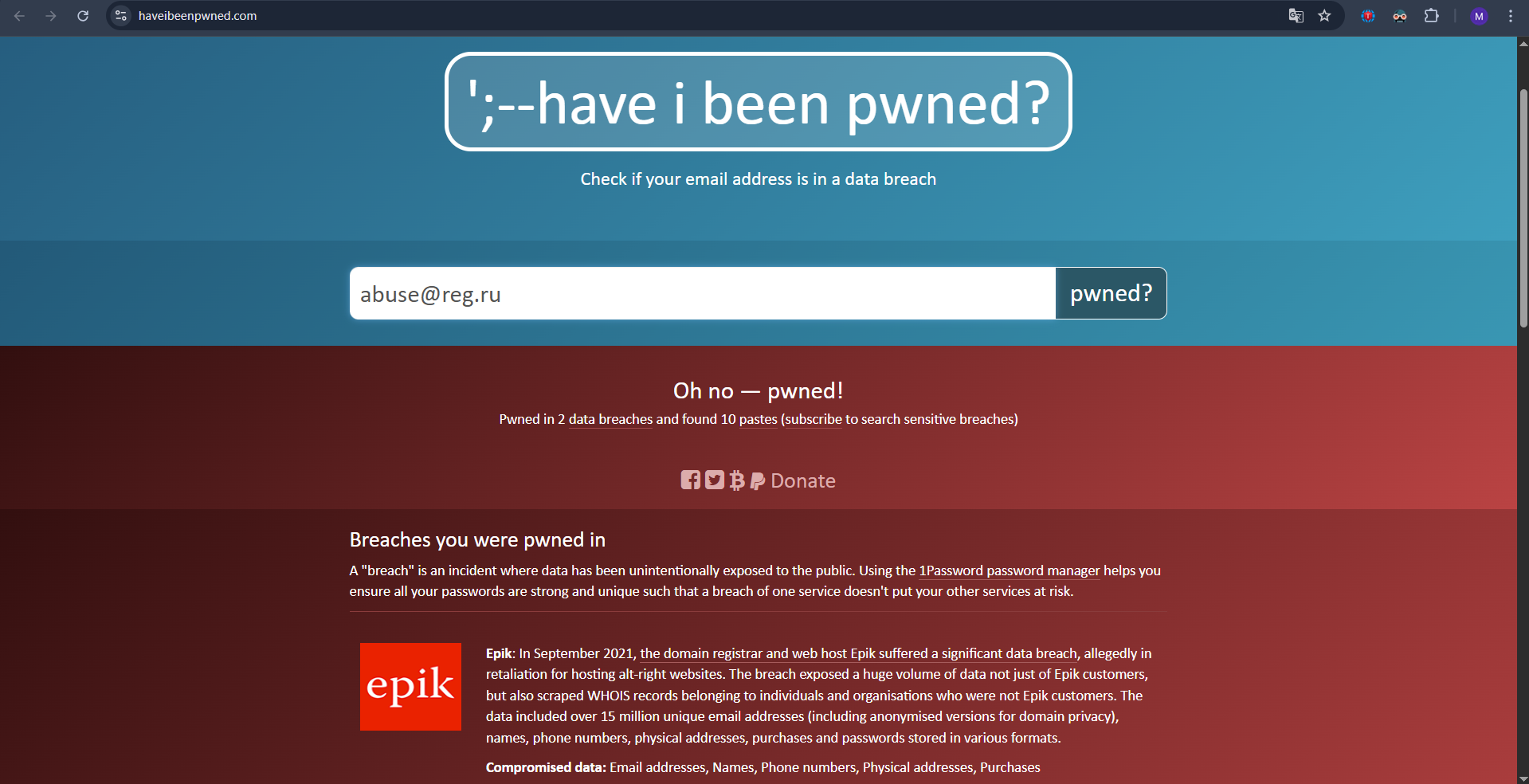
### Технические инструменты для выполнения работы

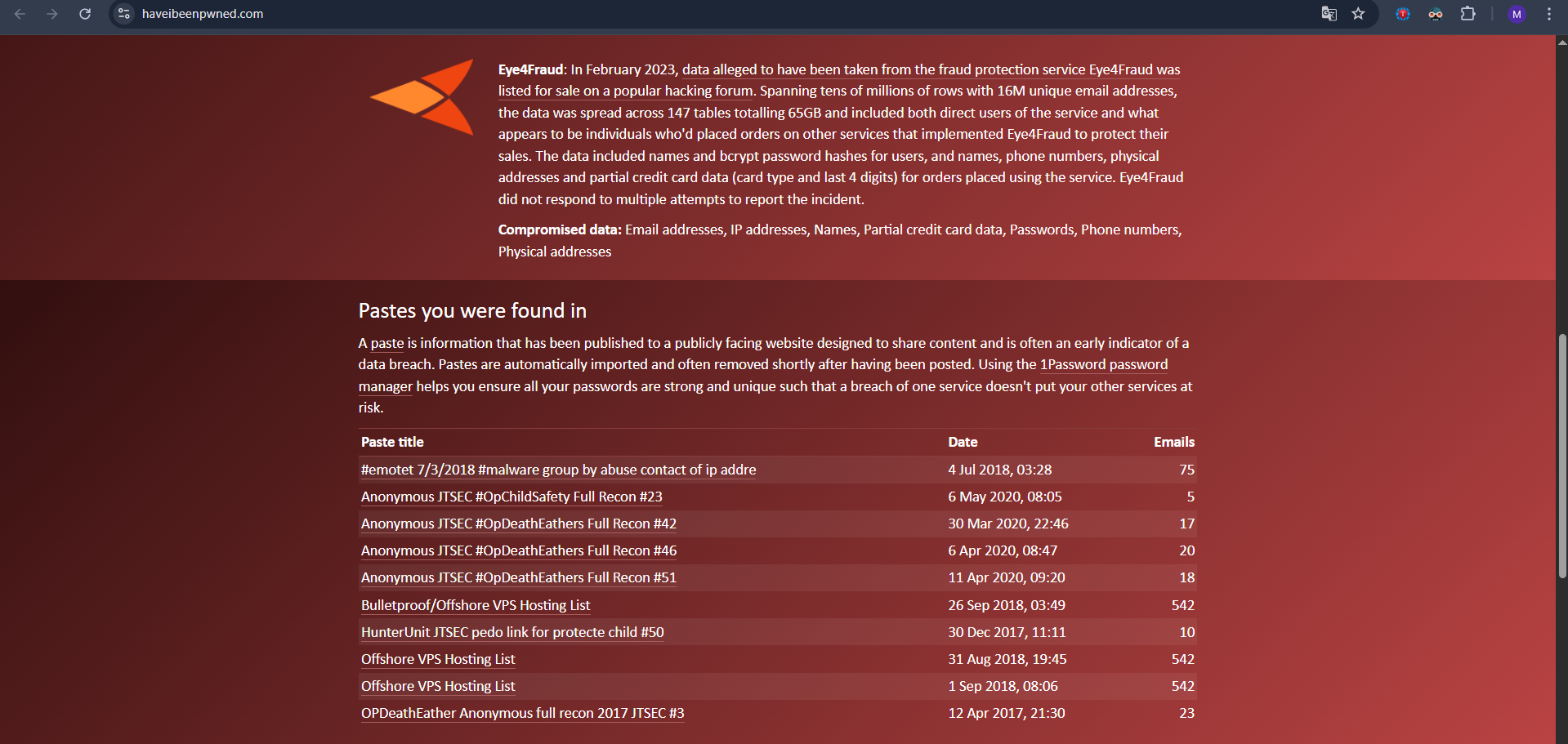
* <https://haveibeenpwned.com/>
* <https://pastebin.com/>

### ЗАДАНИЕ 1

Проверить электронные ящики с помощью Haveibeenpwned? (Предоставьте результаты с помощью скриншотов). Что-то интересное?





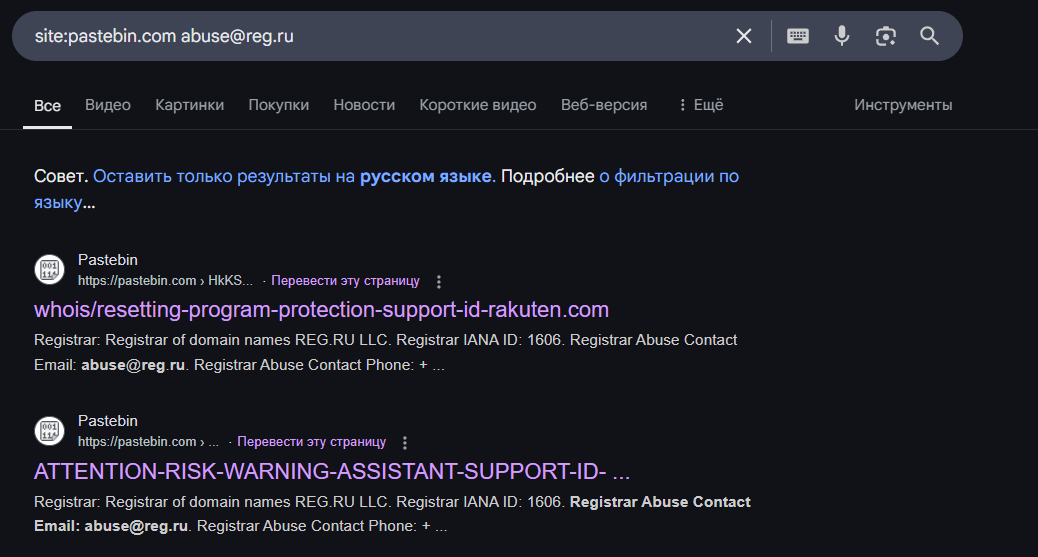


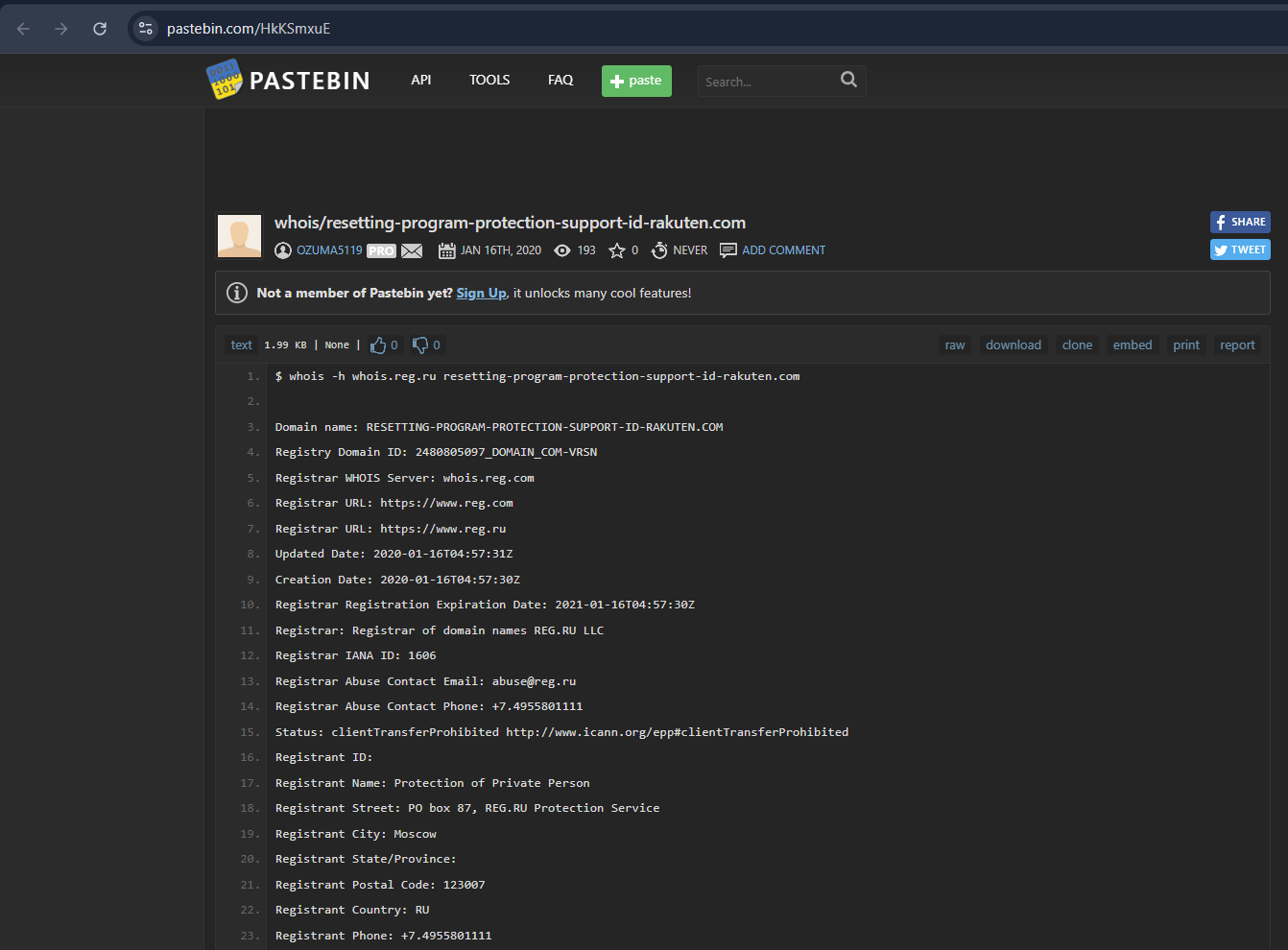
**Ответ:**

При проверке [abuse@reg.ru](mailto:abuse@reg.ru) было обнаружено, что данный email адрес был найден в двух утечках баз данных.

### ЗАДАНИЕ 2

Проверить электронные ящики, домены и IP-адреса с помощью Pastebin? (Предоставьте результаты с помощью скриншотов). Что-то интересное?







**Ответ:**

Была найдена информация о abuse@reg.ru