

Министерство образования Республики Беларусь
Учреждение образования
«Гомельский государственный университет
имени Франциска Скорины»

Отчёт по лабораторной работе №1
«Сбор предварительной информации»

Выполнил студент группы МС-42:

Казак И.В.

Проверил:

Старший преподаватель

Грищенко В.В.

Гомель 2022

Цель работы: Целью лабораторной работы является обучение методам и средствам сбора предварительной информации в Интернет об анализируемой КС.

Ход работы.

Шаг 1. Перейдём по адресу <https://hb.by/whois.aspx>. Укажем домен bsmu.by.

Статус доменного имени:

Доменное имя **bsmu.by** ✕ занято или недоступно.

Whois-информация о доменном имени:

Domain name: bsmu.by
Registrar: Reliable Software, Ltd
Org: Учреждение образования "БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ"
Country: BY
Address: 220116, -, г. Минск, пр-т Дзержинского, д. 83, -
Registration or other identification number: 100582412
Phone: +375173481606
Email: HIDDEN!
Name Server: u1.hoster.by
Name Server: u2.hoster.by
Update Date: 2022-08-09
Creation Date: 2002-09-20
Expiration Date: 2024-10-07

У данного домена 2 Name Server'а.

Определим IP адреса данных серверов.

u1.hoster.by has address 93.125.30.201
u1.hoster.by has IPv6 address 2a0a:7d80:1:1::4:0
Диапазон IP адресов - 93.125.30.0 - 93.125.30.255

Responsible organisation: [Reliable Software, Ltd.](#)
Abuse contact info: abuse@hoster.by

inetnum: [93.125.30.0 - 93.125.30.255](#)
netname: HOSTERBY-6
org: [ORG-RSL39-RIPE](#)
country: BY
admin-c: [SP17043-RIPE](#)
tech-c: [D0616-RIPE](#)
status: ASSIGNED PA
mnt-by: [BYGIS-MNT](#)
mnt-by: [by-hosterby-1-mnt](#)
mnt-routes: [AS6697-MNT](#)
created: 2010-04-19T15:41:37Z
last-modified: 2022-04-06T12:13:08Z
source: RIPE

route: [93.125.30.0/24](#)
descr: DELEGATED FROM BELPAK
origin: AS6697
mnt-by: [AS6697-MNT](#)
created: 2010-04-19T14:50:21Z
last-modified: 2010-04-19T20:34:37Z
source: RIPE

u2.hoster.by has address 178.172.137.158

u2.hoster.by has IPv6 address 2a0a:7d80:3:2::b

Диапазон IP адресов - 93.125.30.0 - 93.125.30.255

Responsible organisation: [Reliable Software, Ltd.](#)
Abuse contact info: abuse@hoster.by

inetnum: [178.172.136.0 - 178.172.139.255](#)
netname: HOSTERBY
country: BY
admin-c: [SP17043-RIPE](#)
tech-c: [D0616-RIPE](#)
status: ASSIGNED PA
mnt-routes: [AS12406-MNT](#)
mnt-by: [AS35594-MNT](#)
mnt-by: [by-hosterby-1-mnt](#)
created: 2019-03-28T07:28:42Z
last-modified: 2019-03-28T07:28:42Z
source: RIPE

route: [178.172.136.0/22](#)
descr: BN for HOSTERBY
origin: AS12406
mnt-by: [AS12406-MNT](#)
created: 2019-03-28T07:43:57Z
last-modified: 2021-11-16T07:14:55Z
source: RIPE

Выделенный диапазон IP адресов организации – 195.50.4.0 – 195.50.7.255

Responsible organisation: [Institution Central Information and Analytical Center at the Ministry of Education of Belarus](#)
Abuse contact info: abuse@becloud.by

inetnum: [195.50.4.0 - 195.50.7.255](#)
netname: BECLOUD
descr: Belarusian Cloud Technologies
country: BY
admin-c: [AC24735-RIPE](#)
tech-c: [AC24735-RIPE](#)
tech-c: [VP13896-RIPE](#)
abuse-c: [AA26310-RIPE](#)
status: ASSIGNED PA
mnt-by: [AS5498-MNT](#)
mnt-domains: [BCTBY-MNT](#)
mnt-routes: [BCTBY-MNT](#)
mnt-lower: [BCTBY-MNT](#)
created: 2016-07-01T12:18:56Z
last-modified: 2019-04-26T13:59:39Z
source: RIPE

route: [195.50.4.0/22](#)
descr: BeCloud IPv4 route 2
origin: AS60330
mnt-by: [BCTBY-MNT](#)
created: 2016-07-01T13:05:30Z
last-modified: 2016-07-01T13:07:17Z
source: RIPE# Filtered

Шаг 2. Перейдём по адресу <https://network-tools.com/nslookup/> и зададим параметры: домен – bsmu.by, тип запроса – ANY. Определим почтовый сервер организации.

Returned Data

Name	TTL Until Refresh	Class	Type	Data
bsmu.by.	300	IN	SOA	u1.hoster.by. support.hoster.by. 2022092911 43200 7200 604800 600
bsmu.by.	300	IN	TXT	"v=spf1 a mx ptr include:neolocation.net ~all"
bsmu.by.	300	IN	TXT	"202203090638423nenzmelz08v8tumrbw8j2jlnzaobnjb5m6a4x95hmpf03adr5"
bsmu.by.	300	IN	TXT	"google-site-verification=TRvgwyJYz2uezFQkiv0C3ef35IX0HPCO2xp34-oT5ic"
bsmu.by.	300	IN	TXT	"globalsign-domain-verification=gS2A_gHzgyNJTHVimkNZ8k18p5NRQCeiKkLuOfWDSO"
bsmu.by.	300	IN	TXT	"MS=ms54233608"
bsmu.by.	300	IN	A	195.50.7.146
bsmu.by.	300	IN	MX	10 mail.bsmu.by.
bsmu.by.	300	IN	NS	u1.hoster.by.
bsmu.by.	300	IN	NS	u2.hoster.by.

Почтовый сервер организации – mail.bsmu.by.

Шаг 3. Выполним предыдущие проверки используя средства nslookup, host, dig.


Google Admin Toolbox Dig:

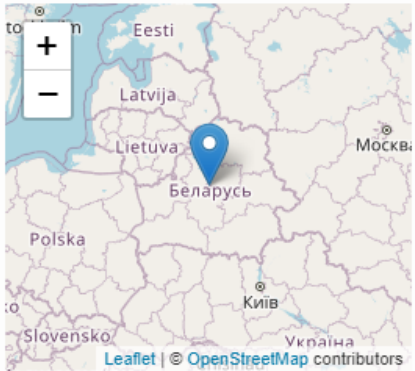
```
bsmu.by. 600 IN NS u1.hoster.by.
bsmu.by. 600 IN NS u2.hoster.by.
bsmu.by. 3600 IN MX 10 mail.bsmu.by.
bsmu.by. 3600 IN A 195.50.7.146
bsmu.by. 600 IN TXT
"202203090638423nenzmelz08v8tumrbw8j2jlnzaobnjb5m6a4x95hmpf03adr5"
bsmu.by. 600 IN TXT "MS=ms54233608"
bsmu.by. 600 IN TXT "globalsign-domain-
verification=gS2A_gHzgyNJTHVimkNZ8k18p5NRQCeikKLuOfWDSO"
bsmu.by. 600 IN TXT "google-site-
verification=TRvgwyJYz2uezFQkiv0C3ef35lX0HPC02xp34-oT5ic"
bsmu.by. 600 IN TXT "v=spf1 a mx ptr include:neolocation.net ~all"
bsmu.by. 600 IN SOA u1.hoster.by. support.hoster.by. 2022092911 43200 7200
604800 600
```

Check-host.by:

Местонахождение сайта и IP адреса: bsmu.by

DB-IP (01.11.2022)

IP адрес	195.50.7.146
Имя ресурса	195.50.7.146
IP диапазон	195.50.4.0-195.50.7.255 CIDR
Провайдер	BeCloud 2
Организация	
Страна	 Belarus (BY)
Регион	Minsk City
Город	Minsk (Lieninski rajon)
Часовой пояс	Europe/Minsk, GMT+0300
Местное время	09:35:08 (+03) / 2022.11.14
Индекс	220030



Leaflet | © OpenStreetMap contributors

При поддержке **DB-IP**

IPGeolocation.io (13.10.2022)


IP адрес	195.50.7.146
Имя ресурса	195.50.7.146
IP диапазон	195.50.7.0-195.50.7.255 CIDR
Провайдер	Belarusian Cloud Technologies LLC
Организация	Belarusian Cloud Technologies LLC
Страна	 Belarus (BY)
Регион	Minsk
Город	Minsk
Часовой пояс	Europe/Minsk, GMT+0300
Местное время	09:35:08 (+03) / 2022.11.14
Индекс	220036



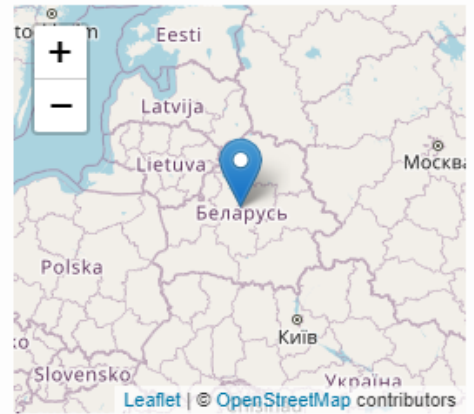
Leaflet | © OpenStreetMap contributors

При поддержке **IPGeolocation.io**


IP2Location (03.11.2022)

IP адрес	195.50.7.146
Имя ресурса	195.50.7.146
IP диапазон	195.50.0.0-195.50.31.255 CIDR
Провайдер	
Организация	
Страна	 Belarus (BY)
Регион	Minskaya voblasts'
Город	Minsk
Часовой пояс	+03:00
Местное время	09:35:08 (+0300) / 2022.11.14
Индекс	220088

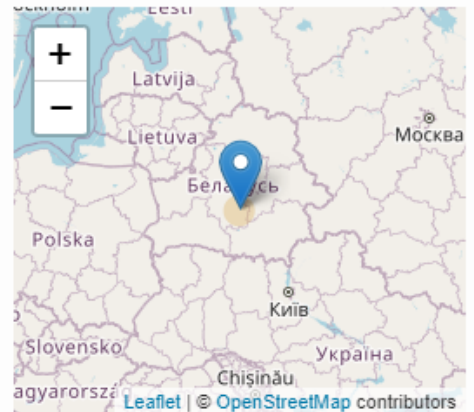
При поддержке IP2Location



MaxMind GeoIP (01.11.2022)

IP адрес	195.50.7.146
Имя ресурса	195.50.7.146
IP диапазон	
Провайдер	
Организация	
Страна	 Belarus (BY)
Регион	
Город	
Часовой пояс	Europe/Minsk, GMT+0300
Местное время	09:35:08 (+03) / 2022.11.14
Индекс	

При поддержке MaxMind GeoIP

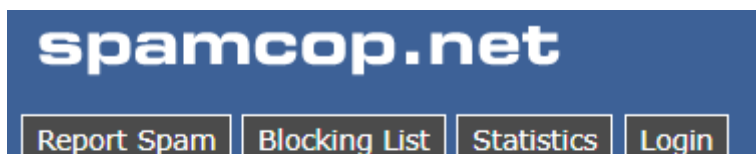


Nslookup

```
C:\Users\igoro>nslookup bsmu.by
тхЕтхЕ: secondary.dns.yandex.ru
Address: 77.88.8.1

Не заслуживающий доверия ответ:
Ь : bsmu.by
Address: 195.50.7.146
```

Шаг 4. Проверим наличие узлов найденных сетей в базах данных спам-отправителей:



Host bsmu.by (checking ip) = 195.50.7.146

Query bl.spamcop.net - 195.50.7.146

Lookup another:

([Help](#)) ([Trace IP](#)) ([TalosIntelligence Lookup](#))

195.50.7.146 not listed in bl.spamcop.net

Шаг 5. Проверим возможность выполнения переноса зоны на первичном и вторичном DNS-серверах:

```
>
C:\Users\igoro>nslookup
тхЁтхЁ яю ёьюйрэш■: dns.google
Address: 8.8.8.8

> server u1.hoster.by
тхЁтхЁ яю ёьюйрэш■: u1.hoster.by
Addresses: 2a0a:7d80:1:1::4:0
          93.125.30.201

> set type=any
> ls -dbsmu.by
Unrecognized command: ls -dbsmu.by
> ls -d bsmu.by
[u1.hoster.by]
*** Can't list domain bsmu.by: BAD ERROR VALUE
DNS-сервер отклонил передачу зоны bsmu.by на данный компьютер. Если это
ошибка, проверьте параметры безопасности передачи зоны для bsmu.by на DNS-
сервере по IP-адресу 2a0a:7d80:1:1::4:0.
```

```

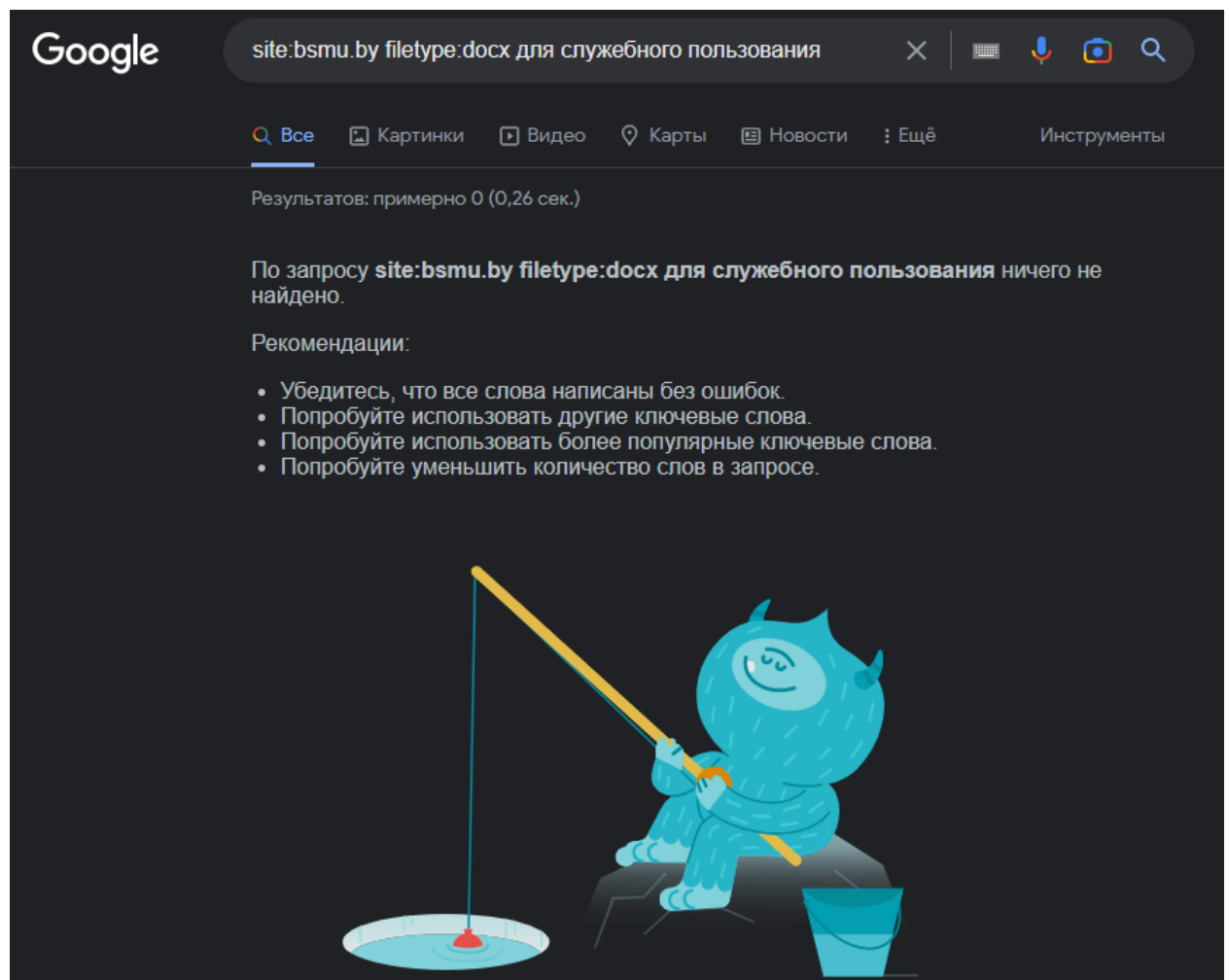
>
C:\Users\igoro>nslookup
ѠхѠтхѠ яю ѡююѠрѡш■: dns.google
Address: 8.8.8.8

> server u2.hoster.by
ѠхѠтхѠ яю ѡююѠрѡш■: u2.hoster.by
Addresses: 2a0a:7d80:3:2::b
           178.172.137.158

> set type=any
> ls -d bsmu.by
[u2.hoster.by]
*** Can't list domain bsmu.by: BAD ERROR VALUE
DNS-сервер отклонил передачу зоны bsmu.by на данный компьютер. Если это
ошибка, проверьте параметры безопасности передачи зоны для bsmu.by на DNS-
сервере по IP-адресу 2a0a:7d80:3:2::b.

```

Шаг 6. Найдём потенциально интересующую нас информацию в google.



Результатов: примерно 2 (0,30 сек.)

<https://www.bsmu.by> > nauch_tex_nich > karta2 ▾ DOC

Регистрационная карта - БелИСА

6 авг. 2009 г. — Победителей, 7, 220004, г. Минск. Кому: ГУ «БелИСА». Гриф ограничения доступа (отметить). Коммерческая тайна, **Для служебного пользования** ...

<https://www.bsmu.by> > universitet > nauka ▾ DOC

Информационная карта - БелИСА

6 авг. 2009 г. — Победителей, 7, 220004, г. Минск. Кому: ГУ «БелИСА». Гриф ограничения доступа (отметить). Коммерческая тайна, **Для служебного пользования** ...

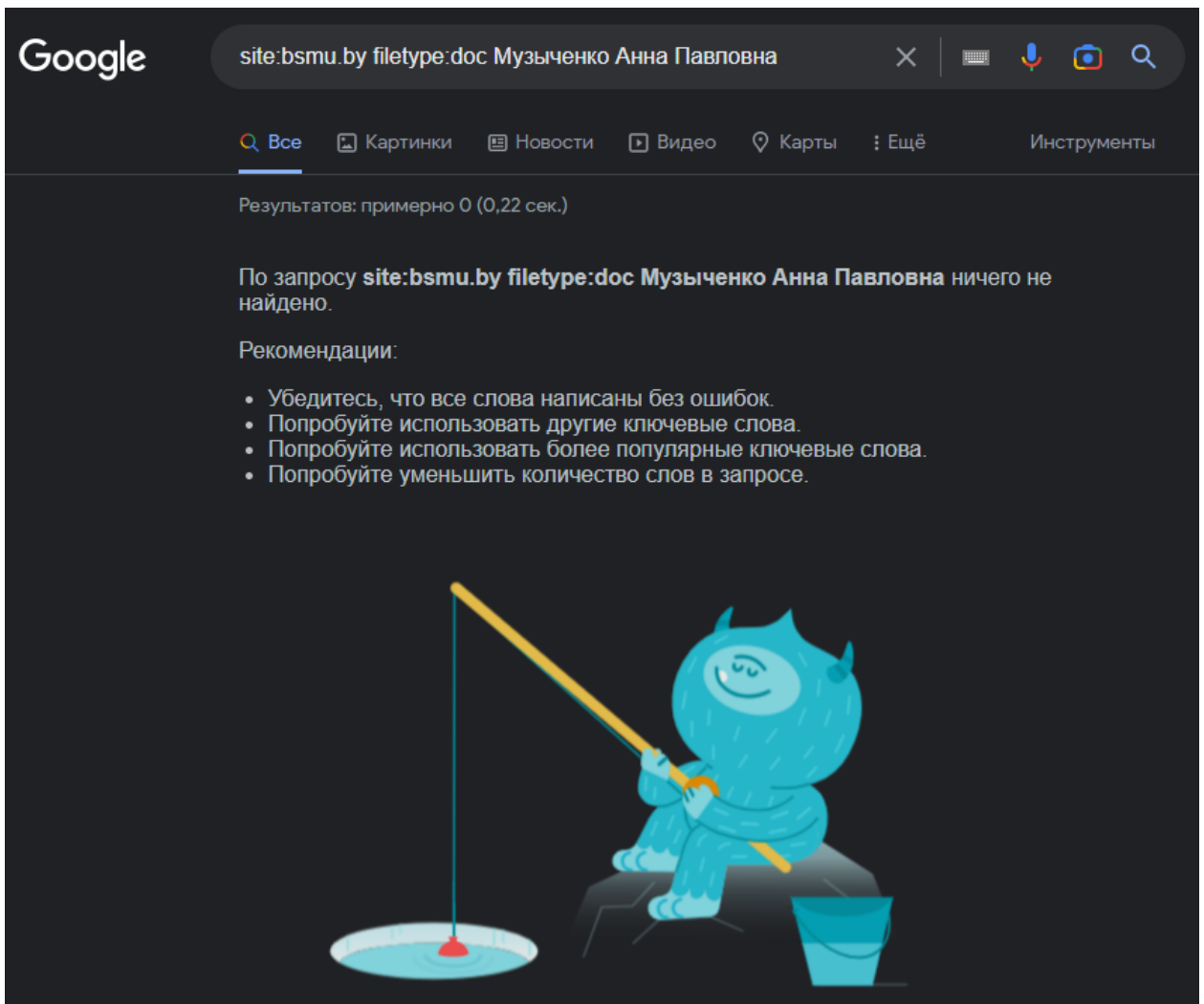
Результатов: примерно 0 (0,20 сек.)

По запросу **site:bsmu.by filetype:doc секретно** ничего не найдено.

Рекомендации:

- Убедитесь, что все слова написаны без ошибок.
- Попробуйте использовать другие ключевые слова.
- Попробуйте использовать более популярные ключевые слова.
- Попробуйте уменьшить количество слов в запросе.





Шаг 7. Используя веб-инструмент traceroute, расположенный на веб-ресурсе <http://network-tools.com>, определим маршруты прохождения IP-дейтаграмм до исследуемой сети.

Traceroute Check for: **195.50.7.146**

traceroute to 195.50.7.146 (195.50.7.146), 10 hops max, 60 byte packets

```
1 216.182.237.221 (216.182.237.221) 7.953 ms 216.182.237.219 (216.182.237.219) 29.256 ms 216.182.237.213 (216.182.237.213) 7.268 ms
2 100.65.19.64 (100.65.19.64) 70.187 ms 100.65.19.32 (100.65.19.32) 70.272 ms 100.65.18.64 (100.65.18.64) 98.697 ms
3 100.66.8.136 (100.66.8.136) 17.488 ms 100.66.8.122 (100.66.8.122) 20.634 ms 100.66.8.218 (100.66.8.218) 15.647 ms
4 100.66.11.200 (100.66.11.200) 14.505 ms 100.66.11.96 (100.66.11.96) 14.876 ms 100.66.10.74 (100.66.10.74) 17.386 ms
5 241.0.6.134 (241.0.6.134) 0.424 ms 241.0.6.137 (241.0.6.137) 0.498 ms 241.0.6.142 (241.0.6.142) 0.476 ms
6 240.0.176.24 (240.0.176.24) 0.623 ms 240.0.176.23 (240.0.176.23) 0.290 ms 240.0.176.17 (240.0.176.17) 0.312 ms
7 242.2.45.97 (242.2.45.97) 5.573 ms 242.2.44.225 (242.2.44.225) 4.624 ms 242.2.45.1 (242.2.45.1) 0.520 ms
8 52.93.237.213 (52.93.237.213) 2.654 ms 52.93.237.211 (52.93.237.211) 2.230 ms 72.21.222.16 (72.21.222.16) 1.601 ms
9 52.93.237.244 (52.93.237.244) 2.334 ms 150.222.31.20 (150.222.31.20) 1.863 ms 52.93.237.228 (52.93.237.228) 1.978 ms
10 150.222.30.105 (150.222.30.105) 1.475 ms 150.222.30.113 (150.222.30.113) 1.503 ms 150.222.30.117 (150.222.30.117) 1.403 ms
```

Вывод: в ходе лабораторной работы изучили методы и средства сбора предварительной информации в Интернет об анализируемой компьютерной сети.