Гомельский Государственный Университет
им. Ф. Скорины

Лабораторная работа №1.
Сбор предварительной информации

Проверил:
Грищенко В.В.

Студент МС – 42:
Кузнецов Ю.В.

г. Гомель

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

Постановка задачи: выполнить предварительный сбор информации о домене bru.by. Работа выполняется на АРМ, имеющем доступ в сеть Интернет.

Последовательность действий

Шаг 1. Перейти по адресу https://whois.by. Указать в строке поиска в базе данных домен bru.by. Проанализировать полученные данные. Найти DNS-имена. Проанализировать данные по администраторам и контактным лицам организации. Найти используемые почтовые адреса.

```
Domain Name: bru.by
Registrar: Reliable Software, Ltd
Org: Межгосударственное образовательное учреждение высшего образования "Белорусско-Российский университет"
Country: BY
Address: 212000, г.Могилев, пр.Мира, д.43
Registration or other identification number: 700008843
Phone: +375222258436
Email: HIDDEN! Details are available at http://www.cctld.by/whois/
Name Server: ns1.bru.by
IP Address: 82.209.221.3
Name Server: ns2.bru.by
IP Address: 178.124.158.150
Updated Date: 2020-03-24
Creation Date: 2008-07-24
Expiration Date: 2022-04-27
-------------------------------------------
Service provided by Reliable Software, Ltd.

Домен: bru.by
Регистратор: Reliable Software, Ltd
Org: Межгосударственное образовательное учреждение высшего образования "Белорусско-Российский университет"
Country: BY
Address: 212000, г.Могилев, пр.Мира, д.43
Registration or other identification number: 700008843
Phone: +375222258436
Email: HIDDEN! Details are available at http://www.cctld.by/whois/
Сервер: ns1.bru.by
IP Address: 82.209.221.3
Сервер: ns2.bru.by
IP Address: 178.124.158.150
Дата изменения: 2020.03.24 00:00:00 MSK
Дата регистрации: 2008.07.24 00:00:00 MSD
Дата окончания: 2022.04.27 00:00:00 MSK
-------------------------------------------
Service provided by Reliable Software, Ltd.
```

Шаг 2. Перейти по адресу http://network-tools.com/nslook. Задать параметры: домен – bru.by, тип запроса – ANY. Определить почтовый сервер организации.

```
Name    TTL Until Refresh   Class   Type    Data
bru.by. 3600    IN  A   82.209.221.3
bru.by. 3600    IN  NS  ns2.bru.by.
bru.by. 3600    IN  NS  ns1.bru.by.
bru.by. 3600    IN  SOA ns1.bru.by. root.bru.by. 401 900 600 86400 3600
bru.by. 3600    IN  MX  10 mailhub.bru.by.
bru.by. 3600    IN  TXT "v=spf1 mx include:_spf.elasticemail.com -all"
```

Шаг 3. Выполнить предыдущие проверки, используя средства nslookup, host и dig.

```
dig bru.by

; <<>> DiG 9.11.3-1ubuntu1.3-Ubuntu <<>> bru.by
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56540
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;bru.by.                IN  A

;; ANSWER SECTION:
bru.by.         2555    IN  A   82.209.221.3

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Sep 29 12:51:05 +03 2020
;; MSG SIZE  rcvd: 51
```

```
id 35520
opcode QUERY
rcode NXDOMAIN
flags QR RD RA
;QUESTION
http://bru.by/. IN A
;ANSWER
;AUTHORITY
. 86396 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2020092900 1800 900 604800 86400
;ADDITIONAL

3.3) host (cmd)

 host bru.by
bru.by has address 82.209.221.3
```

Шаг 4. Определить DNS-имена и роли узлов из выделенных диапазонов IP-адресов. Использовать веб-средства http://dnsstuff.com.

DNSreport Results for bru.by

Export

Overall Results: 1 FAIL | 5 WARNING | 27 PASS | 5 INFO

PARENT

Status	Test Name	Information
PASS	Parent zone provides NS records	Parent zone exists and provides NS records. This is good because some domains, usually third or fourth level domains, such as 'example.co.uk' do not have a direct parent zone. This is legal but can cause confusion. The NS Records provided are (nameserver | IP Address | TTL): ns1.bru.by. | 82.209.221.3 ns2.bru.by. | 178.124.158.150
PASS	Number of nameservers	At least 2 (RFC2182 section 5 recommends at least 3), but fewer than 8 NS records exist (RFC1912 section 2.8 recommends that you have no more than 7). This meets the RFC minimum requirements, but is lower than the upper limits that some domain registrars have on the number of nameservers. A larger number of nameservers reduce the load on each and, since they should be located in different locations, prevent a single point of failure. The NS Records provided are: ns1.bru.by. | 82.209.221.3 | TTL=3600 ns2.bru.by. | 178.124.158.150 | TTL=3600

NS

Status	Test Name	Information
PASS	Unique nameserver IPs	All nameserver addresses are unique. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data: ns1.bru.by. | 82.209.221.3 ns2.bru.by. | No Glue
PASS	All nameservers respond	All nameservers responded. We were able to get a timely response for NS records from your nameservers, which indicates that they are running correctly and your zone (domain) is valid. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data: ns1.bru.by. | 82.209.221.3 ns2.bru.by. | No Glue
FAIL	Open DNS servers	Some or all nameservers responded to recursive queries. This should be addressed as soon as possible. Open DNS servers (i.e. externally facing DNS servers that answer recursively) increase the chances of cache poisoning, can degrade performance of your DNS, and can cause your DNS servers to be used in an attack (read RFC5358 section 4 for recommended nameserver configuration). The nameservers that responded to recursive queries are: ns1.bru.by. | 82.209.221.3 [test] See this page for info on closing open DNS servers
PASS	All nameservers authoritative	All nameservers answered authoritatively for the zone. This indicates that the zones for this domain are set up correctly on your nameservers and that we should be able to get good responses to further queries.
PASS	NS list matches parent list	NS list matches list from parent zone. This indicates that your parent nameservers are 'aware' of the correct authoritative nameservers for your domain. This ensures less overhead for DNS queries, because an extra DNS resolution step is not required.
PASS	NS address list matches parent zone	NS addresses matches list from parent zone. This indicates that your parent nameservers are 'aware' of the correct authoritative nameservers for your domain. This ensures less overhead for DNS queries, because an extra DNS resolution step is not required.
PASS	Stealth nameservers	No stealth nameservers discovered. There is very little chance that there will be 'confusion' when resolving your domain records from the parent nameservers. There appear to be no 'extra' nameservers listed that the parent might try to refer to and cause DNS resolution delays.
INFO	Stealth nameservers respond	No stealth nameservers to test. This is simply a note to indicate that you do not have any stealth nameservers to test, which is what is normally expected of domains.
PASS	TCP allowed	All nameservers respond to queries via TCP. It is important that your DNS servers respond to both TCP and UDP connections. TCP Port 53 is used for large queries and responses, zone transfers, and is part of the DNSSEC standard.
WARN	Nameserver software version	One or more nameservers responded to version queries. This can be considered a breach of security. If a malicious person or program had access to a version-specific exploit for your DNS server, displaying the version info openly will make their attack much easier. This should be removed or obscured. The nameservers that responded to version queries are: 82.209.221.3 responded with "Microsoft DNS 6.1.7601 (1DB15F75)"
PASS	All nameservers have identical records	All of your nameservers are providing the same list of nameservers.
PASS	All nameserver addresses are public	All of your nameserver addresses are public. If there were any private IPs, they would not be reachable, causing DNS delays.

SOA

Status	Test Name	Information
PASS	SOA record check	All nameservers provided a SOA record for the zone. This is good because your nameservers should be configured in a master slave relationship, which allows uniform updates and agreement of resource record data. The SOA records provided are: Primary nameserver: ns1.bru.by. Hostmaster E-mail address: root@bru.by. Serial #: 401 Refresh: 900 Retry: 600 Expire: 86400 Minimum: 3600
PASS	SOA serial agreement	All nameserver SOAs agree on the serial number. This means that your nameservers are using the same data (unless you have different sets of data with the same serial number, which would be very bad)!
WARN	SOA field check	One or more SOA fields are outside recommended ranges. Values that are out of specifications could cause delays in record updates or unnecessary network traffic. The SOA fields out of range are: serial | 401 | SERIAL - we check that your serial number matches the recommended format found in RFC1912 section 2.2. refresh | 900 | REFRESH - expected range should be between 1200 and 43200 seconds. retry | 600 | RETRY - needs to be less than or equal to half the REFRESH. expire | 86400 | EXPIRE - RFC1912 suggests a value between 1209600 to 2419200.

MX

Status	Test Name	Information
WARN	MX records check	Only one MX record exists within the zone. This is ok, but it is a better practice to have at least two mail servers operating on a domain, to ensure more reliable mail deliverability. The MX record provided is: preference = 10 mailhub.bru.by. [178.124.158.150]
PASS	Differing mailserver addresses	All hostnames referenced by MX records resolve to different IP addresses. It is important that you have different IP addresses for your MX records, as it ensures that there is not a single point of failure for mail delivery. The hostname IP addresses are: 82.209.221.3 has mailhub.bru.by. | 178.124.158.150 listed.
PASS	Reverse DNS entries for MX servers	All addresses referenced by MX records have matching reverse DNS entries. This is good because many mail platforms and spam-prevention schemes require consistency between MX hostnames and IP address PTR records, aka reverse DNS.

MAIL

Status	Test Name	Information
PASS	All IP addresses public	All mailserver IP addresses are public. If there were any private IPs, they would not be reachable.
PASS	Connect to mail server	All connections to Mailservers port 25 are successful. The standard port for SMTP transactions is 25, so your servers should be operating on that port. The Mailserver addresses are: 178.124.158.150 | connected
PASS	SMTP banner	All banner greetings comply with SMTP specified format. 178.124.158.150 | 220 mailhub.bru.by Microsoft ESMTP MAIL Service ready at Tue, 29 Sep 2020 09:57:30 +0300
PASS	SMTP greeting	Mailserver greetings are RFC5321 compliant. This ensures that your mail server is easily recognizable by other mail servers. 178.124.158.150 | 250-mailhub.bru.by Hello [74.115.13.4]250-SIZE250-PIPELINING250-DSN250-ENHANCEDSTATUSCODES250-AUTH NTLM LOGIN250-8BITMIME250-BINARYMIME250 LOCHOWING
PASS	Acceptance of NULL sender	Mailserver accepts mail from the null sender address. Mailservers are required to accept mail from a null sender, because this is how delivery status notifications/DSNs are delivered. 178.124.158.150 | 250 2.1.0 Sender OK
WARN	Acceptance of postmaster	Mailserver rejected mail to postmaster. Mailservers are required by RFC822 6.3, RFC1123 5.2.7, and RFC2821 4.5.1 to have a valid postmaster address that is accepting mail. The Mailserver provided is: 178.124.158.150 | timed out during interaction
WARN	Acceptance of abuse	Mailserver rejected mail to abuse. Mailservers are required by RFC2142 Section 2 to have a valid abuse address that is accepting mail. 178.124.158.150 | timed out during interaction
INFO	Acceptance of address literals	Mailserver rejected mail to address literals. Mailservers are technically required by RFC1123 section 5.2.17 to accept mail to domain literals (i.e. IP addresses instead of domains). This ensures backwards compatibility and can help with delivery in certain non-optimal situations. Hte a DNS server being down/unresponsive. 178.124.158.150 | unexpected response to [RCPT TO: <postmaster@[178.124.158.150]>] | 550 5.7.1 Unable to relay
PASS	Open relay	Mailserver does not appear to be an open relay. This is good. It is important to make sure that external mail servers do not relay mail for domains they are not authoritative for, so that they cannot be abused by third-parties to send unauthorized mail. 178.124.158.150 | 550 5.7.1 Unable to relay

WWW

Status	Test Name	Information
INFO	WWW record check	Domain has a WWW hostname provided through one or more CNAME lookups, which will slow down clients attempting to resolve this host. www.bru.by. | bru.by. | 3600 bru.by. | 82.209.221.3 | 3600
PASS	Domain record	The domain literal has an address record, the records found are: bru.by. | 82.209.221.3 | 3600
PASS	IP Address(es) valid	All addresses are public. If there were any private IPs, they would not be reachable, causing problems reaching your web site.
PASS	WWW enabled	We connected to WWW, the title data found is: 82.209.221.3 : [page title not found]
PASS	SSL enabled	SSL is enabled. This is good since this will encrypt data that passes from your customer's computer to your website, helping to prevent hackers from using this data. The certificate data is: 82.209.221.3 : certificate issuer [C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3]; subject [CN = *.bru.by]

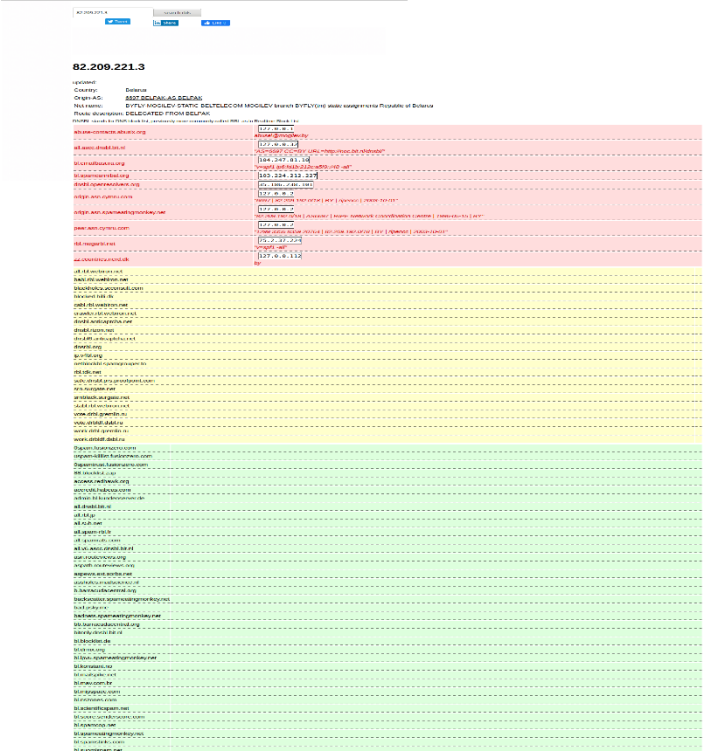
DNSSEC

Status	Test Name	Information
INFO	DNSSEC records check	No DNSSEC records created for this zone. Many major institutions and government agencies are planning to move to DNSSEC. You may want to consider an implementation plan for the zone specified. If you implemented DNSSEC for your zone we would be able to run further tests.

SPF

Status	Test Name	Information
INFO	SPF record check	This domain has an SPF record, or an SPF formatted TXT record. SPF usage may have a negligible impact on spam prevention and if implemented incorrectly cause serious mail delivery problems for remote users. This software does not check the content of your SPF record to test if it is well designed only that it exists. Your SPF record(s) for each nameserver is/are: "v=spf1 mx include:_spf.elasticemail.com -all"
PASS	SPF formatted TXT record exists	An SPF formatted TXT record was found. This configuration is in wide use as a verification mechanism. Note: this test does not verify the design of this record only that it exists (listing includes one for each nameserver). "v=spf1 mx include:_spf.elasticemail.com -all"
PASS	SPF value covers incoming mailservers	The SPF value allows mail delivery from all mailservers in the domain. The SPF results are: domain of bru.by designates 178.124.158.150 as permitted sender

Шаг 5. Проверить наличие узлов найденных сетей в базах данных спам-отправителей и бот-сетях, используя для этого веб-средства http://www.spamcop.net и http://rbls.org.

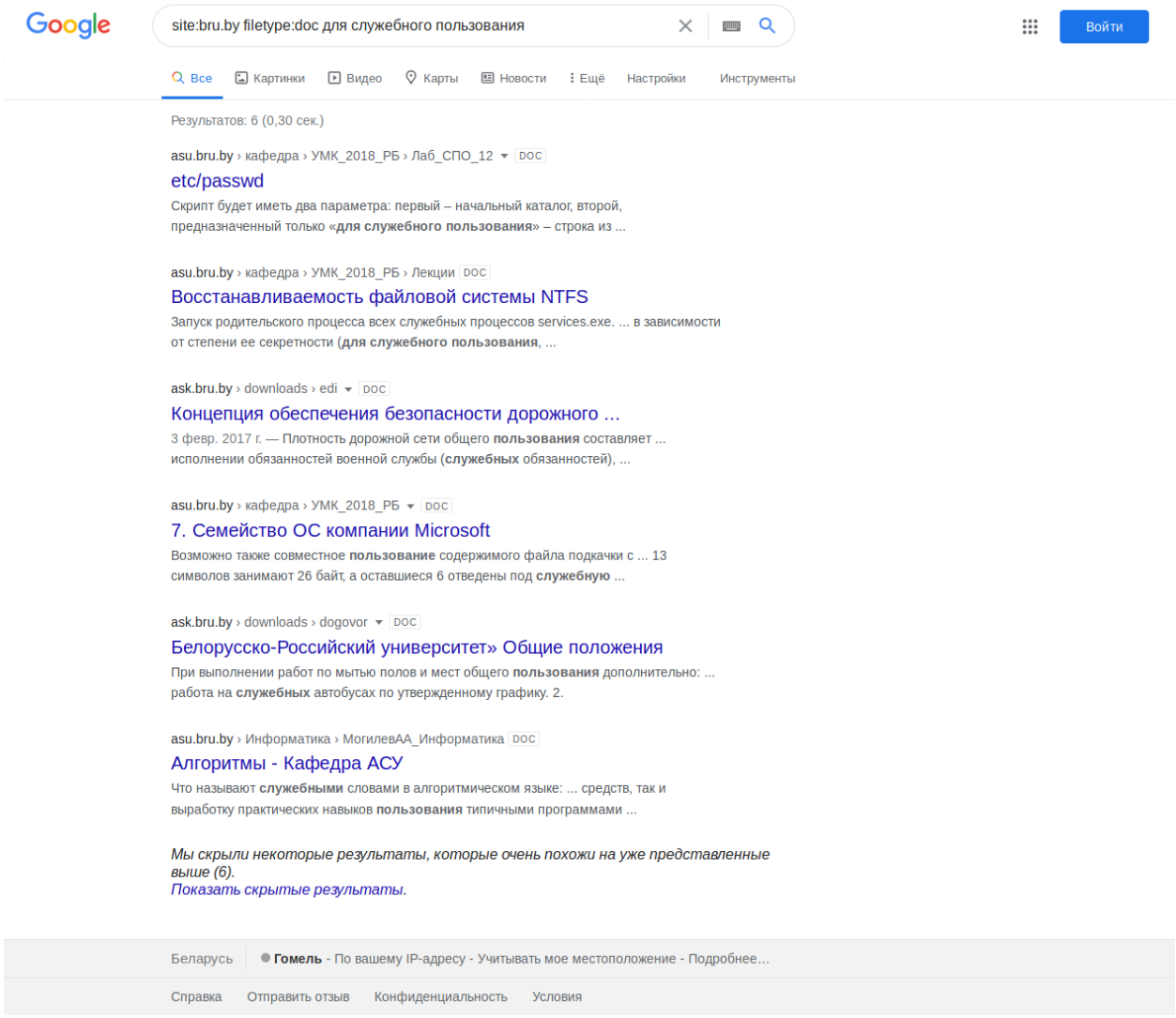


Шаг 6. Проверить возможность выполнения переноса зоны на первичном и вторичном DNS-серверах:

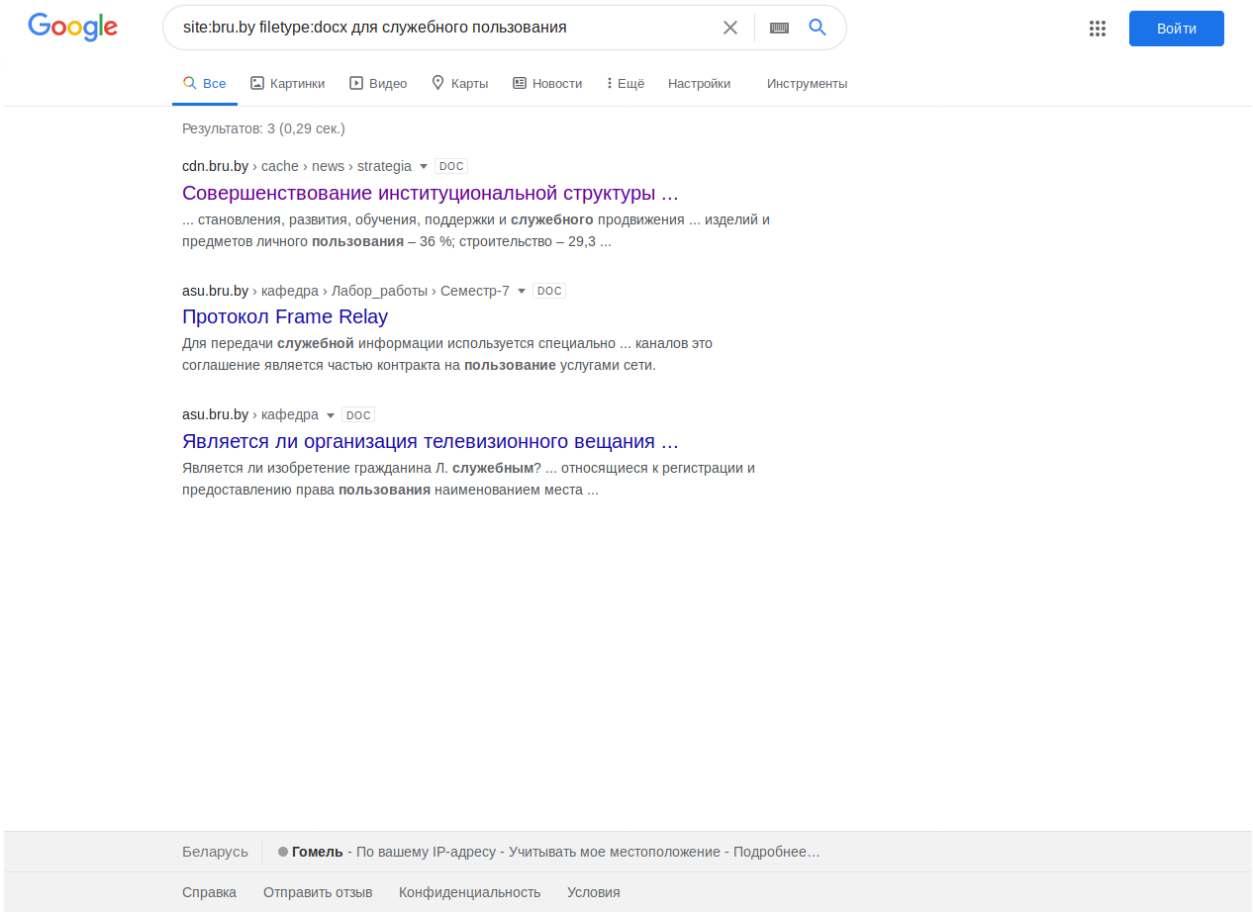
C:\nslookup
>server ns.bru.by
>set type=any
>bru.by

Шаг 7. Перейти по адресу http://google.ru. Задать следующие поисковые запросы и проанализировать результаты:

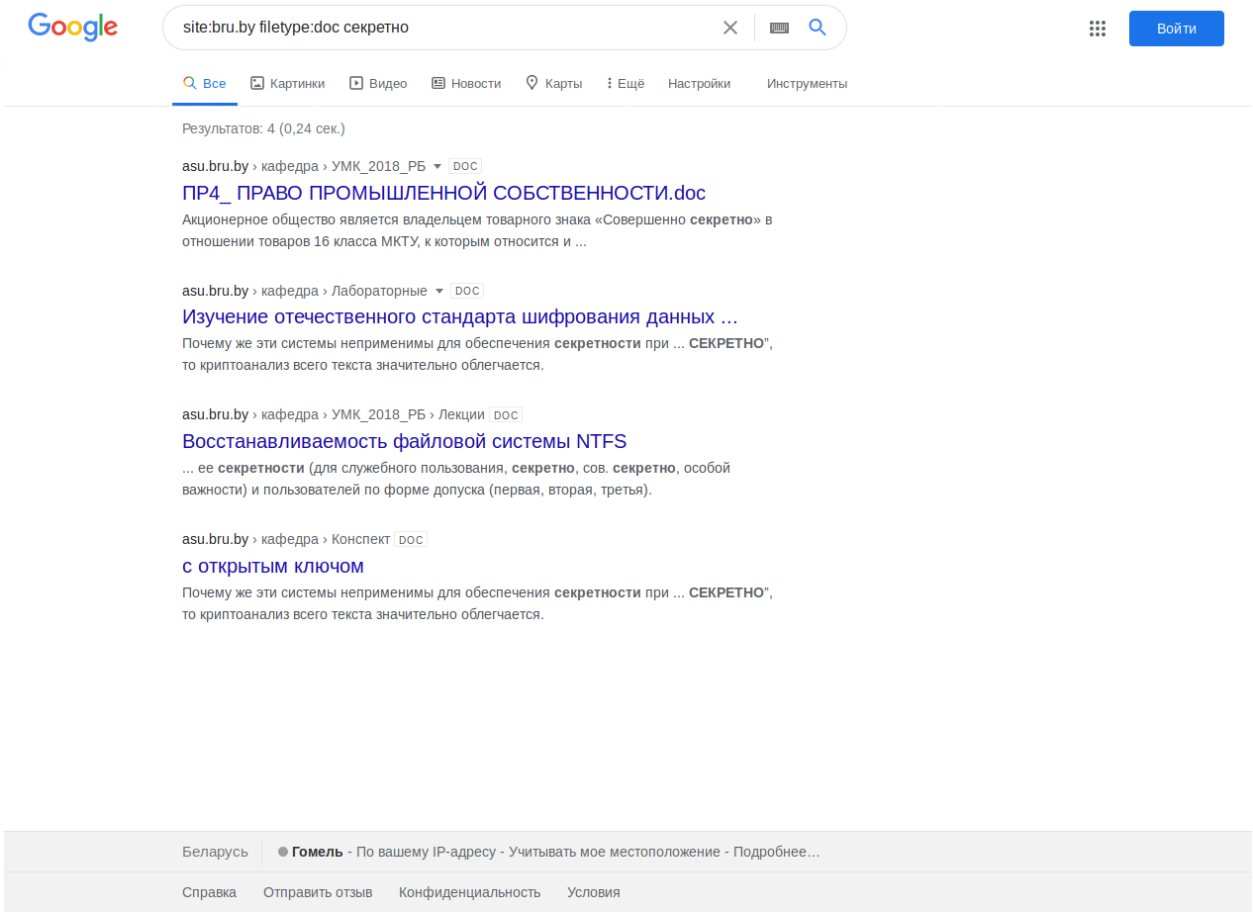
- «site:bru.by filetype:docx для служебного пользования»;



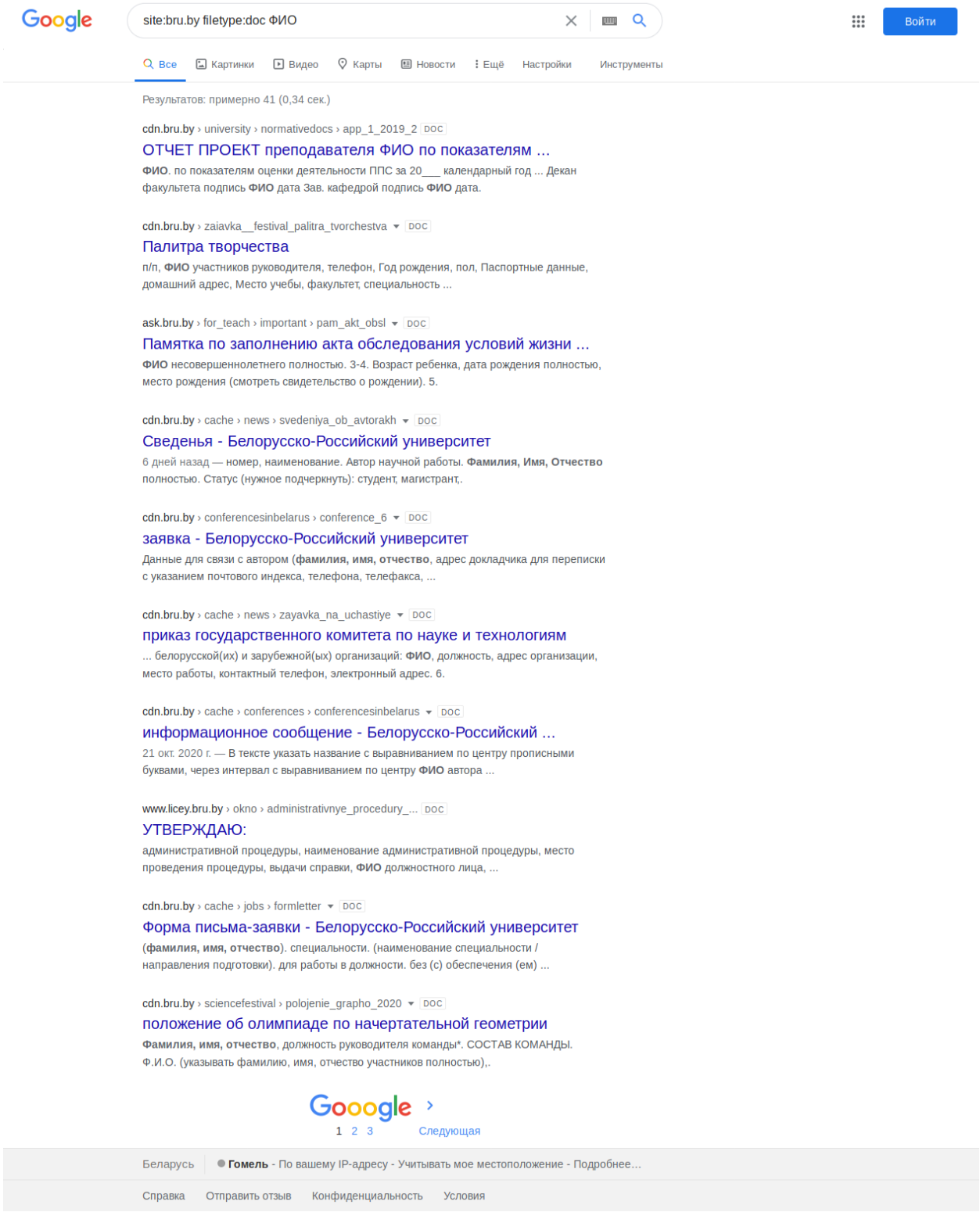
- «site:bru.by filetype:pdf для служебного пользования»;



- «site:bru.by filetype:doc секретно»;



- «site:bru.by filetype:doc ФИО».



Шаг 8. Используя веб-инструмент traceroute, расположенный на вебресурсе http://network-tools.com, определить маршруты прохождения IPдейтаграмм до исследуемой сети.

Traceroute Check for: **'82.209.221.3'**

traceroute to 82.209.221.3 (82.209.221.3), 10 hops max, 60 byte packets
1 45.79.12.201 (45.79.12.201) 0.536 ms 45.79.12.202 (45.79.12.202) 1.885 ms 1.938 ms
2 45.79.12.2 (45.79.12.2) 0.632 ms 0.596 ms 45.79.12.6 (45.79.12.6) 0.451 ms
3 dls-b22-link.telia.net (62.115.172.134) 0.903 ms 0.971 ms 0.873 ms
4 atl-b24-link.telia.net (62.115.120.112) 18.645 ms 18.634 ms 18.592 ms
5 ash-bb2-link.telia.net (62.115.125.129) 29.925 ms
e2432.ccr21.mci01.atlas.cogentco.com (154.54.3.134) 11.413 ms rest-bb1-
nk.telia.net (62.115.125.190) 32.335 ms
be2832.ccr42.ord01.atlas.cogentco.com (154.54.44.170) 23.458 ms prs-bb4-
nk.telia.net (62.115.122.158) 122.396 ms
be2832.ccr42.ord01.atlas.cogentco.com (154.54.44.170) 23.242 ms
ffm-bb2-link.telia.net (62.115.114.99) 121.050 ms
be2718.ccr22.cle04.atlas.cogentco.com (154.54.7.130) 29.802 ms 30.002 ms
8 be2993.ccr31.yyz02.atlas.cogentco.com (154.54.31.226) 36.829 ms ffm-b7-
link.telia.net (80.91.249.105) 123.745 ms ffm-b7-link.telia.net (80.91.247.73) 120.917 ms
9 rue-svc071499-lag003387.c.telia.net (213.248.96.179) 149.283 ms
be3260.ccr22.ymq01.atlas.cogentco.com (154.54.42.90) 45.615 ms rue-
svc071499-lag003387.c.telia.net (213.248.96.179) 148.670 ms
10 ie1.net.belpak.by (93.85.80.93) 150.980 ms
be3042.ccr21.lpl01.atlas.cogentco.com (154.54.44.161) 113.614 ms 113.393 ms