**Гомельский государственный университет**

**имени Франциска Скорины**

**Лабораторная работа №1.**

**Сбор предварительной информации**

**Выполнил Назаров Д. В.**

**Проверил Грищенко В. В.**

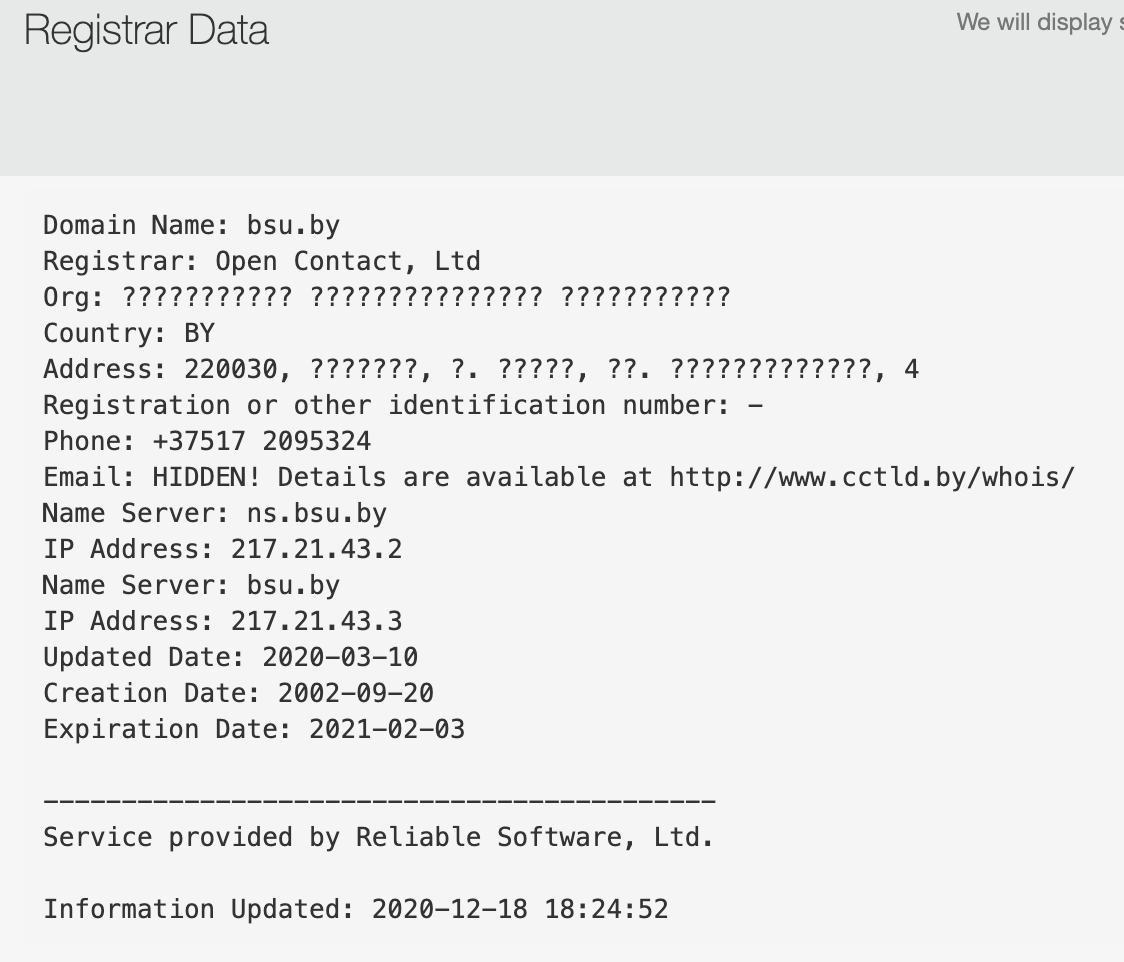
**г. Гомель 2020**

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

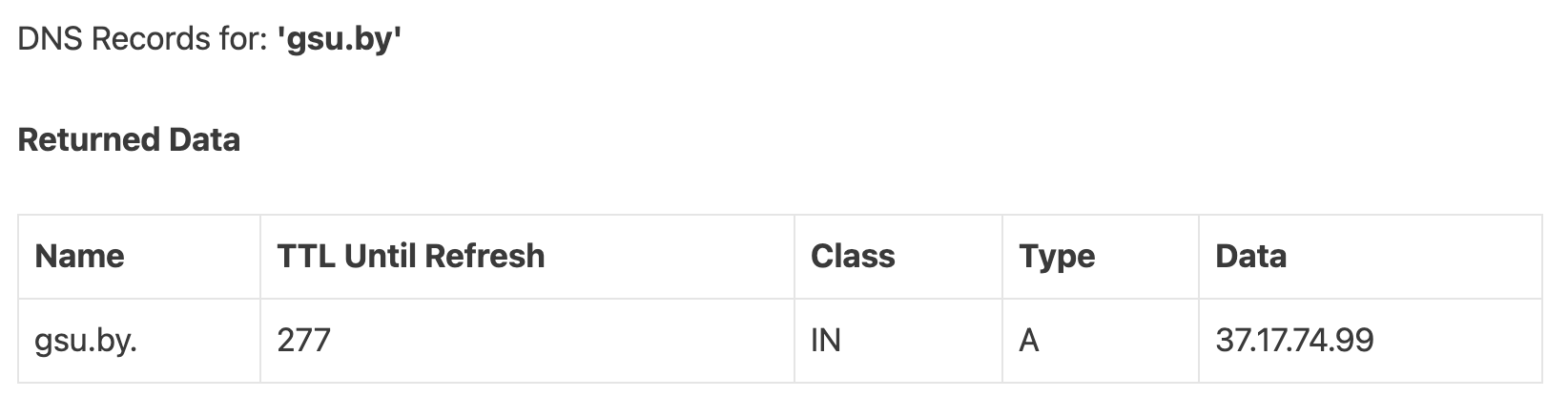
**Постановка задачи:** Выполнить предварительный сбор информации о домене bsu.by. Работа выполняется на АРМ, имеющем доступ в сеть Интернет.

**Последовательность действий**

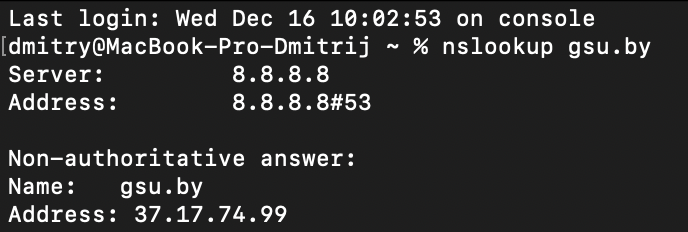
**Шаг 1.** Перейти по адресу https://whois.by. Указать в строке поиска в базе данных домен bsu.by. Проанализировать полученные данные. Найти DNS-имена. Проанализировать данные по администраторам и контактным лицам организации. Найти используемые почтовые адреса.

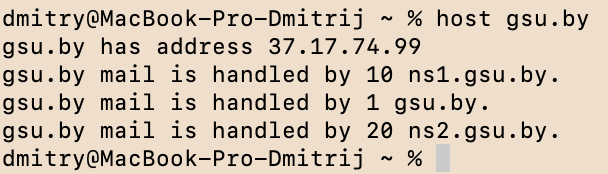


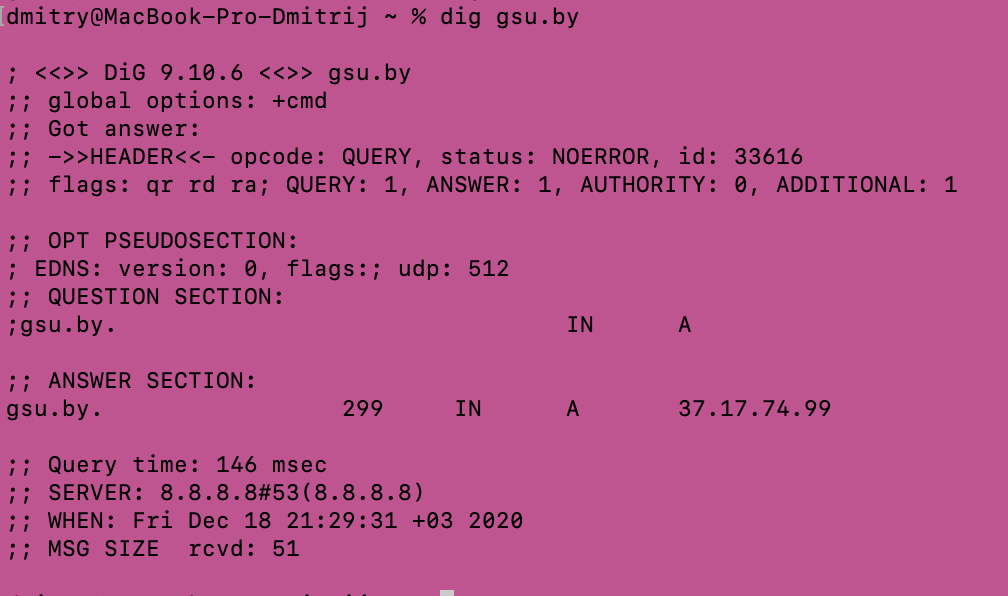
**Шаг 2.** Перейти по адресу <http://network-tools.com/nslook>. Задать параметры: домен – gsu.by, тип запроса – ANY. Определить почтовый сервер организации.



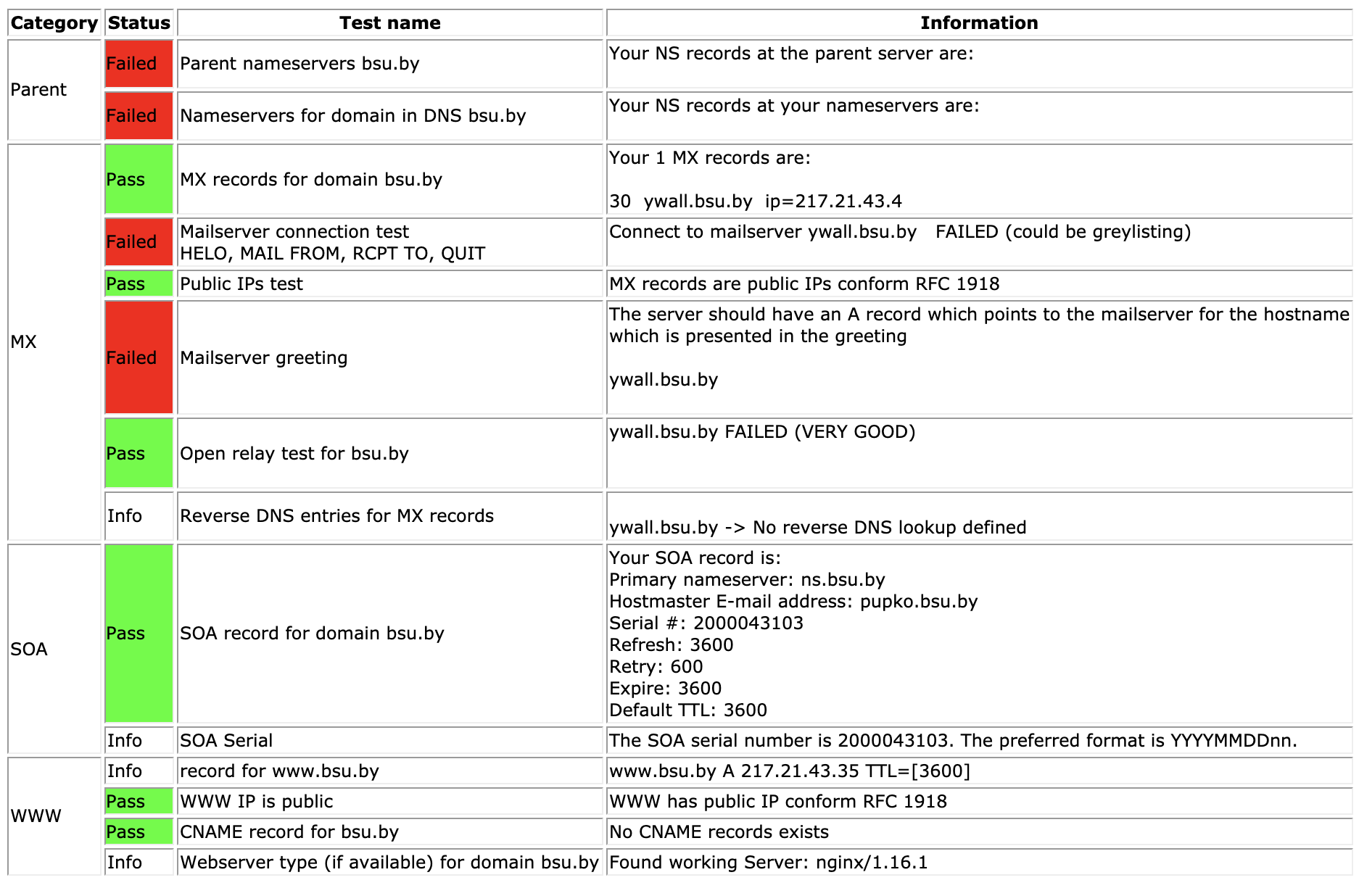
**Шаг 3.** Выполнить предыдущие проверки, используя средства nslookup, host и dig.







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



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

|  |  |
| --- | --- |
| fulldom.rfc-clueless.org | 127.0.0.1 |
| postmaster.rfc-clueless.org | 127.0.0.3 |

|  |  |
| --- | --- |
| contacts.abuse.net |  |
| ex.dnsbl.org |  |
| in.dnsbl.org |  |
| whois.rfc-clueless.org |  |

|  |  |
| --- | --- |
| 0spamurl.fusionzero.com |  |
| \_vouch.dwl.spamhaus.org |  |
| abuse.rfc-clueless.org |  |
| abuse.rfc-ignorant.org |  |
| bl.deadbeef.com |  |
| blacklist.netcore.co.in |  |
| bogusmx.rfc-clueless.org |  |
| bogusmx.rfc-ignorant.org |  |
| bsb.empty.us |  |
| bsb.spamlookup.net |  |
| dbl.spamhaus.org |  |
| dbl.suomispam.net |  |
| dnsbl.othello.ch |  |
| dnsrbl.swinog.ch |  |
| dob.sibl.support-intelligence.net |  |
| dsn.rfc-clueless.org |  |
| dsn.rfc-ignorant.org |  |
| dyndns.rbl.jp |  |
| elitist.rfc-clueless.org |  |
| fresh.spameatingmonkey.net |  |
| fresh10.spameatingmonkey.net |  |
| fresh15.spameatingmonkey.net |  |
| jwrh.dnsbl.net.au |  |
| mailsl.dnsbl.rjek.com |  |
| multi.surbl.org |  |
| nobl.junkemailfilter.com |  |
| postmaster.rfc-ignorant.org |  |
| rddn.dnsbl.net.au |  |
| reputation-domain.rbl.scrolloutf1.com |  |
| reputation-ns.rbl.scrolloutf1.com |  |
| rhsbl.rymsho.ru |  |
| rhsbl.scientificspam.net |  |
| rhsbl.sorbs.net |  |
| rhsbl.zapbl.net |  |
| ubl.nszones.com |  |
| uri.blacklist.woody.ch |  |
| uribl.abuse.ro |  |
| uribl.pofon.foobar.hu |  |
| uribl.spameatingmonkey.net |  |
| uribl.zeustracker.abuse.ch |  |
| urired.spameatingmonkey.net |  |
| url.rbl.jp |  |
| urlsl.dnsbl.rjek.com |  |
| zebl.zoneedit.com |  |

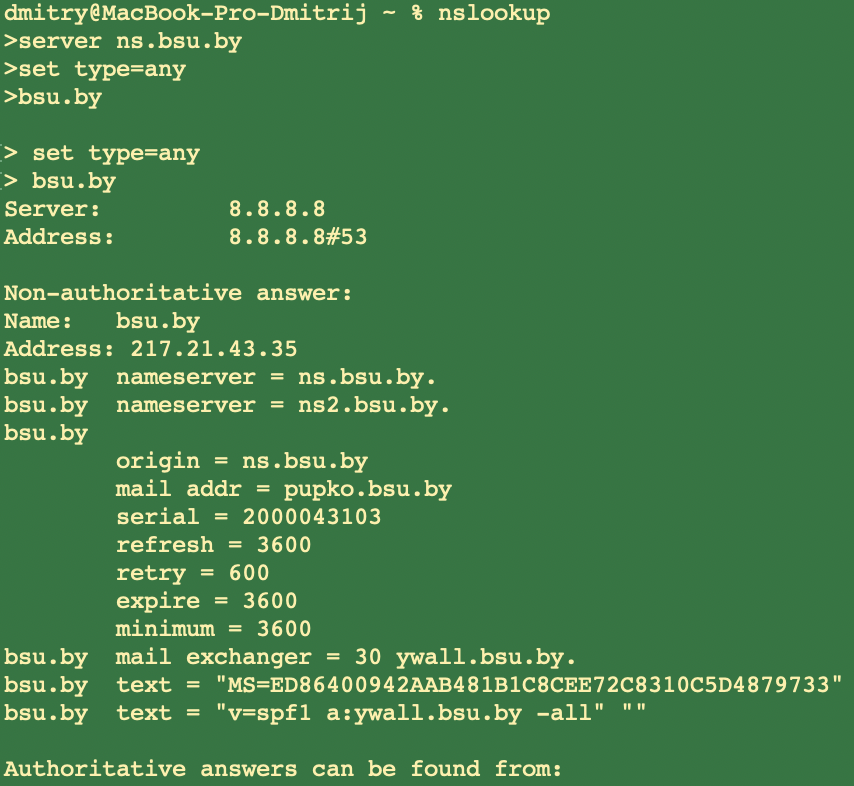
**Шаг 6.** Проверить возможность выполнения переноса зоны на первичном и вторичном DNS-серверах:

**C:\nslookup**

**>server ns.bsu.by**

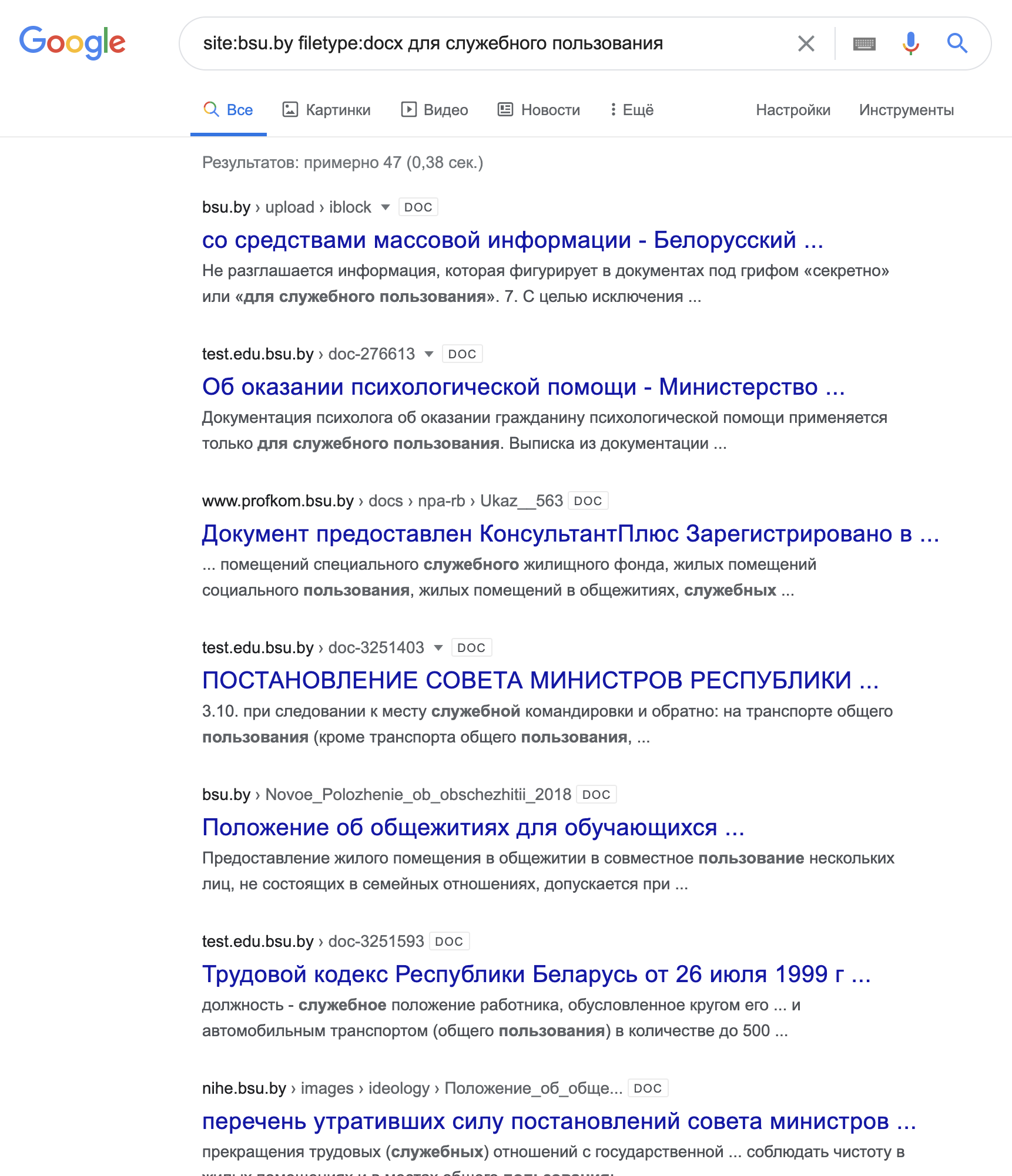
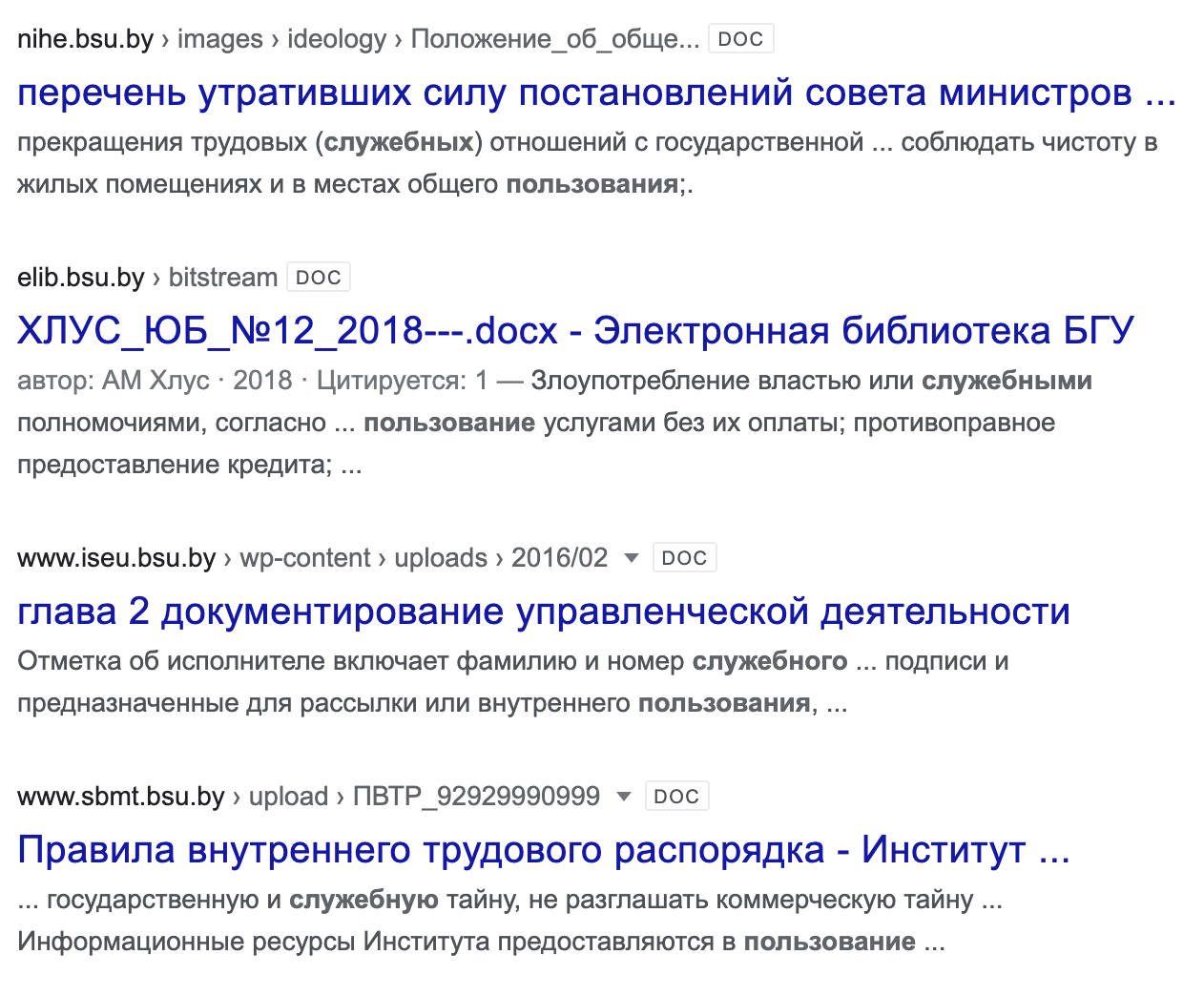
**>set type=any**

**>bsu.by**

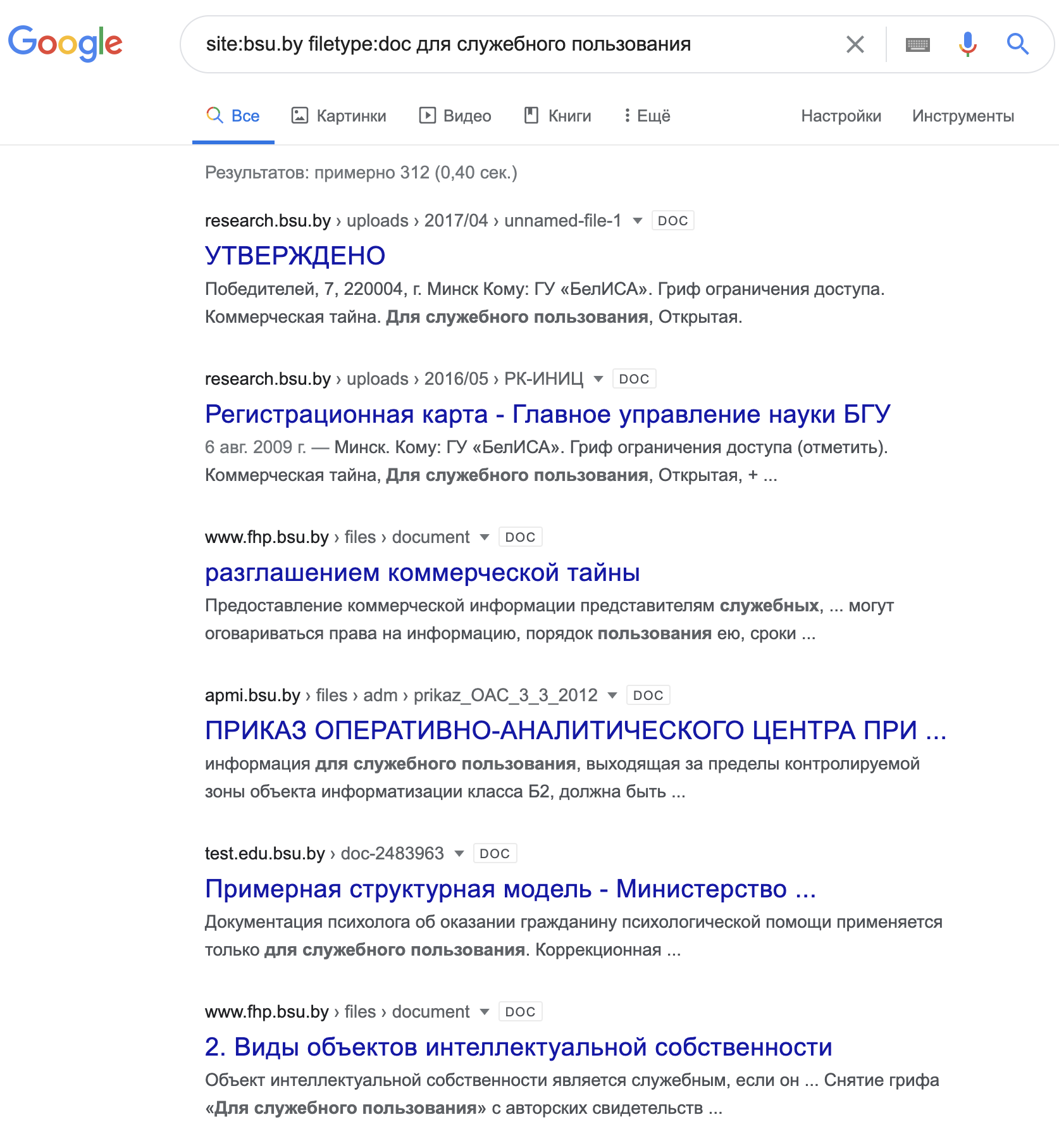
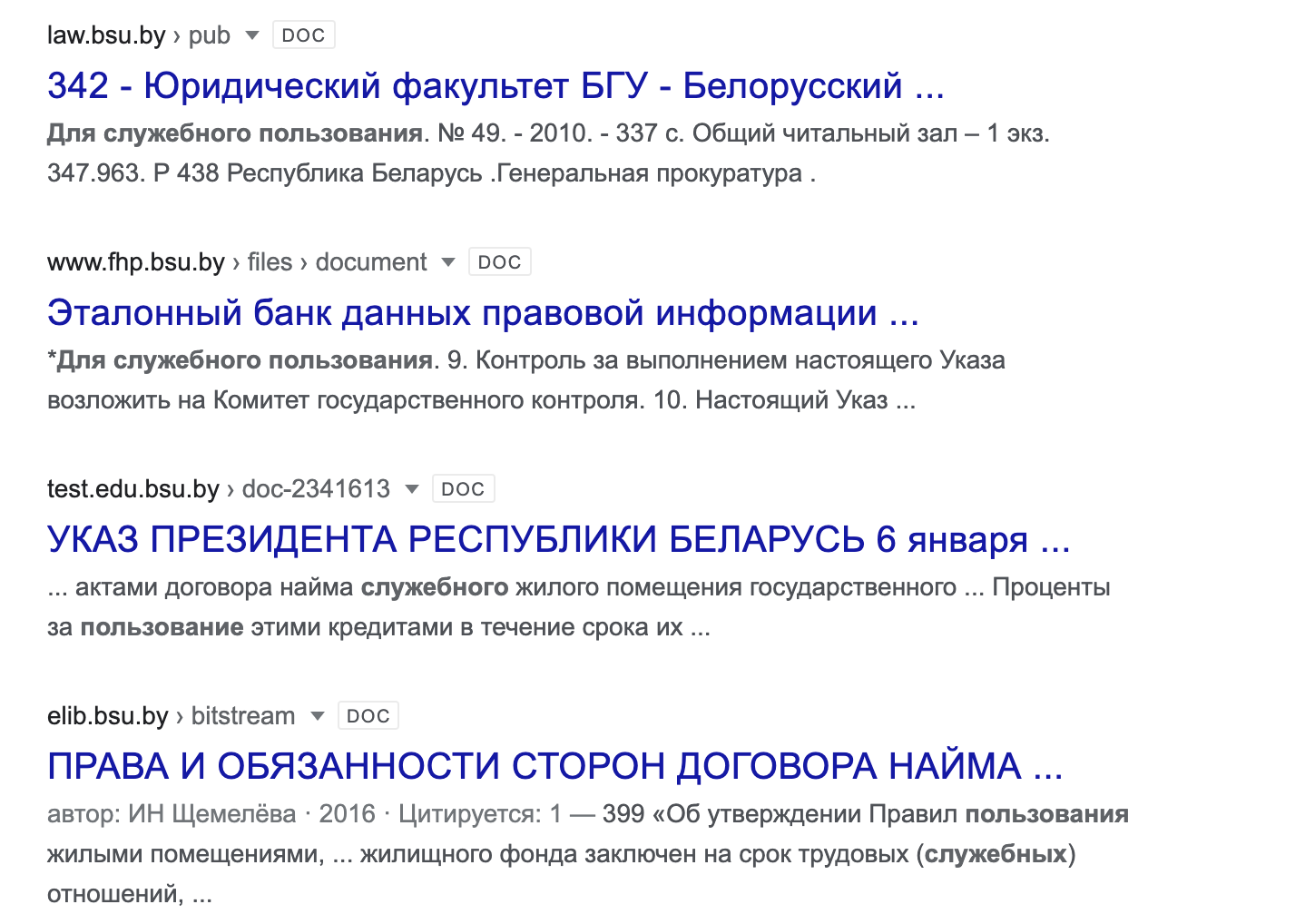
****

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

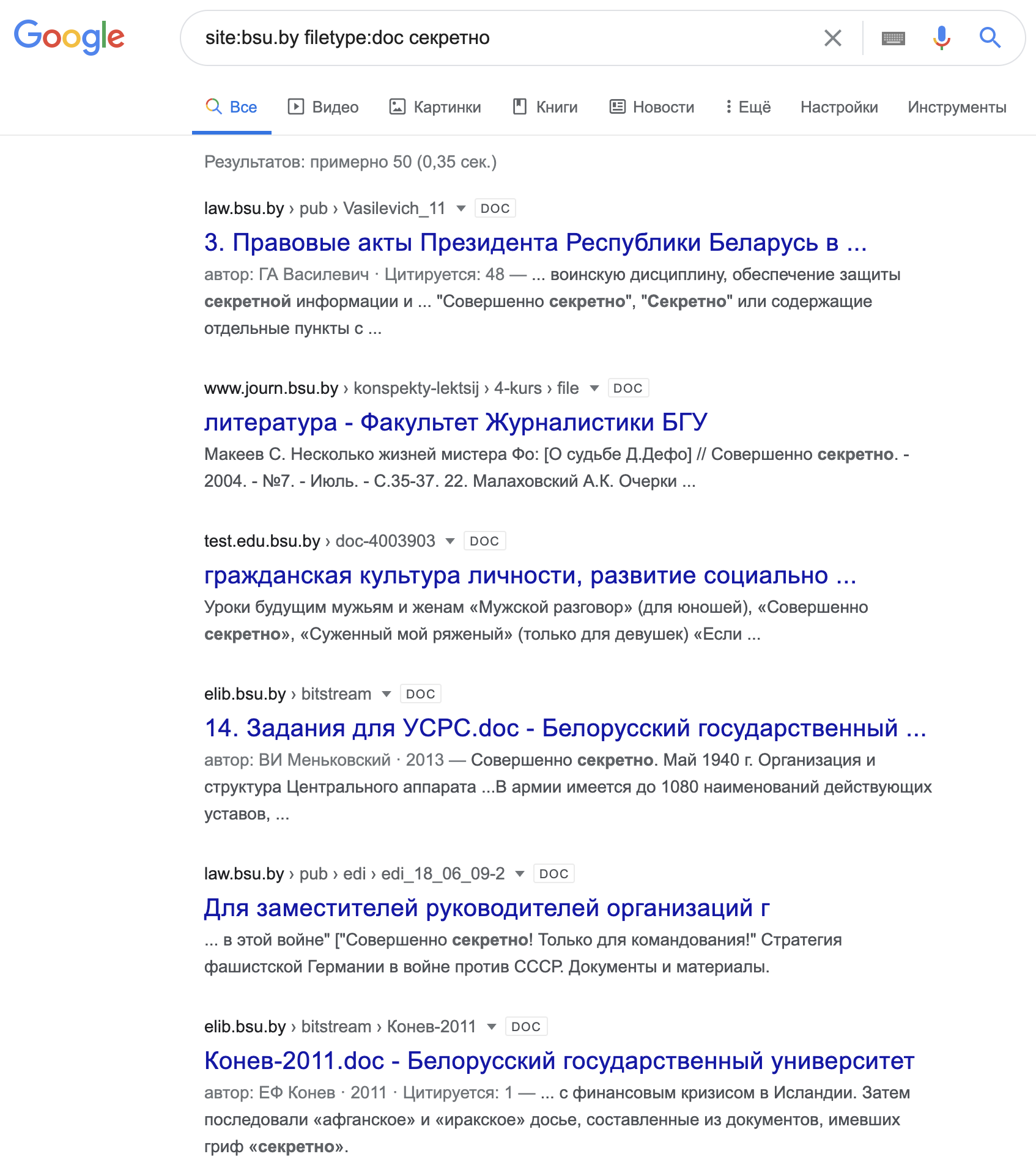
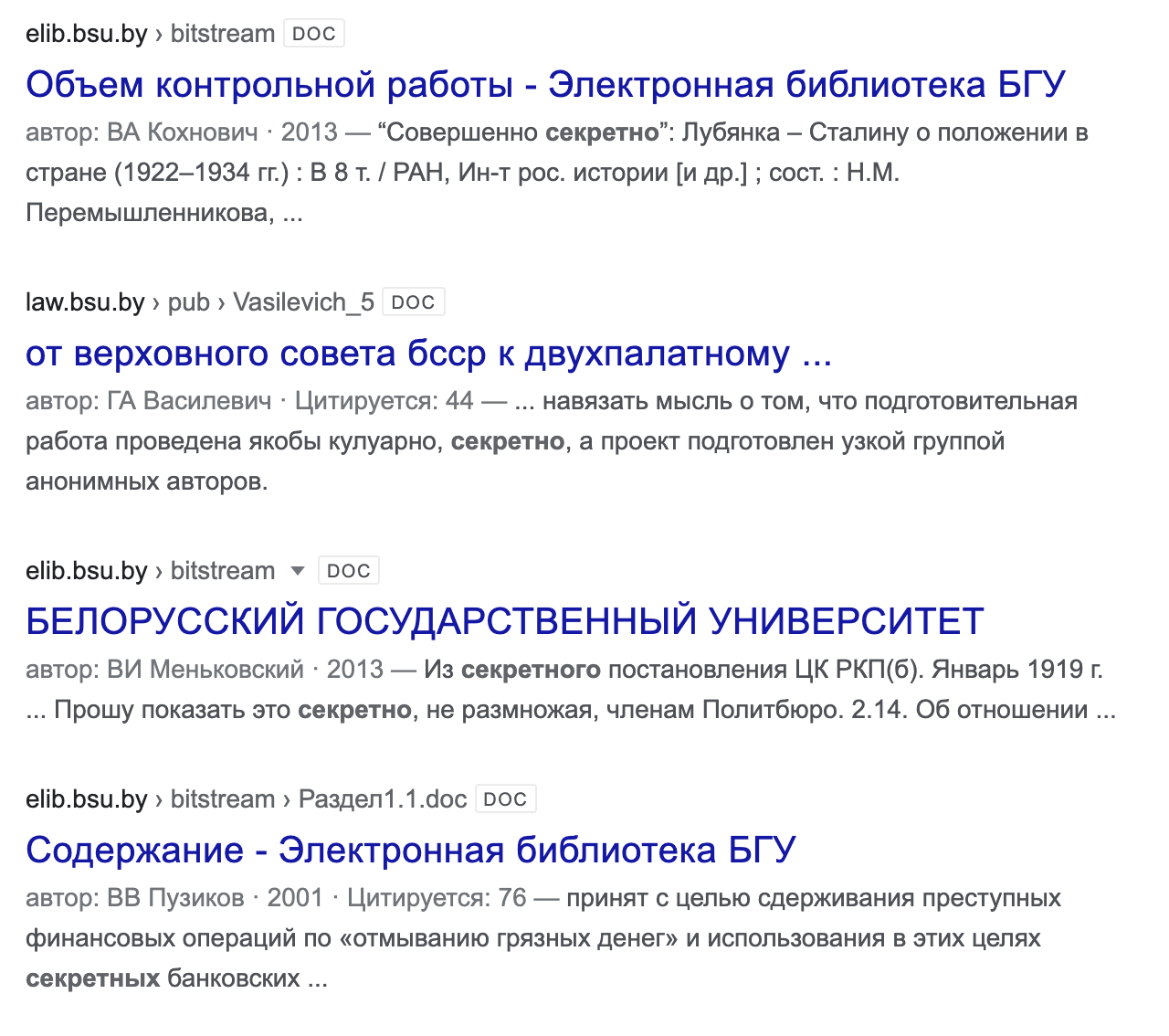
* «site:bsu.by filetype:docx для служебного пользования»;

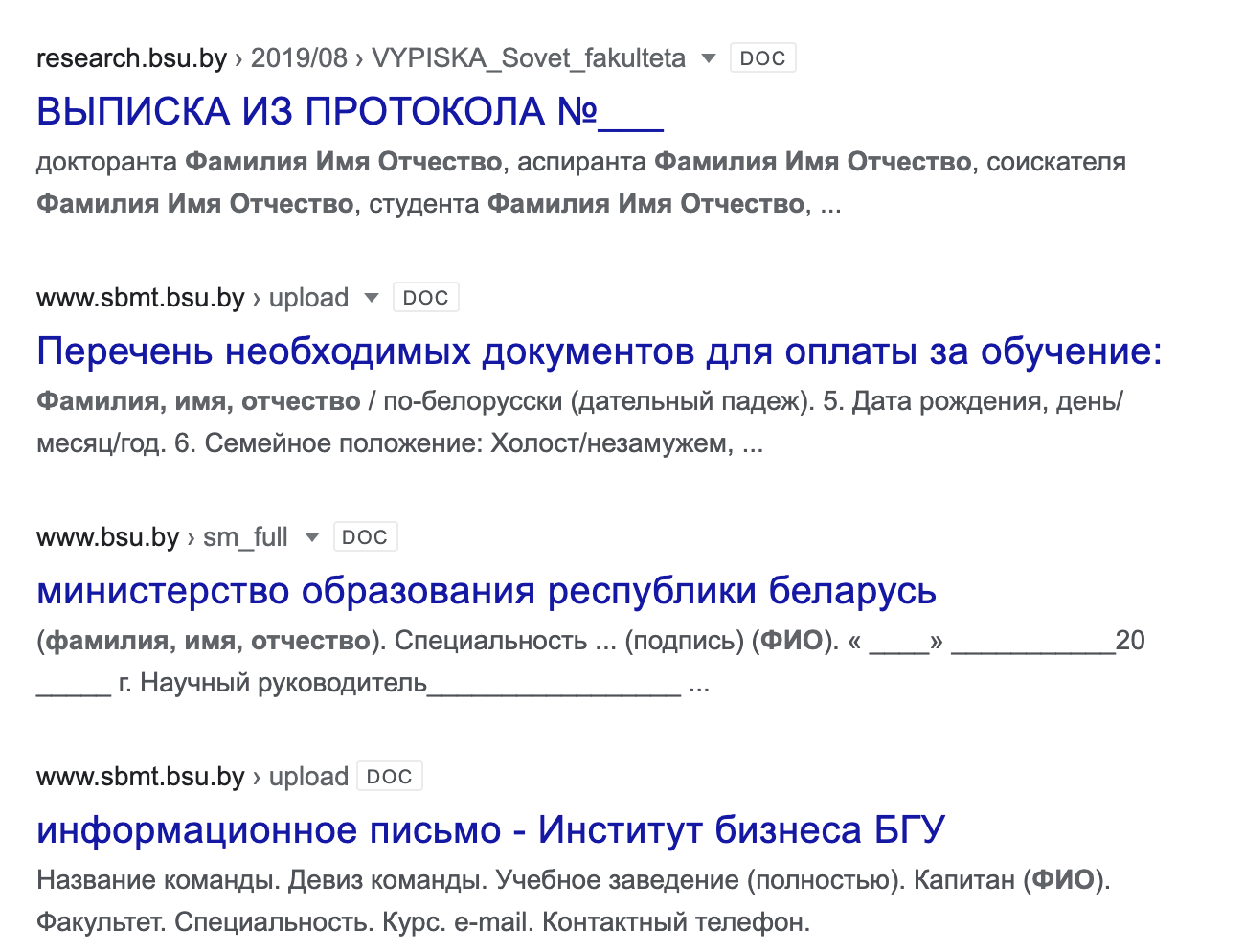
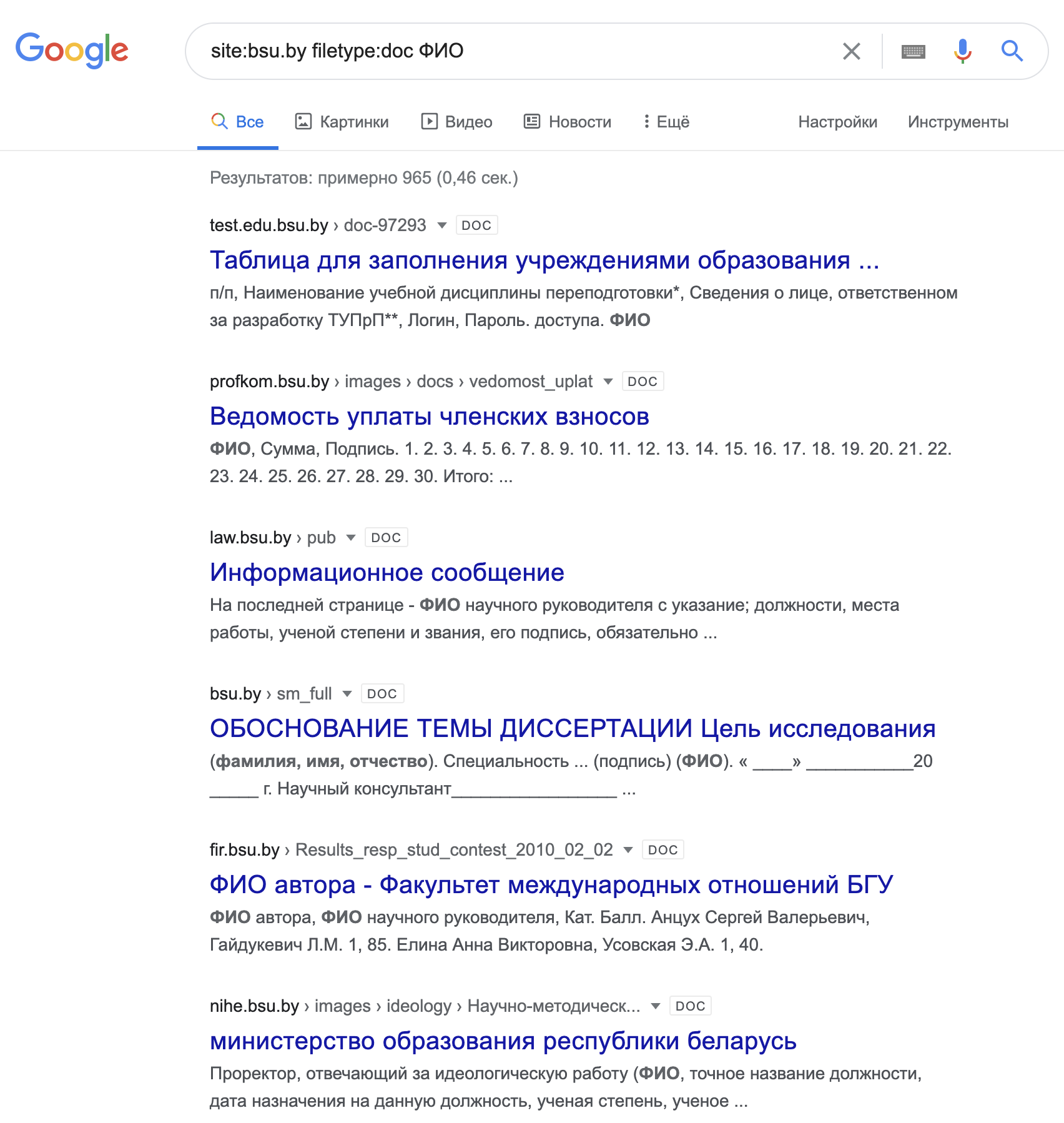
* «site:bsu.by filetype:doc для служебного пользования»;

* «site:bsu.by filetype:doc секретно»;

* «site:bsu.by filetype:doc ФИО»



**Шаг 8.** Используя веб-инструмент traceroute, расположенный на веб ресурсе http://network-tools.com, определить маршруты прохождения IP дейтаграмм до исследуемой сети.



**BSU.BY**

Domain Name: bsu.by

Registrar: Open Contact, Ltd

Org: Белорусский государственный университет

Country: BY

Address: 220030, Минский, г. Минск, пр. Независимости, 4

Registration or other identification number: -

Name Server: ns.bsu.by

IP Address: 217.21.43.2

Name Server: bsu.by

Updated Date: 2020-03-10

Creation Date: 2002-09-20

Expiration Date: 2021-02-03

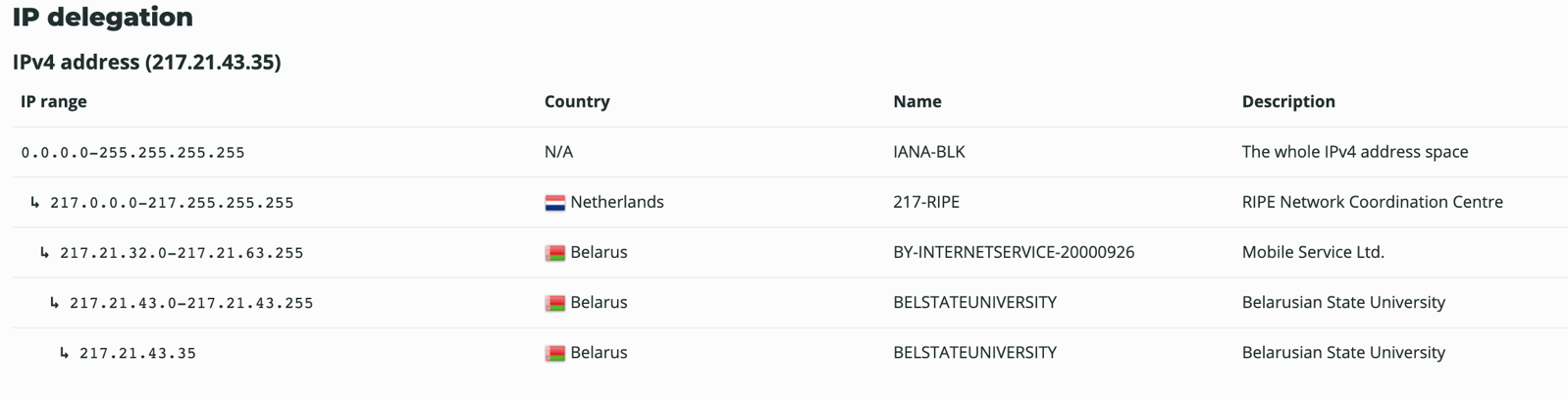
Registration or other identification number: -

Phone: +37517 2095324

Name Server: ns.bsu.by

|  |  |
| --- | --- |
| Web server | nginx/1.16.1 |
| Server Address | [http://bsu.by](http://bsu.by/) |
| cache-control | no-store, no-cache, must-revalidate |
| connection | close |
| content-encoding | gzip |
| content-type | text/html; charset=UTF-8 |
| date | Wed, 16 Sep 2020 06:26:49 GMT |
| expires | Thu, 19 Nov 1981 08:52:00 GMT |
| p3p | policyref="/bitrix/p3p.xml", CP="NON DSP COR CUR ADM DEV PSA PSD OUR UNR BUS UNI COM NAV INT DEM STA" |
| pragma | no-cache |
| server | nginx/1.16.1 |
| transfer-encoding | chunked |
| vary | HTTPS |
| x-powered-by | PHP/7.2.29 |
| x-powered-cms | Bitrix Site Manager (a3c1e3c1b64020155003de3420017dbf) |
| Time to contact web server | 2.229275 seconds |

Dns admin: [pupko@bsu.by](mailto:pupko@bsu.by)



Tracker: Googletagmanager

Scripts: AJAX

**SERVERS**

* *ns1.gsu.by.* → 82.209.212.222
* *ns2.gsu.by.* → 37.17.74.99
* **37.17.74.0/24:**
  + *ns2.gsu.by.*
* **82.209.212.0/24:**
  + *ns1.gsu.by.*
* Primary nameserver: data-server.main.gsu.unibel.by.
* Hostmaster (e-mail): sa.gsu.by.

**MAIL SERVERS**

* **gsu.by.**:220 gsu.by Microsoft ESMTP MAIL Service, Version: 8.5.9600.16384 ready at Wed, 16 Sep 2020 09:44:46 +0300
* **ns1.gsu.by.**:220 gsu.by Microsoft ESMTP MAIL Service, Version: 8.5.9600.16384 ready at Wed, 16 Sep 2020 09:44:46 +0300
* **ns2.gsu.by.**:220 gsu.by Microsoft ESMTP MAIL Service, Version: 10.0.17763.1 ready at Wed, 16 Sep 2020 09:44:46 +0300
* *gsu.by.* → 82.209.212.222
* *ns1.gsu.by.* → 82.209.212.222
* *ns2.gsu.by.* → 37.17.74.99

SFP Enabled

SPAMCOMP - false

**DNS Zone Transfer:**

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> axfr @ns.bsu.by bsu.by

; (1 server found)

;; global options: +cmd

; Transfer failed.

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> axfr @bsu.by bsu.by

; (1 server found)

;; global options: +cmd

; Transfer failed.

**DNS Amplification**

IP address 82.209.212.222 is **not vulnerable** to DNS Amplification attacks.

**Open recursive resolver detected on 37.17.74.99**

IP address 37.17.74.99 is **vulnerable** to DNS Amplification attacks.

**DNSSEC**

