Гомельский Государственный Университет

им. Ф. Скорины

**Лабораторная работа №1.**

**Сбор предварительной информации**

**Проверил: Студент МС – 42:**

Грищенко В.В. Старик Я. П.

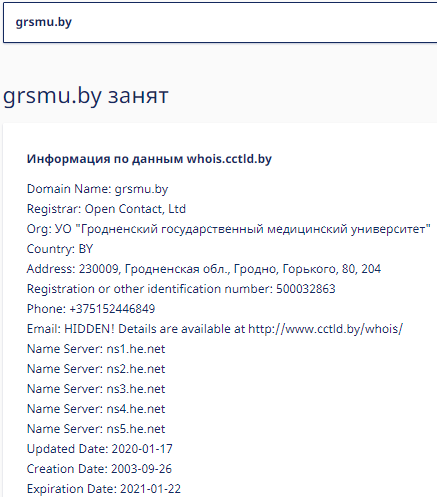
**г. Гомель**

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

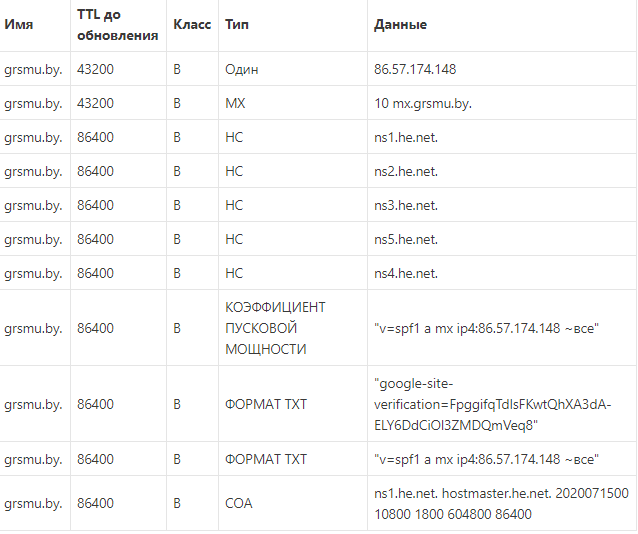
**Постановка задачи:** Выполнить предварительный сбор информации о домене grsmu.by. Работа выполняется на АРМ, имеющем доступ в сеть Интернет.

**Последовательность действий**

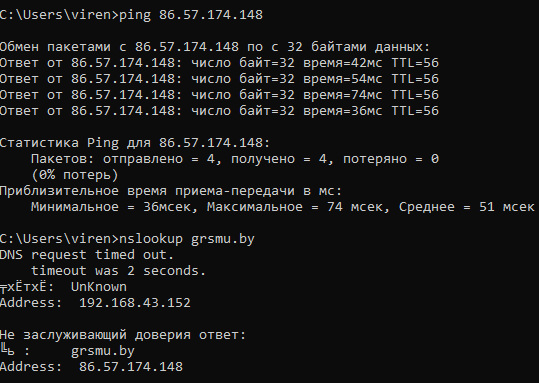
**Шаг 1.** Перейти по адресу https://whois.by. Указать в строке поиска в базе данных домен grsmu.by. Проанализировать полученные данные. Найти DNS-имена. Проанализировать данные по администраторам и контактным лицам организации. Найти используемые почтовые адреса.



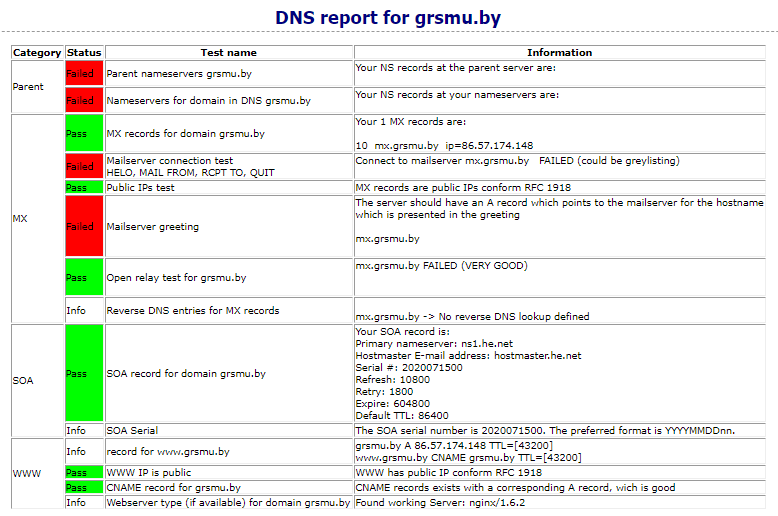
**Шаг 2.** Перейти по адресу <http://network-tools.com/nslook>. Задать параметры: домен – grsmu.by, тип запроса – ANY. Определить почтовый сервер организации.



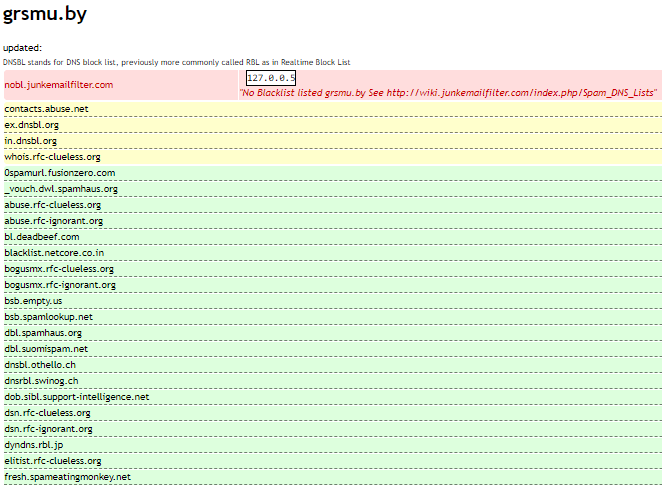
**Шаг 3.** Выполнить предыдущие проверки, используя средства nslookup, host и dig.



**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>.





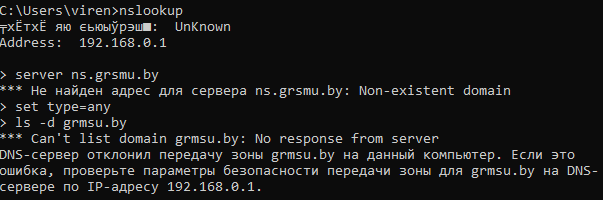
**Шаг 6.** Проверить возможность выполнения переноса зоны на первичном и вторичном DNS-серверах:

**nslookup**

**server ns.grmsu.by**

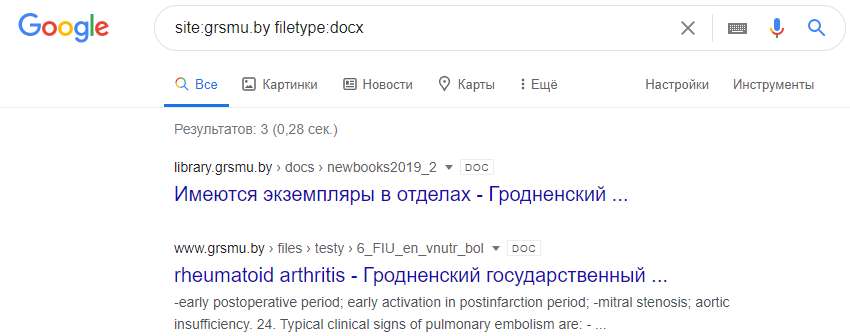
**set type=any**

**grmsu.by**

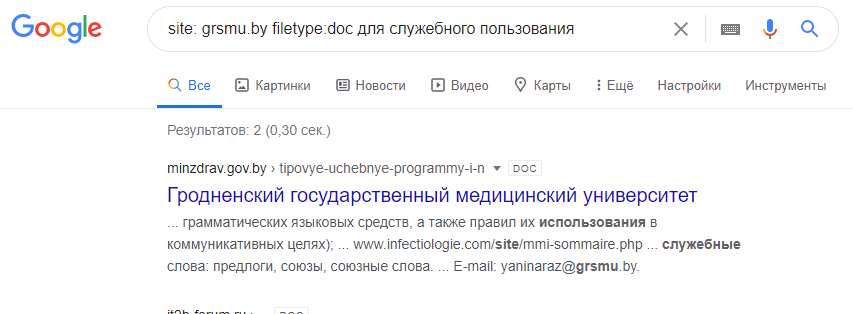


**Шаг 7.** Перейти по адресу http://google.ru. Задать следующие поисковые запросы и проанализировать результаты:

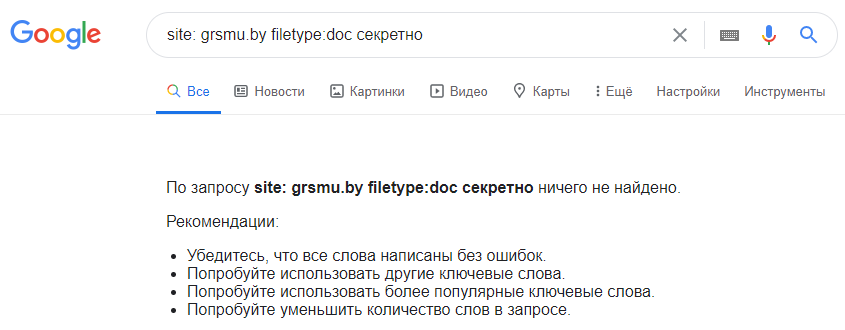
* «site:grsmu.by filetype:docx для служебного пользования»;



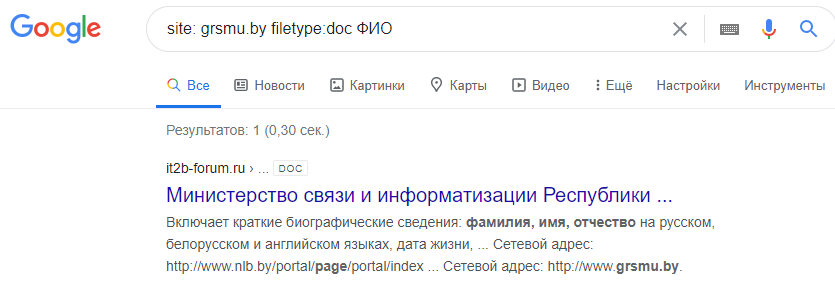
* «site: grsmu.by filetype:doc для служебного пользования»;



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



* «site: grsmu.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.

