## Министерство образования Республики Беларусь

## Учреждение образования

Отчёт по лабораторной работе №1

«Сбор предварительной информации»

Выполнил:

Студент группы МС-42

Кнышев Н.В.

Проверил: Грищенко В.В.

## Лабораторная работа №1

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

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

Шаг 1. Перейти по адресу https://www.whois.com Проанализировать полученные данные. Найти DNS-имена и IP-адреса серверов имен.

### uoggmk.by Updated 1 second ago 🗘 Domain name: uoggmk.by Registrar: Reliable Software, Ltd Org: Учреждение образования "Гомельский государственный машиностроительный кол Country: BY Address: 246027, -, г. Гомель, ул. Объездная, д. 2, -Registration or other identification number: 400082322 Phone: +375293327330 Email: HIDDEN! Details are available at https://whois.cctld.by Name Server: ns1.g-cloud.by Name Server: ns2.g-cloud.by Name Server: ns3.g-cloud.by Update Date: 2022-08-26 Creation Date: 2020-05-18 Expiration Date: 2023-05-18 Service provided by Belarusian Cloud Technologies LLC

#### Результаты проверки домена uoggmk.by

#### Информация о домене

#### Регистратор:

OOO "Надежные программы" Reliable Software, Ltd

#### Владелец домена:

Учреждение образования "Гомельский государственный машиностроительный колледж" ВҮ, г. Гомель, -, 246027, ул. Объездная, д. 2, -

Регистрационный или иной идентификационный номер: 400082322

Телефон: +375293327330 E-mail: admin@uoggmk.by

#### DNS-серверы:

ns1.g-cloud.by ns2.g-cloud.by ns3.g-cloud.by

#### Состояние:

Дата создания: 2020-05-18

Дата последнего обновления: 2022-08-26

Дата окончания: 2023-05-18

# Шаг 2. Перейти по адресу http://network-tools.com/nslook. Определить почтовый сервер организации.

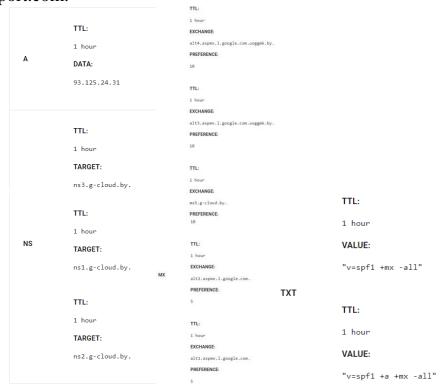
Name	TTL Until Refresh	Class	Туре	Data
uoggmk.by.	300	IN	TXT	"v=spf1 +a +mx -all"
uoggmk.by.	300	IN	TXT	"v=spf1 +mx -all"
uoggmk.by.	300	IN	MX	5 alt2.aspmx.l.google.com.
uoggmk.by.	300	IN	MX	10 mg1.g-cloud.by.
uoggmk.by.	300	IN	MX	10 alt3.aspmx.l.google.com.uoggmk.by.
uoggmk.by.	300	IN	MX	10 alt4.aspmx.l.google.com.uoggmk.by.
uoggmk.by.	300	IN	MX	20 ms5.g-cloud.by.
uoggmk.by.	300	IN	MX	3 aspmx.l.google.com.uoggmk.by.
uoggmk.by.	300	IN	MX	5 alt1.aspmx.l.google.com.
uoggmk.by.	300	IN	NS	ns3.g-cloud.by.
uoggmk.by.	300	IN	NS	ns1.g-cloud.by.
uoggmk.by.	300	IN	NS	ns2.g-cloud.by.
uoggmk.by.	300	IN	Α	93.125.24.31
uoggmk.by.	300	IN	SOA	g-cloud.by. support.g-cloud.by. 2020041026 3600 3600 604800 86400

Почтовые сервера организации находятся под типом Мх. Шаг 3. Выполнить предыдущие проверки, используя средства host и dig.

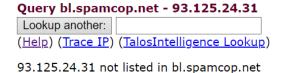
```
uoggmk.by has address 93.125.24.31
uoggmk.by mail is handled by 3 aspmx.l.google.com.uoggmk.by.
uoggmk.by mail is handled by 10 alt4.aspmx.l.google.com.uoggmk.by.
uoggmk.by mail is handled by 10 mg1.g-cloud.by.
uoggmk.by mail is handled by 10 ms5.g-cloud.by.
uoggmk.by mail is handled by 5 alt1.aspmx.l.google.com.
uoggmk.by mail is handled by 5 alt2.aspmx.l.google.com.
uoggmk.by mail is handled by 10 alt3.aspmx.l.google.com.uoggmk.by.
```

```
| Solicy |
```

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



Шаг 5. Проверить наличие узлов найденных сетей в базах данных спамотправителей и бот-сетях.



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

```
C:\Users\Nikita Knyshev>nslookup

тхЁтхЁ яю выюыўрэшш: csp1.zte.com.cn

Address: fe80::1

> server uoggmk.by

тхЁтхЁ яю выюыўрэшш: uoggmk.by

Address: 93.125.24.31

> set type=any

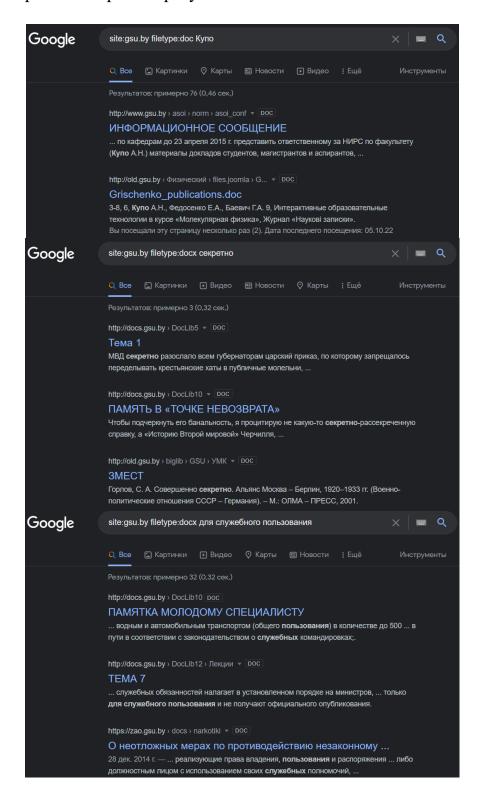
> ls-d uoggmk.by

DNS request timed out.

    timeout was 2 seconds.

*** He найден адрес для сервера uoggmk.by: Timed out >
```

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



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

Traceroute Check for: 93.125.24.31

traceroute to 93.125.24.31 (93.125.24.31), 10 hops max, 60 byte packets

- 1 216.182.237.223 (216.182.237.223) 6.046 ms 216.182.237.221 (216.182.237.221) 19.574 ms 216.182.237.219 (216.182.237.219) 16.359 ms
- 2 100.65.18.128 (100.65.18.128) 16.342 ms 100.65.18.192 (100.65.18.192) 16.325 ms 100.65.17.0 (100.65.17.0) 22.019 ms
- 3 100.66.8.148 (100.66.8.148) 19.983 ms 100.66.8.32 (100.66.8.32) 20.213 ms 100.66.8.88 (100.66.8.88) 17.925 ms
- 4 100.66.10.76 (100.66.10.76) 18.838 ms 100.66.10.78 (100.66.10.78) 12.556 ms 100.66.10.132 (100.66.10.132) 21.251 ms
- 5 241.0.6.138 (241.0.6.138) 0.574 ms 241.0.6.140 (241.0.6.140) 0.568 ms 241.0.6.133 (241.0.6.133) 0.547 ms
- 6 240.0.176.21 (240.0.176.21) 0.532 ms 240.0.176.16 (240.0.176.16) 0.317 ms 240.0.176.28 (240.0.176.28) 0.300 ms
- 7 242.2.44.1 (242.2.44.1) 0.367 ms 242.2.45.97 (242.2.45.97) 0.874 ms 242.2.44.193 (242.2.44.193) 0.315 ms
- 8 52.93.237.215 (52.93.237.215) 1.814 ms 52.93.237.239 (52.93.237.239) 1.854 ms 15.230.36.95 (15.230.36.95) 2.187 ms
- 9 150.222.30.198 (150.222.30.198) 1.474 ms 52.93.237.252 (52.93.237.252) 1.959 ms 52.93.237.240 (52.93.237.240) 2.159 ms
- 10 150.222.30.95 (150.222.30.95) 1.339 ms 54.240.242.159 (54.240.242.159) 1.447 ms 54.240.242.97 (54.240.242.97) 5.903 ms