

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования «Тульский государственный
университет»

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДЫ СБОРА ИНФОРМАЦИИ ОБ ОБЪЕКТЕ ЗАЩИТЫ

отчет о
лабораторной работе №2

по дисциплине

ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Выполнила:	ст. гр. 230711	Павлова В.С.
Проверил:	асс. каф. ИБ	Греков М.М.

Тула, 2023 г.

ЦЕЛЬ РАБОТЫ

Цель: ознакомиться с основными пассивными методами сбора информации об исследуемом объекте наблюдения, использование которых допускается правовым полем РФ.

ЗАДАНИЕ НА РАБОТУ

1. Используя поисковую систему определить актуальный домен сайта ТулГУ
2. Найти на сайте ТулГУ образцы всех открытых документов, с использованием инструментов Google dorks. Например, используя запрос `filetype:pdf site:tulsu.ru`
3. Определить наличие файлов `xls`, `xlsx` и `log` в открытом доступе, используя Google dorks.
4. Определить широту и долготу расположения сервера ТулГУ при помощи поиска в системе Shodan.io, при наличии возможности регистрации.
5. Определить IP адрес сайта ТулГУ при помощи сервиса Censys.io при наличии возможности регистрации и его использования.
6. Определить IP адрес сервера ТулГУ и историю перемещения доменного имени при помощи сервиса ViewDNS.info
7. Получить данные о сайте ТулГУ при помощи сервиса 2ip.ru
8. Найти данные о себе при помощи использования возможностей сайта osintframework.com.
9. Найти в сети интернет и предоставить скриншот своей страницы в любой социальной сети за любую дату 2020 года, используя сервис web.archive.org.

ХОД РАБОТЫ

1. Актуальный домен сайта ТулГУ – <https://tulsu.ru/> (рисунок 1).

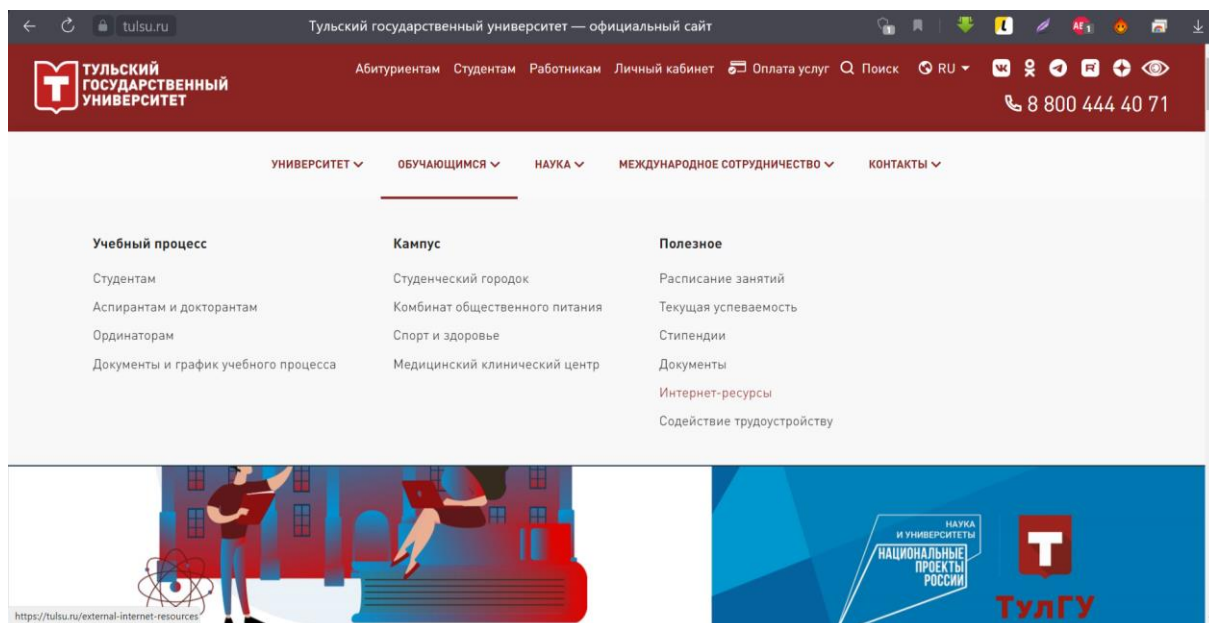


Рисунок 1 – Актуальный домен сайта

2. Результат поиска образцов всех открытых документов, с использованием инструментов Google dorks (рисунок 2). Их доменное имя начинается на: tulsu.ru/modules/download.php?file_id=

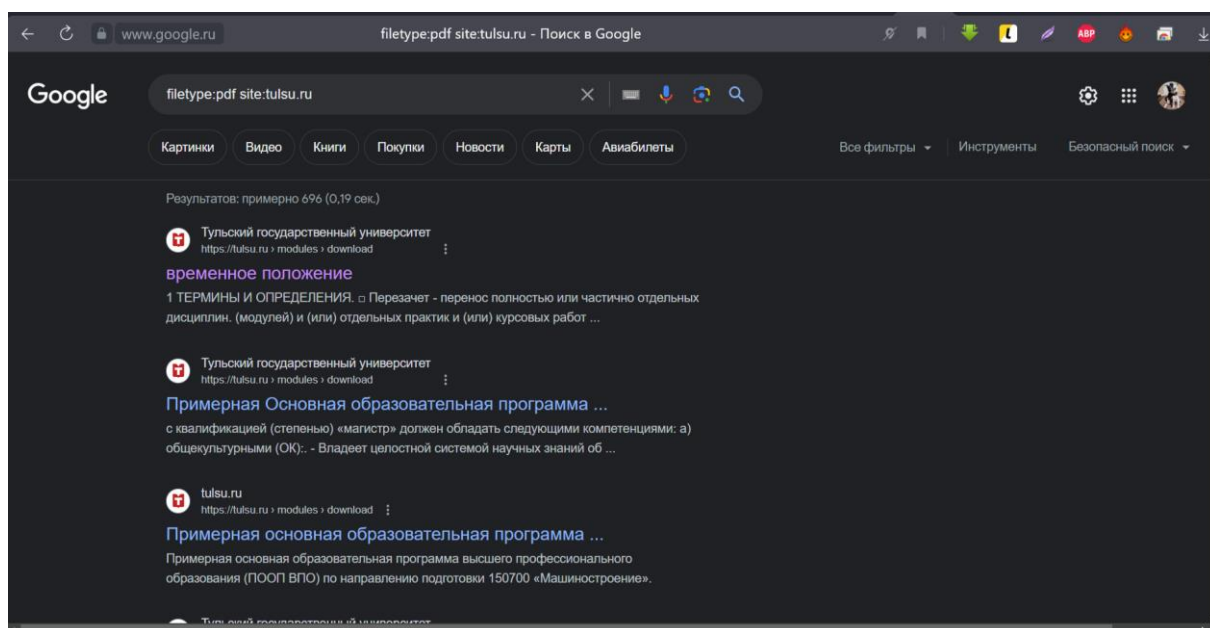


Рисунок 2 – Образцы открытых документов

3. Результат проверки наличия файлов xls, xlsx и log в открытом доступе с использованием Google dorks (рисунки №3.1 – 3.3).

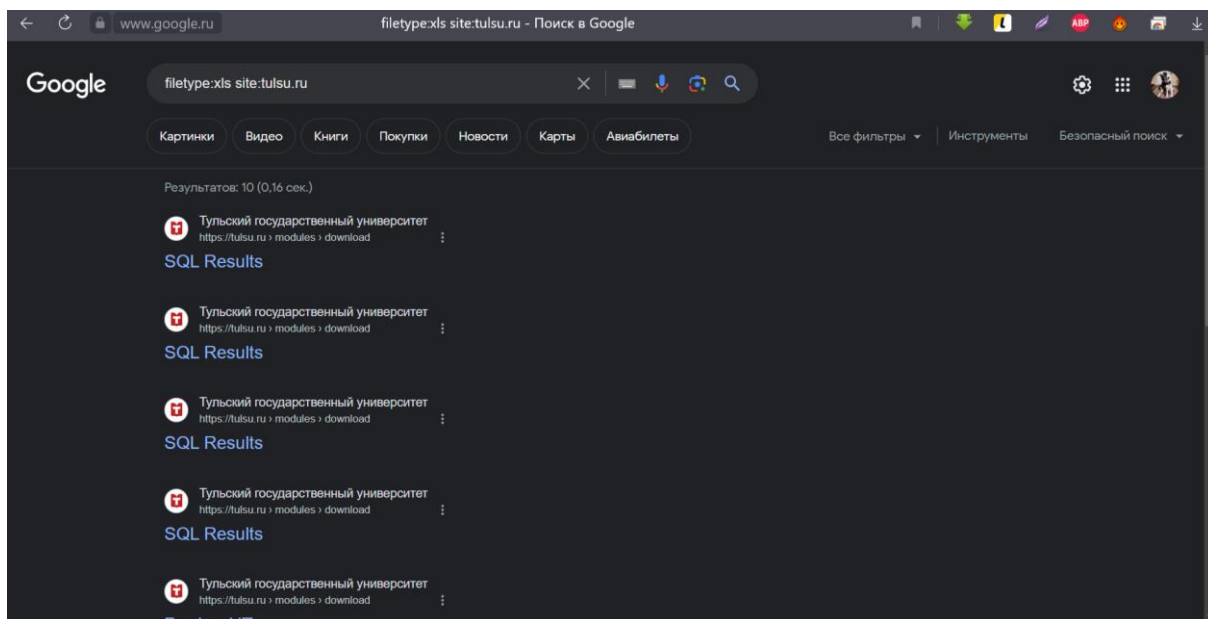


Рисунок 3.1 – Результат поиска файлов xls

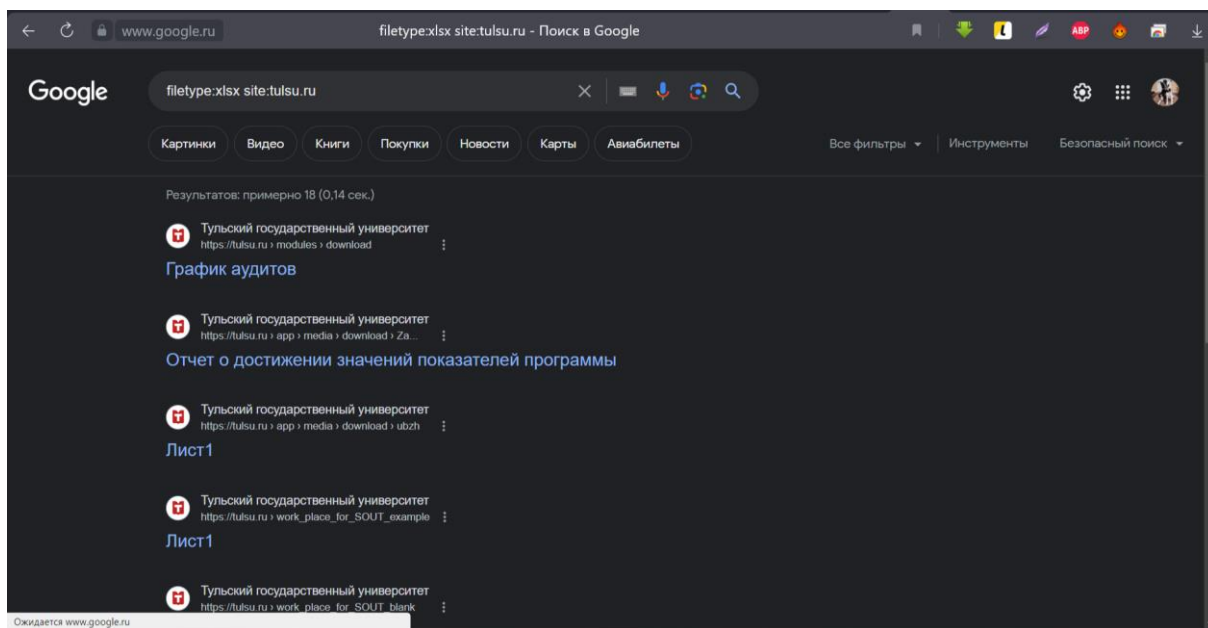


Рисунок 3.2 – Результат поиска файлов xlsx

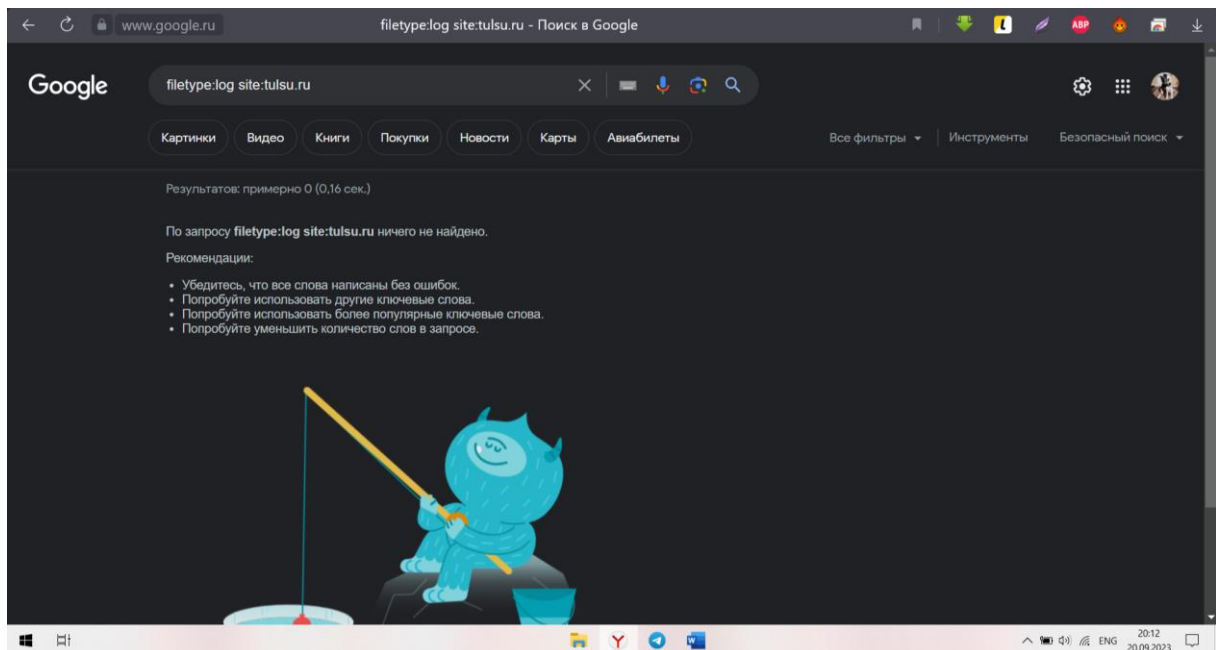


Рисунок 3.3 – Результат поиска файлов log

4. Широта и долгота расположения сервера ТулГУ, полученная при помощи поиска в системе Широта и долгота расположения сервера:

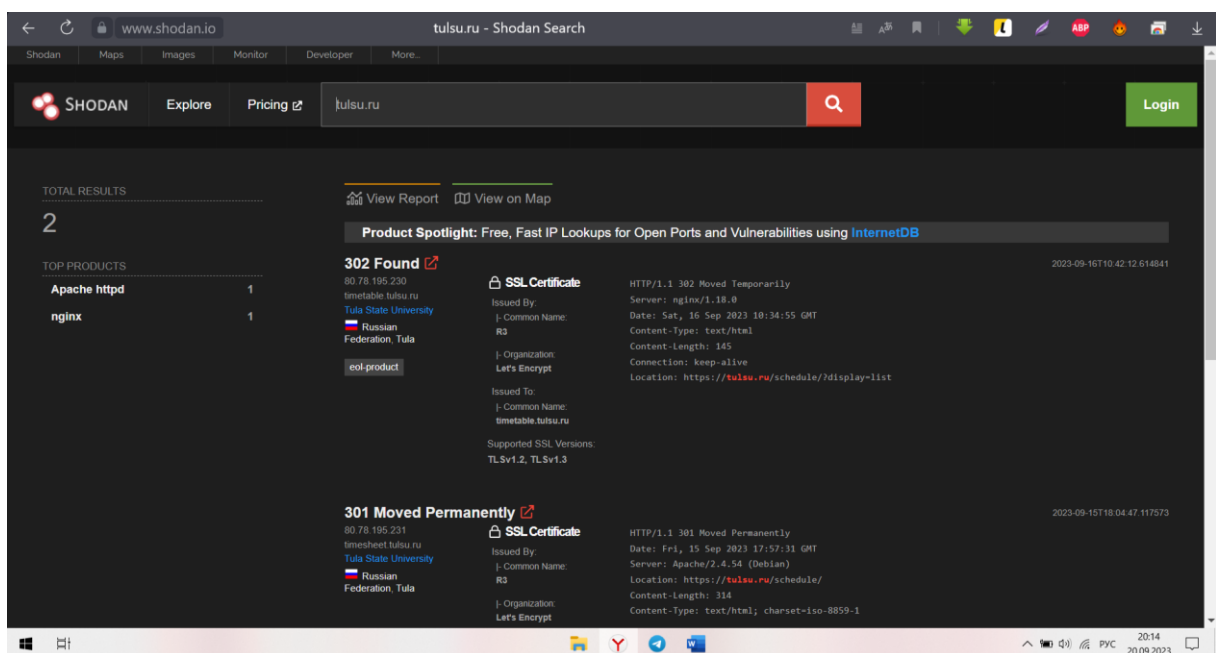


Рисунок 4 – Широта и долгота расположения сервера

5. IP-адрес сайта ТулГУ, определенный при помощи сервиса Censys.io:

Сертификаты

tulsu.ru

Поиск

Результаты

Сообщения

Фильтры хостов

Метки:

7 удаленный доступ

3 База данных

2 bootstrap

2 общий доступ к файлам

2 jquery

Еще

Автономная система:

10 TULSUIISP автономная система для Тульского государственного университета, расположенного в Туле, Россия.

2 ВЫБЕРИТЕ

1 ВЫБЕРИТЕ хостинг-MSK

Расположение:

13 Россия

Сервисные фильтры

Названия сервисов:

32 HTTP

5 SSH

5 НЕИЗВЕСТНО

3 FTP

2 MYSQL

Еще

Порты:

Хосты

Результатов: 13 Время: 0.63с

80.78.195.251

Debian Linux

TULSUIISP - автономная система для Тульского государственного университета, распо

Россия. (21143)

Тульская область, Россия

bootstrap

jquery

80/HTTP

443/HTTP

80.78.195.231

Debian Linux

TULSUIISP - автономная система для Тульского государственного университета, распо

Россия. (21143)

Тульская область, Россия

80/HTTP

443/HTTP

80.78.200.185

TULSUIISP автономная система для Тульского государственного университета, расположенного в Туле, I

Тульская область, Россия

shellinabox

страница входа в систему

443/НЕИЗВЕСТНО

12320/HTTP

12321/HTTP

80.78.195.230

TULSUIISP автономная система для Тульского государственного университета, расположенного в Туле, I

Тульская область, Россия

80/HTTP

443/HTTP

79.143.30.168 (dveri-vidnoe.ru)

Debian Linux

SELECTEL-MSK (50340)

Москва, Россия

удаленный доступ

22/SSH

80/HTTP

443/HTTP

80.78.195.219

TULSUIISP автономная система для Тульского государственного университета, расположенного в Туле, I

Рисунок 5 – IP-адрес сайта ТулГУ

6. IP-адрес сервера ТулГУ и история перемещения доменного имени, определенная при помощи сервиса ViewDNS.info:

Тесты записей WWW		
Статус	Тестовый пример	Информация
	Запись WWW	<p>www.tulsu.ru Записи A являются:</p> <p>www.tulsu.ru. CNAME tulsu.ru. [TTL=7200]</p> <p>tulsu.ru. A 80.78.200.185 [TTL=7200]</p>
	WWW Запись имеет общедоступный IP	Хорошо! IP-адреса записей A, возвращенных для вашей WWW-записи являются общедоступными IP-адресами.
	Поиск по WWW CNAME	Хорошо! У вас есть запись CNAME для вашей записи WWW, которая возвращает связанную запись A! Это экономит дополнительный по который задержал бы время загрузки вашего сайта.

Рисунок 6 – IP-адрес сервера и история перемещения

7. Получить данные о сайте ТулГУ при помощи сервиса 2ip.ru

6

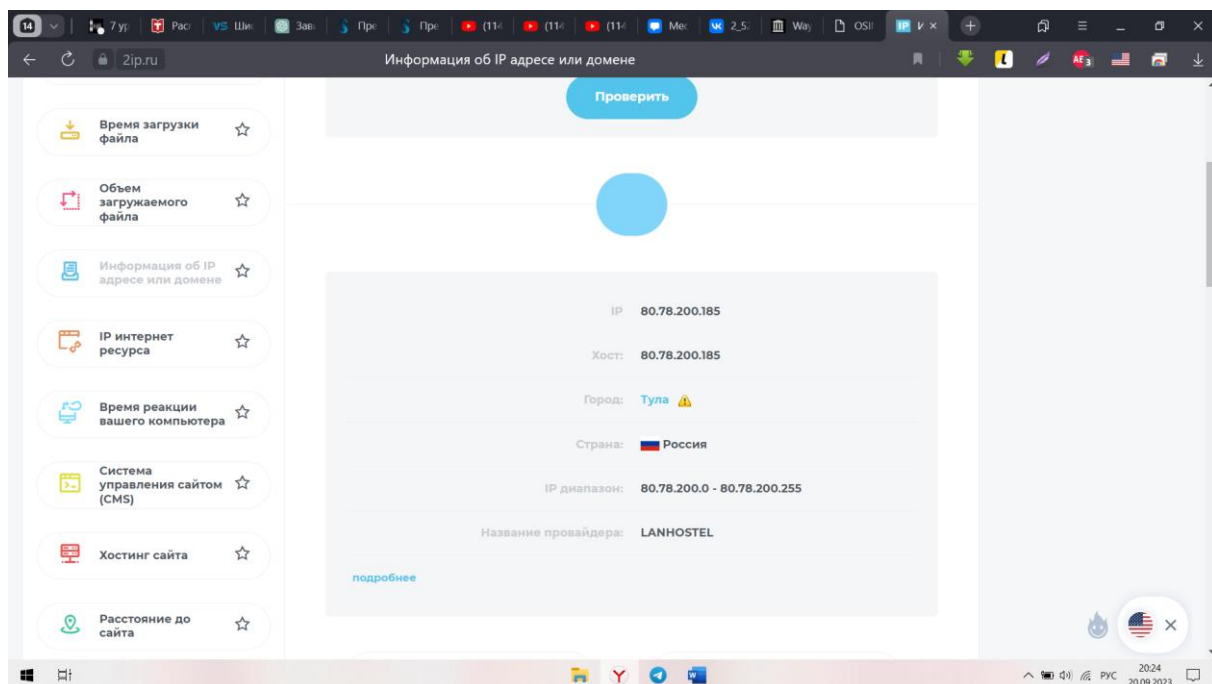


Рисунок 7 – Данные о сайте ТулГУ

8. Результат поиска данных о себе при помощи использования возможностей сайта osintframework.com.

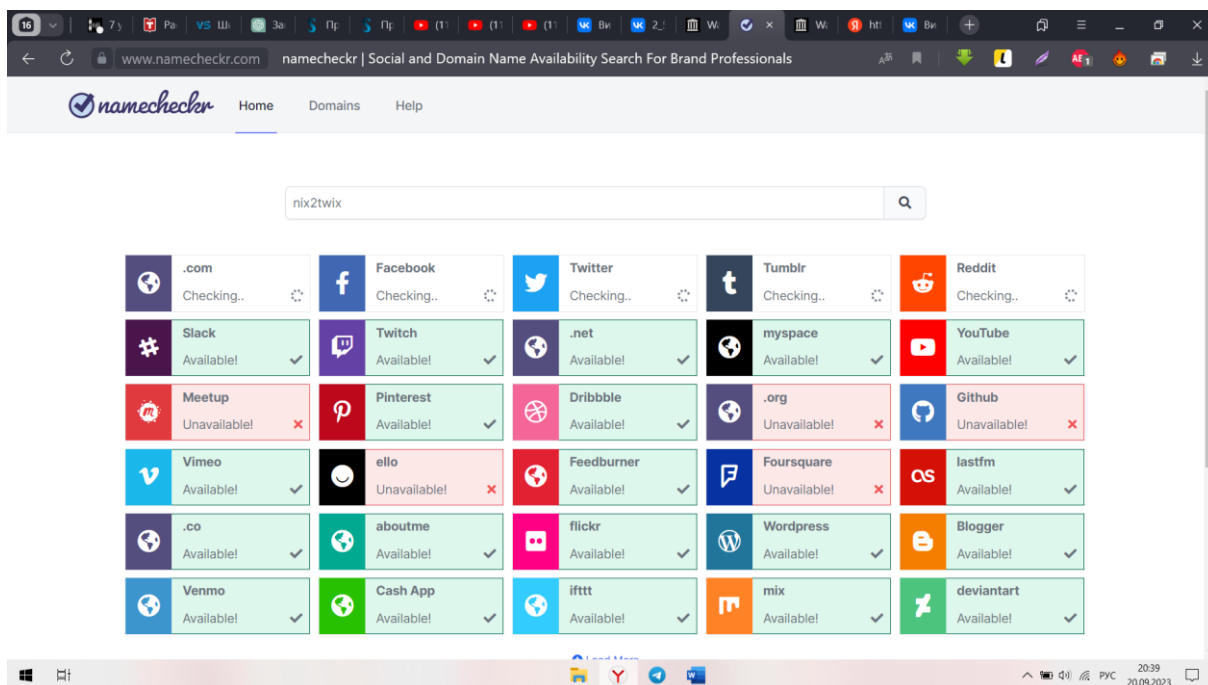


Рисунок 8 – Данные о никнейме, полученные с использованием osintframework.com

9. Найти в сети интернет и предоставить скриншот своей страницы в любой социальной сети за любую дату 2020 года, используя сервис web.archive.org.

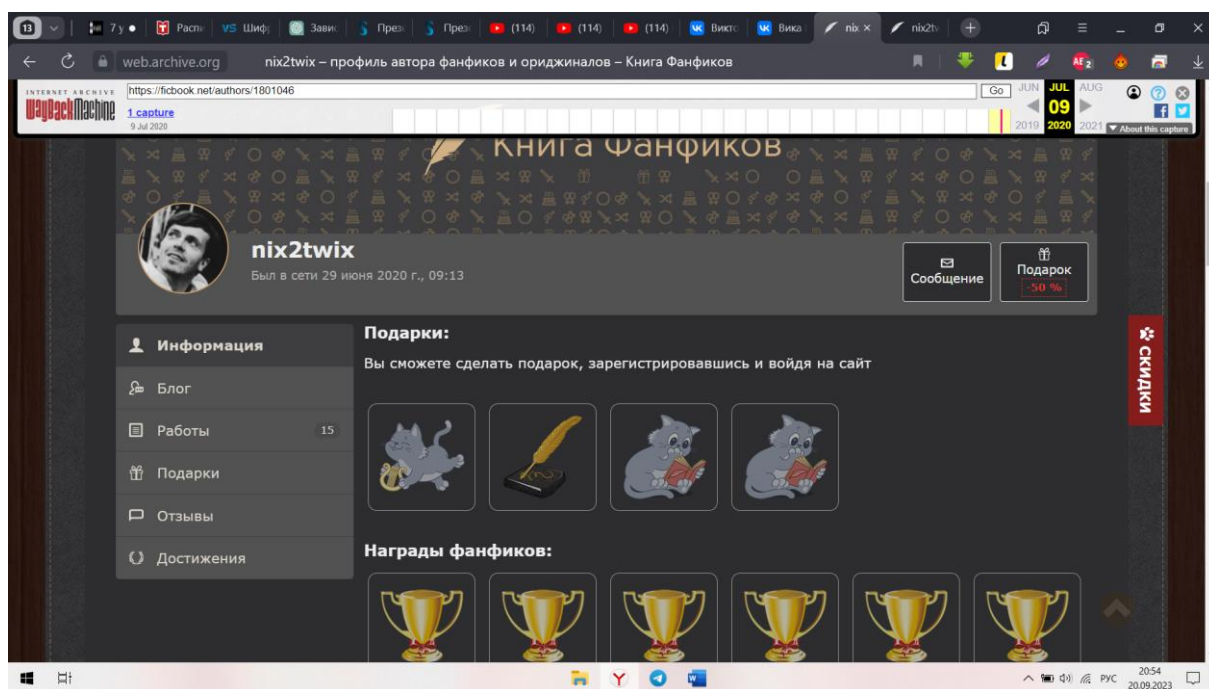


Рисунок 9 – Страница на Книге Фанфиков из архива 2020 года

ВЫВОД

В ходе выполнения данной лабораторной работы я ознакомилась с основными методами сбора информации об исследуемом объекте наблюдения, использование которых допускается правовым полем РФ.