ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ

УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ

им. проф. М. А. БОНЧ-БРУЕВИЧА»

**OSINT. РАЗВЕДКА НА ОСНОВЕ ОТКРЫТЫХ ИСТОЧНИКОВ**

Пояснительная записка к курсовой работы

по дисциплине

«Маршрутизация и коммутация компьютерных сетей»

Направление 09.03.02 – Информационные системы

и технологии

Факультет Информационных систем и технологий

Кафедра Безопасности информационных систем

Курс 3

Семестр 5

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Исполнитель

Проверил ст. преп. каф. БИС студ. гр. ИСТ-831

\_\_\_\_\_\_\_\_\_\_\_ Гвоздков И.В. \_\_\_\_\_\_\_\_\_\_\_Пономарев Е.И.

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2020 г.

2020

Содержание

[ВВЕДЕНИЕ 3](#__RefHeading___Toc516_2482701993)

[1 Исследование OSINT 4](#__RefHeading___Toc518_2482701993)

[1.1 Терминология 4](#__RefHeading___Toc520_2482701993)

[1.2 Цель атаки OSINT 4](#__RefHeading___Toc522_2482701993)

[1.3 Методы разведки 4](#__RefHeading___Toc524_2482701993)

[1.4 Современный OSINT 6](#__RefHeading___Toc1711_2975477739)

[2 Инструментарий 6](#__RefHeading___Toc526_2482701993)

[3 Анализ существующих средств и методов решения задач 8](#__RefHeading___Toc778_607153587)

[3.1 Анализ автоматизированных средств разведки 8](#__RefHeading___Toc780_607153587)

[3.2 Анализ ручных средств разведки 12](#__RefHeading___Toc782_607153587)

[4 Пример атаки OSINT 13](#__RefHeading___Toc528_2482701993)

[4.1 Maltego 13](#__RefHeading___Toc530_2482701993)

[4.2 Censys 14](#__RefHeading___Toc532_2482701993)

[5 Пример ручной таргетированной OSINT-атаки 16](#__RefHeading___Toc1727_2975477739)

[ЗАКЛЮЧЕНИЕ 25](#__RefHeading___Toc536_2482701993)

[Список литературы 26](#__RefHeading___Toc538_2482701993)

# ВВЕДЕНИЕ

С погружением человечества в информационную эпоху все больше данных об человеке или компании утекают в Интернет. Для среднестатического злоумышленника — это хорошая возможность получить несанкционнированный доступ к корпоративной информации. Более того, OSINT не предполагает наличия у атакующего каких-либо развитых и узконаправленных проффесиональных навыков, так как для совершения достаточно лишь доступа к сети Интернет(или другому информационному ресурсу).

Особенно легко для разведчика осуществлять таргетированную атаку, которая базируется на социальные сети цели, потому что с повышением количества различного рода ресурсов для взаимодействия между людьми повышается и количество личных данных пользователя, которые компании могут использовать в своих целях, в том числе и для продажи третим лицам. Например, социальная сеть Вконтакте продает личные телефоны пользователей сторонним компаниям, в соответствии с их предпочтитаемой целевой аудиторией.

Также не стоит считать, что разведка - это исключительно ручной труд. Существует огромное количество написанных программистами утилит, помогающих в этом деле: от консольных скриптов до больших мануфактурных программ с GUI-интерфейсом и визуализацией получаемых данных. Нужно заметить, что даже если злоумышленник не смог найти нужную для его цели утилиту для парсинга данных, то обладая средним уровнем владения популярным скриптовым языком программирования, он может в кратчайшие сроки написать свою программу, тем самым пополняя и без того большую базу облегчающих жизнь инструментов.

# 1 Исследование OSINT

# 1.1 Терминология

Open Source Intelligence (OSINT) – это любая информация о цели, человеке или организации, которая может быть собрана из общедоступных источников. На практике, это обычно означает информацию, найденную в Интернете, хотя этот термин не ограничивается строго Интернетом, а скорее означает все общедоступные источники. Технически любая публичная информация попадает в категорию OSINT, будь-то книги или отчеты в публичной библиотеке, статьи в газете или заявления в пресс-релизе.

# 1.2 Цель атаки OSINT

.Собирая информацию и анализируя данные из открытых источников, злоумышленник или [пентестер](http://withsecurity.ru/chto-takoe-pentest-i-dlya-chego-on-nuzhen) имеет возможность сформировать полноценный профиль жертвы, определить существующие и потенциальные уязвимости. Целенаправленные кибератаки, как и военные атаки, начинаются с предварительной разведки, и первый этап цифровой разведки – это OSINT, пассивное получение разведданных без предупреждения цели. Без активного вовлечения своей жертвы, злоумышленник или же пентестер, может использовать полученную информацию для построения модели угрозы, разработки плана атаки или защиты.

# 1.3 Методы разведки

.

Существует множество механизмов и методов Open Source Intelligence, однако не все из них будут работать для Вашей цели. Некоторые из них могут работать, другие – нет, но это неотъемлемая часть стратегии OSINT – Вам нужно выяснить, какие источники хороши, а какие не имеют отношения к Вашим исследованиям. Прежде, чем приступить к сбору информации из открытых источников необходимо определиться с задачей:

* Что я ищу?
* Какая цель поиска?
* Кто или что является моей целью?
* Каким образом я буду выполнять сбор и анализ данных?

Ответы на эти вопросы – первый шаг в OSINT.

Наиболее популярные методы OSINT доступные всем и каждому, используемые в кибербезопасности против человека и организаций:

* определение сотрудников (ФИО, должности), а также программное обеспечение, с которым работают сотрудники;
* сбор информации через поисковые системы Google (особенно с помощью Google Dorks), Yandex, Yahoo, Bing и другие;
* анализ информации в социальных сетях (ВКонтакте, Facebook, Одноклассники и тому подобное), на форумах, блогах и других виртуальных ресурсах;
* поиск по фотографии, например, через Google, Yandex, TinEYE и другие подобные ресурсы;
* определение контактных номеров телефона и дальнейший поиск по номеру в социальных сетях, мессенджерах, иных сайтах;
* просмотр сохранённых копий сайтов через Google;
* изучение веб-сайтов в архиве Интернета, например, через сервис Wayback Machine;
* использование Google Maps и других источников спутниковых изображений для получения географического положения пользователей.

# 1.4 Современный OSINT

С развитием социальных сетей все больше людей загружает на свои страницы большое количество личной информации, которая без труда может быть получена злоумышленником. Данным способом пользуются в первую очередь при анализе какой-либо личности, либо ее деятельности. Стоит упомянуть, что в социальные сети могут утечь и корпоративные данные пользователя. Например, в ноябре 2020 года журналист из Нидерландов зашел на трансляцию министров обороны ЕС после того, как один из министров случайно выложил в Twitter логин и пароль от учетной записи.

Разведка на основе социальных сетей может иметь под собой разные умыслы:

* анализ личности человека для последующей эффективной атаки социальной инженерии;
* поиск случайно утекших секретных данных;
* составления баз личных данных(например, для совершения массовой спам-рассылки для целевой аудитории);
* изучения социальных связей человека(чаще всего используется для бытовых целей);

# 2 Инструментарий

Сбор информации из широкого круга источников – это трудоемкая работа, но существует множество инструментов, позволяющих упростить сбор разведданных. Наиболее популярные специализированные OSINT технологии, также доступные всем и каждому, однако требующие более продвинутого уровня владения и знания информационных технологий:

* поиск через [OSINT Framework](https://u.to/SIkdFw), который содержит в себе ссылки на большую коллекцию ресурсов для решения самых разнообразных задач – от сбора адресов электронной почты до поиска в социальных сетях и dark Web'e;
* использование автоматизированных инструментов OSINT для получения информация, например через [Spiderfoot](https://u.to/R4kdFw), [Maltego](https://u.to/SokdFw), [Recon-ng](https://u.to/TokdFw), [FOCA](https://u.to/SYkdFw) и другие;
* применение инструментов для поиска подключенных к Интернету устройств, например, через поисковую систему [Shodan или Censys](https://u.to/TYkdFw);
* использование инструменты сбора данных о людях, такие как [Pipl](https://u.to/8obrFA), которые помогут вам раскрыть много информации о людях в одном месте;
* сбор информации через метапоисковую систему [Searx](https://u.to/T4kdFw), позволяющую собирать данные анонимно, из более чем 70 поисковых сервисов;
* отслеживание местоположения человека по его фотографиям, например, через сервис [GeoCreepy](https://u.to/S4kdFw);
* ещё один замечательный инструмент, который Вы можете использовать для сбора общедоступной информации, является [Metagoofil](https://u.to/RYkdFw) – использует поисковую систему Google для извлечения общедоступных PDF-файлов, документов Word, Powerpoint и Excel из заданного домена;
* применения специальных OSINT-расширений, таких, как [Open Source Intelligence Browser Extension](https://u.to/RIkdFw);
* изучения служб DNS, доменов, поддоменов и IP-адресов;
* применения иных инструментов [Kali Tools](https://u.to/AOtoEQ) позволяющий выполнять не только разведку, но и множество иных задач;
* нахождение работающих служб, через сканирование портов в инфраструктуре целевой компании;

Все вышеперечисленное – лишь малая часть программ применяемых для разведки на основе открытых данных. Последним шагом в стратегии OSINT будет перевод всех полученных цифровых данных в удобочитаемый формат, чтобы были понятны и доступны людям далёким от компьютерных технологий.

# 3 Анализ существующих средств и методов решения задач

В основном, все методы разведки можно разделить на автоматизированные и ручные(выполняемые непосредственно человеком)

Характерные особенности автоматизированной разведки:

* низкое время выполнения разведки;
* большой выбор утилит, что позволяет получить информацию разного рода;
* низкий порок входа для выполнения разведки;
* при необычности цели разведки данный способ становится почти бесполезным;

Характерные особенности ручной разведки:

* выше вероятность получить ценную информацию;
* требует наличие специальных навыков;
* большие затраты по времени;
* есть возможность контролировать каждый этап разведки и действовать согласно случаю;

# 3.1 Анализ автоматизированных средств разведки

Одно из самых популярных средств автоматизированной разведки — это Maltego.

Maltego — это инструмент для построение и анализа связей между различными субъектами и объектами. Её особенностями являются: визуализирование полученных данных, разведка на основе открытых источников, комбинирование для глубокого анализа данных полученных из закрытых и открытых источников, автоматический анализ открытых источников и автоматическое построение взаимосвязей между обнаруженными объектами.

Maltego — это программа, которая может быть использована для выявления отношений и реальных связей между:

* людьми;
* группами людей (социальные сети);
* компаниями;
* организациями;
* веб-сайтами;
* доменами;
* DNS именами;
* сетевыми блоками;
* IP-адресами;
* факторами;
* аффилированности;
* документами и файлами;

Пример действия Maltego приведен в разделе 4.1.

Также стоит выделить поисковик Censys.

Censys — поисковик по интернету вещей. Подобно Shodan, он опрашивает все публично доступные IP-адреса и протоколирует их отклики. В результате создается своеобразная карта интернета, на которой можно искать любые устройства с сетевым интерфейсом, изучать характер распространения уязвимостей или, выбрав критерии, смотреть за актуальным состоянием глобальной сети.

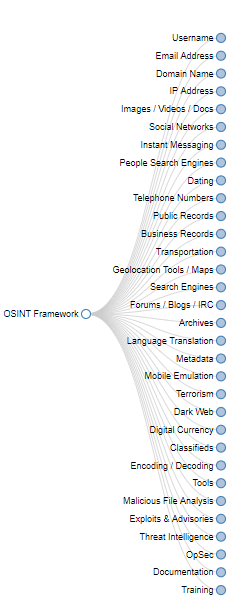
Пример сканирования посковиком Censys приведен в разделе 4.2.

Стоит заметить один из самых больших листингов OSINT-утилит — это OSINT FRAMEWORK. На данном сайте любой человек может найти нужные для его целей программу, исходя из его начальных данных и типов получаемых данных или раздела поиска. Данные разделы:

* обучение;
* документация;
* OpSec;
* анализ угроз;
* подвиги и советы;
* анализ вредоносных файлов;
* инструменты;
* кодирование / декодирование;
* объявления;
* цифровая валюта;
* темная паутина;
* терроризм;
* мобильная эмуляция;
* метаданные;
* языковой перевод;
* архивы;
* форумы / Блоги / IRC;
* поисковые системы;
* инструменты геолокации / Карты;
* транспорт;
* деловые записи;
* публичные записи;
* телефонные номера;
* знакомства;
* поисковые системы людей;
* мгновенное сообщение;
* социальные сети;
* изображения / Видео / Документы;
* IP-адрес;
* доменное имя;
* адрес электронной почты;
* имя пользователя;

Примечания

Изображение, демонстрирующее данный сайт приведено на рисунке 1.

Рисунок 1 — Демонстрация сайта c листингом программ.

# 3.2 Анализ ручных средств разведки

Чаще всего ручная разведка применяется, когда составляется подробный портрет личности человека(анализ социальных сетей) или когда нужен более тонкий подход, с которым обычные стандартные OSINT-программы не справляются.

Пример ручного анализа приведен в разделе 5.

# 4 Пример атаки OSINT

# 4.1 Maltego

Посредством обычного стандартного сканирования(без подключения дополнительных модулей) домена sut.ru посредством программы Maltego стала доступна следующая информация:

* информация о субдоменах;
* несколько email-адресов, связанных напрямую с доменом;
* имена и фамилии людей, связанных с email-адресами;

Стоит заметить, что сканирование произошло быстро и не заняло и больше 15 секунд, что для такого рода данных является хорошим результатом.

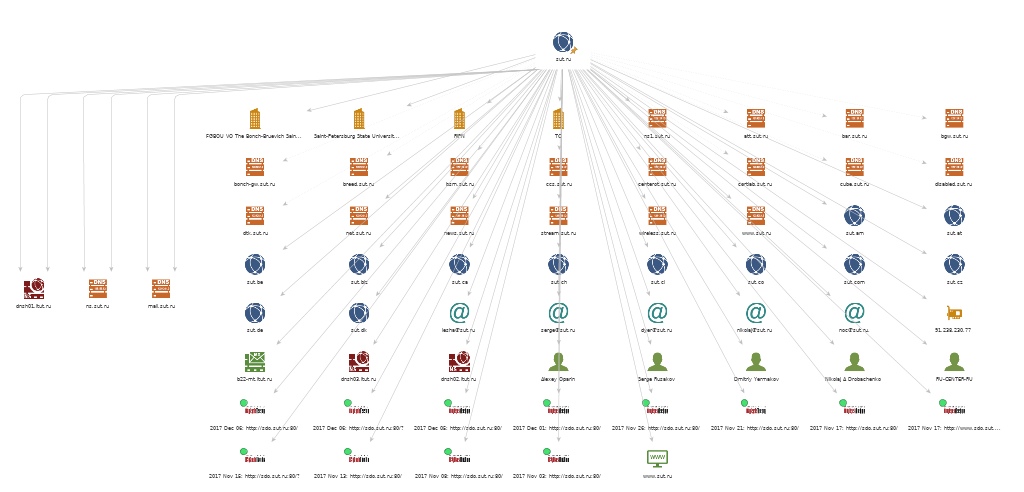
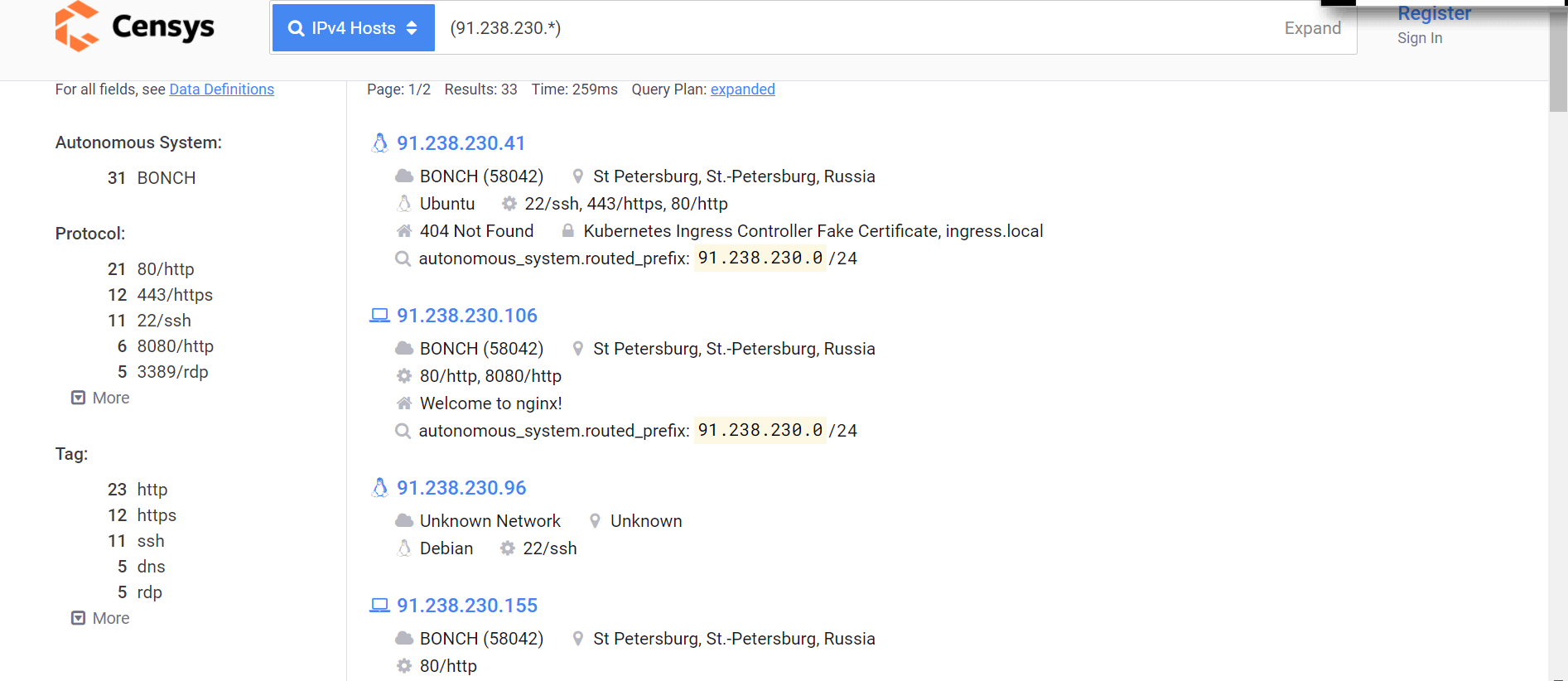
Результат сканирования приведен на рисунке 2.

Рисунок 2 - Результат сканирования программы Maltego.

# 4.2 Censys

Посредством поиска на ресурсе Censys ip-адреса домена sut.ru было найдено 31 ip-адреса, связанных с целью.

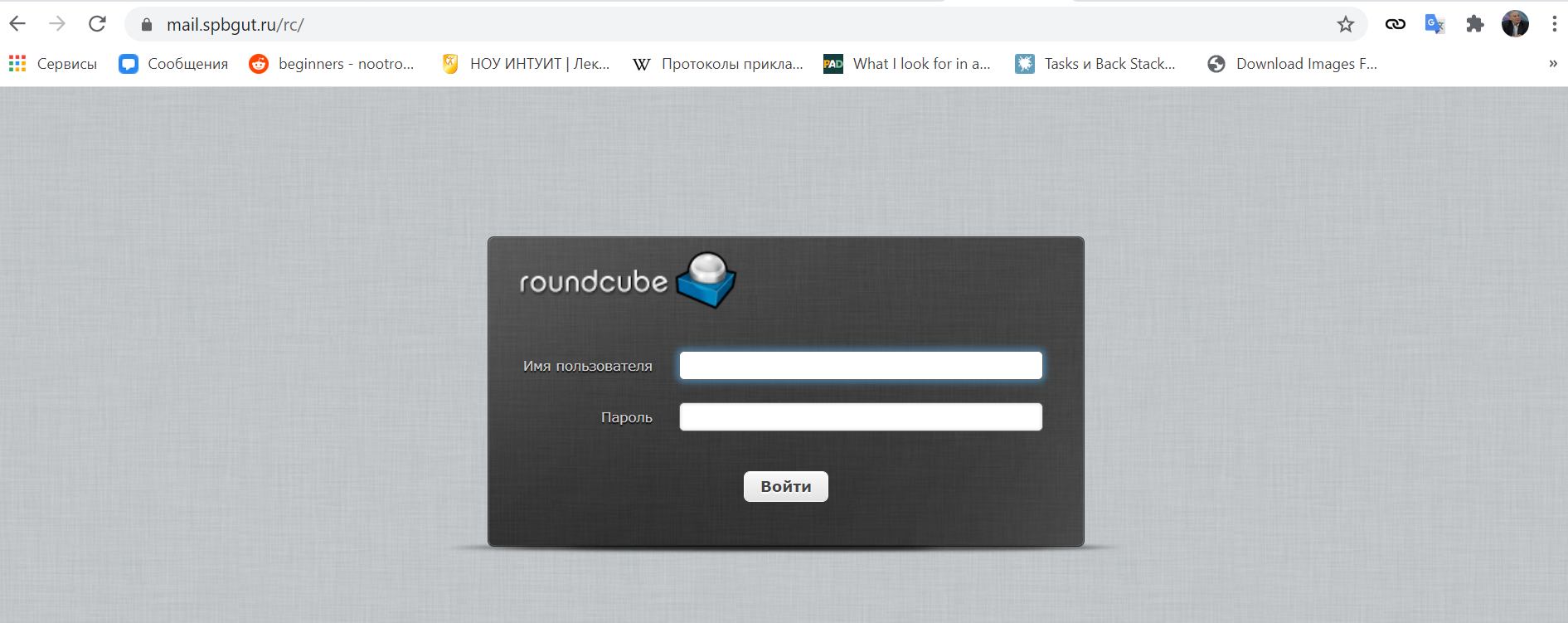
Результат поиска приведен на рисунке 3.

Рисунок 3 - Результат сканирования на ресурсе Censys.

Например, один из выведенных результатов является почтовым сервером СПБГУТ, что в купе с email-адресами, полученными в разделе 3.1 открывает путь к «грубой» атаке — брутфорсу.

Почтовой сервер приведен на рисунке 4.

Также стоит заметить, что данный сервер в виде субдомена был представлен в качестве результата сканирования программой Maltego в разделе 3.1.

Рисунок 4 - Почтовой сервер.

В качестве еще одного примера хочется привести еще один ip-адрес, использующий старую авторизацию http-basic, пароль и логин в которой также можно перебрать программным способом. Например, программы hydra и medusa, используя многопоточность и мультипроцессорность, позволяют добиться большой скорости перебора данной авторизации.

Http-basic авторизация на одном из найденных ресурсов приведена на рисунке 5.

# 

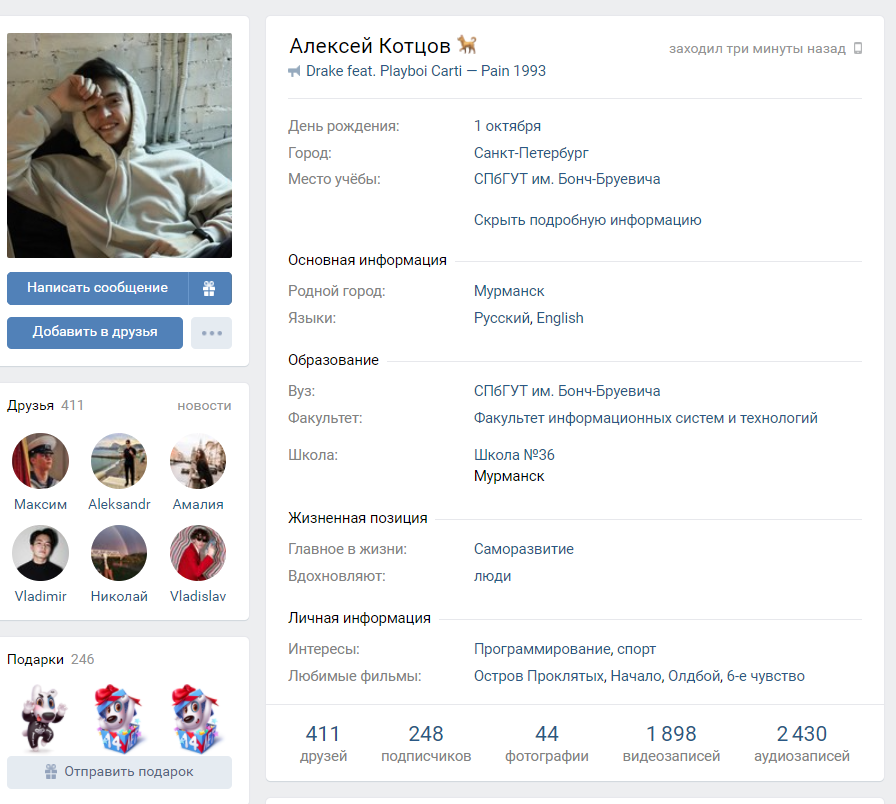
Рисунок 5 - Http-авторизация на найденном сервере.

# 5 Пример ручной таргетированной OSINT-атаки

Приведем пример сбора информации о личности, имея только страничку человека в социальных сетях. Страница нашей цели в социальной сети Вконтакте приведена на рисунке 6.

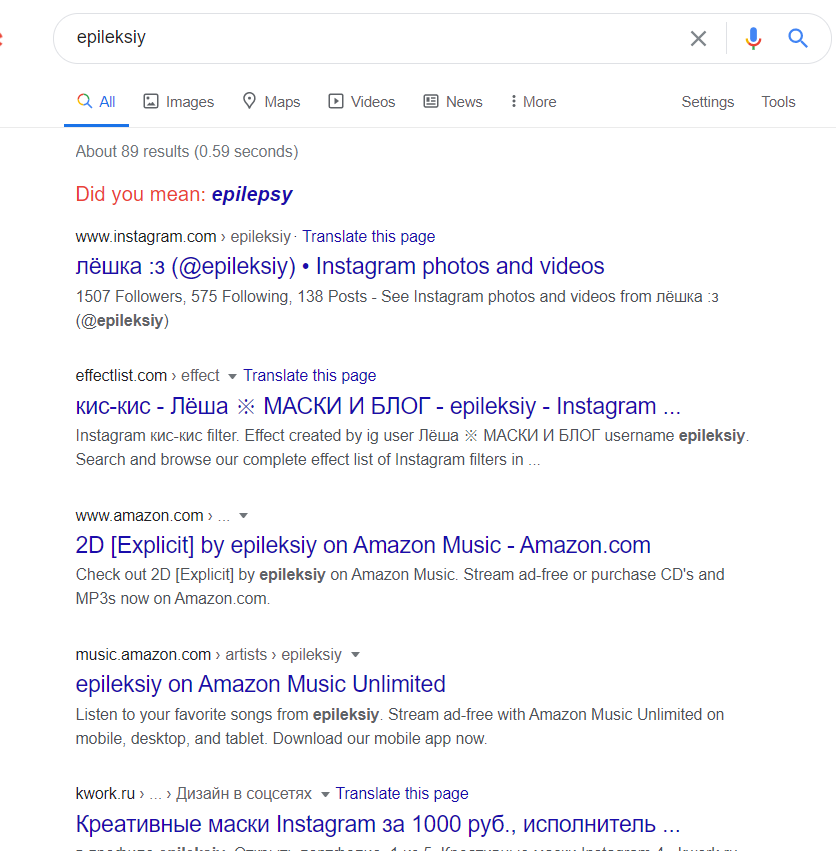
Исходя из страницы можно уже получить следующие данные о личности человека:

* обучается в СПБГУТ;
* день и месяц его рождения;
* место его предыдущего обучения;
* его примерные увлечения, исходя из список его сообществ;

Рисунок 6 - Страница цели в Вконтакте.

Как раз из списка его сообществ, можно наайти его личное сообщество, из которого мы получили его никнейм.

Следующим этапом является поисковой запрос с его никнеймом в Google, который приведен на рисунке 7.

Рисунок 7 - Поисковой запрос с никнеймом цели.

Данный этап дал доступ к следующей информации:

* страница на бирже фриланса, что позволило узнать род деятельности цели;
* страница в еще одной популярной социальной сети;

Страница на бирже фриланса приведена на рисунке 8.

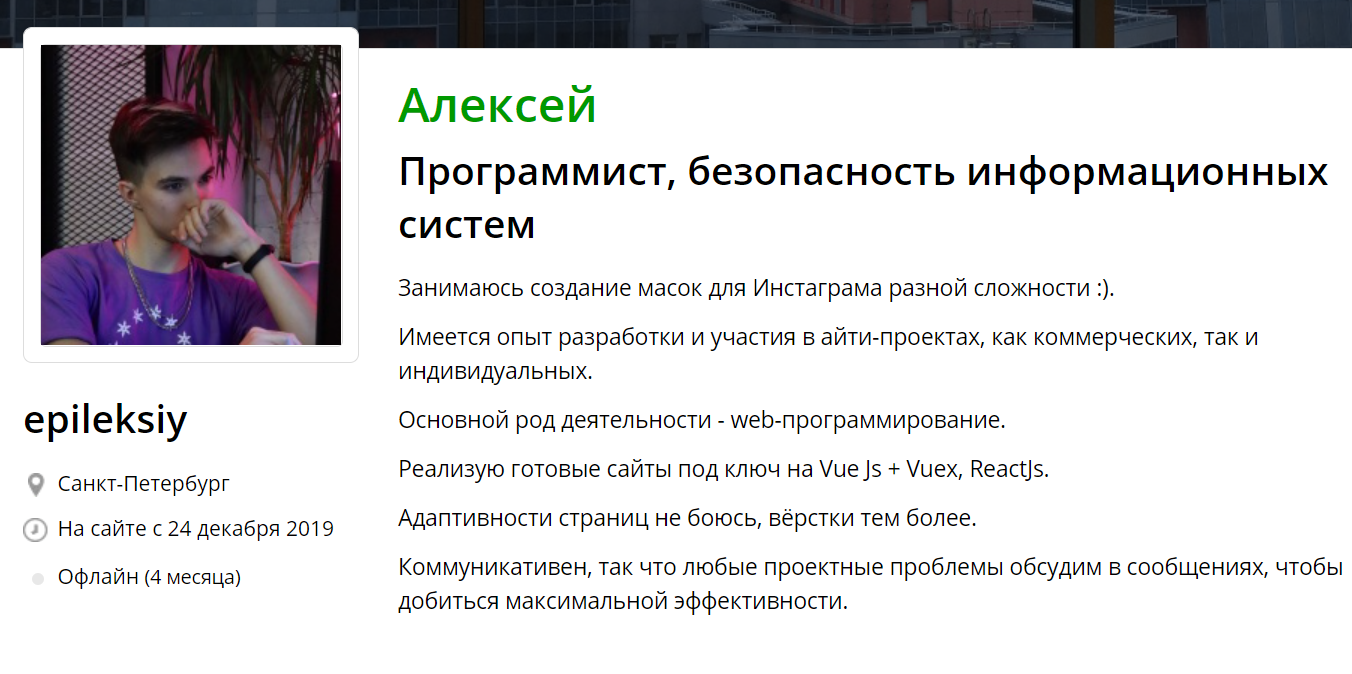
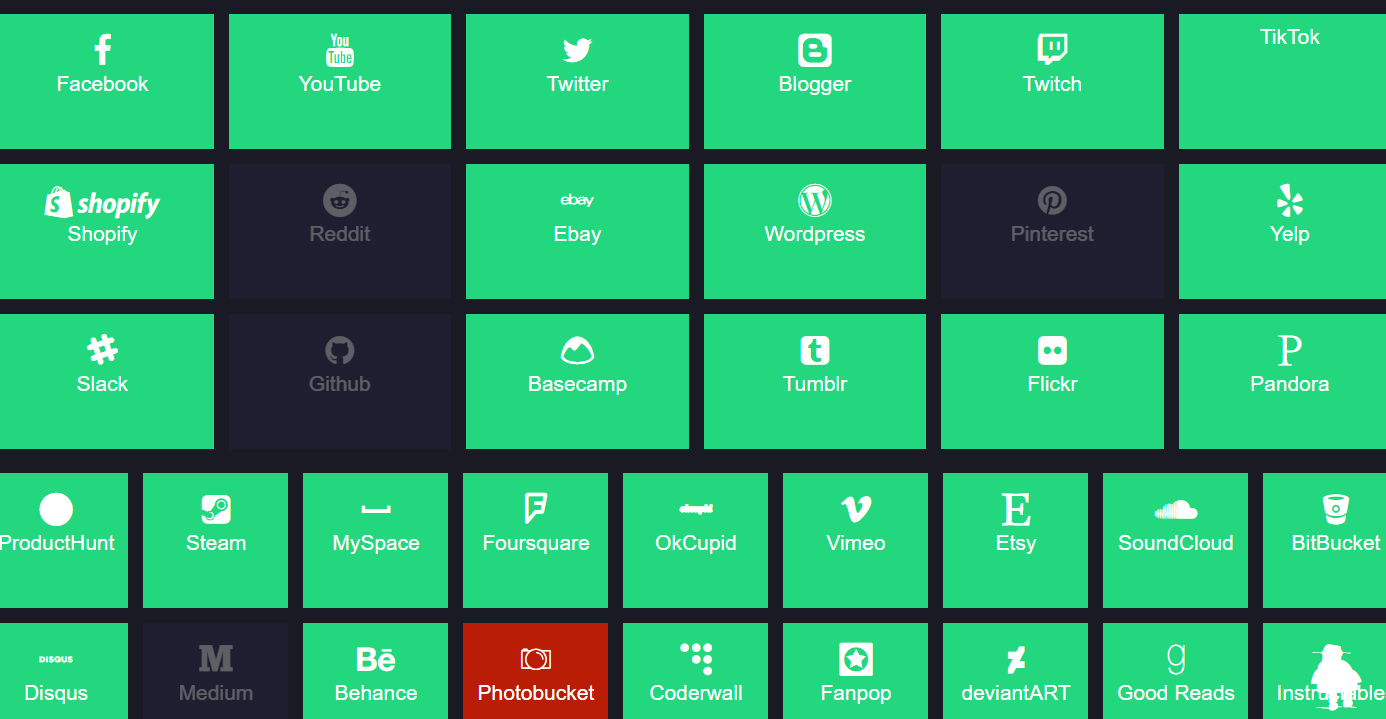


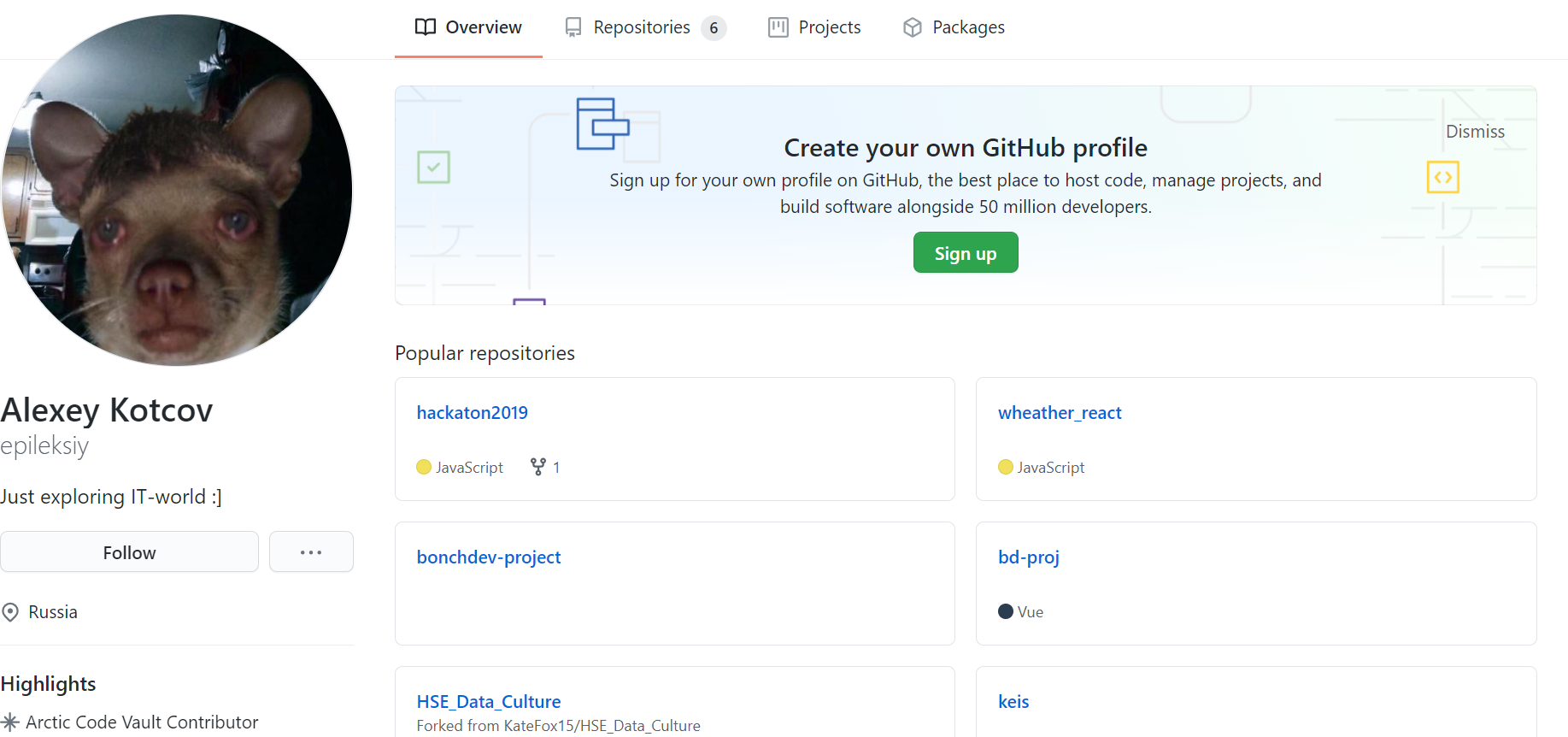
Рисунок 8 - Страница цели на бирже фриланса.

Воспользуемся онлайн-ресурсом, который ищет по нику страницы в различных социальных сетях. Поиск других страниц цели приведен на рисунке 9.

Рисунок 9 - Поиск других страниц цели.

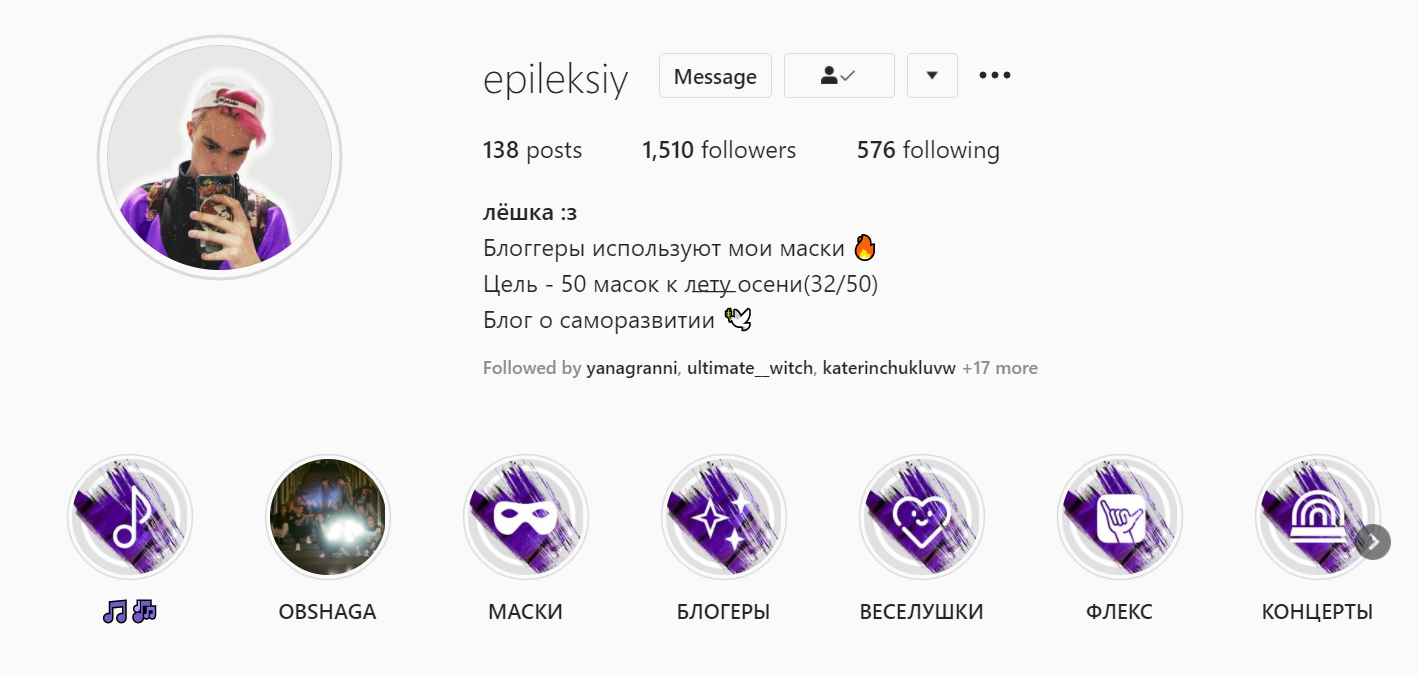
Благодаря вышеперечисленному этапу была найдена Github-страница пользователя, что дает доступ к его информационным проектам и позволяет оценить уровень его компетенции в данной области.

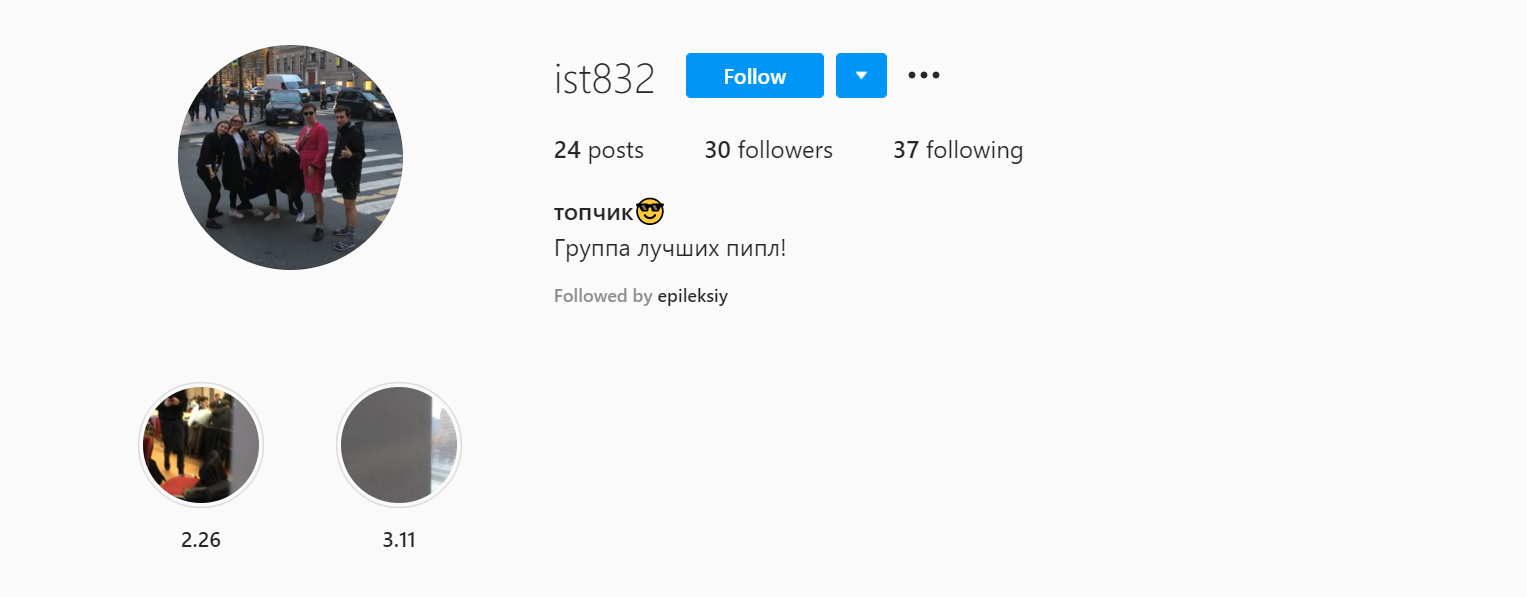
Найденная Github-страница приведена на рисунке 10.

Рисунок 10 - Страница с проектами цели.

Проверяя страницу и подписки цели в другой популярном ифнормационном ресурсе находим страницу учебной группы, в которой, вероятнее всего, и состоит наша цель.

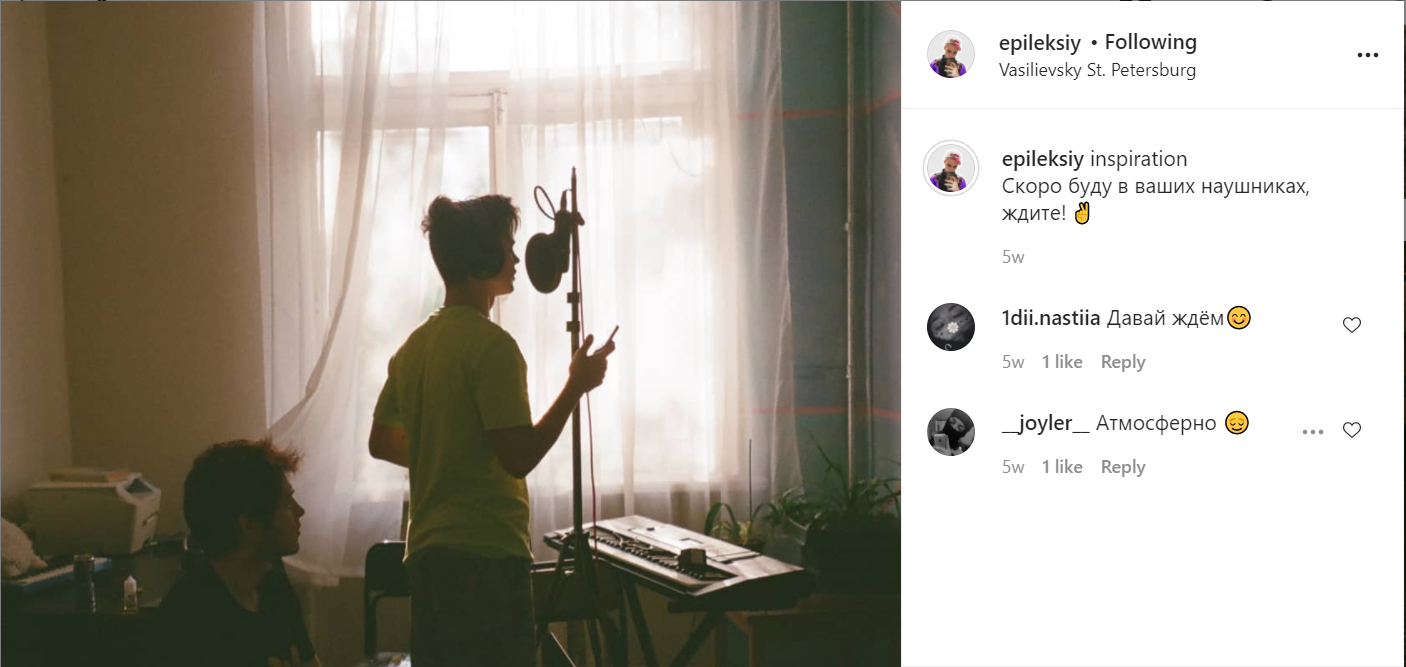
Страница цели и страница учебной группы приведены на рисунках 11 и 12 соответственно.

Рисунок 11 - Страница цели в сети Instagram..

Рисунок 12 - Страница учебной группы в сети Instagram.

Также с помощью анализа учетной записи в социальной сети Instagram выясняется, что цель проживает в общежитии, которое находится в одном конкретном районе.

Фотография с геотегом района проживания цели приведена на рисунке 13.

Рисунок 13 - Фотография с геотегом района проживания цели.

Исходя из вышеполученных данных можно получить точный адрес проживания жертвы. Для этого следует найти адреса всех общежитий учебного заведения цели и отсортировать по району.

Так как цель явно не обучается в колледже при СПБГУТ, то под все описания подходит только одно учреждение ля проживания.

Точный адрес данного учреждения приведен на рисунке 14.

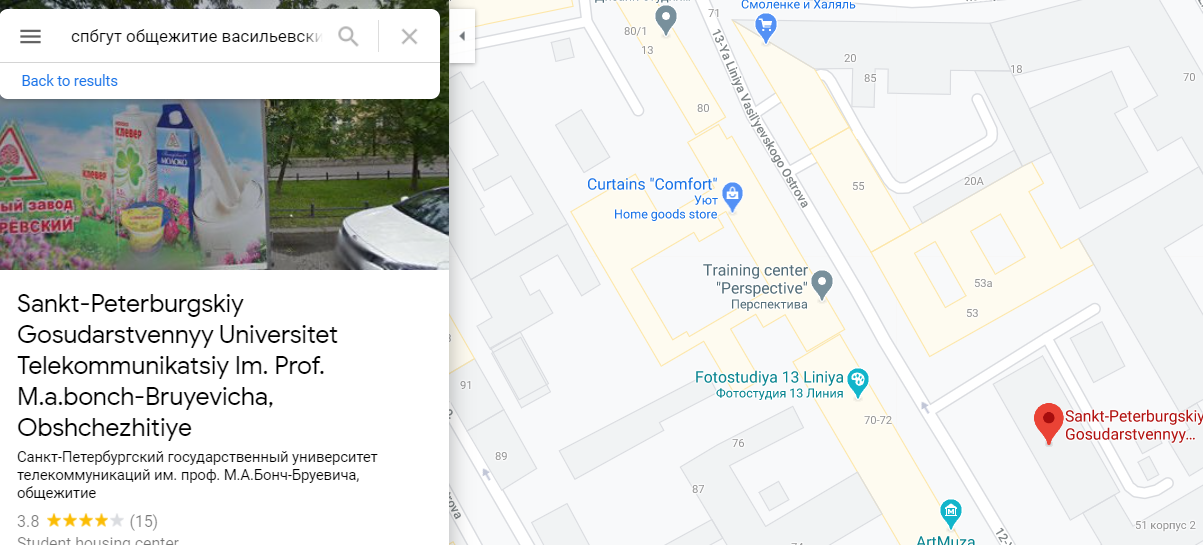


Рисунок 14 - Точный адрес общежития, в котором проживает цель.

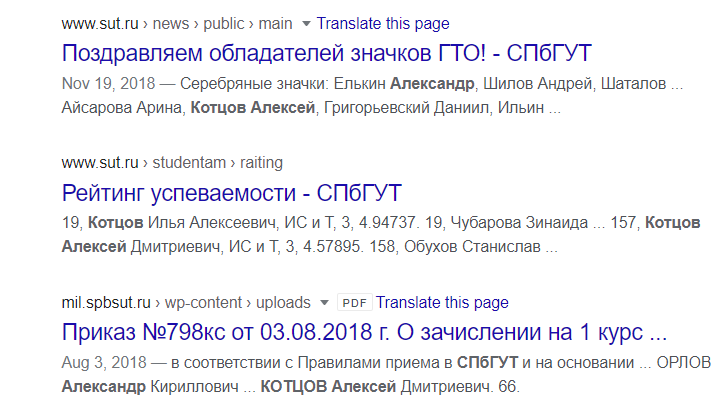
Также разными способами комбинируя фио цели, наименование учебного заведения и никнейм в поисковой системе можно добиться результата, который приведен на рисунке 15.

Рисунок 15 - Дополнительные данные, полученные путем простого поиска.

Вышеприведенный этап дал нам доступ к следующим данным:

* количество баллов за ЕГЭ цели;
* рейтинг успеваемости цели;
* участие в различных соревнованиях, что позволяет получить больше данных об увлечениях цели;

Подводим итог ручной OSINT-атаки. Имея одну страницу в Вконтакте пользователя удалось получить следующие данные:

* учебное заведение;
* день и месяц его рождения;
* точный адрес проживания;
* место его предыдущего обучения;
* примерные увлечения;
* учебная группа;
* хобби;
* количество баллов за ЕГЭ;
* рейтинг успеваемости цели;
* участие в различных соревнованиях;
* род деятельности;

Данная информация, полученная в кратчайшие сроки без использования различных программ, позволяет сформировать довольно подробный портрет личности человека, что значительно повышает вероятность успешной атаки посредством социальной инженерии.

# ЗАКЛЮЧЕНИЕ

Для хорошего специалиста по информационной безопасности важно ограничить поток данных, который течет в общедоступное пространство, поэтому один из необходимых для работы навыков как раз должен быть нацелен на консультацию рядовых сотрудников и сокрытие секретных корпоративных данных.

Подводя итог проделанной работы, отметим проводимые исследования и их результаты. В ходе курсовом проекта было проведено исследование технологии атаки OSINT и структуры данной атаки.

Были описаны цели данной атаки и разнообразные методы ее реализации.

Также были совершенны две демонстрационные атаки OSINT, одна из которых показывает действие популярной крупной программы Maltego, а другая описывает ручную разведку пользователя, а также примерный ход мысли злоумышленника.

# Список литературы

1. Что такое Maltego?. URL: https://kali.tools/?p=127 [дата обращения 27.11.2020].
2. Osintframework. URL: https://osintframework.com/ [дата обращения 27.11.2020].
3. Open Source Intelligence. URL:https://tssolution.ru/audit-informatsionnoy-bezopasnosti/osint [дата обращения 27.11.2020].
4. OSINT.URL:https://amonitoring.ru/service/osint/consulting/ [дата обращения 27.11.2020]