

**Министерство науки и высшего образования Российской Федерации  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет прикладной информатики**

**Дисциплина:**

**«Основы кибербезопасности»**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3**

**«Пассивная разведка и расширение поверхности атаки с помощью общедоступных  
инструментов»**

**Выполнил:**

Швалов Даниил Андреевич, студент группы К4112с

---

(подпись)

**Проверил:**

Кравчук Алексей Владимирович, доцент практики

---

(отметка о выполнении)

---

(подпись)

Санкт-Петербург  
2025 г.

## **СОДЕРЖАНИЕ**

1 Введение.....	3
2 Ход работы.....	3
2.1 Использование поисковых сервисов для поиска интернет-устройств и открытых сервисов.....	3
2.2 Поиск поддоменов организации.....	19
2.3 Визуальный поиск интересных сервисов с помощью httpx.....	30
2.4 Перебор web-директорий.....	33
2.5 Автоматизация: subfinder с API (Censys, Shodan, Netlas).....	34
3 Вывод.....	35

## 1 Введение

Цель работы:

- 1) изучить методы пассивной разведки (OSINT) для увеличения внешней поверхности атаки организации (всех открытых сетевых ресурсов, которые могут стать целями злоумышленников);
- 2) освоить работу с поисковыми сервисами для поиска интернет-устройств и открытых сервисов: Shodan, Censys и/или Netlas;
- 3) оценить риски, связанные с обнаруженными открытыми ресурсами, и понять, какие меры можно предпринять для сокращения поверхности атаки (в том числе из Приказа № 17 ФСТЭК и Методич.документа).

## 2 Ход работы

### 2.1 Использование поисковых сервисов для поиска интернет-устройств и открытых сервисов

В начале работы в почтовом сервисе Proton Mail была зарегистрирована и подтверждена новая электронная почта. Это видно на рисунке 1.

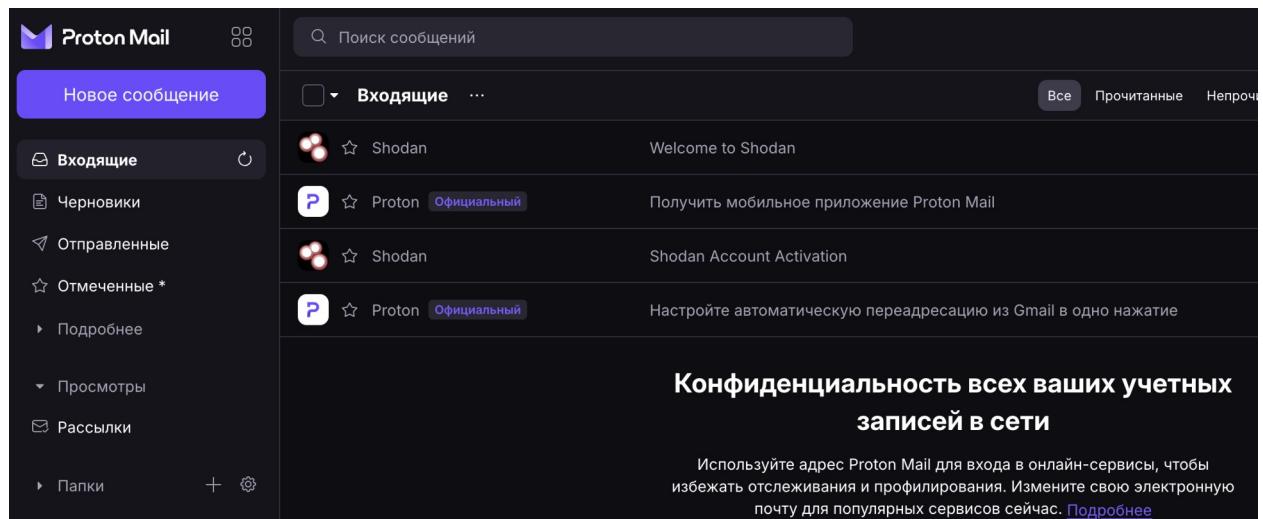


Рисунок 1 — Зарегистрированная электронная почта в сервисе Proton Mail

После этого ранее зарегистрированная электронная почта Proton Mail была использована при регистрации аккаунта в Shodan, что видно на рисунке 2.

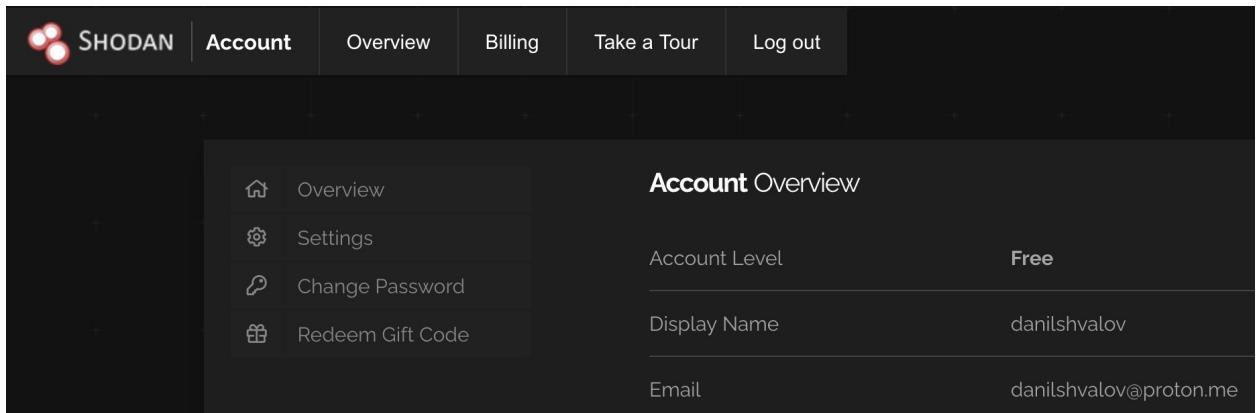


Рисунок 2 — Зарегистрированный аккаунт в Shodan

После регистрации с помощью поисковой строки и фильтра «`hostname:"itmo.ru"`» была найдена информация о сайте itmo.ru. Результат поиска в Shodan представлен на рисунке 3.

Category	Details	Count
TOP PORTS	Nextcloud (port 81), ITMO University (port 147), Yandex.Cloud LLC (port 38), etc.	226
TOP ORGANIZATIONS	ITMO University, Yandex.Cloud LLC, Saint-Petersburg State University of Information, Vuztelecomcentre, Intertelecomservice Ltd.	147
TOP PRODUCTS	nginx, Apache httpd, OpenSSH, Postfix smtpd, GitLab Self-Managed	53
TOP OPERATING SYSTEMS	Ubuntu, Linux	43

Рисунок 3 — Информация о itmo.ru в Shodan

После этого был открыт подраздел «Top Ports». Как видно на рисунке 4, у itmo.ru есть множество портов, которые нежелательно оставлять открытыми в Интернет, например, следующие порты:

- 1) 111 — этот порт чаще всего используется для удаленного вызова процедур внутри локальной сети;
- 2) 3306 и 5432 — эти порты используются для доступа к выполнению SQL в MySQL и PostgreSQL соответственно;
- 3) 3389 — этот порт используется для подключения к удаленному рабочему столу.

Открытие вышеперечисленных портов может привести к угрозам безопасности, особенно если ПО, использующее эти порты, использует настройки по умолчанию (например, стандартные логин и пароль). Также по рисунку 4 можно сделать следующие выводы:

- 1) к некоторым страницам возможен доступ по HTTP, а не по HTTPS (об этом говорит доступ по 80 порту);
- 2) некоторые порты были выставлены в Интернет непреднамеренно, например, 8001, 8003, 8082, 8888.

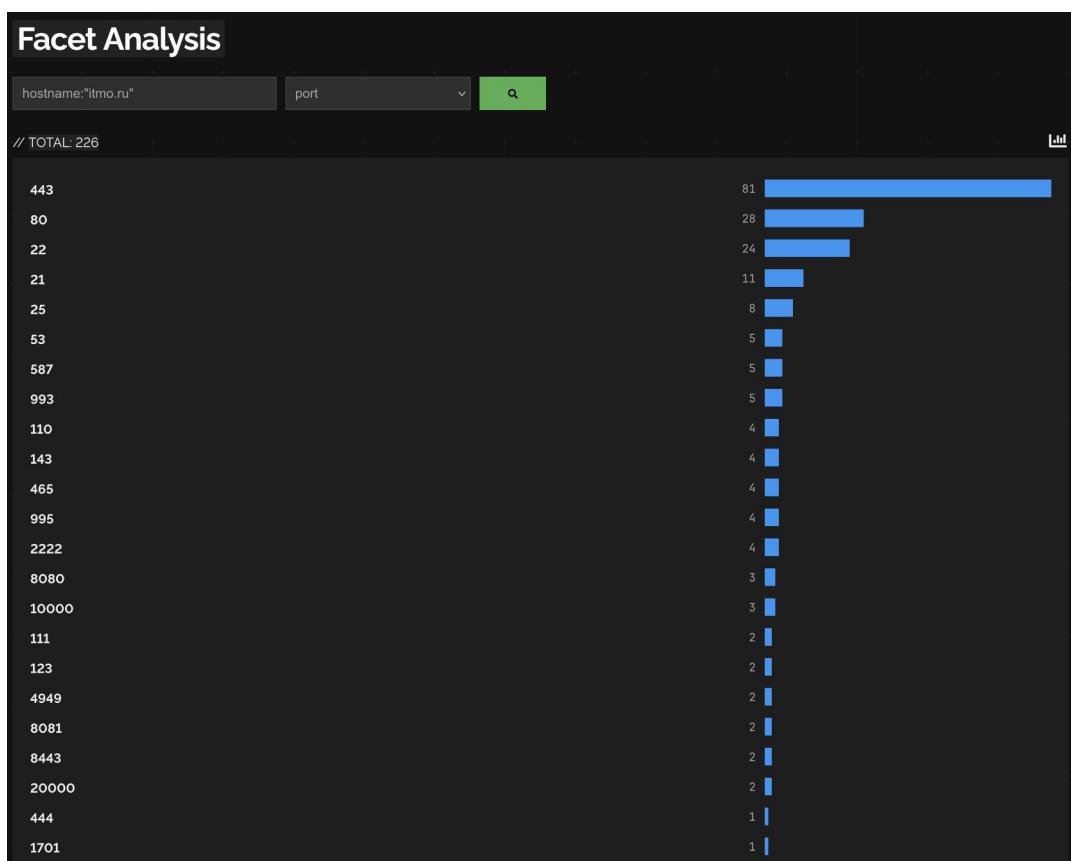


Рисунок 4 — Подраздел «Top Ports»

В таблице 1 приведена информация о сервисах, работающих на определенных портах.

Таблица 1 — Информация о сервисах, работающих на определенных портах

№ п/п	IP-адрес	Порт	Сервис, работающий на порте	Примечание
1	77.234.222.59	22	SSH, т. е. зашифрованный доступ к оболочке удаленного сервера по TCP	Используется стандартный порт SSH, что не очень хорошо с т. з. ИБ, т. к. может использоваться для брут-форса паролей
2	77.234.222.92	2222	SSH, т. е. тоже самое, что и 22 порт	Используется очень распространенный порт SSH, что не очень хорошо с т. з. ИБ, т. к. может использоваться для брут-форса паролей
3	77.234.215.140	3306	Стандартный порт для доступа к выполнению SQL в СУБД MySQL	Порт для доступа к MySQL лучше не открывать в Интернет, тем более стандартный, т. к. он может использоваться для брут-форса паролей и несанкционированному доступу к данным
4	77.234.222.91	3389	RDP, т. е. удаленный рабочий стол	Порт для доступа к RDP лучше не открывать напрямую, вместо этого следует предоставлять доступ к RDP через VPN. Для минимизации рисков можно использовать другой порт для RDP. Открытый RDP порт может использоваться для брут-форса паролей, MitM-атак, эксплуатации уязвимостей ПО

5	77.234.216.51	5060	SIP, т. е. протокол для установления сеанса для IP-телефонии	Открытие SIP порта в Интернет может привести к спам-звонкам, DDoS, перехвату данных. Чтобы избежать этого, следует скрывать SIP порт под VPN.
6	77.234.222.54	5432	Стандартный порт для доступа к выполнению SQL в СУБД PostgreSQL	Порт для доступа к PostgreSQL лучше не открывать в Интернет, тем более стандартный, т. к. он может использоваться для брут-форса паролей и несанкционированному доступу к данным
7	77.234.216.51	7443	Oracle Application Server, т. е. для доступа к серверам приложений и административным интерфейсам	Стандартный порт для доступа к Oracle Application Server, может привести к угрозам из-за эксплуатации уязвимостей ПО и выполнения вредоносного кода. По возможности порт лучше не открывать или прятать под VPN
8	77.234.222.93	10000	Webmin, т. е. ПО для администрирования ОС через веб-интерфейс	Используется стандартный порт Webmin, что не очень хорошо с т. з. ИБ, т. к. может использоваться для брут-форса паролей. Лучше всего скрывать доступ к Webmin под VPN

После этого был открыт подраздел «Top Organizations», представленный на рисунке 5.

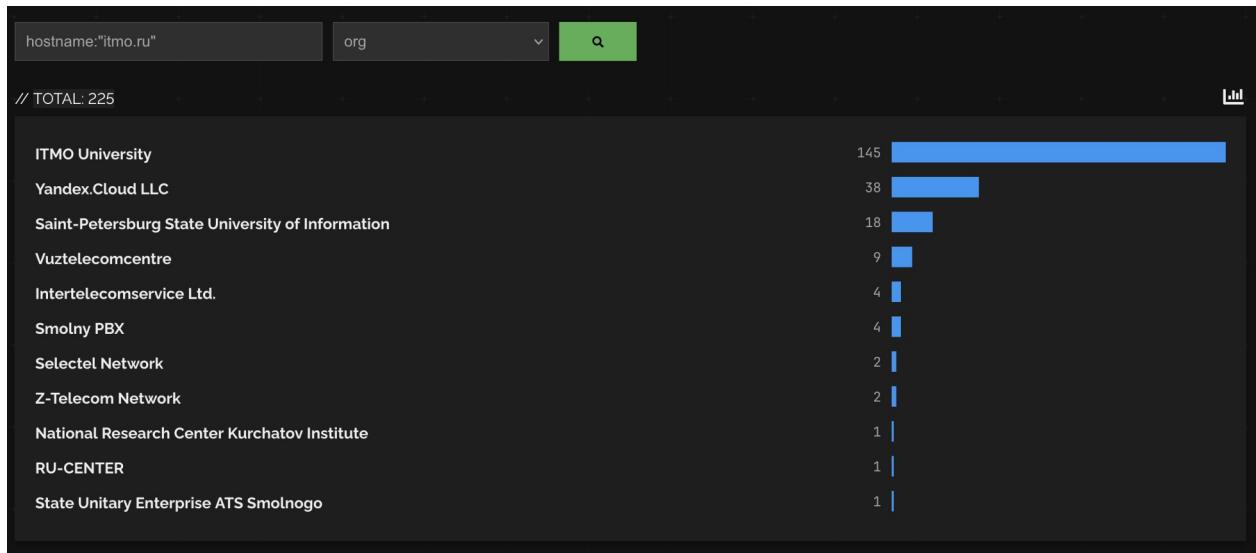


Рисунок 5 — Содержимое подраздела «Top Organizations» для itmo.ru

Как видно на рисунке 6, с помощью этого подраздела можно получить информацию об используемых портах и IP-адресах, используемом ПО и ОС в инфраструктуре организации.

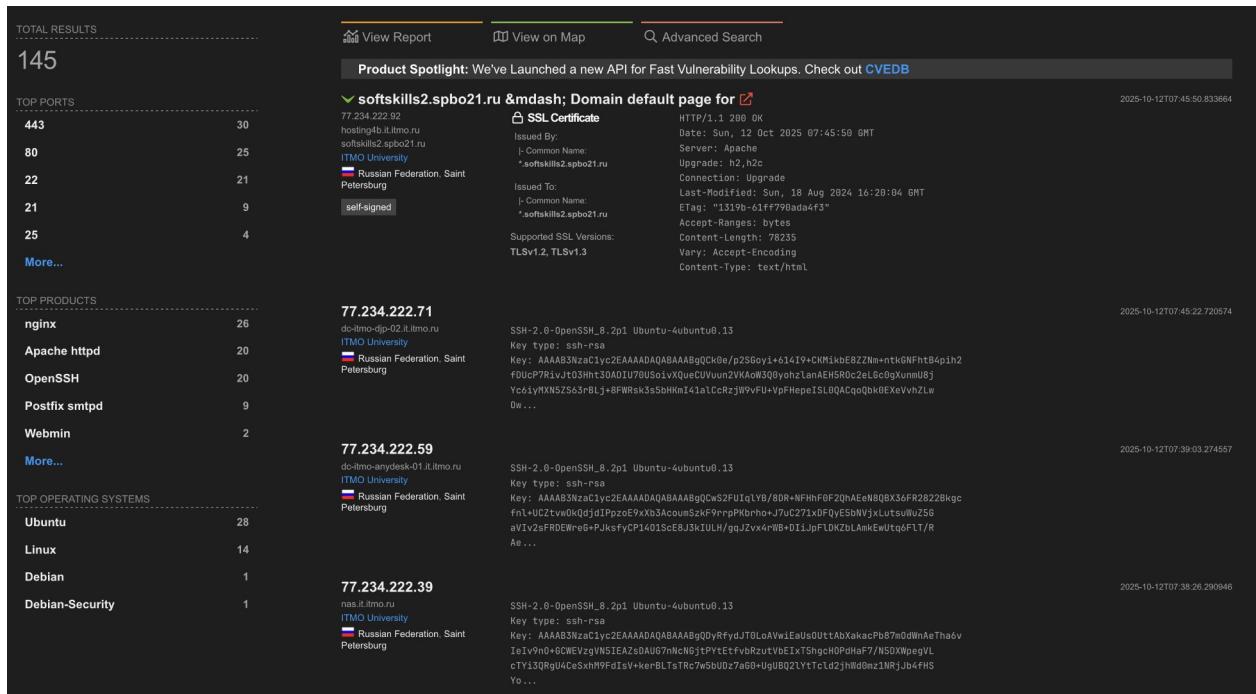


Рисунок 6 — Информация об инфраструктуре у организации ITMO University  
В таблице 2 представлен анализ вышеперечисленных организаций.

Таблица 2 — Анализ организаций

<b>Организация</b>	<b>Возможная интерпретация</b>
ITMO University (145)	Большая часть IP действительно принадлежит подсетям, зарегистрированным на сам университет (у ИТМО есть собственная автономная система, AS60340, и пул адресов). Это основная инфраструктура вуза.
Yandex.Cloud LLC (38)	Некоторые сервисы ИТМО (например, веб-сайты, тестовые порталы, API, возможно облачные лаборатории) размещены в облаке Яндекса.
Saint-Petersburg State University of Information (18)	Также часть основной инфраструктуры вуза, принадлежит ИТМО, в ней размещены различные веб-сайты и порталы, в т. ч. ISU.
Vuztelecomcentre (9)	Является структурным подразделением департамента ИКИ Университета ИТМО и выполняет ряд функций департамента.
Intertelecomservice Ltd. (4)	Некоторые сервисы ИТМО (например, веб-сайт библиотеки, хранилище статических данных) размещены в облаке ООО «ИТКС».
Smolny PBX (4)	Некоторые сервисы ИТМО (например, itmo.ru) размещены в инфраструктуре АТС Смольного
Selectel Network (2)	Некоторые сервисы ИТМО (например, ISU) размещены в облаке Selectel.
Z-Telecom Network (2)	Некоторые сервисы ИТМО (например, bal-itmo.ru) размещены в облаке Z-Telecom.
National Research Center Kurchatov Institute (1)	Некоторые инфраструктурные службы ИТМО (например, GitLab) размещены в Курчатовском институте
RU-CENTER (1)	АО «Региональный Сетевой Информационный Центр», крупнейший регистратор доменных имён и хостинг-провайдер в России.

State Unitary Enterprise ATS Smolnogo (1)	Смольный, инфраструктура Правительства Санкт-Петербурга. Вероятно, сетевой сегмент, предоставленный вузу для связей с городскими системами.
--	---

После этого был открыт подраздел «Top Products», представленный на рисунке 7.

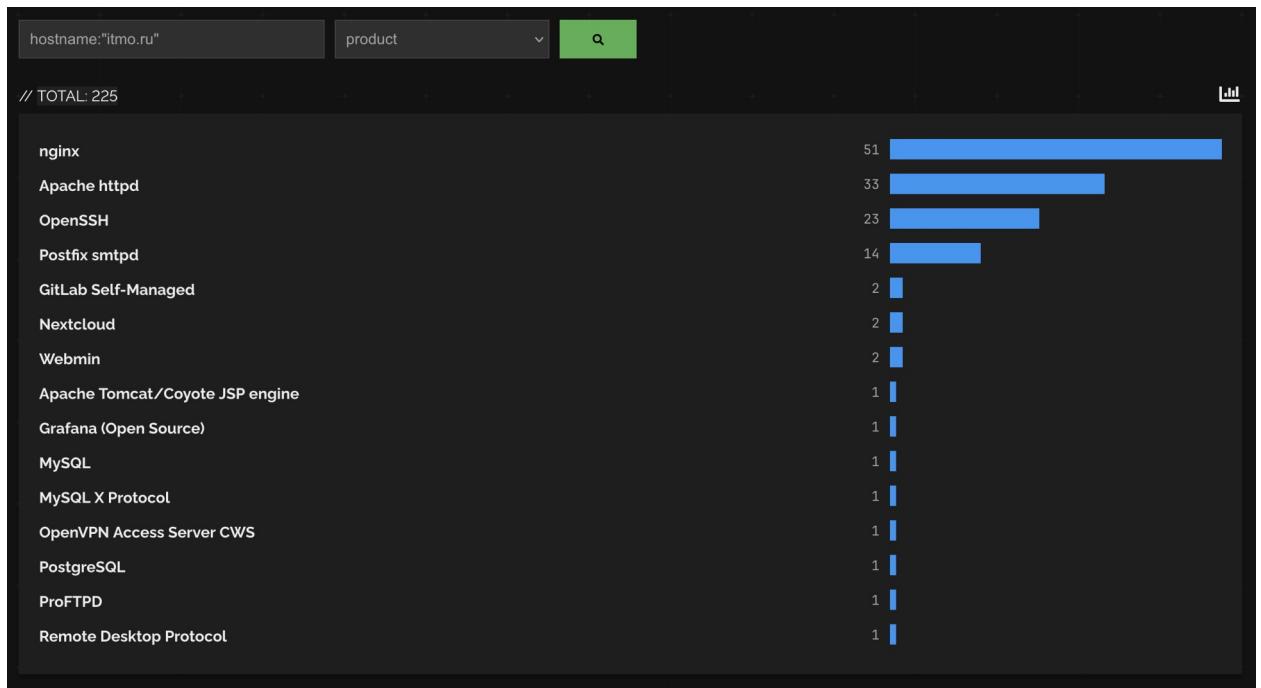


Рисунок 7 — Содержимое подраздела «Top Products» для itmo.ru

С помощью этого подраздела можно получить подробную информацию о ПО, которое используется в инфраструктуре ИТМО. Например, на рисунке 8 приведена информация об использовании nginx в инфраструктуре ИТМО. Как видно на рисунке, в Shodan можно определить, какие порты и версии используются ПО, на каких IP-адресах было обнаружено ПО.

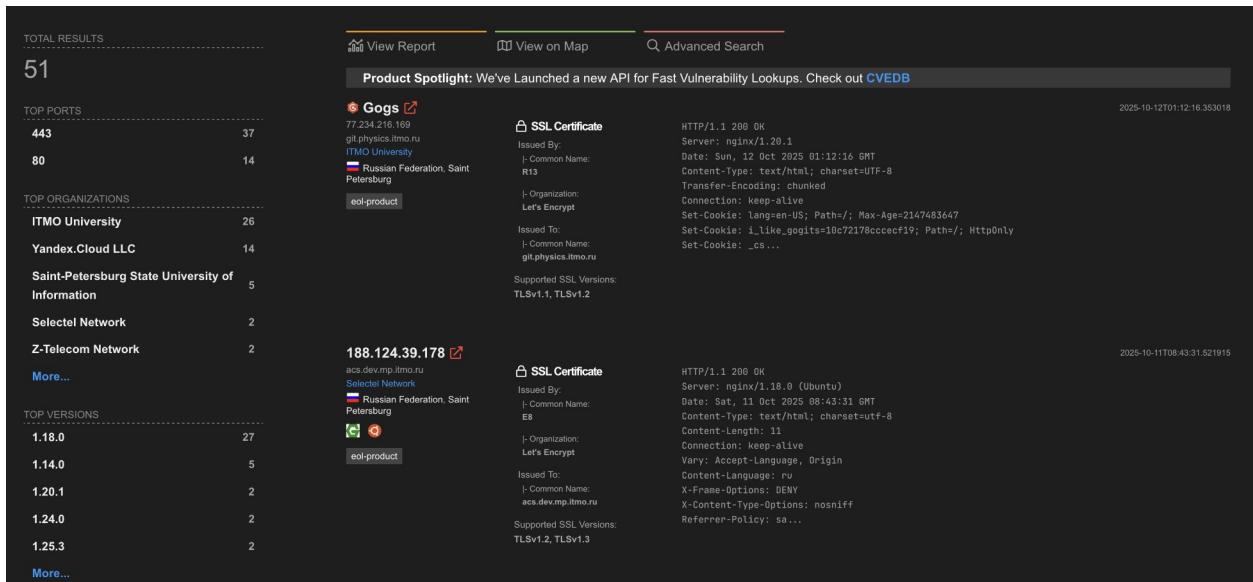


Рисунок 8 — Информация о nginx в инфраструктуре ИТМО

Как видно на рисунке 7, у ИТМО открыт доступ как к вполне ожидаемому ПО (например, nginx, Apache httpd, OpenSSH), так и к ПО, которое не должно иметь выход в Интернет (например, Grafana, Webmin), т. к. это может повлечь за собой риски в безопасности. В таблице 3 приведены сервисы, наиболее критичные с точки зрения возможности взлома.

Таблица 3 — Сервисы, наиболее критичные с точки зрения возможности взлома

Название ПО	Краткое описание того, какие возможности предоставляются злоумышленнику
Webmin	Полный контроль над сервером, кража конфиденциальных данных или секретов, установка ВПО, использование для дальнейших атак на внутреннюю сеть, отказ в обслуживании
Remote Desktop Protocol	Полный контроль над сервером, кража конфиденциальных данных или секретов, установка ВПО, фишинговые атаки, утечка данных, использование для дальнейших атак на внутреннюю сеть, блокировка системы

MySQL	Кража конфиденциальных, персональных данных или секретов, удаление или изменение данных, которое может привести к отказу в обслуживании, фишинговые атаки, доступ к другим системам
PostgreSQL	Кража конфиденциальных, персональных данных или секретов, удаление или изменение данных, которое может привести к отказу в обслуживании, фишинговые атаки, доступ к другим системам
Grafana	Несанкционированный доступ к внутренним системам, контроль систем мониторинга, возможность повышения привилегий при неправильной настройке прав доступа, использование скомпрометированной системы для атак на другие ресурсы, утечка слабых мест системы

В качестве аналога Shodan был выбран сервис Netlas. После регистрации в первую очередь с помощью вкладки «IP/Domain info» была получена базовая информация о домене: регистрант, MX и NS записи, связанные домены, IP-адрес. Данная информация в интерфейсе Netlas представлена на рисунке 9.

The screenshot shows the Netlas.io web interface. At the top, there's a navigation bar with links for 'Search', 'Discover', 'Scan', and 'Datastore'. On the left, there's a sidebar with icons for 'Host' (selected), 'IP alias', 'D whois', and 'Logs'. The main search bar contains the query 'itmo.ru'. Below the search bar, the results for 'itmo.ru' are displayed, showing an A record at 51.250.120.146. The 'Whois data for itmo.ru' section shows the registrant as ITMO University, emails as 'Not available on your subscription plan', and phones as 'Not available on your subscription plan'. It also lists the registrar as RU-CENTER-RU and emails as 'Not available on your subscription plan'. The 'Phone' field is also listed as 'Not available on your subscription plan'. The 'Related domains' section lists several subdomains like ai-programs.itmo.ru, ec.itmo.ru, aicltr.itmo.ru, monitoring.it.itmo.ru, and preview.dc-edu.itmo.ru. The 'MX records' section shows emx.mail.ru, and the 'NS records' section shows ns.itmo.ru, ns5.itmo.ru, ns3.itmo.ru, and ns2.itmo.ru. At the bottom, sections for 'Reputation Score' (not available) and 'Exposed Web Services & Software' (no exposed ports found) are shown.

Рисунок 9 — Поиск базовой информации о домене

После этого с помощью вкладки «Response searches» были найдены все ответы на запросы по домену my.itmo.ru. В данном разделе отображается такая информация, как тело ответа, IP-адрес сервера, примерное расположение сервера, порты, на которые отвечает сервер.

DESCRIPTION	RESPONSE	WHOIS	CVE	CONTACTS	...
Europe / RU City: Moscow Moscow Location: 55.7483, 37.6171 ISP: Yandex.Cloud LLC ASN: 200350 Port: 80/tcp Protocol: http	<pre> 1+ { 2+   "headers": { 3+     "date": [ 4+       "Sun, 14 Sep 2025 21:11:36 GMT" 5+     ], 6+     "content_type": [ 7+       "text/html" 8+     ], 9+     "location": [ 10+       "https://my.itmo.ru" 11+     ], 12+     "connection": [ 13+       "keep-alive" 14+     ], 15+     "content_length": [ </pre>				...
Europe / RU City: Moscow Moscow Location: 55.7483, 37.6171	<pre> 1+ { 2+   "headers": { 3+     "date": [ 4+       "Sun, 14 Sep 2025 21:11:47 GMT" </pre>				...

Рисунок 10 — Информация об ответах на запросы по домену my.itmo.ru

После этого с помощью вкладки «DNS Search» были найдены все поддомены itmo.ru. В результатах поиска представлена такая информация как уровень домена, значение A, NS и MX записей, а также DNS-зона. Список найденных поддоменов представлен на рисунке 11.

Domain	Type	IP Address	MX
trac.lcps.itmo.ru	A	51.250.120.169	-
warehouse.it.itmo.ru	A	77.234.222.58	-
bars.itmo.ru	A	31.41.155.212	-
t-masters.itmo.ru	A	51.250.120.169	-
www.ecinn.itmo.ru	A	185.215.4.10	-
faculty.itmo.ru	A	77.234.212.24	-
remote.it.itmo.ru	A	77.234.222.59	-
olymp.physics.itmo.ru	A	77.234.203.238	-
moodle.itmo.ru	A	51.250.115.130	-
sm.itmo.ru	A	77.234.222.55	-

Summary: Zones (434), Levels (4, 3).

Рисунок 11 — Поиск поддоменов itmo.ru

После этого с помощью вкладки «IP WHOIS Search» была найдена информация о IP-адресе 77.234.215.138. Как видно на рисунке 12, для данного IP-адреса удалось получить название и номер AS, описание и примерный адрес.

DESCRIPTION	NET INFO	RELATED NETS	CONTACTS	RAW	...
Russia/RU CIDR: 77.234.212.0/22 Created: 09/11/2007 Updated: 10/29/2015 Registry: ripencc Abuse: not available	Network: 77.234.212.0 - 77.234.215.255 (CIDR: 77.234.212.0/22, Net size: 1023) Name: ITMO-NET Description: Saint-Petersburg State University of Information Technologies, Mechanics and Optics Kronverksky, 49 197101, St.Petersburg, Russian Federation Handle: ITMO-RIPE Address: RU, IT March Operations, St. Petersburg, Russia AS name: ITMO-AS ITMO AS number: 42289				

Filter mapping:  
Addressing: ip  
Information: abuse, asn, net, related\_nets  
Service fields: timestamp, raw

Рисунок 12 — Поиск информации по IP-адресу

После этого с помощью вкладки «Discover» был построен график с

информацией о домене. Для этого, как показано на рисунках 13-14, был добавлен узел с доменом itmo.ru.

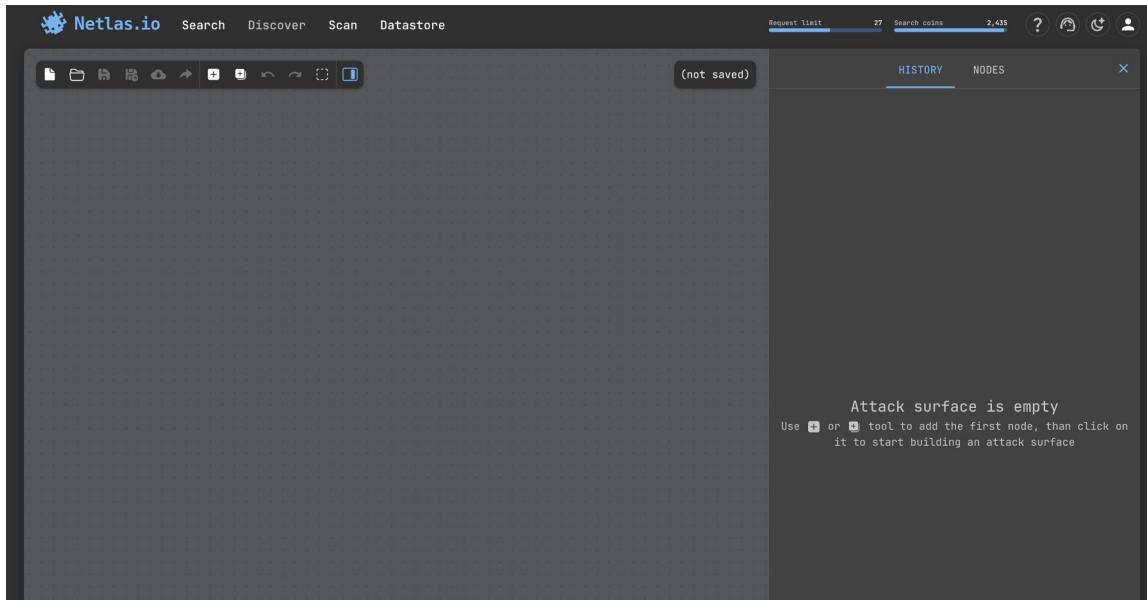


Рисунок 13 — Вкладка Discover

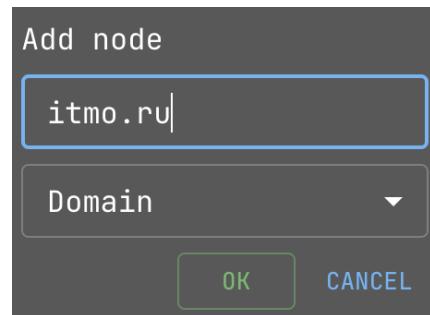


Рисунок 14 — Добавление узла

После добавления в узле появилась подробная информация о домене: TXT и A записи, NS и почтовые сервера, а также поддомены, что видно на рисунке 15.

The screenshot shows a list of domain records for 'itmo.ru'. It includes:

- TXT records for domain (19)**: A list of 19 entries starting with '\_globalsign-domain-verification='.
- Mailservers for domain (1)**: An entry for 'emx.mail.ru'.
- NS servers for domain (4)**: Entries for 'ns.itmo.ru', 'ns2.itmo.ru', 'ns3.itmo.ru', and 'ns5.itmo.ru'.
- A records for domain (1)**: An entry for '51.250.120.146'.
- Subdomains (434)**: A list of subdomains including '1.s3.itmo.ru', '1c-srv.itmo.ru', '1cdbftmi.it.itmo.ru', '1csrvftmi.it.itmo.ru', and '2.s3.itmo.ru'.
- Organization from WHOIS (1)**: A note stating 'This data is not available on your subscription plan'.
- Hosts with domain in certificate (35)**: A note stating 'This data is not available on your subscription plan'.

Рисунок 15 — Информация о домене

Данная информация также была добавлена на график с помощью кнопки «Add & Group». Благодаря этому получилось построить небольшой график, с помощью которого можно визуализировать поверхность атаки. Получившийся график представлен на рисунке 16.

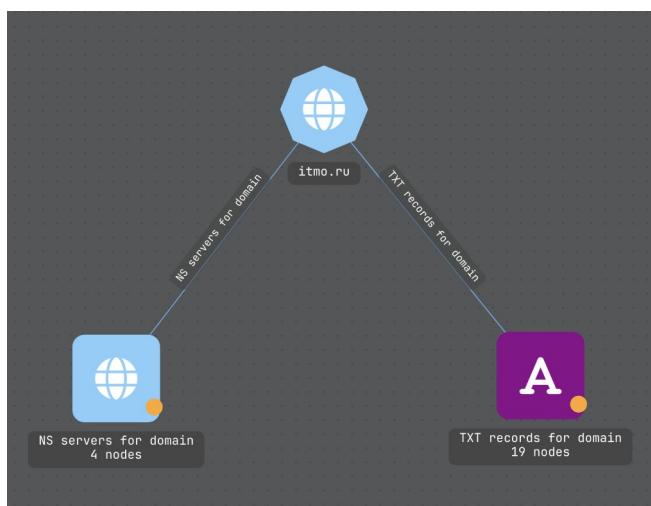


Рисунок 16 — Получившийся график

После этого в Shodan с помощью фильтра «`hostname:"itmo.ru"` `http.html:"ifmo"`» был найден IP-адрес поддомена `aip.itmo.ru`, относящийся к Академии информатики и программирования. Результат поиска в Shodan представлен на рисунке 17.

The screenshot shows the Shodan search interface with the query `hostname:"itmo.ru" http.html:"ifmo"`. The results section displays one entry:

**Академия информатики и программирования**

77.234.215.138 **SSL Certificate**

Issued By: Let's Encrypt

- Common Name: `R13`

- Organization: Let's Encrypt

Issued To: `aip.itmo.ru`

- Common Name: `aip.itmo.ru`

Supported SSL Versions: `TLSv1, TLSv1.1, TLSv1.2`

HTTP/1.1 200 OK  
Server: nginx/1.20.1  
Date: Mon, 22 Sep 2025 11:29:39 GMT  
Content-Type: text/html; charset=utf-8  
Content-Length: 30604  
Connection: keep-alive  
X-Powered-By: Magic power  
X-Content-Type-Options: nosniff  
X-Frame-Options: SAMEORIGIN  
X-XSS-Protection: 1; mode=block  
Strict-Trans...

Рисунок 17 — Информация о `aip.itmo.ru`

Полученный IP-адрес был скопирован и вставлен в сервис поиска 2IP. Результат поиска представлен на рисунке 18.

**77.234.215.138**

Тип адреса: IPv4

Местоположение: Санкт-Петербург, Россия

Провайдер: СПБНИИ ИТМО

ASN (BGP): 42289

Подсети: 77.234.212.0 - 77.234.215.255

Домашняя страница AS: vuztc.ru

Abuse: abuse@vuztc.ru

Хост: vkolymp.ifmo.ru

Часовой пояс: Europe/Moscow

**Карта**

59°56'03.4"N 30°20'06.4"E Увеличить карту

Швеция  
Норвегия  
Дания  
Польша  
Беларусь  
Германия  
Ирландия  
Россия

Быстрые клавиши Картографические данные ©2025 Google, INEGI - Установка

Рисунок 18 — Информация о IP-адресе 77.234.215.138

Из результатов поиска, представленного на рисунке 18, был скопирован номер автономной сети. После этого он был использован в сервисе bgp.he.net. На вкладке «Prefixes v4», которая представлена на рисунке 19, представлены подсети, относящиеся к ИТМО.

The screenshot shows the 'Prefixes v4' section of the bgp.he.net website. At the top, there's a logo for Hurricane Electric Internet Services and a search bar. Below that, the AS number 'AS42289 ITMO University' is displayed. The main content is a table with columns: 'Prefix', 'Description', and 'Visibility'. The table lists various IP prefixes and their associated organizations. Most entries show 100% visibility, except for one entry which shows 0% visibility. The table also includes a footer indicating 'Showing 1-14 of 14' results.

Prefix	Description	Visibility
77.234.192.0/19	ITMO University	100% 796/796
77.234.196.0/23	ITMO University	100% 796/796
77.234.196.0/24	Vuztelecomcentre	100% 796/796
77.234.199.0/24	Saint-Petersburg State University	100% 796/796
77.234.203.0/24	Cashpur Ulia	100% 796/796
77.234.205.0/24	Smolny PBX	100% 796/796
77.234.207.0/28		0% 1/796
77.234.209.0/24	Intertelecomservice Ltd.	100% 796/796
77.234.210.0/24	RU-ITMO	100% 796/796
77.234.217.0/24	State Unitary Enterprise "ATS Smolnogo"	100% 796/796
77.234.219.0/24	State Unitary Enterprise "ATS Smolnogo"	100% 796/796
77.234.223.0/24	Intertelecomservice Ltd.	100% 796/796
194.85.160.0/22	Saint-Petersburg State University of Information	100% 796/796
194.85.164.0/23	Saint-Petersburg State University of Information	100% 796/796

Рисунок 19 — Информация о префиксах IPv4

По подсетям с рисунка 19 можно сделать следующие выводы:

- 1) Академия информатики и программирования размещена внутри инфраструктуры ИТМО;
- 2) часть инфраструктуры ИТМО размещена на собственных адресах, часть на адресах, относящихся к другим организациям и провайдерам;
- 3) поскольку инфраструктура ИТМО размещается не только на своих мощностях, но и на мощностях внешних организаций, то одним из слабых мест при атаке может быть какая-либо из внешних организаций.

В таблице 4 приведены меры защиты информации из Приказа ФСТЭК №17, касающиеся размещения публичных интерфейсов в открытом доступе.

Таблица 4 — Меры защиты информации из Приказа ФСТЭК №17, касающиеся размещения публичных интерфейсов в открытом доступе

Мера из нормативных документов ФСТЭК	Описание меры
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, односторонняя передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы

## 2.2 Поиск поддоменов организации

Для выполнения последующих заданий был установлен дистрибутив Kali Linux. После окончания установки были обновлены репозитории пакетов и установлены все необходимые пакеты. Процесс установки пакетов представлен на рисунке 20.

```
(a1㉿kali)-[~]
└─$ sudo apt update
[sudo] password for a1:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
743 packages can be upgraded. Run 'apt list --upgradable' to see them.

(a1㉿kali)-[~]
└─$ mkdir -p ~/osintlab_3/

(a1㉿kali)-[~]
└─$ cd osintlab_3

(a1㉿kali)-[~/osintlab_3]
└─$ sudo apt install -y tree curl nmap jq gobuster dnsutils seclists dnsrecon
Note, selecting 'bind9-dnsutils' instead of 'dnsutils'
tree is already the newest version (2.2.1-1).
tree set to manually installed.
curl is already the newest version (8.15.0-1).
curl set to manually installed.
nmap is already the newest version (7.95+dfsg-3kali1).
nmap set to manually installed.
gobuster is already the newest version (3.8.0-2).
gobuster set to manually installed.
bind9-dnsutils is already the newest version (1:9.20.11-4+b1).
dnsrecon is already the newest version (1.2.0-3).
dnsrecon set to manually installed.
Upgrading:
  libjq1

Installing:
  jq  seclists

Summary:
  Upgrading: 1, Installing: 2, Removing: 0, Not Upgrading: 742
  Download size: 557 MB
  Space needed: 1,970 MB / 46.0 GB available
```

Рисунок 20 — Установка необходимых пакетов

После этого с помощью curl был загружен скрипт для установки пакета feroxbuster. После скачивания с помощью утилиты cat было проверено содержимое загруженного скрипта. Как видно на рисунке 21, в скрипте не было обнаружено криминала. Поэтому, как видно на рисунке 22, пакет feroxbuster был успешно установлен с помощью ранее загруженного скрипта.

```

└─(a1㉿kali)-[~/osintlab_3]
$ curl -sL https://raw.githubusercontent.com/epi052/feroxbuster/main/install-nix.sh -o install_feroxbuster.sh
└─(a1㉿kali)-[~/osintlab_3]
$ cat install_feroxbuster.sh
#!/usr/bin/env bash

BASE_URL=https://github.com/epi052/feroxbuster/releases/latest/download
MAC_ZIP=x86_64-macos-feroxbuster.zip
MAC_URL="$BASE_URL/$MAC_ZIP"

LIN32_ZIP=x86-linux-feroxbuster.zip
LIN32_URL="$BASE_URL/$LIN32_ZIP"

LIN64_ZIP=x86_64-linux-feroxbuster.zip
LIN64_URL="$BASE_URL/$LIN64_ZIP"

EMOJI_URL=https://gist.github.com/epi052/8196b550ea51d0907ad4b93751b1b57d/raw/6112c9f32ae07922983fdc549c54fd3fb9a38e4c/NotoColorEmoji.ttf

INSTALL_DIR="${1:-$(pwd)}"

echo "[+] Installing feroxbuster to ${INSTALL_DIR}!"

which unzip &>/dev/null
if [ "$?" != "0" ]; then
    echo "[!] unzip not found, exiting."
    exit -1
fi

if [[ "$(uname)" == "Darwin" ]]; then
    echo "[=] Found MacOS, downloading from $MAC_URL"

    curl -sLO "$MAC_URL"
    unzip -o "$MAC_ZIP" -d "${INSTALL_DIR}" >/dev/null
    rm "$MAC_ZIP"
elif [[ "$(expr substr $(uname -s) 1 5)" == "Linux" ]]; then
    if [[ ${getconf LONG_BIT} = 32 ]]; then
        echo "[=] Found 32-bit Linux, downloading from $LIN32_URL"

        curl -sLO "$LIN32_URL"
        unzip -o "$LIN32_ZIP" -d "${INSTALL_DIR}" >/dev/null
        rm "$LIN32_ZIP"
    else
        echo "[=] Found 64-bit Linux, downloading from $LIN64_URL"

        curl -sLO "$LIN64_URL"
        unzip -o "$LIN64_ZIP" -d "${INSTALL_DIR}" >/dev/null
        rm "$LIN64_ZIP"
    fi
fi

if [[ "$(fc-list NotoColorEmoji | wc -l)" -gt 0 ]]; then
    echo "[=] Found Noto Emoji Font, skipping install"
else
    echo "[=] Installing Noto Emoji Font"
    mkdir -p ~/.fonts
    pushd ~/.fonts 2>&1 >/dev/null

```

Рисунок 21 — Загрузка и проверка скрипта для установки feroxbuster

```

└─(a1㉿kali)-[~/osintlab_3]
$ bash install_feroxbuster.sh
[+] Installing feroxbuster to /home/a1/osintlab_3!
[=] Found 64-bit Linux, downloading from https://github.com/epi052/feroxbuster/releases/latest/download/aarch64-linux-feroxbuster.zip
[=] Found Noto Emoji Font, skipping install
[+] Installed feroxbuster
[-] path: /home/a1/osintlab_3/feroxbuster
[-] version: 2.13.0

```

Рисунок 22 — Установка feroxbuster

После этого с помощью скрипта `install_golang.sh` был установлен `go1.24.3`. Процесс установки и проверки `go` представлен на рисунке 23.

```

└─(a1㉿kali)-[~/osintlab_3]
$ bash install_golang.sh
Собираю пакет для go1.24.3, arch=arm64, tar=go1.24.3.linux-arm64.tar.gz
Скачиваем https://dl.google.com/go/go1.24.3.linux-arm64.tar.gz...
% Total    % Received % Xferd  Average Speed   Time   Time     Current
          Dload  Upload Total Spent   Left Speed
100 71.3M  100 71.3M    0      0  9531k      0:00:07  0:00:07  --::--  9.9M
go1.24.3.linux-arm64.tar.gz: OK
SHA OK
dpkg-deb: warning: root directory /tmp/tmp.fGwZivsgdb/golang-1.24.3-local_1.24.3-1_arm64 has unusual owner or group 1000:1000
dpkg-deb: hint: you might need to pass --root-owner-group, see <https://wiki.debian.org/Teams/Dpkg/RootlessBuilds> for further details
dpkg-deb: warning: ignoring 1 warning about the control file(s)
dpkg-deb: building package 'golang-1.24.3-local' in '/home/a1/osintlab_3/golang-1.24.3-local_1.24.3-1_arm64.deb'.
Собрано: /home/a1/osintlab_3/golang-1.24.3-local_1.24.3-1_arm64.deb
Устанавливаем...
[sudo] password for a1:
Selecting previously unselected package golang-1.24.3-local.
(Reading database ... 416555 files and directories currently installed.)
Preparing to unpack .../golang-1.24.3-local_1.24.3-1_arm64.deb ...
Unpacking golang-1.24.3-local (1.24.3-1) ...
Setting up golang-1.24.3-local (1.24.3-1) ...
update-alternatives: using /usr/local/go/bin/go to provide /usr/bin/go (go) in auto mode
update-alternatives: using /usr/local/go/bin/gofmt to provide /usr/bin/gofmt (gofmt) in auto mode
Processing triggers for kali-menu (2025.3.2) ...
Установка завершена. Проверьте версию:
go version go1.24.3 linux/arm64
Пакет установлен как golang-1.24.3-local_1.24.3-1_arm64.deb

└─(a1㉿kali)-[~/osintlab_3]
$ go version
go version go1.24.3 linux/arm64

└─(a1㉿kali)-[~/osintlab_3]
$ go env GOROOT GOPATH GOBIN
/usr/local/go
/home/a1/go

```

Рисунок 23 — Установка go1.24.3

После этого с помощью go был установлен pdtm. Процесс установки и проверки версии pdtm представлен на рисунках 24-25.

```

└─(a1㉿kali)-[~/osintlab_3]
$ go install -v github.com/projectdiscovery/pdtm/cmd/pdtm@latest
go: downloading github.com/projectdiscovery/pdtm v0.1.3
go: downloading github.com/logrusorgru/aurora/v4 v4.0.0
go: downloading github.com/projectdiscovery/gologger v1.1.54
go: downloading github.com/projectdiscovery/goflags v0.1.74
go: downloading github.com/projectdiscovery/utils v0.4.18
go: downloading github.com/logrusorgru/aurora v2.0.3+incompatible
go: downloading github.com/charmbracelet/glamour v0.10.0
go: downloading github.com/google/go-github v17.0.0+incompatible
go: downloading golang.org/x/oauth2 v0.29.0
go: downloading github.com/cnfs/structhash v0.0.0-20250313080605-df4c6cc74a9a
go: downloading github.com/google/shlex v0.0.0-20191202100458-e7afc7fbc510
go: downloading github.com/pkg/errors v0.9.1
go: downloading golang.org/x/exp v0.0.0-20250408133849-7e4ce0ab07d0
go: downloading gopkg.in/yaml.v3 v3.0.1
go: downloading github.com/asaskevich/govalidator v0.0.0-20230301143203-a9d515a09cc2
go: downloading github.com/mattn/go-isatty v0.0.20
go: downloading github.com/microcosm-cc/bluemonday v1.0.27
go: downloading github.com/saintfish/chardet v0.0.0-20230101081208-5e3ef4b5456d
go: downloading github.com/ebitengine/purego v0.8.4
go: downloading github.com/Masterminds/semver/v3 v3.3.1
go: downloading github.com/cheggaaa/pb/v3 v3.1.7
go: downloading github.com/google/go-github/v30 v30.1.0
go: downloading github.com/google/uuid v1.6.0
go: downloading github.com/minio/selfupdate v0.6.1-0.20230907112617-f11e74f84ca7
go: downloading github.com/projectdiscovery/machineid v0.0.0-20240226150047-2e2c51e35983
go: downloading github.com/zcalusic/sysinfo v1.1.3
go: downloading github.com/projectdiscovery/blackrock v0.0.1
go: downloading github.com/json-iterator/go v1.1.12
go: downloading github.com/miekg/dns v1.1.65
go: downloading github.com/tidwall/gjson v1.18.0
go: downloading golang.org/x/sys v0.32.0
go: downloading github.com/aymericdouceur v0.2.0
go: downloading golang.org/x/net v0.39.0
go: downloading github.com/google/go-querystring v1.1.0
go: downloading github.com/muesli/termenv v0.16.0
go: downloading github.com/yuin/goldmark v1.7.11
go: downloading github.com/yuin/goldmark-emoji v1.0.6

```

Рисунок 24 — Установка pdtm

```
(a1㉿kali)-[~/osintlab_3]
$ which pdtm && pdtm -version
/home/a1/go/bin/pdtm

██████████
projectdiscovery.io

[INF] Current Version: v0.1.3
```

Рисунок 25 — Проверка версии pdtm

После этого с помощью pdtm были установлены пакеты nuclei, subfinder и dnsx. Как видно на рисунке 26, установка была завершена успешно.

```
(a1㉿kali)-[~/osintlab_3]
$ pdtm -i nuclei,subfinder,dnsx

██████████
projectdiscovery.io

[INF] Current pdtm version v0.1.3 (latest)
[WRN] Run `source ~/.zshrc` to add $PATH (/home/a1/.pdtm/go/bin)
[INF] installing nuclei...
[INF] installed nuclei 3.4.10 (latest)
[INF] installing subfinder...
[INF] installed subfinder 2.9.0 (latest)
[INF] installing dnsx...
[INF] installed dnsx 1.2.2 (latest)
```

Рисунок 26 — Установка nuclei, subfinder, dnsx с помощью pdtm

Для домена itmo.ru было проверено содержимое robots.txt. Как видно на рисунке 27, в robots.txt есть большое количество Disallow-записей. Однако ни в одной ссылке по Disallow-записям не удалось найти ничего интересного: все либо скрыто под авторизацией, либо ведет на обычные статические

страницы без каких-то конфиденциальных данных.

```
User-agent: *

Disallow: /index.php
Disallow: /cms/
Disallow: /cms3/
Disallow: /cms5/
Disallow: /go.php
Disallow: /news/2314/
Disallow: /panel/
Disallow: /module/
Disallow: /album/
Disallow: /album2/
Disallow: /en/
Disallow: /cn/
Disallow: /catalog/
Disallow: /brand/
Disallow: /new_in_shop/
Disallow: /premium/
Disallow: /person/
Disallow: /sale/
Disallow: /mobile_news/
Disallow: /mobile_events/
Disallow: /sveden/
Disallow: /listpartner/partners.htm
Disallow: /ru/site/sajty_kafedr.htm
Disallow: /ru/page/338/sajty_kafedr.htm
Disallow: /ru/page/269/bazovye_kafedry.htm
Disallow: /ru/viewdepartment/87/kafedra_holodilnyh_vstanovok.htm
Disallow: /ru/viewdepartment/84/kafedra_upravleniya_gosudarstvennymi_informacionnymi_sistemami.htm
Disallow: /ru/viewdepartment/24/kafedra_kompyuternyh_tehnologiy.htm
Disallow: /ru/stat/224/set_bazovyh_magisterskih_kafedr_innovacionnogo_tipa_pri_vysokotekhnologichnyh_organizaciyah.htm
Disallow: /ru/viewdepartment/34/kafedra_nanotehnologiy_i_materialovedeniya.htm
Disallow: /ru/viewdepartment/397/kafedra_finansovogo_menedzhmenta_i_audita.htm
Disallow: /ru/viewdepartment/112/kafedra_svetoiodnyh_tehnologiy_bazovaya.htm
Disallow: /ru/viewdepartment/104/kafedra_promyshlennoy_ekologii.htm
Disallow: /ru/viewdepartment/8/kafedra_filosofii.htm
Disallow: /ru/viewdepartment/107/kafedra_istorii,_filosofii_i_socialnyh_praktik.htm
Disallow: /ru/viewdepartment/17/kafedra_kompyuternoy_teplofiziki_i_energofizicheskogo_monitoringa.htm
Disallow: /ru/viewdepartment/15/kafedra_lazernyh_tehnologiy_i_lazernoy_tekhniki.htm
Disallow: /ru/viewdepartment/44/kafedra_monitoringa_i_prognozirovaniya_informacionnyh_ugroz.htm
Disallow: /ru/viewdepartment/380/kafedra_marketinga_i_kommunikaciya.htm
Disallow: /ru/viewdepartment/111/kafedra_intellektualnoy_sobstvennosti_i_upravleniya_innovaciyami.htm
Disallow: /ru/viewdepartment/396/kafedra_proizvodstvennogo_menedzhmenta_i_transfera_tehnologiy.htm
Disallow: /ru/viewdepartment/382/kafedra_tehnologicheskikh_mashin_i_oborudovaniya.htm
Disallow: /ru/viewdepartment/395/kafedra_ekonomiki_i_strategicheskogo_menedzhmenta.htm
Disallow: /ru/viewdepartment/1/kafedra_menedzhmenta.htm
Disallow: /ru/viewdepartment/4/centr_dizayna_i_multimedia.htm
Disallow: /ru/viewdepartment/86/kafedra_holodilnyh_mashin_i_nizkopotencialnoy_energetiki.htm
Disallow: /ru/viewdepartment/12/kafedra_teoreticheskoy_i_prikladnoy_mehaniki.htm
Disallow: /ru/viewdepartment/19/kafedra_elektroniki.htm
Disallow: /ru/viewdepartment/51/kafedra_inzhenernoy_fotoniki.htm
Disallow: /ru/viewdepartment/78/kafedra_tehnologicheskogo_predprinimatelstva_i_upravleniya_innovaciyami.htm
```

Рисунок 27 — Содержимое robots.txt

После этого с помощью сайта <https://www.exploit-db.com/google-hacking-database> были найдены dork-запросы для поиска различной чувствительной информации. Так, например, с помощью dork-запроса, представленного на рисунке 28, получилось найти закрытый SSH-ключ на GitHub.

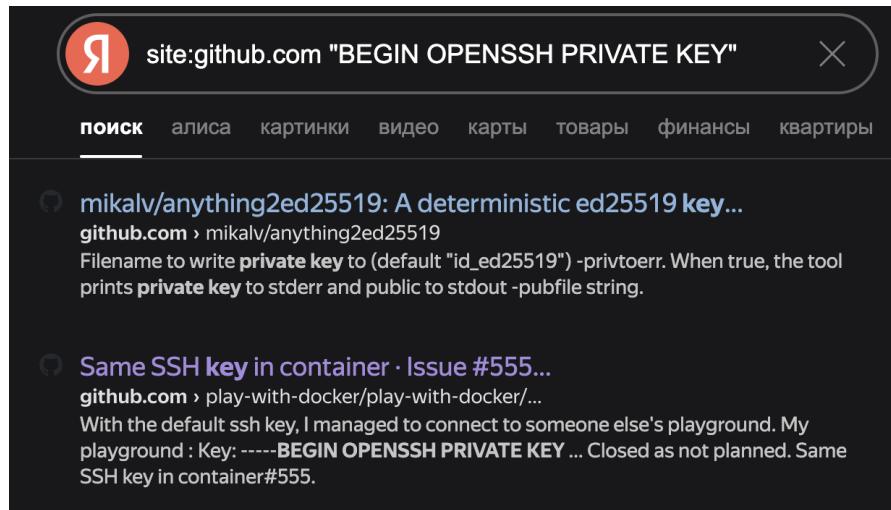


Рисунок 28 — Dork-запрос для поиска закрытого SSH-ключа

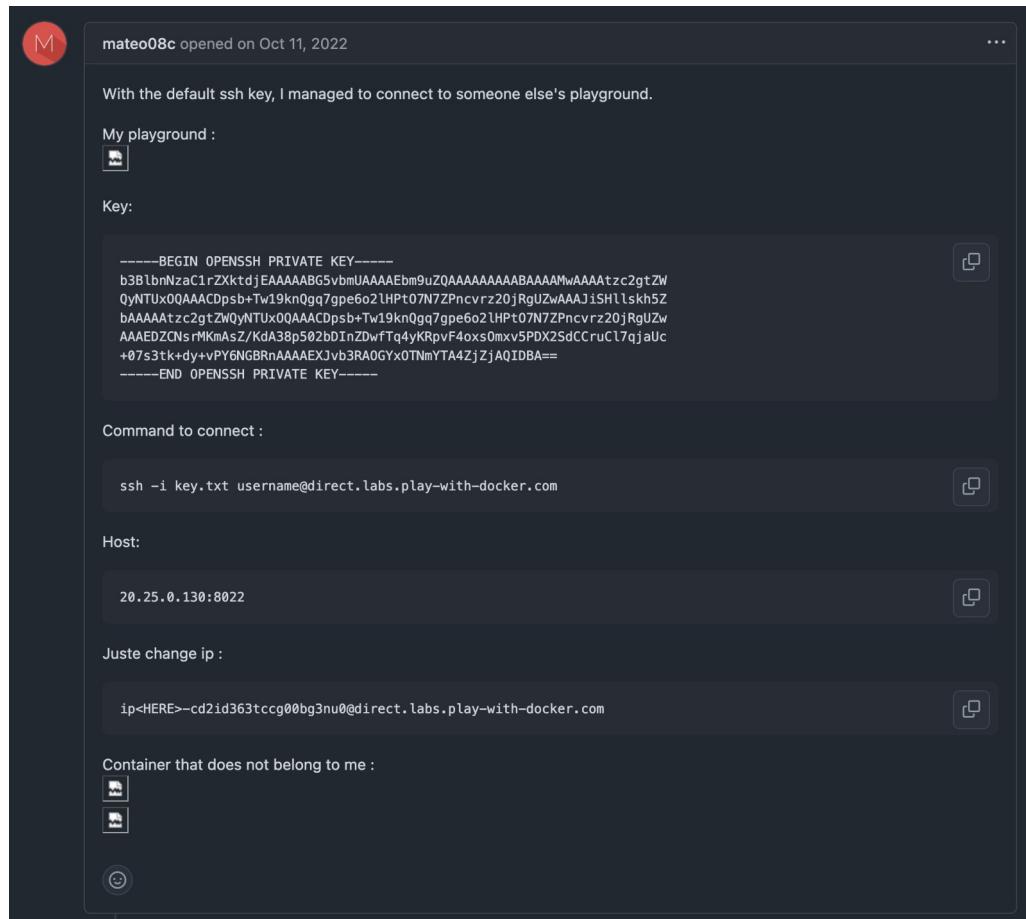


Рисунок 29 — Найденный закрытый SSH-ключ

Также с помощью dork-запроса, представленного на рисунке 30, получилось найти токены для AWS, что видно на рисунке 31.

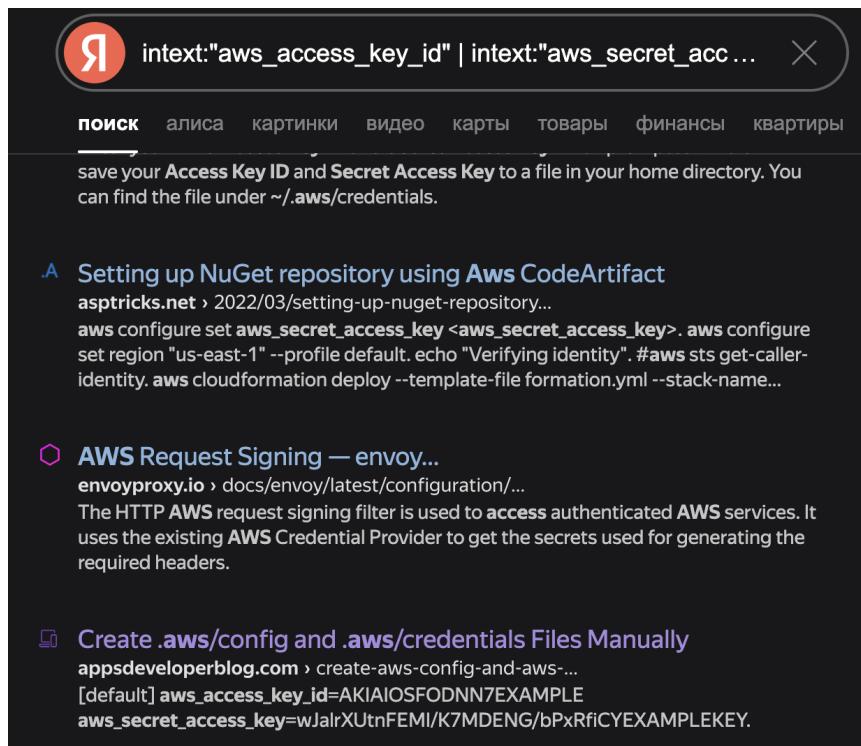


Рисунок 30 — Dork-запрос для поиска токенов для AWS

## Create ~/.aws/credentials File

```
1. sudo vi ~/.aws/credentials
```

Once the new file is created, provide your AWS credentials in there. For example:

```
1. [default]
2. aws_access_key_id=AKIAIOSFODNN7EXAMPLE
3. aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfCYEXAMPLEKEY
```

Рисунок 31 — Найденные токены для AWS

Таким образом, с помощью dork-запросов получилось достаточно просто и быстро найти потенциально конфиденциальную информацию.

После этого с помощью <https://crt.sh/?q=%25.itmo.ru>, как видно на рисунке 32, был получен список сертификатов, выданных для поддоменов itmo.ru. Данная информация была экспортирована в формат JSON, что видно на рисунке 33.

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	7022358760	2022-06-28	2022-06-28 2022-09-26	ct.itmo.ru	ct.itmo.ru	C=US, O=Let's Encrypt, CN=R3	
	7021703622	2022-06-28	2022-06-28 2022-09-26	ct.itmo.ru	ct.itmo.ru	C=US, O=Let's Encrypt, CN=R3	
	7016738451	2022-06-27	2022-06-27 2022-09-25	media.ec.itmo.ru	www.ct.itmo.ru	C=US, O=Let's Encrypt, CN=R3	
	7015649957	2022-06-27	2022-06-27 2022-09-25	media.ec.itmo.ru	media.ec.itmo.ru	C=US, O=Let's Encrypt, CN=R3	
	7010776851	2022-06-26	2022-06-26 2022-09-24	technopark.itmo.ru	technopark.itmo.ru	C=US, O=Let's Encrypt, CN=R3	
	7009463165	2022-06-26	2022-06-26 2022-09-24	technopark.itmo.ru	technopark.itmo.ru	C=US, O=Let's Encrypt, CN=R3	
	7007628873	2022-06-25	2022-06-25 2022-09-23	lib.itmo.ru	lib.itmo.ru	C=US, O=Let's Encrypt, CN=R3	
	7005532219	2022-06-25	2022-06-25 2022-09-23	lib.itmo.ru	www.lib.itmo.ru	C=US, O=Let's Encrypt, CN=R3	
	7006769355	2022-06-25	2022-06-25 2022-09-23	agni.itmo.ru	lib.itmo.ru	C=US, O=Let's Encrypt, CN=R3	
	7004651931	2022-06-25	2022-06-25 2022-09-23	agni.itmo.ru	agni.itmo.ru	C=US, O=Let's Encrypt, CN=R3	
	7001590368	2022-06-24	2022-06-24 2022-09-22	tefl.itmo.ru	tefl.itmo.ru	C=US, O=Let's Encrypt, CN=R3	
	6999068233	2022-06-24	2022-06-24 2022-09-22	tefl.itmo.ru	www.tefl.itmo.ru	C=US, O=Let's Encrypt, CN=R3	
	7000509428	2022-06-24	2022-06-24 2022-09-22	events.itmo.ru	tefl.itmo.ru	C=US, O=Let's Encrypt, CN=R3	
					www.events.itmo.ru	www.events.itmo.ru	C=US, O=Let's Encrypt, CN=R3

Рисунок 32 — Информация о сертификатах поддоменов itmo.ru

```

[{"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "ct.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "ct.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "media.ec.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "media.ec.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "media.ec.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "technopark.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "lib.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "lib.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "lib.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "agni.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "agni.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "agni.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "tefl.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "tefl.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "tefl.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "tefl.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "events.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "events.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "events.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "youtrack.it.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "youtrack.it.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "drone.lcps.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "drone.lcps.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "bonustrack.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "bonustrack.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "phealth2022.actcognitive.org", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "phealth2022.actcognitive.org", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "api.it.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "api.it.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "pswd.it.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "pswd.it.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "isu.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "isu.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "isu.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "recycle.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "recycle.itmo.ru", ...}, {"id": "183267", "issuer_name": "C=US, O=Let's Encrypt, CN=R3", "common_name": "recycle.itmo.ru", ...}]

```

Рисунок 33 — Информация о сертификатах поддоменов itmo.ru в формате

JSON

Из полученных поддоменов были выбраны наиболее интересные для злоумышленника:

- 1) id.itmo.ru — поддомен, который используется как SSO, т. е. центр аутентификации. Представляет интерес для злоумышленников, т. к. в случае успешного взлома может открыть неправомерный доступ к другим системам;
- 2) it.itmo.ru — поддомен, который используется для внутренней инфраструктуры ИТМО. Представляет интерес для злоумышленников, т. к. при успешном взломе какой-либо из внутренних систем злоумышленники

могут скомпрометировать инфраструктуру в целом;

3) admin.itmo.ru — поддомен, который используется для администрирования my.itmo.ru. Представляет интерес для злоумышленников, т. к. при взломе может открыть доступ к нарушению работы my.itmo.

После этого с помощью утилиты dnsrecon был проверен механизм zone transfer для домена itmo.ru. Как видно на рисунке 34, механизм zone transfer закрыт.

```
(a1㉿kali)-[~/osintlab_3]
$ dnsrecon -t axfr -d itmo.ru
[*] Checking for Zone Transfer for itmo.ru name servers
[*] Resolving SOA Record
[+]      SOA ns.itmo.ru 77.234.194.2
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS ns3.itmo.ru 77.234.216.2
[+]      NS ns2.itmo.ru 77.234.221.75
[+]      NS ns5.itmo.ru 51.250.74.203
[+]      NS ns.itmo.ru 77.234.194.2
[*] Removing any duplicate NS server IP Addresses ...
[*]
[*] Trying NS server 77.234.221.75
[+] 77.234.221.75 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 51.250.74.203
[+] 51.250.74.203 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 77.234.216.2
[+] 77.234.216.2 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*]
[*] Trying NS server 77.234.194.2
[+] 77.234.194.2 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
```

Рисунок 34 — Проверка механизма zone transfer для itmo.ru

После этого с помощью утилиты dnsrecoot был получен CSV-файл с поддоменами itmo.ru. Как видно на рисунках 35-36, для itmo.ru удалось найти 231 поддомен.

```

(a1㉿kali)-[~/osintlab_3]
└─$ dnsrecon -t crt -d itmo.ru -c dnsrecon_crt_output.xls
[*] crt: Performing Crt.sh Search Enumeration against itmo.ru...
[*]   *.dis.itmo.ru wildcard
[*]   *.itmo.ru wildcard
[*]   *.itmo.ru wildcard
[*] A ct.itmo.ru 185.215.4.10
[*] A media.ec.itmo.ru 51.250.3.72
[*] A technopark.itmo.ru 185.215.4.29
[*] A lib.itmo.ru 185.129.100.112
[*] A agni.itmo.ru 51.250.54.78
[*] A tefl.itmo.ru 185.215.4.34
[*] A events.itmo.ru 84.201.187.10
[*] A youtrack.it.itmo.ru 77.234.222.74
[*] A drone.lcps.itmo.ru 77.234.213.6
[*] A bonustrack.itmo.ru 185.215.4.33
[*] A api.it.itmo.ru 77.234.222.58
[*] A pswd.it.itmo.ru 77.234.216.50
[*] A recycle.itmo.ru 77.234.222.71
[*] A id.itmo.ru 51.250.121.80
[*] A ecinn.itmo.ru 185.215.4.10
[*] A radius.it.itmo.ru 77.234.216.50
[*] A apps.dc-edu.itmo.ru 51.250.29.111
[*] A preview.dc-edu.itmo.ru 51.250.29.111
[*] A studio.dc-edu.itmo.ru 51.250.29.111
[*] A dc-edu.itmo.ru 51.250.29.111
[*] A live.itmo.ru 51.250.120.137
[*] A alumni.itmo.ru 185.215.4.33
[*] A ichem.itmo.ru 51.250.120.169
[*] A sm.itmo.ru 77.234.222.55
[*] A art.online.itmo.ru 185.215.4.33
[*] A hyperjump.itmo.ru 51.250.120.169
[*] A vc.itmo.ru 185.215.4.10
[*] A competition.future.itmo.ru 185.215.4.13

```

Рисунок 35 — Команда для поиска всех поддоменов itmo.ru

```

[*]      A abit.itmo.ru 51.250.55.122
[*]      A slalom.itmo.ru 77.234.203.238
[*]      A captcha.itmo.ru 51.250.120.169
[*]      A cloud.physics.itmo.ru 77.234.203.238
[*]      A www.itmo.ru 51.250.54.78
[+] 231 Records Found
[*] Saving records to CSV file: dnsrecon_crt_output.xls

(a1㉿kali)-[~/osintlab_3]
└─$ cat dnsrecon_crt_output.xls
Type,Name,Address,Target,Port,String
A,ct.itmo.ru,185.215.4.10,,,
A,media.ec.itmo.ru,51.250.3.72,,,
A,technopark.itmo.ru,185.215.4.29,,,
A,lib.itmo.ru,185.129.100.112,,,
A,agni.itmo.ru,51.250.54.78,,,
A,tefl.itmo.ru,185.215.4.34,,,
A,events.itmo.ru,84.201.187.10,,,
A,youtrack.it.itmo.ru,77.234.222.74,,,
A,drone.lcps.itmo.ru,77.234.213.6,,,
A,bonustrack.itmo.ru,185.215.4.33,,,
A,api.it.itmo.ru,77.234.222.58,,,
A,pswd.it.itmo.ru,77.234.216.50,,,
A,recycle.itmo.ru,77.234.222.71,,,
A,id.itmo.ru,51.250.121.80,,,
A,ecinn.itmo.ru,185.215.4.10,,,
A,radius.it.itmo.ru,77.234.216.50,,,
```

Рисунок 36 — Найденные поддомены itmo.ru

После этого с помощью утилиты curl был скачан словарь, по которому производился полный перебор списка доменов. Процесс скачивания словаря представлен на рисунке 37.

```
[a1㉿kali)-[~/osintlab_3]
$ curl -fSL -C - https://wordlists-cdn.assetnote.io/data/manual/best-dns-wordlist.txt -o best-dns-wordlist.txt
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
                                         Dload  Upload Total Spent   Left  Speed
100  134M  100  134M    0      0  10.0M       0  0:00:13  0:00:13 --:--:-- 10.3M
```

Рисунок 37 — Скачивание словаря best-dns-wordlist

После этого с помощью утилиты gobuster был выполнен перебор доменных имен по словарю. В итоге, как видно на рисунке 38, был получен список поддоменов и их IP-адресов.

Рисунок 38 — Перебор доменных имен по словарю с помощью gobuster

## 2.3 Визуальный поиск интересных сервисов с помощью httpx

После этого с помощью утилиты wget был скачан пакет httpx. После завершения загрузки архив был распакован с помощью утилиты unzip. Данный процесс показан на рисунках 39-40.

Рисунок 39 — Скачивание httpx

```
(a1㉿kali)-[~/osintlab_3]
└─$ unzip httpx.zip -d httpx
Archive: httpx.zip
  inflating: httpx/LICENSE.md
  inflating: httpx/README.md
  inflating: httpx/httpx

(a1㉿kali)-[~/osintlab_3]
└─$ cd httpx

(a1㉿kali)-[~/osintlab_3/httpx]
└─$ ls
httpx LICENSE.md README.md

(a1㉿kali)-[~/osintlab_3/httpx]
```

Рисунок 40 — Распаковка httpx

После этого ранее полученный список доменов и IP-адресов был преобразован в список доменов с помощью утилиты awk. Это показано на рисунке 41.

```
(a1㉿kali)-[~/osintlab_3/httpx]
└─$ awk '{print $1}' resolved.txt > names.txt

(a1㉿kali)-[~/osintlab_3/httpx]
└─$ cat names.txt
ns2.itmo.ru
secure.itmo.ru
mail.itmo.ru
cloud.itmo.ru
support.itmo.ru
ns.itmo.ru
www.itmo.ru
sip.itmo.ru
admin.itmo.ru
store.itmo.ru
email.itmo.ru
my.itmo.ru
gw.itmo.ru
login.itmo.ru
ns3.itmo.ru
wiki.itmo.ru
cdn.itmo.ru
news.itmo.ru
connect.itmo.ru
crm.itmo.ru
new.itmo.ru
```

Рисунок 41 — Валидированный список доменных имён

После этого был запущен сбор информации о доменах с помощью httpx, что видно на рисунке 42.

```
(ai㉿kali)-[~/osintlab_3/httpx]
└─$ ./httpx -l names.txt -status-code -title -tech-detect -follow-redirects -screenshot -server -ip -cname -store-response -store-chain -store-vision-recon-cluster -random-agent -o "httpx_scan_$(date '+%Y-%m-%d_%H%M%S').zip"
[INFO] Current httpx version v1.6.10 (outdated)
[WARN] UI Dashboard is disabled, Use -dashboard option to enable
[launcher.Browser]2025/10/12 16:40:33 Download: https://playwright.azureedge.net/builds/chromium/1067/chromium-linux-arm64.zip
[launcher.Browser]2025/10/12 16:40:34 Progress: 0%
[launcher.Browser]2025/10/12 16:40:35 Progress: 0%
[launcher.Browser]2025/10/12 16:40:36 Progress: 1%
[launcher.Browser]2025/10/12 16:40:37 Progress: 18%
[launcher.Browser]2025/10/12 16:40:38 Progress: 21%
[launcher.Browser]2025/10/12 16:40:38 Progress: 22%
[launcher.Browser]2025/10/12 16:40:39 Progress: 30%
[launcher.Browser]2025/10/12 16:40:40 Progress: 37%
[launcher.Browser]2025/10/12 16:40:41 Progress: 44%
[launcher.Browser]2025/10/12 16:40:42 Progress: 51%
[launcher.Browser]2025/10/12 16:40:43 Progress: 57%
[launcher.Browser]2025/10/12 16:40:44 Progress: 64%
[launcher.Browser]2025/10/12 16:40:46 Progress: 70%
[launcher.Browser]2025/10/12 16:40:47 Progress: 76%
[launcher.Browser]2025/10/12 16:40:48 Progress: 84%
[launcher.Browser]2025/10/12 16:40:49 Progress: 91%
[launcher.Browser]2025/10/12 16:40:50 Progress: 98%
[launcher.Browser]2025/10/12 16:40:52 Downloaded: /home/ai/.cache/rod/browser/chromium-1131003
[launcher.Browser]2025/10/12 16:40:50 Progress: 100%
[launcher.Browser]2025/10/12 16:40:51 Progress: 37%
[launcher.Browser]2025/10/12 16:40:52 Progress: 91%
[launcher.Browser]2025/10/12 16:40:52 Downloaded: /home/ai/.cache/rod/browser/chromium-1131003
http://ns2.itmo.ru [200] [Apache/2.2.22 (Debian)] [77.234.221.75] [Apache HTTP Server:2.2.22,Debian]
https://mincraft.itmo.ru [404] [nginx/1.18.0 (Ubuntu)] [91.206.15.171] [Nginx:1.18.0,Ubuntu]
https://cdn.itmo.ru [404] [nginx] [95.181.182.182] [cl-m0598ifa3.edgenet.ru] [Amazon Web Services,Nginx]
https://ns2.itmo.ru [200] [nginx/1.18.0 (Ubuntu)] [51.250.60.89] [Nginx:1.18.0,Ubuntu]
https://email.itmo.ru [200] [Welcome to nginx!] [nginx/1.18.0 (Ubuntu)] [51.250.60.89] [Nginx:1.18.0,Ubuntu]
https://eduroom.itmo.ru [200] [[Страница ошибки]] [51.250.120.169] [HTTPS,Yandex,Metrika]
https://help.itmo.ru [200] [[Страница ошибки]] [51.250.120.169] [HTTPS,Yandex,Metrika]
https://120.itmo.ru [200] [[Страница ошибки]] [51.250.120.169] [HTTPS,Yandex,Metrika]
https://login.itmo.ru [403] [[Доступ запрещен - ИСУ ИТМО]] [nginx] [77.234.212.21] [Bootstrap,Nginx]
```

Рисунок 42 — Сбор информации о доменах с помощью httpx

После завершения работы httpx в каталоге output/screenshot появились снимки экрана, а также HTML-страница screenshot.html. Содержимое screenshot.html представлено на рисунке 43.

Response Info	Screenshot
<b>Host:</b> <a href="http://ns2.itmo.ru">http://ns2.itmo.ru</a> <b>Title:</b> <b>Status Code:</b> 200 <b>Webserver:</b> Apache/2.2.22 (Debian) <b>Technologies:</b> [Apache HTTP Server:2.2.22 Debian]	 <p>It works! This is the default web page for this server. The web server is running but no content has been added yet.</p>
<b>Host:</b> <a href="https://mincraft.itmo.ru">https://mincraft.itmo.ru</a> <b>Title:</b> <b>Status Code:</b> 404 <b>Webserver:</b> nginx/1.18.0 (Ubuntu) <b>Technologies:</b> [Nginx:1.18.0 Ubuntu]	 <p>Whitelabel Error Page This application has no configuration that allows it to run as a webapp. See the 'Run as' section for details. The web server is running but no content has been added yet.</p>
<b>Host:</b> <a href="https://cdn.itmo.ru">https://cdn.itmo.ru</a> <b>Title:</b> <b>Status Code:</b> 403 <b>Webserver:</b> nginx	 <p>This URL did not open in their web browser and will be blocked. Reason: Forbidden Details: You do not have permission to view this resource. Status: 403 Forbidden HTTP/2.0</p>

Рисунок 43 — Содержимое screenshot.html

Из просканированных доменов часть из них уже не работает (возвращает 404 или 500), часть из них представляет из себя закрытые под

id.itmo.ru страницы, а часть из них является страницами-визитками. Из интересного, получилось найти домен crm.itmo.ru, ведущий на страницу авторизации Битрикс24, что видно на рисунке 44.

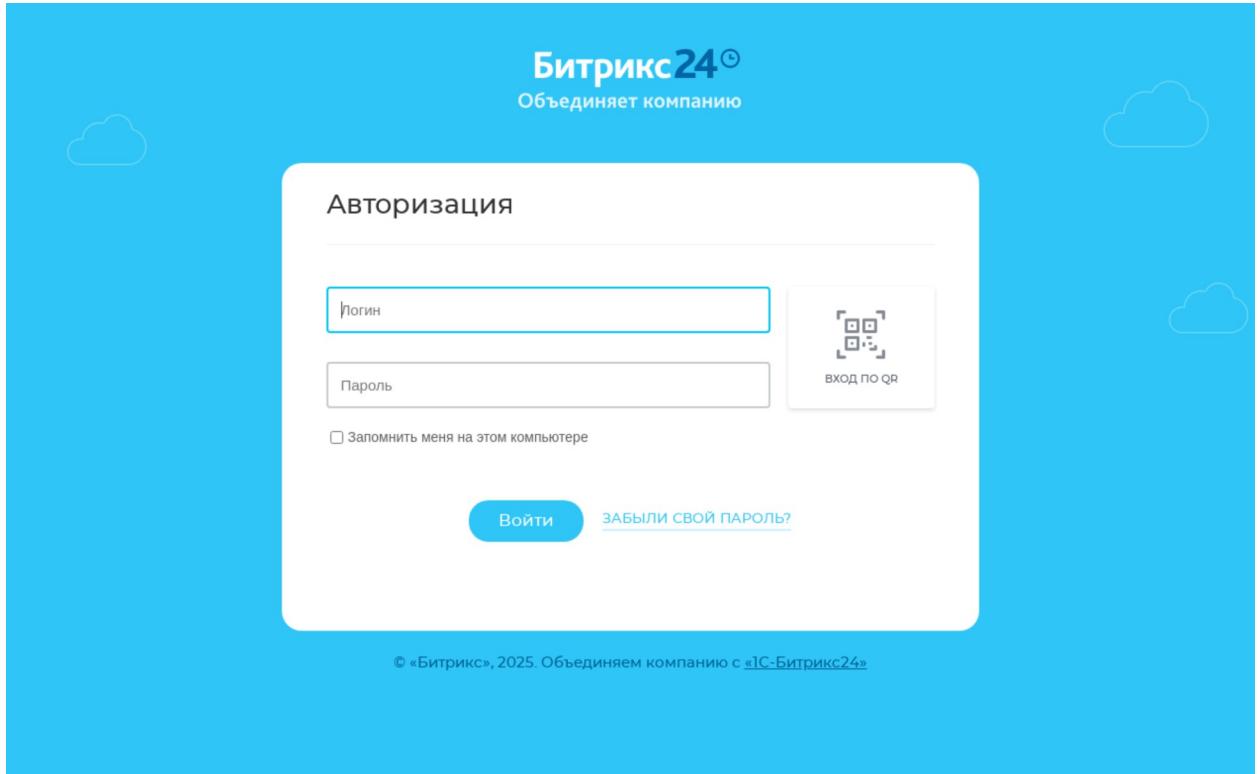


Рисунок 44 — Страница, отображаемая при переходе на crm.itmo.ru

## 2.4 Перебор web-директорий

После этого с помощью утилиты feroxbuster был выполнен перебор web-директорий <https://gitisu.itmo.ru> по словарю `raft-medium-words-lowercase.txt`. Процесс работы утилиты представлен на рисунке 45.

```
[a1㉿kali)-[~/osintlab_3]
└─$ ./feroxbuster -u "https://gitisu.itmo.ru" -w "/usr/share/seclists/Discovery/Web-Content/raft-medium-words-lowercase.txt" -x js,php,txt,json -t 50 -k -q -n -r -s 200,204,301,302,307,401,403,405 -o "ferox_1.txt"
200  GET   206l   1078w   28010c https://gitisu.itmo.ru/gitlab//users/sign_in
200  GET   274l   1398w   52252c https://gitisu.itmo.ru/gitlab//search
200  GET   295l   1075w   27936c https://gitisu.itmo.ru/gitlab//users/sign_in
200  GET   364l   2639w   76044c https://gitisu.itmo.ru/gitlab//help
200  GET   280l   1073w   27935c Auto-filled URL found in like response and created new filter; toggle off with --dont-filter
200  GET   1l    10w     49c https://gitisu.itmo.ru/gitlab//admin.js
200  GET   7l    16w     248c https://gitisu.itmo.ru/gitlab//search.js
401  GET   1l    10w     49c https://gitisu.itmo.ru/gitlab//admin.txt
401  GET   1l    10w     61c https://gitisu.itmo.ru/gitlab//admin.json
200  GET   274l   1398w   52260c https://gitisu.itmo.ru/gitlab//search.php
200  GET   4l    1133w   52260c https://gitisu.itmo.ru/gitlab//help.js
200  GET   364l   2639w   76044c https://gitisu.itmo.ru/gitlab//public.php
200  GET   413l   1051w   59687c https://gitisu.itmo.ru/gitlab//public
200  GET   1l    148w   4289c https://gitisu.itmo.ru/gitlab//public.json
200  GET   413l   1854w   59759c https://gitisu.itmo.ru/gitlab//explore
200  GET   85l    237w   2299c https://gitisu.itmo.ru/gitlab//robots.txt
200  GET   309l   1518w   53926c https://gitisu.itmo.ru/gitlab//explore/snippets
200  GET   364l   1857w   58854c https://gitisu.itmo.ru/gitlab//explore/groups
401  GET   0l    0w      49c https://gitisu.itmo.ru/gitlab//dashboard
401  GET   1l    10w     49c https://gitisu.itmo.ru/gitlab//dashboard.js
401  GET   1l    10w     49c https://gitisu.itmo.ru/gitlab//dashboard.txt
401  GET   1l    10w     61c https://gitisu.itmo.ru/gitlab//dashboard.json
```

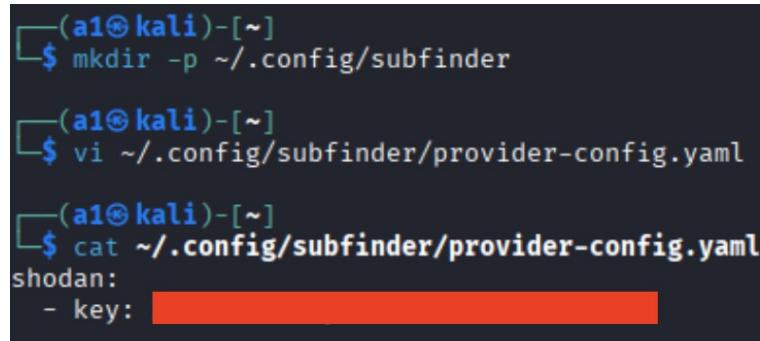
Рисунок 45 — Перебор web-директорий с помощью утилиты feroxbuster

В итоге, ничего интересного, кроме основной формы аутентификации в

GitLab найти не удалось.

## 2.5 Автоматизация: subfinder с API (Censys, Shodan, Netlas)

После этого был создан конфиг провайдеров для утилиты subfinder, в которой был указан API-ключ для Shodan. Это видно на рисунке 46.



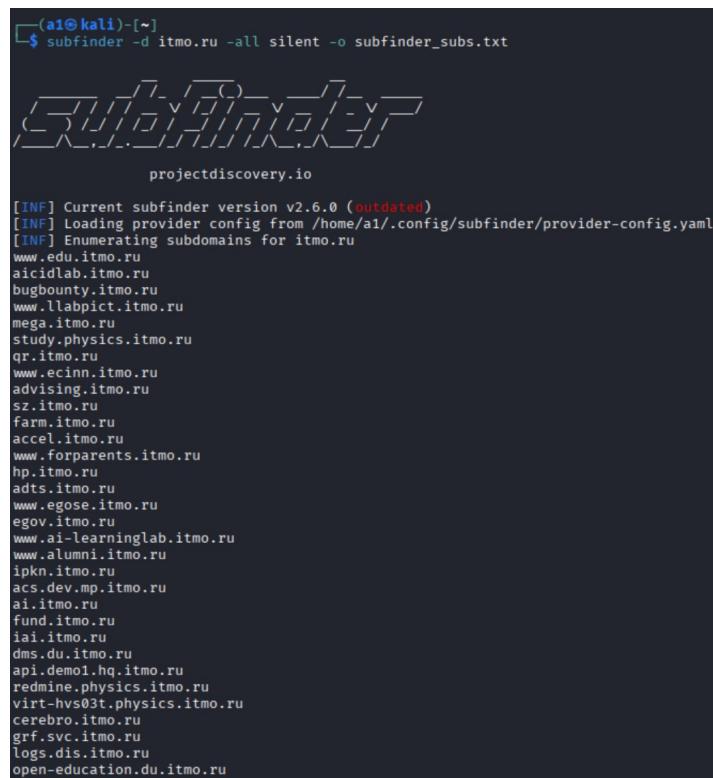
```
(a1㉿kali)-[~]
$ mkdir -p ~/.config/subfinder

(a1㉿kali)-[~]
$ vi ~/.config/subfinder/provider-config.yaml

(a1㉿kali)-[~]
$ cat ~/.config/subfinder/provider-config.yaml
shodan:
  - key: [REDACTED]
```

Рисунок 46 — Конфиг провайдеров для утилиты subfinder

После этого subfinder был запущен с помощью команды, представленной на рисунке 47.



```
(a1㉿kali)-[~]
$ subfinder -d itmo.ru -all silent -o subfinder_subdomains.txt

projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/a1/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for itmo.ru
www.edu.itmo.ru
aicidlab.itmo.ru
bugbounty.itmo.ru
www.llabpict.itmo.ru
mega.itmo.ru
study.physics.itmo.ru
qr.itmo.ru
www.ecinn.itmo.ru
advising.itmo.ru
sz.itmo.ru
farm.itmo.ru
accel.itmo.ru
www.forparents.itmo.ru
hp.itmo.ru
adts.itmo.ru
www.egose.itmo.ru
egov.itmo.ru
www.ai-learninglab.itmo.ru
www.alumni.itmo.ru
ipkn.itmo.ru
acs.dev.mp.itmo.ru
ai.itmo.ru
fund.itmo.ru
iai.itmo.ru
dms.du.itmo.ru
api.demo1.hq.itmo.ru
redmine.physics.itmo.ru
virt-hvs03t.physics.itmo.ru
cerebro.itmo.ru
grf.svc.itmo.ru
logs.dis.itmo.ru
open-education.du.itmo.ru
```

Рисунок 47 — Использование и вывод утилиты subfinder

Как видно на рисунке 47, удалось получить схожий список доменов, что был получен ранее с помощью других средств.

### **3 Вывод**

В ходе выполнения данной лабораторной работы были изучены методы пассивной разведки для увеличения внешней поверхности атаки организации, освоена работа с поисковыми сервисами для поиска интернет-устройств и открытых сервисов, оценены риски, связанные с обнаруженными открытыми ресурсами.