

Google Dorks Cheat Sheet for OSINT

Название:	Описание:	Пример использования:
Дорки, уточняющие содержание запроса		
*	Позволяет пропускать слово во фразе	Поиск пропущенной части ФИО – "Иванов Георгий *"
-	Исключает слово из поисковой выдачи	Одновременно происходящие события: нужны протесты в Италии, а не в Аргентине. Протесты Италия –Аргентина
" "	Один из самых важных дорков, выдающий вам исключительно точное совпадение вашему запросу	Поиск информации по ФИО: "Николаев Сергей Владимирович"
()	Помогает сгруппировать сложный запрос, который состоит из неоднородных элементов.	Ермолов (учредитель OR генеральный директор)

* Перед поиском включите VPN (выберите в нем страну, по которой будет проводиться поиск) и очистите куки, это сделает ваш поиск более эффективным.

Дорки, уточняющие содержание запроса pt. 2

 	Это выражение обозначает аргумент «или», также он может использоваться для комбинации дорков (выдача будет содержать хотя бы один элемент из указанных).	Поиск информации по родственникам: Гаврилов ("Игорь" «Егор»)
AROUND(X)	Поиск элементов которые находятся на расстоянии (X) слов. Важно: нужно прописывать элементы в кавычках, иначе выдача будет касаться и синонимов.	"Егоров" contact AROUND(5) "e-mail"
before: / after:	Дословно — «до» и «после». Ищет содержимое в рамках от заданной даты (гггг-мм-дд), либо до неё, либо после. При комбинации позволяет выставить рамки временного периода.	"TOS Update" after:2022-12-01 / "TOS Update" after:2022-12-01 before:2022-12-05

Дорки для поиска файлов

filetype: ext:	Позволяет искать проиндексированные файлы. <u>Список</u> индексируемых файлов, также включает в себя: db, log, html, mpeg, mov, flv	filetype:pdf "Абакумов Иван Андреевич"
source:	Отличается от дорка site: тем, что для него не требуется полный DNS, что гипотетически может увеличить выдачу	source:bank "аффилированные лица" filetype:pdf

Дорки по поиску содержимого сайтов

site:	Поиск по содержимому сайта, рекомендуется использовать с другими дорками. Не обязательно указывать сайт, можно например обойтись TLD	site:cia.gov filetype:xlsx
cache:	Просмотр сохраненной в кэше страницы, полезно для просмотра удаленной или измененной информации	Сайт https://ubl.com старый, недоступен. Через кэш находим его последнее состояние. cache:ubl.com

Дорки по поиску содержимого сайтов pt. 2

inurl:	Поиск по элементу, который должен находиться в искомом URL. Работает в основном только с первым ключевым словом после него. Между двоеточием и элементом нельзя ставить пробел.	inurl:admin filetype:xls
allinurl:	Поиск по нескольким элементам, которые должны одновременно находиться в одном URL. Учитывает все элементы после него и НЕ РАБОТАЕТ с другими дорками. После него можно ставить пробел.	allinurl: upload wp content
intitle:	Поиск по элементу, который должен находиться в искомом заголовке страницы («название», с которым вы сталкиваетесь в первую очередь, когда производите поиск). Работает в основном только с первым ключевым словом после него. Между двоеточием и элементом нельзя ставить пробел.	intitle:cafe "de jaren"

Дорки по поиску содержимого сайтов pt. 3

allintitle:	Поиск по нескольким элементам, которые должны быть в заголовке. Работает со всеми элементами после него. Между двоеточием и элементом можно ставить пробел.	allintitle: cafe de jaren reviews
intext:	Поиск по элементу, который должен находиться в искомом тексте страницы (именно в body-сегменте, а не где угодно по странице). Работает в основном только с первым ключевым словом после него, но можно формулировать целые фразы (например, с помощью кавычек). Между двоеточием и элементом нельзя ставить пробел.	intext:cv intext:curriculum vitae "passport details" ext:doc - template
allintext:	Поиск по элементами, которые должны находиться в искомом тексте страницы (именно в body-сегменте, а не где угодно по странице). Работает со всеми элементами после него. После него можно ставить пробел.	allintext: argentina 2006 metro

Yandex Dorks Cheat Sheet for OSINT

Название:	Описание:	Пример использования:
Дорки, уточняющие содержание запроса		
!	Будут найдены документы со словом в заданной форме (число, падеж, время).	Список !участников
+	Будут найдены документы, в которых обязательно содержатся слова, выделенные дорком +	+Егоров +Емейл +E-mail
" "	Будут найдены документы, содержащие эту цитату.	"gavril.pononov@gmail.com"
*	Заменяет собой пропущенное/неизвестное слово.	Смирнов Сергей *
	Оператор "или". Выдача запросов, в которых присутствует хотя бы одно из слов запроса.	Смирнов (Егор Вадим)
lang:	Будут показаны документы на выбранном языке. <u>Формат языка: ISO 639-1</u>	passport lang:en mime:pdf

Дорки по поиску содержимого сайтов

(искомый элемент) url:хоста/папка/*	Поиск по элементу, которые содержат все страницы по любому адресу после известной его части, т.е. вам известен раздел, а конечная папка может быть любой.	Поиск по всем страницам с упоминанием слова "паспорт" в новостном разделе Госуслуг: паспорт url:www.gosuslugi.ru/life/*
site:url	Производит поиск только по определенному сайту.	site:tass.ru выборы
host:url	Поиск страниц по хосту.	Выдача с элементом "закон" на поддомене pravo: host:pravo.gov.ru закон
domain:	Поиск по определенному домену (любого уровня).	Выдача сайтов с элементом "закон" на домене ru: domain:ru "закон"

Дорки для поиска файлов

mime:	Будут показаны документы в выбранном формате поддерживаемые файлы: pdf xls ods rtf ppt odp swf odt odg doc	mime:pdf «Абакумов Иван Андреевич»
--------------	--	---

Дорки по дате последнего изменения

date:ГГГГММДД

Поиск по
определенной дате
день в день.

date:20221231

**date:<ГГГГММДД
date:<=ГГГГММДД
date:>ГГГГММДД
date:=>ГГГГММДД**

Поиск выдачи
раньше
определенного дня;
раньше или в один
день;
позже;
позже или в один
день.

**новый закон date:
<=20220915**

**date:ГГГГММДД..ГГГГ
ММДД**

Поиск в
определенном
интервале дат.

**date:20221231..2023010
5
"афиша"**

date:ГГГГММ*

Поиск в
определенном
месяце.

**date:200109*
"Америка"**

date:ГГГГ*

Поиск в
определенном году.

**date:2022*
"Чемпионат мира"**

Linkedin Dorks Cheat Sheet for OSINT

" "	Поиск конкретного элемента. Важно: КОРРЕКТНО на LinkedIn работают только такие кавычки.	"Annie" Jackson
NOT	Исключение элемента из поиска. Только капс.	developer NOT
OR	Поиск по нескольким альтернативным элементам из списка, если нужен любой из нескольких вариантов. Только капс.	sales OR marketing OR advertising
AND	Поиск по нескольким элементам из списка, если нужны одновременно два и больше из них. Только капс.	senior AND accountant AND finance
()	Поиск с объединением нескольких элементов, как в обычном математическом примере, чтобы отделить элементы с одной функцией от других.	junior (artist OR designer) NOT (3D OR digital)

Twitter Dorks Cheat Sheet for OSINT

" "	Поиск точной фразы.	"elections in America"
OR	Поиск по нескольким альтернативным элементам из списка, если нужен любой из нескольких вариантов. Только капс.	спать OR играть
lang:	Выдача твитов на определенном языке.	lang:pt "Lissabon"
from:nickname	Выдача твитов от определенного пользователя. После двоеточия пишется никнейм (тот, который с @).	from:elonmusk
to:	Выдача твитов к определенному юзеру. После двоеточия пишется никнейм (тот, который с @).	from:Grimezsz
since:YYYY-MM-DD / until:YYYY-MM-DD	Ограничивает выдачу твитов по датам (от/до), можно использовать как в паре, так и один.	since:2022-12-30 until:2023-01-02 "new year"
-	Исключение элемента из выдачи.	мясо -веганы

Помните, что простой filetype:pdf редко приносит плоды, дорки должны составляться конкретно под запрос, и научиться вы этому должны сами, методом проб и ошибок.

Рекомендую, найдя нужный файл, попробовать написать различные запросы, чтобы добиться максимального поднятия его в поисковой выдаче. Таким образом вы можете практиковать составление запросов и их оптимизацию.

Также советую взглянуть на следующие материалы:

- [Google Hacking Database](#) – библиотека уже готовых запросов, изучив их, вы сможете составлять более сложные конструкции, что повысит эффективность вашего поиска.
- [Dork search](#) – это конструктор дорков, который облегчит вам некоторые моменты освоения темы.
- Если вы не знакомы с темой в целом, попробуйте начать с [этой статьи по Google доркам](#).

Авторы: [Schwarz_Osint](#) и [@vali_ax](#)