

# Open-source-инструменты для разработчика

которые мы заслужили



**@akuleshov7**

Андрей Кулешов

Руководитель разработки  
платформы данных



# Разработчик с разносторонним опытом



@akuleshov7

Андрей Кулешов

Руководитель разработки  
платформы данных



# Разработчик с разносторонним опытом



@akuleshov7

Андрей Кулешов

Руководитель разработки  
платформы данных



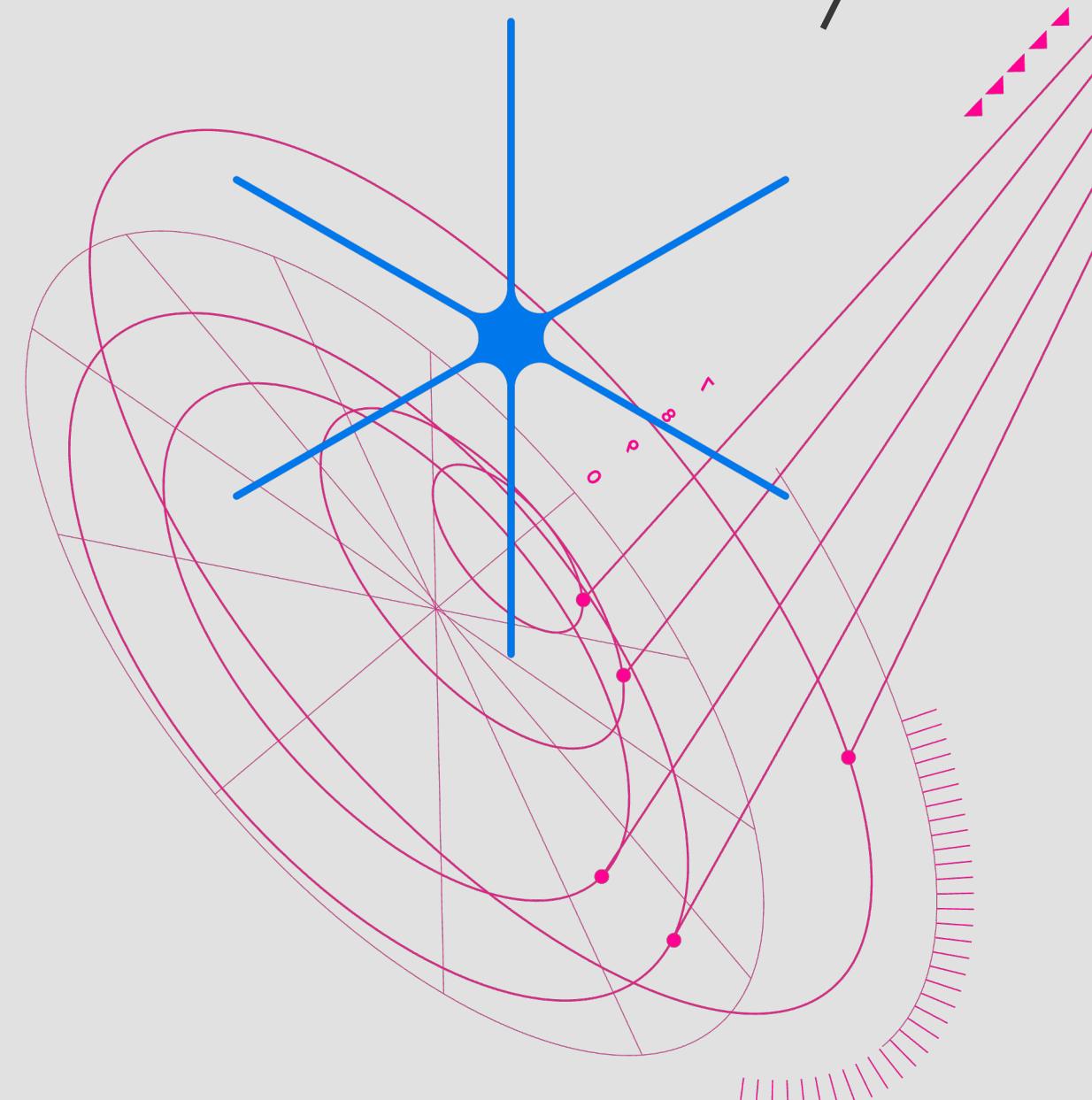
Мой Github



# Дисклеймер!

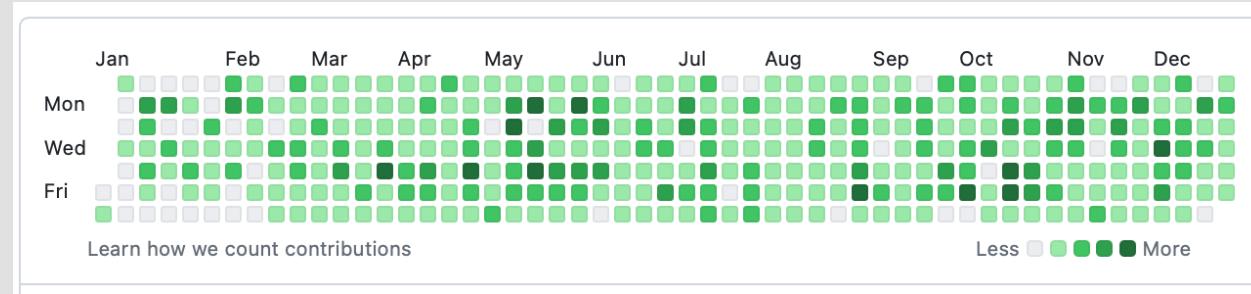


phd 2X pt

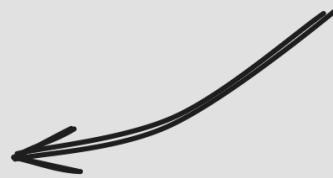


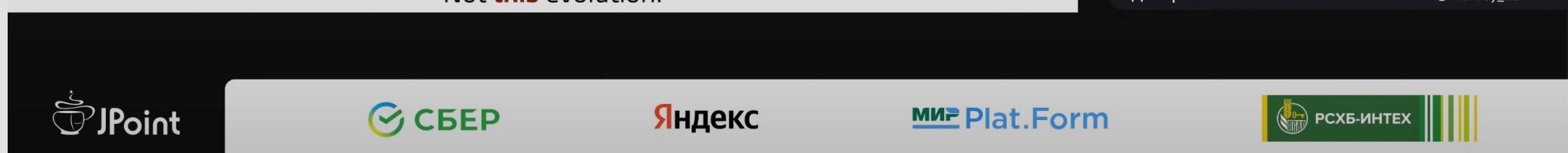
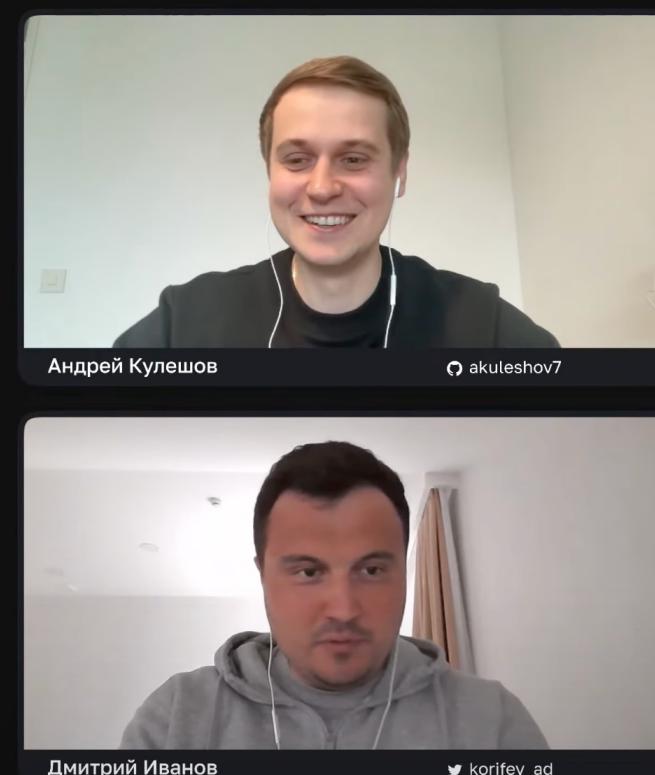
**Почему я хочу  
поговорить на эту тему?**

# Почему я хочу поговорить на эту тему?

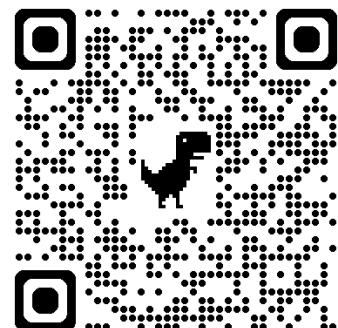


Пара моих  
последних лет





Дмитрий Иванов, Андрей Кулешов – Пирамида  
потребностей Маслоу для Java/Kotlin-разработчика



00

# Предисловие

Немного про экосистемы

phd 2X pt



*Open-source* –  
это флагман  
инструментов  
разработчика



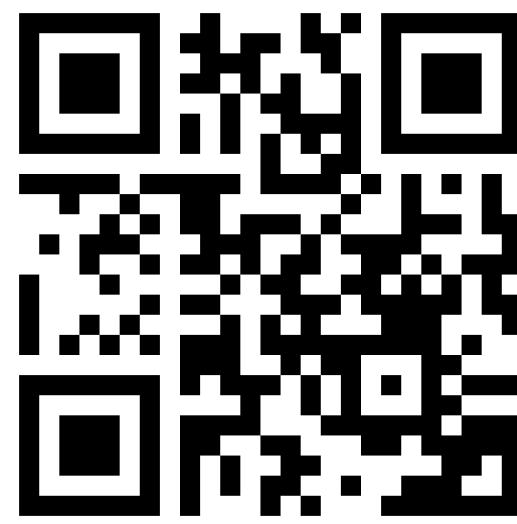
**Open-source –**  
это флагман  
инструментов  
разработчика



Знакомство,  
*Octocat*

# Github – лидер идей и мнений

Пример отличного DevTool'a



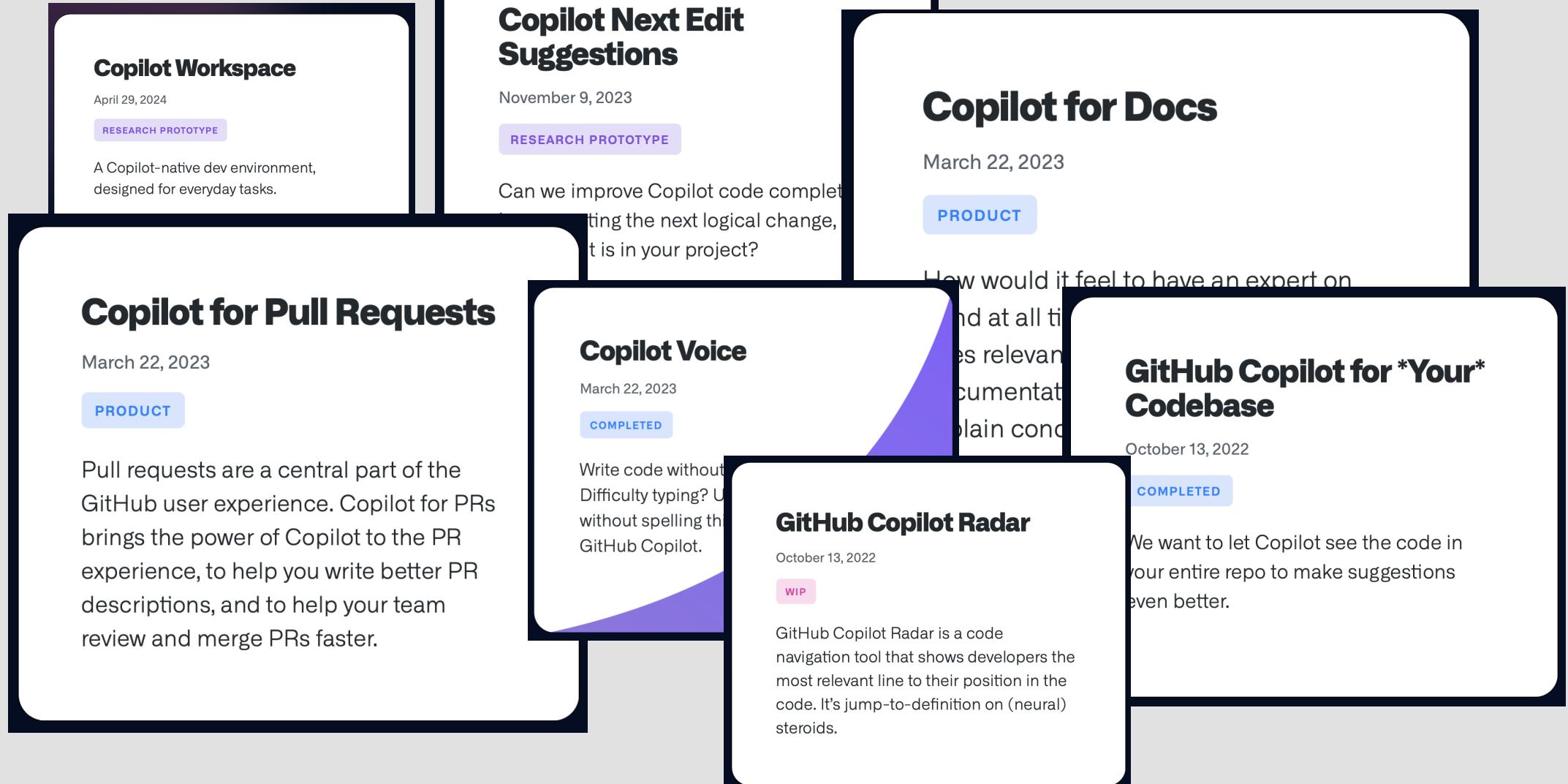
<https://githubnext.com>



GitHub Next

**GitHub Next investigates the future of software development.**

We are a team of researchers and engineers at GitHub, exploring things beyond the adjacent possible. We prototype tools and technologies that will change our craft. We identify new approaches to building healthy, productive software engineering teams.



**Copilot Workspace**

April 29, 2024

RESEARCH PROTOTYPE

A Copilot-native dev environment, designed for everyday tasks.

**Copilot Next Edit Suggestions**

November 9, 2023

RESEARCH PROTOTYPE

Can we improve Copilot code completion by suggesting the next logical change, based on what is in your project?

**Copilot for Pull Requests**

March 22, 2023

PRODUCT

Pull requests are a central part of the GitHub developer experience. Copilot for PRs brings the power of Copilot to the PR experience, to help you write better PR descriptions, and to help your team review and merge PRs faster.

**Copilot Voice**

March 22, 2023

IMPLEMENTED

Write code without thinking. Difficulty typing? Use voice input. Without spelling things out, Copilot will understand what you mean.

**Copilot for Docs**

March 22, 2023

PRODUCT

How would it feel to have an expert on your team at all times? With Copilot for Docs, you can have access to relevant documentation, code samples, and plain English explanations.

**GitHub Copilot for \*Your\* Codebase**

October 13, 2022

COMPLETED

We want to let Copilot see the code in your entire repo to make suggestions even better.

**GitHub Copilot Radar**

October 13, 2022

WIP

GitHub Copilot Radar is a code navigation tool that shows developers the most relevant line to their position in the code. It's jump-to-definition on (neural) steroids.

Что-то кроме accusmentov?

## Incremental CodeQL

October 11, 2022

RESEARCH PROTOTYPE

Faster feedback about security vulnerabilities on your PRs.

## Realtime GitHub

November 9, 2023

RESEARCH PROTOTYPE

Multiplayer collaboration for your whole repo.

## Collaborative Workspaces

October 14, 2022

NAPKIN SKETCH

As we increasingly work together remotely, how might we unify our workflows to enable remote collaboration for developers? GitHub Next explores what "working together" means, beyond multiple cursors and a shared code editor.

**ДОКЛАД**

**phd 2**

специализированных методов

Михаил Парфенов  
Архитектор Application Security  
независимый эксперт

15:00–16:00

**GENERAL DEVELOPMENT**

**ДОКЛАД**

Мультиязычный анализ кода при помощи графовой БД и предметно-ориентированного языка

В докладе рассматривается промежуточное представление исходного кода, называемое графом свойств кода (CPG), которое объединяет принципы классического анализа программ, а также графы потоков управления и зависимостей программ в единую языковозависимую структуру данных, путем обхода графа позволяющую моделировать шаблоны типичных уязвимостей (например, целочисленное переполнение или переполнение буфера).

Кроме того, уделяется внимание практическим аспектам работы с CPG, таким как сохранение графа в графовую базу данных и использование предметно-ориентированного языка для создания простого в использовании инструмента поиска уязвимостей, не привязанного к конкретному языку программирования.

16:00–17:00

**GENERAL DEVELOPMENT**

**ДОКЛАД**

Разработка своего языка

В обычных рабочих задачах задачи, для решения которых из них: о возможных подходах

Виктор Смирнов

Andrey Shcheglov

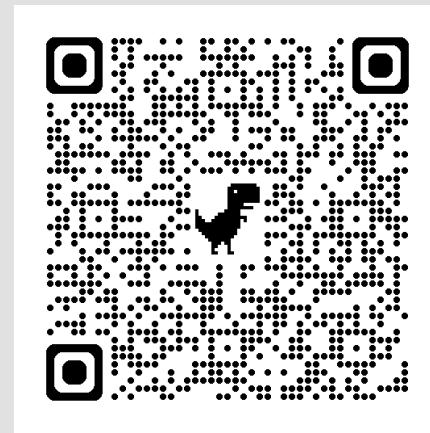
Зал «Фобос»

Зал «Деймос»

## Мультиязычный анализ кода при помощи графовой БД и предметно-ориентированного языка

GENERAL DEVELOPMENT ДОКЛАД

15:00–16:00 24 мая



Доклад  
от моей  
ex-команды  
Huawei про CodeQL  
и около



# 01

## Базовые *DevTools\**

И вот мы начали свой open-source проект...



\* Пропуская этап выбора языка, его компилятора, систем сборки и так далее

# **I**DE – Integrated Development Environment

**IDE – Integrated Development Environment**  
экосистема для полного цикла  
индивидуальной локальной разработки

# IDE: десктопные



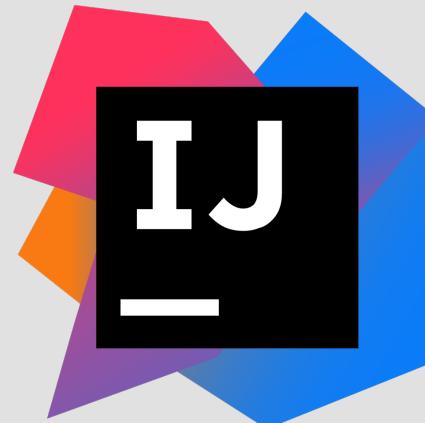
JetBrains



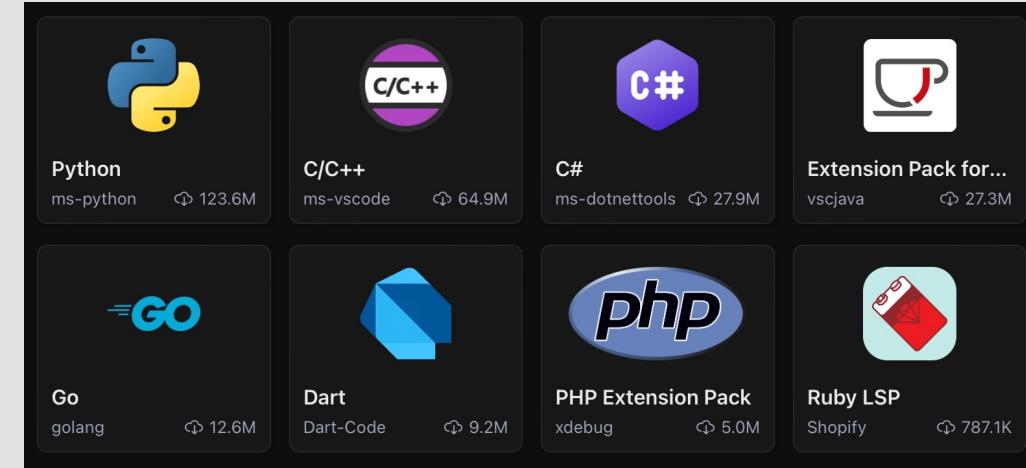
Java™



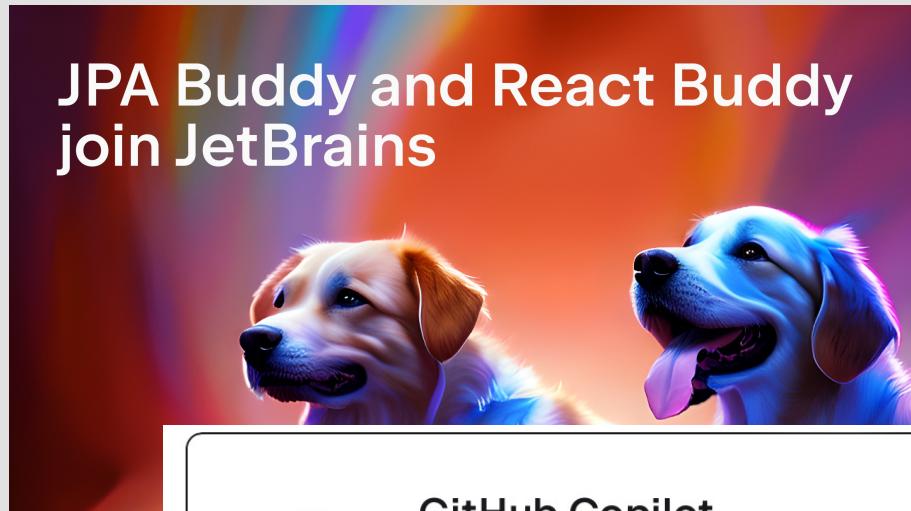
And more



Microsoft



# IDE: плагины



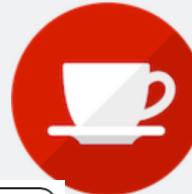
 GitHub Copilot  
★★★☆☆ 4.5  
GitHub

What's GitHub Copilot? GitHub Copilot is your AI-powered coding assistant, offering assistance throughout your software development process.

12,214,259 downloads      Free

Visual Studio | Marketplace

Visual Studio Code > Programming Languages > Language Support for Java(TM) by Red Hat

 Language Support for Java(TM) by Red Hat

Red Hat [redhat.com](https://redhat.com) | 35,034,775 installs | ★★★★☆ (163) | Free

Java Linting, Intellisense, formatting, refactoring, Maven/Gradle support and more...

[Install](#)   [Trouble Installing?](#)

[Overview](#)   Version History   Q & A   Rating & Review

Language support for Java™ for Visual Studio Code

 VS MARKETPLACE   **V1.30.0**   INSTALLS   **35M**   CHAT   ON GITTER   BUILD   PASSING

 LICENSE   **EPL-2.0**

Provides Java™ language support via [Eclipse™ JDT Language Server](#), which utilizes [Eclipse™ JDT](#), [M2Eclipse](#) and [ildship](#).

# IDE: плагины



JET BRAINS Marketplace Edu Courses Themes Plugin Ideas Build Plugins Sign In ? Search

User Interface Code Tools Fun Stuff +4 more

 Rainbow Brackets ★★★★★ 5 stars Zhihao Zhang ✓

Some features of the plugin require a paid subscription. [Learn more](#)  
Compatible with IntelliJ IDEA (Ultimate, Community), Android Studio and 15 more

Overview Versions Reviews Pricing Lifetime license(永久许可) 国区年付折扣 Why freemium Have issue? Privacy Notices EULA Check ▶

Included In

Productivity bundle ★★★★★

---

```
public class FlatMap {
    no usages
    public static <T, U, R> Optional<R> flatMap2(Optional<T> opt1,
                                                 Optional<U> opt2,
                                                 BiFunction<T, U, Optional<R>> func) {
        return opt1.flatMap(a →
            opt2.flatMap(b →
                func.apply(a, b)
            )
        );
    }
    {
        {
            (((((((( ))))))))
        }
    }
}
```

no usages

```
<div>
    <div>
        <div class="form-group">
            <label class="form-control-label col-sm-2">
                Rainbow Brackets is awesome!
            </label>
            <div class="col-sm-10">
                <input id="model" name="model" type="text"/>
                <div>Just install it!</div>
            </div>
        </div>
        <a>
            <div>Rainbow HTML/XML tags</div>
        </a>
    </div>

```

Rainbow HTML/XML tags

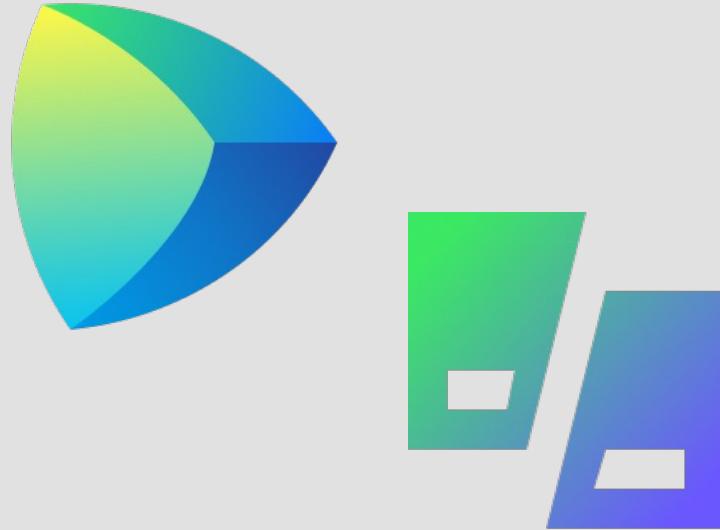
***IDE – Integrated Development Environment***  
экосистема для полного цикла  
индивидуальной локальной разработки

***IDE – Integrated Development Environment***  
экосистема для полного цикла  
индивидуальной (?) локальной (?)  
разработки

# IDE: Cloud/Web



JetBrains



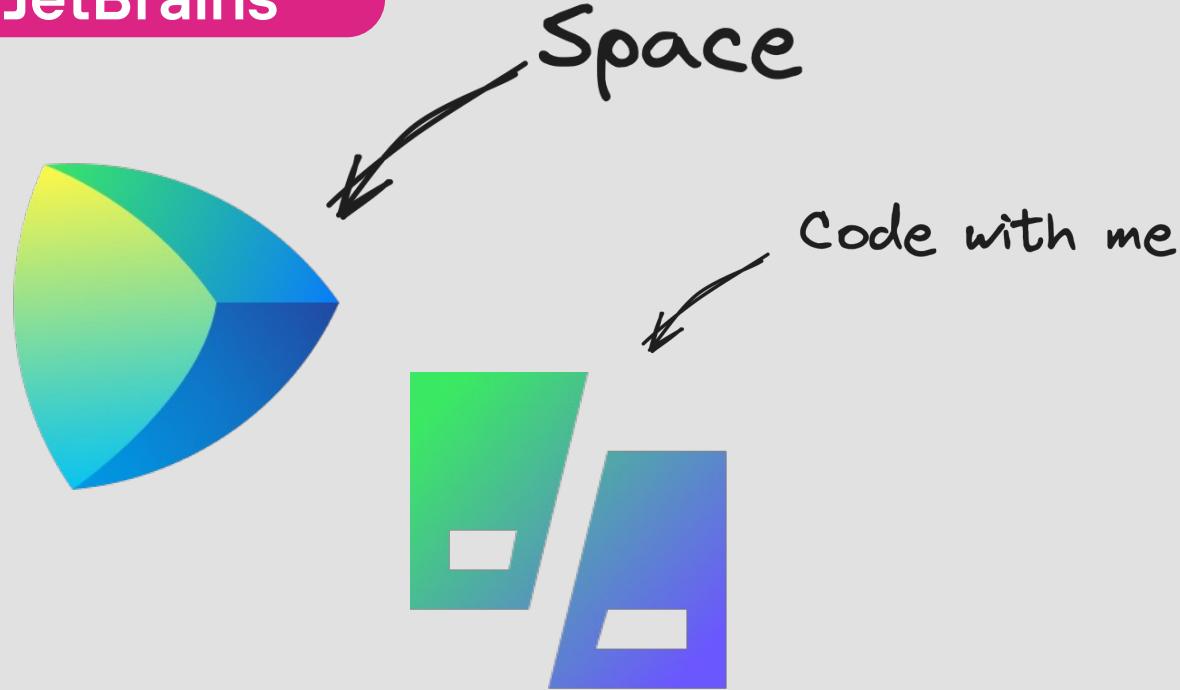
Microsoft



# IDE: Cloud/Web



JetBrains



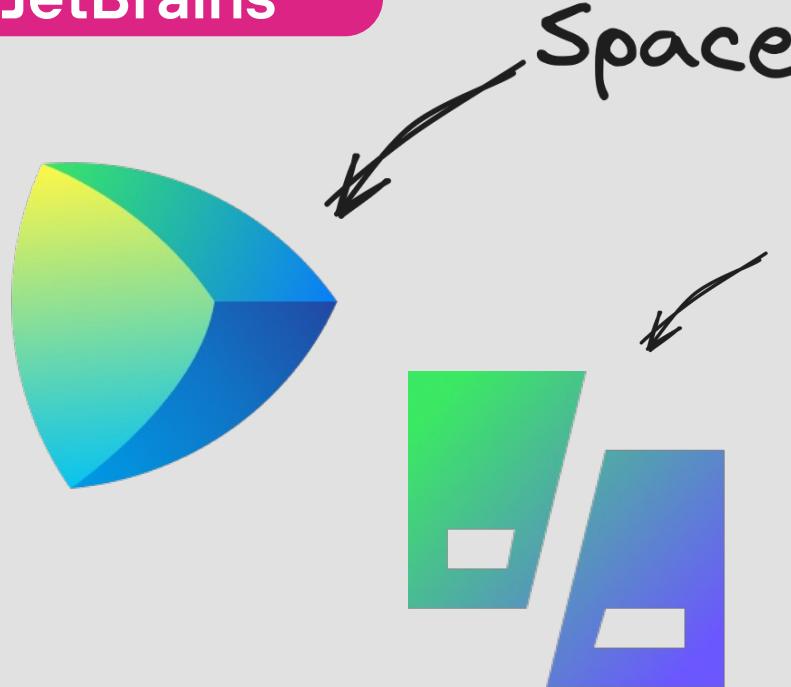
Microsoft



# IDE: Cloud/Web



JetBrains



Microsoft



VS code  
for the web

codespaces

# Devcontainers

<https://github.com/devcontainers>



## Dev Containers

Microsoft [microsoft.com](https://microsoft.com) | 24,270,223 installs | ★★★★☆ (50) | Free

Open any folder or repository inside a Docker container and take advantage of Visual Studio Code's full feature set.

[Install](#) [Trouble Installing?](#)

# *Git хостинг – платформа для хранения исходного кода*

***Git хостинг – платформа для  
хранения исходного кода  
экосистема для привлечения  
коммьюнити и совместного  
кодинга***

OPEN SOURCE HEROES BETA

Top Rating ▾ Discover ▾ Awesome ▾ By Country ▾ ☀ LOGIN



### TOP REPOSITORIES

- 1 [diktat](#)  
Strict coding standard for Kotlin and a custom set of rules for detecting code smells, code style issue...
- 2 [save-cli](#)  
Universal test framework for cli tools [ma...
- 3 [save-cloud](#)  
Cluster-based cloud mechanism for runni...
- 4 [diktat-demo](#)  
Demo project to show how diKTat or KTLi...
- 5 [okio-extras](#)  
A set of extensions to Okio, check out ht...
- 6 [benedikt](#)  
A GitHub Action to check your code with c...
- 7 [sarif-utils](#)  
The set of utilities, directed to work with...

**saveourtool**

[Share](#) [in Share](#) [Share](#)

Stars 386  
Global Org. Rank 27,482 (Top 9 %)  
Registered almost 3 years ago

Most used languages

Kotlin 100.0 %

**akuleshov7**

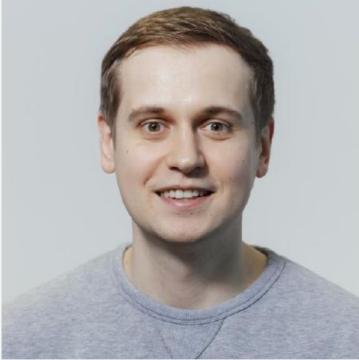
[Share](#) [in Share](#) [Share](#)

Available for Hire

Stars 484  
Global Rank 57,529 (Top 3 %)  
Followers 109  
Following 18  
Registered over 4 years ago

OPEN SOURCE HEROES BETA

Top Rating ▾ Discover ▾ Awesome ▾ By Country ▾ ☀ LOGIN



### TOP REPOSITORIES

- 1 [ktoml](#)  
Kotlin Multiplatform parser and compile-time serializer/deserializer for TOML format (Native, JS, JV...
- 2 [h-yapf](#)  
Customized version of google/yapf with specific code style rules for Python. This project does analy...
- 3 [kotlin-mpp-cli](#)
- 4 [small-interviews](#)  
Samples and questions for interview
- 5 [diktat-examples](#)  
Several examples of usage for diKTat project: <https://github.com/cqfn/diKTat>
- 6 [my-conference-presentations](#)  
My presentations for conferences and meetups
- 7 [kotlinx-serialization-map](#)  
Serialization mechanism from map to a serializable class

The screenshot shows the GitHub Stars homepage with a dark purple background. At the top left is the GitHub logo with the text "Stars". At the top right are navigation links: "Program", "Stars", "Nominate", "Alumni", and a "Sign in" button. Below the navigation is the text "GitHub Stars" and a large, bold, pink text "Go above and beyond". A subtitle below reads: "Recognize and lift up the people who inspire and educate your communities with the GitHub Stars program." A horizontal line separates this from the "Featured Stars" section. The "Featured Stars" section has a heading "Featured Stars" and a subtitle "Meet the shining individuals from the world's largest open source community." To the right is a "View all" button with a right-pointing arrow. The main content area displays eight profile cards, each with a small photo, the name, and the GitHub handle. The profiles are arranged in two rows of four. The first row includes Barbara Forbes (@Ba4bes), Eddie Jaoude (@eddiejaoude), Julio Arruda (@julioarruda), and Dries Vints (@DriesVints). The second row includes Gina Häußge (@GinaHaeusge), Emanuele Belotti (@emanuelebelotti), and others whose names are partially visible.

GitHub Stars

Program Stars Nominate Alumni Sign in

GitHub Stars

# Go above and beyond

Recognize and lift up the people who inspire and educate your communities with the GitHub Stars program.

---

## Featured Stars

Meet the shining individuals from the world's largest open source community.

View all →

Barbara Forbes  
Ba4bes

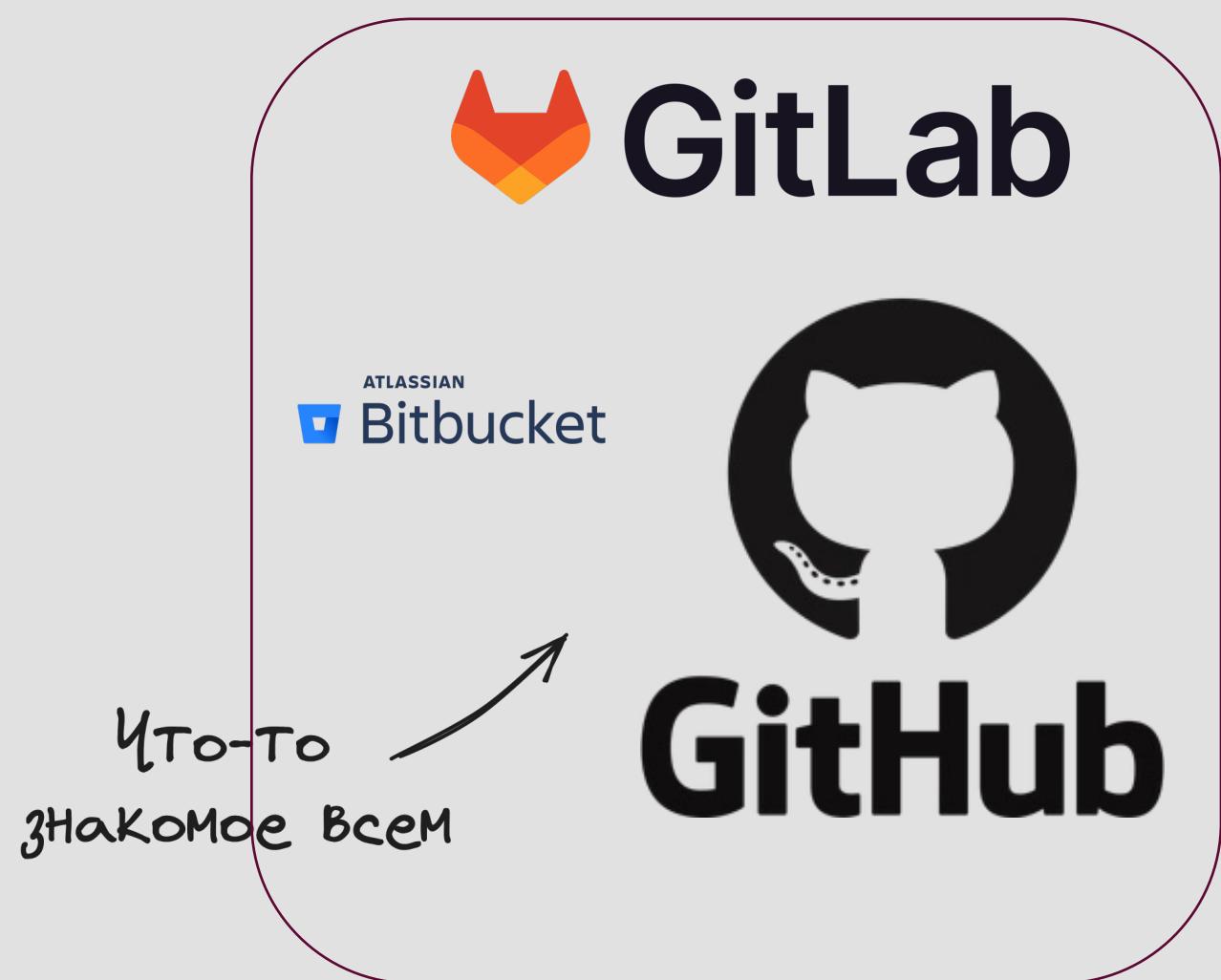
Eddie Jaoude  
eddiejaoude

Julio Arruda  
julioarruda

Dries Vints

Gina Häußge

Emanuele Belotti





# GitLab

ATLASSIAN  
Bitbucket



# GitHub

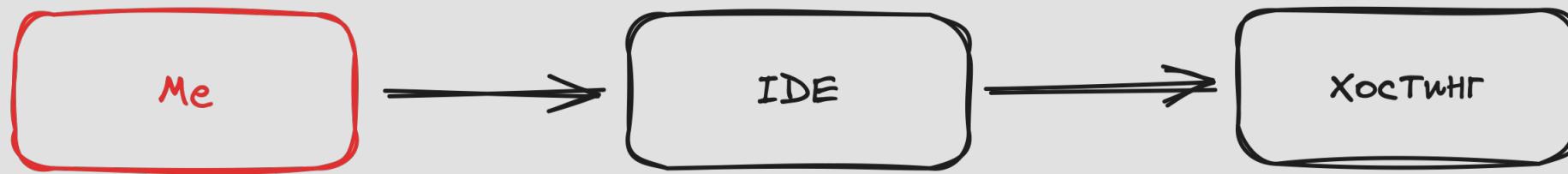
Что-то  
знакомое всем

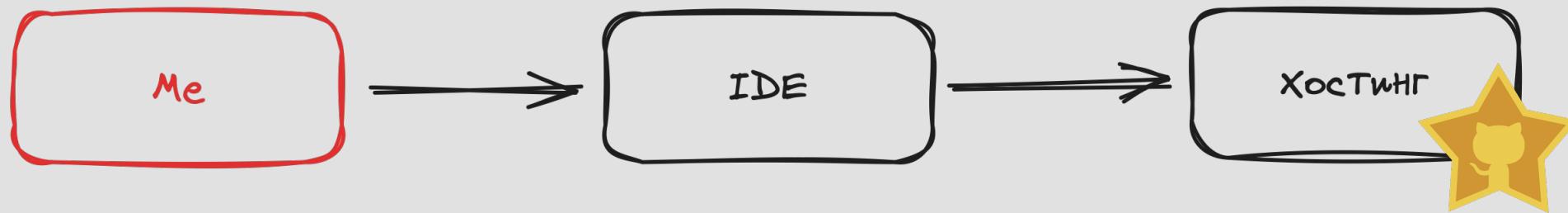
Наша специфика



# gitee



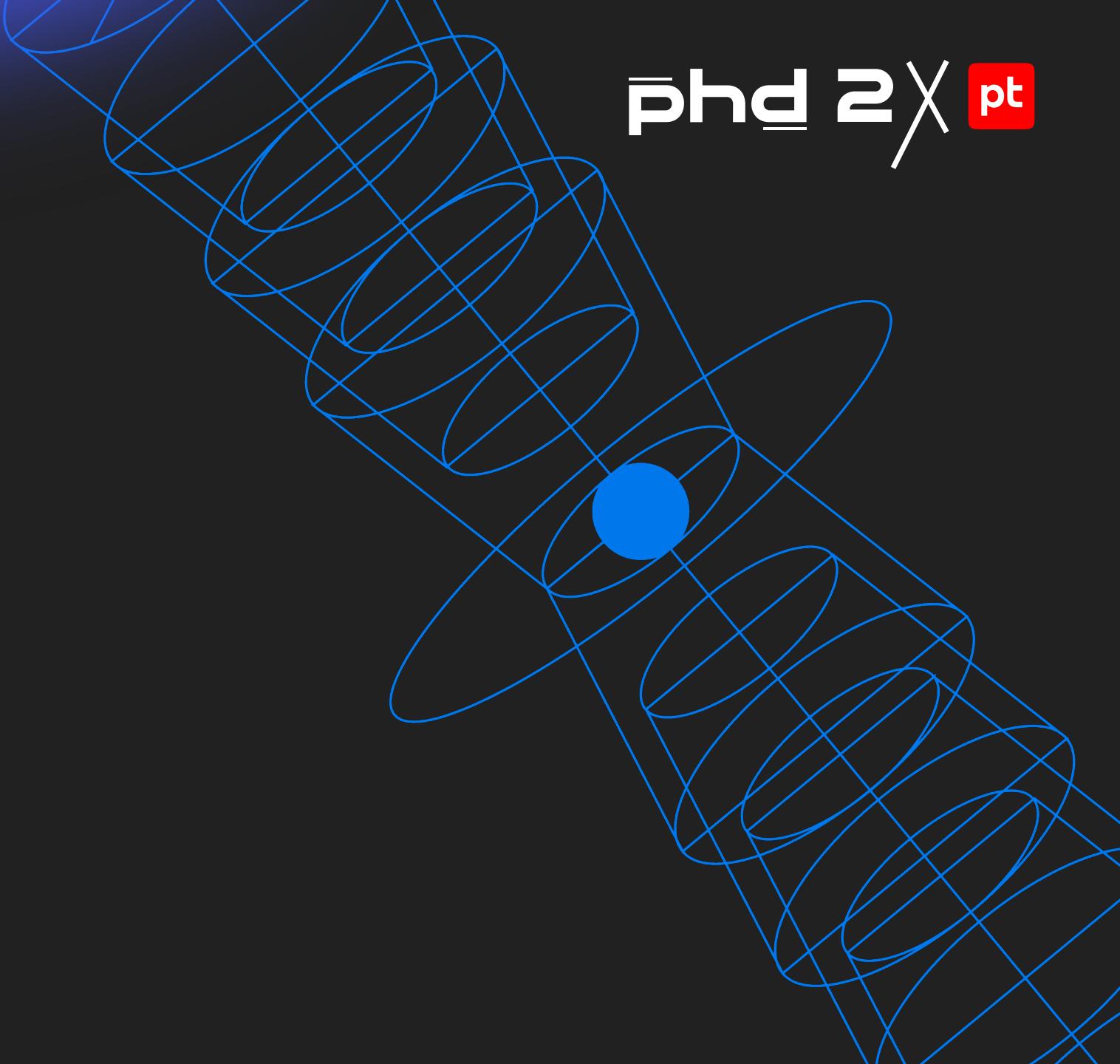




# 02

## *DevTools*

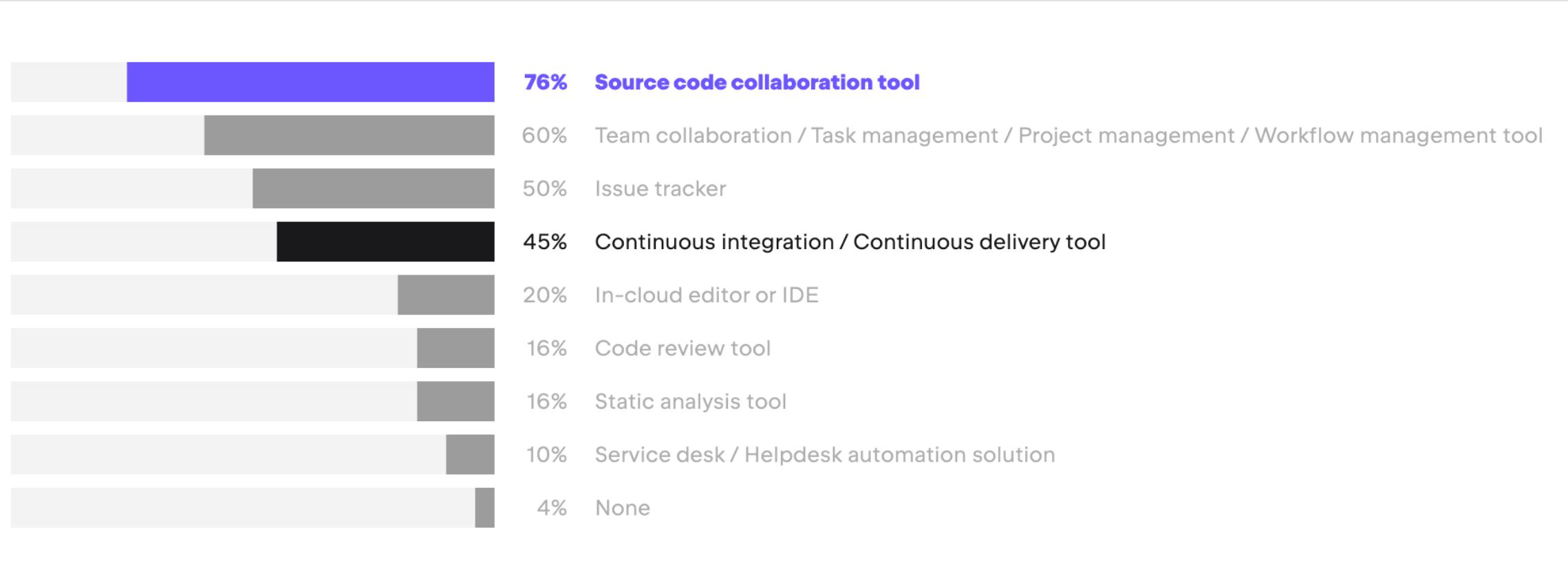
Код выложен, что еще нам нужно?



# CI – Continuous Integration

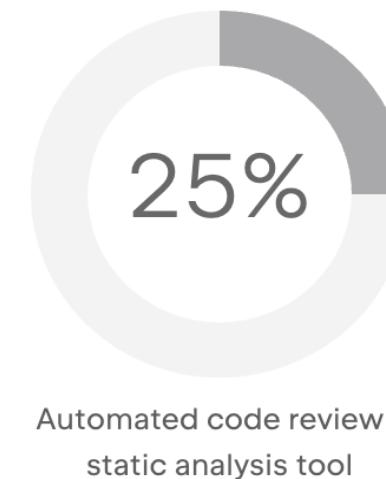
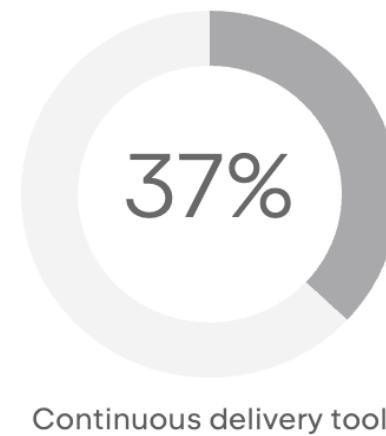
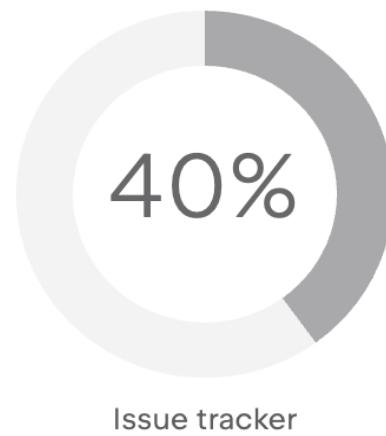
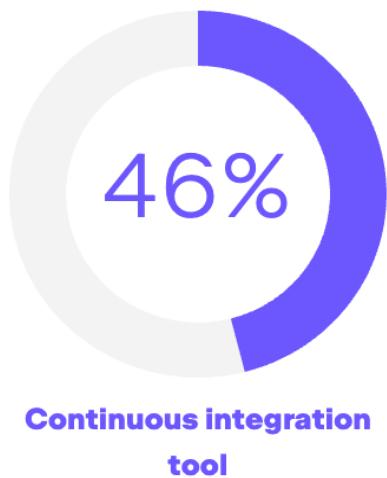
# **CI – Continuous Integration**

## **Сборка и валидации**



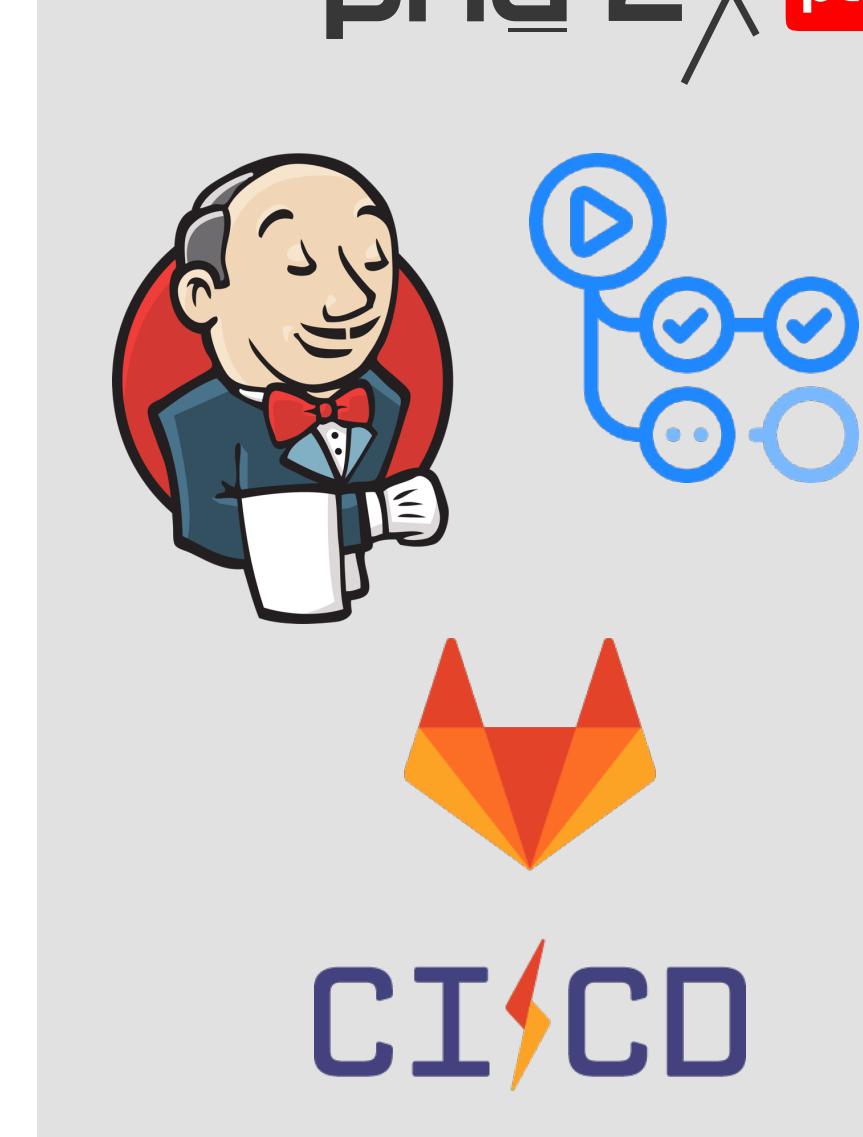
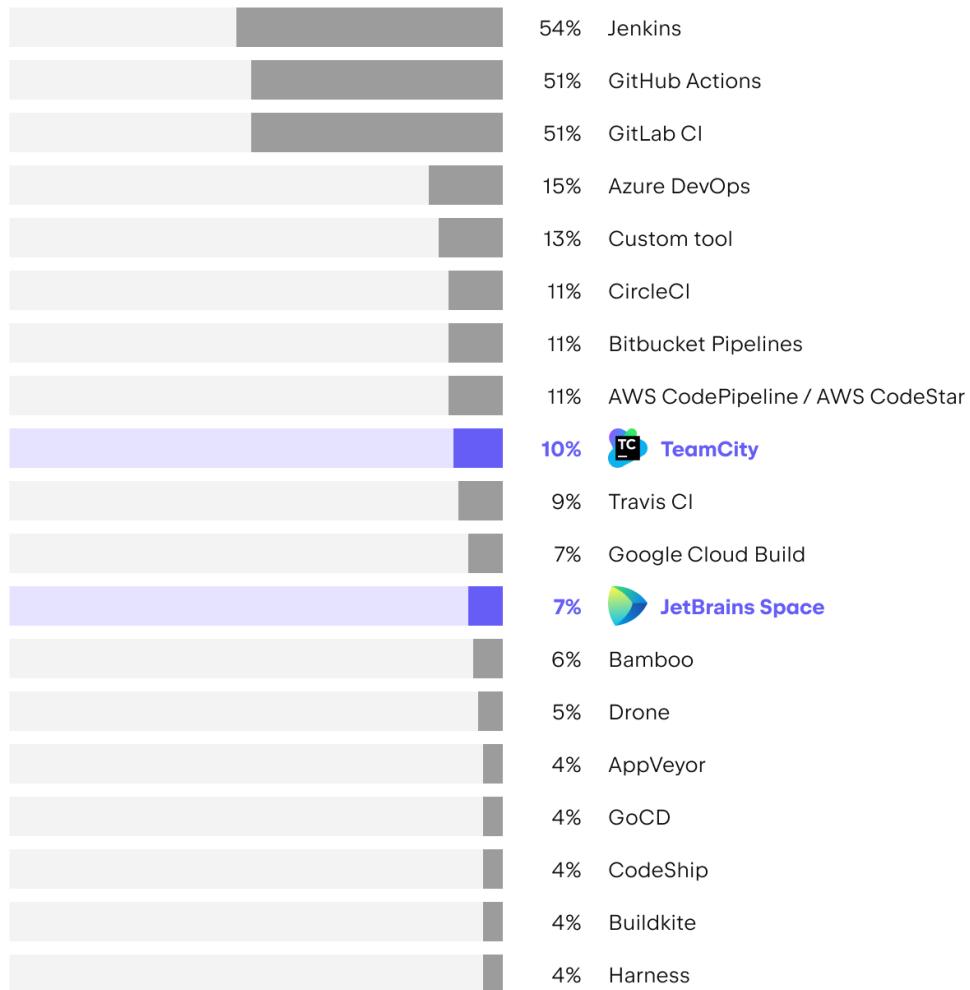
## The State of Developer Ecosystem 2023 Survey

**Do you use any of the following types of tools in the cloud?**



The State of Developer Ecosystem 2023 Survey

### Which Continuous Integration (CI) systems do you regularly use?





# Github Actions – in Action

Screenshot of a GitHub repository showing the Actions tab.

**Repository:** akuleshov7 / ktoml

**Actions Tab:**

- Build and test** (build\_and\_test.yml)
- 254 workflow runs**

Event	Status	Branch	Actor	
Update dependency io.github.gradle-nexus:publish-plugin to v2	Success	main	renovate/io.github.gradle...	2 days ago 15m 45s
Update all non-major dependencies (except core Kotlin)	Failure	main	renovate/all-minor-patch	2 days ago 1m 37s
Update Kotlin core dependencies to v1.9.24 (#268)	Success	main	main	2 days ago 21m 53s
Update all non-major dependencies (except core Kotlin)	Failure	main	renovate/all-minor-patch	2 weeks ago 1m 40s
Update Kotlin core dependencies to v1.9.24	Success	main	renovate/core-kotlin	2 weeks ago 19m 19s

**Actions Sidebar:**

- All workflows
- Build and test** (selected)
- Create release to Maven Central
- pages-build-deployment
- Run detekt
- Run diKTat
- Update yarn.lock generated by Kotlin...
- Management
  - Caches
  - Deployments
  - Attestations
  - Runners

```
name: Build and test
```

```
on:
```

```
  pull_request:
```

```
  push:
```

```
    branches:
```

```
      - 'main'
```

```
jobs:
```

```
  build_and_test:
```

```
    name: Build and test
```

```
    runs-on: macos-latest
```

```
steps:
```

```
  - uses: actions/checkout@v4
```

```
  - uses: gradle/wrapper-validation-action@v1
```

```
  - name: Set up JDK 8
```

```
    uses: actions/setup-java@v3
```

```
    with:
```

```
      java-version: 8
```

```
      distribution: zulu
```

```
name: Build and test
```

```
on:
```

```
  pull_request:
```

```
  push:
```

```
    branches:
```

```
      - 'main'
```

```
jobs:
```

```
  build_and_test:
```

```
    name: Build and test
```

```
    runs-on: macos-latest
```

```
steps:
```

```
  - uses: actions/checkout@v4
```

```
  - uses: gradle/wrapper-validation-action@v1
```

```
  - name: Set up JDK 8
```

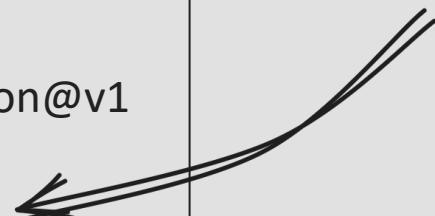
```
    uses: actions/setup-java@v3
```

```
    with:
```

```
      java-version: 8
```

```
      distribution: zulu
```

И снова удобство в шагах



Marketplace / Actions / Benedi.kt

X Delist

 GitHub Action  
**Benedi.kt**  
v2.0.0 Latest version

Use latest version ▾

## A GitHub Action to check your code with *diKTat*

 **Benedi.kt**  
A GitHub Action to check your code with *diKTat*

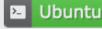
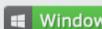
**INSTALLATION**  
Copy and paste the following snippet into your .yml file.

```
- name: Benedi.kt
  uses: saveourtool/benedikt@v2.0.0
```

[Learn more about this action in saveourtool/benedikt](#)

**Table of Contents**

- [Features](#)
- [Usage](#)
- [Configuration](#)
  - [config : custom configuration](#)
  - [reporter : requesting reporter](#)
  - [input-paths : custom input paths](#)
  - [java-distribution : Java distribution](#)
  - [fail-on-error : suppressing lint errors](#)
  - [debug : enabling debug logging](#)
- [Outputs](#)

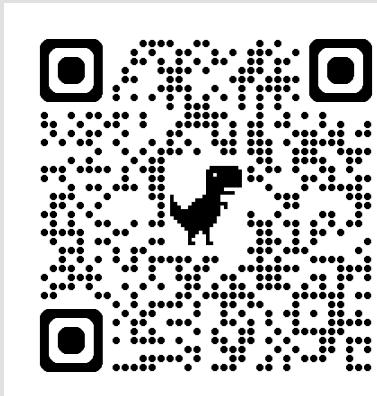
**License** MIT  
**release** v2.0.0  
 Ubuntu  
 macOS  
 Windows

An always updated version of this document is available [here](#) as a PDF e-book.

**Stars** 10

    4  2 

**Benedi.kt** is not certified by GitHub. It is provided by a third-party and is governed by separate terms of service, privacy policy, and support documentation.



# Плагины – абсолютно любой DevTool и не только



[Marketplace / Actions / OpenCommit — improve commits with AI 🐧](#)

 GitHub Action  
OpenCommit — improve commits with AI 🐧  
github-action-v1.0.2 Latest version

[Marketplace / Actions / TODO to Issue](#)

 GitHub Action  
TODO to Issue  
v4.13 Latest version

**TODO to Issue Action**

This action will convert newly committed TODO comments to GitHub issues on push. Optionally, issues can also be closed when the TODOs are removed in a future commit.

Action supports:

- Multiple, customizable comment identifiers (FIXME, etc.),
- Configurable auto-labeling,
- Assignees,
- Milestones,
- Projects (classic).

`todo-to-issue` works with almost any programming language.

**Usage**

Simply add a comment starting with TODO (or any other comment identifiers configured), followed by a colon and/or space.

Here's an example for Python creating an issue named after the TODO description:

```
def hello_world():
    # TODO Come up with a more imaginative greeting
```

[Marketplace / Actions / Metrics embed](#)

 GitHub Action  
Metrics embed  
v3.34 Latest version

**Metrics**

FEATURED ON Product Hunt

Continuous integration failing

Generate metrics that can be embedded everywhere, including your GitHub profile readme! Supports users, organizations, and even repositories!

For user accounts	For organization accounts
<b>Simon Lecocq</b> Joined GitHub 7 years ago Followed by 1223 users 30 Repositories Prefers MIT license 67 Releases 0 Packages 0.10 GB used 844k added, 382k removed	<b>CiHtub</b> Joined GitHub 16 years ago San Francisco, CA 255 members 493 Repositories Prefers MIT license 463 Releases 59 Packages 21.4 GB used 13979 Stargazers 1971 Forkers 146 Watchers

**Customizable with 47 plugins and 335 options!**

Isometric commit calendar	Languages activity
 Full year calendar 	 In-depth analysis (clone and anal repositories) 

Metrics embed is not certified by GitHub. It is provided by a third-party and is governed by separate terms of service, privacy policy, and support documentation.

# Плагины – абсолютно любой DevTool и не только



Marketplace / Actions / generate-snake-game-from-github-contribution-grid

GitHub Action

 **generate-snake-game-from-github-contribution-grid**

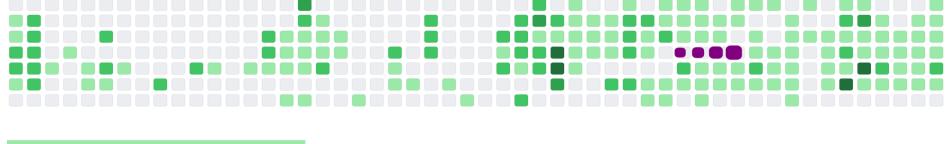
v3.2.0 [Latest version](#)

**Use latest version**

**snk**

action passing release v3.2.0 marketplace snake types TypeScript code style prettier

Generates a snake game from a github user contributions graph



Pull a github user's contribution graph. Make it a snake Game, generate a snake path where the cells get eaten in an orderly fashion.

Generate a [gif](#) or [svg](#) image.

Available as github action. It can automatically generate a new image each day. Which makes for great [github profile readme](#)

Stars [Star 3.8k](#)

Contributors 

Categories Utilities

Links [Platane/snk](#) [Open issues](#) 0 [Pull requests](#) 0 [Report abuse](#)

## Базовый минимум





# *Code Analysis* в CI – обязательный инструмент любого разработчика



**Стиль**

Следование код-стилю



**Паттерны**

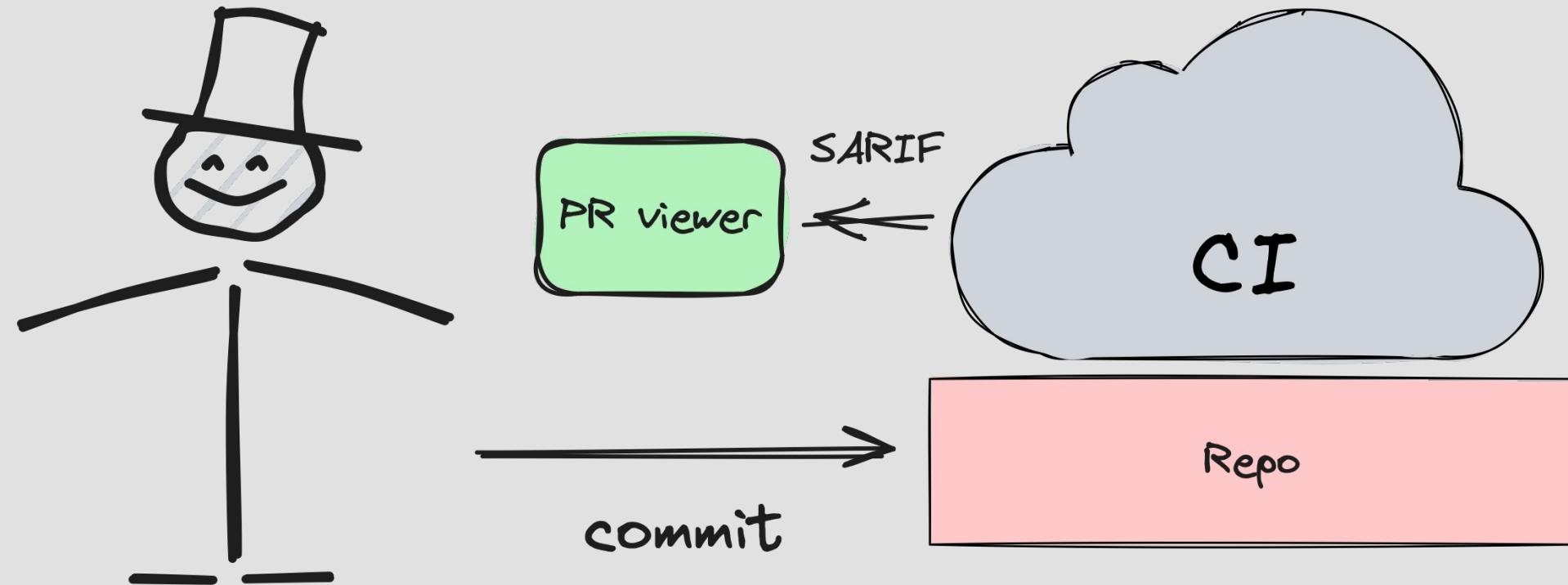
Проблемы дизайна и архитектуры



**Глубокие  
Ошибки**

NPE/Arithmetic errors/etc.

# Github + Sarif = ❤



```
277 +     tasks.forEach {  
278 +         println(it.name)  
279 +     }  
280 + }
```

Check failure

Code scanning / ktlint

[WRONG\_INDENTATION] only spaces are allowed for indentation and each indentation should equal to 4 spaces (tabs are not allowed): no newline at the end of file build.gradle.kts



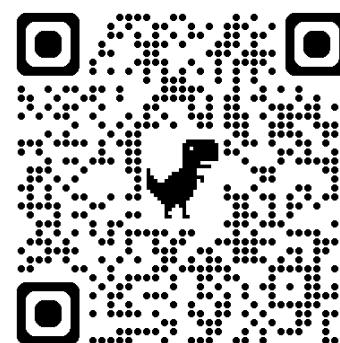
[WRONG\_INDENTATION] only spaces are allowed for indentation and each indentation should equal to 4 spaces (tabs are not allowed): no newline at the end of file build.gradle.kts

[Show more details](#)

[Dismiss alert ▾](#)



Reply...



```
- name: Copy SARIF reports into a single directory
  if: ${{ failure() }}
  run: |
    # ваша логика копирования репортов

- name: Upload SARIF report to Github
  uses: github/codeql-action/upload-sarif@v2
  if: ${{ failure() }}
  with:
    sarif_file: build/diktat-sarif-reports

- name: Upload SARIF artifacts
  uses: actions/upload-artifact@v3
  if: ${{ failure() }}
  with:
    name: sarif-reports
    path: "**/build/diktat-sarif-reports/"
    retention-days: 1
```

```
- name: Copy SARIF reports into a single directory
  if: ${{ failure() }}
  run: |
    # ваша логика копирования репортов

- name: Upload SARIF report to Github
  uses: github/codeql-action/upload-sarif@v2
  if: ${{ failure() }}
  with:
    sarif_file: build/diktat-sarif-reports

- name: Upload SARIF artifacts
  uses: actions/upload-artifact@v3
  if: ${{ failure() }}
  with:
    name: sarif-reports
    path: "**/build/diktat-sarif-reports/"
    retention-days: 1
```



собираете  
отчеты анализа Тора

```
- name: Copy SARIF reports into a single directory
  if: ${{ failure() }}
  run: |
    # ваша логика копирования репортов

- name: Upload SARIF report to Github
  uses: github/codeql-action/upload-sarif@v2
  if: ${{ failure() }}
  with:
    sarif_file: build/diktat-sarif-reports

- name: Upload SARIF artifacts
  uses: actions/upload-artifact@v3
  if: ${{ failure() }}
  with:
    name: sarif-reports
    path: "**/build/diktat-sarif-reports/"
    retention-days: 1
```



отдаёте в API GitHub

```
- name: Copy SARIF reports into a single directory
  if: ${{ failure() }}
  run: |
    # ваша логика копирования репортов

- name: Upload SARIF report to Github
  uses: github/codeql-action/upload-sarif@v2
  if: ${{ failure() }}
  with:
    sarif_file: build/diktat-sarif-reports

- name: Upload SARIF artifacts
  uses: actions/upload-artifact@v3
  if: ${{ failure() }}
  with:
    name: sarif-reports
    path: "**/build/diktat-sarif-reports/"
    retention-days: 1
```



храниTe на  
всякий случай



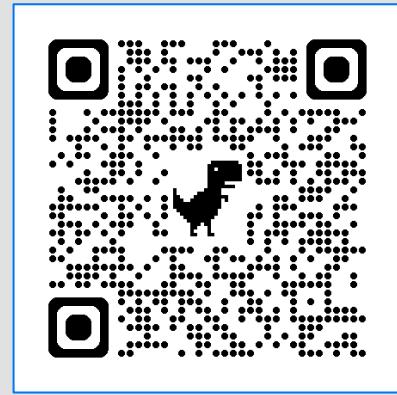
# Static Analysis Results Interchangeable Format

```
{  
...  
"results": [  
  {  
    "level": "error",  
    "message": {  
      "text": "'x' is assigned a value but never used."  
    },  
    "locations": [  
      {  
        "physicalLocation": {  
          "artifactLocation": {  
            "uri": "file:///C:/dev/example.js",  
            "index": 0  
          },  
          "region": {  
            "startLine": 1,  
            "startColumn": 5  
          }  
        }  
      }  
    ],  
    "ruleId": "no-unused-vars",  
    "ruleIndex": 0  
  }  
]  
}
```

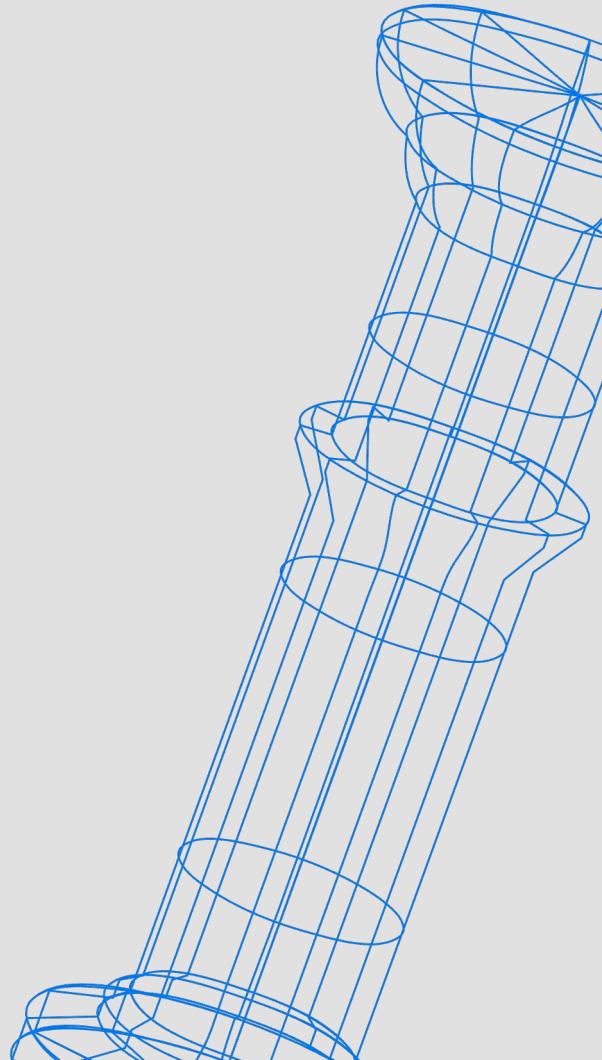
# Агрегаторы анализа



**Spotless:**  
Keep your code spotless



**Super-linter:**  
collection of linters and code  
analyzers, to help validate your  
source code.



# Что еще идет вместе с CI?



# Что еще идет вместе с CI?



## CodeCoverage

codecov commented a minute ago +  
Codecov Report

Merging #2159 into master will increase coverage by -1.09%

	master	#2159	Diff
- Coverage	52.36%	51.27%	-1.09%
Files	125	125	
Lines	11447	11449	+2
- Hits	5994	5871	-123
- Misses	4706	4832	+126
+ Partials	747	746	-1

**Impacted Files**

File	Coverage	Impact
registry/handlers/blobupload.go	45.17% <75.13%> (+4.17%)	✓
registry/handlers/app.go	48.2% <15%> (-7.1%)	✗
registry/handlers/basicauth.go	100% <o> (o)	✓

... and 4 more

I = absolute <relative> (impact) +  
o = not affected  
? = missing data  
Powered by [Codecov](#). Last update 96b02e8...7e162a8

codecov/codecov-action@v3

# Что еще идет вместе с CI?



## CodeCoverage

codecov commented a minute ago

**Codecov Report**

Merging #2159 into master will increase coverage by -1.09%

```
@@      Coverage Diff      @@
##      master      #2159  +/- ##  
=====  
- Coverage  52.36%  51.27%  -1.09%  
=====  
Files      125      125  
Lines     11447    11449    +2  
=====  
- Hits     5994    5871    -123  
- Misses   4706    4832    +126  
+ Partials 747     746     -1
```

Impacted Files	Coverage
registry/handlers/blobupload.go	45.17% <75.13%> (+4.17%) ✓
registry/handlers/app.go	48.2% <15%> (-7.1%) ✘
registry/handlers/basicauth.go	100% <> (o) ✓
... and 4 more	

I = absolute <relative> (impact)  
o = not affected  
? = missing data  
Powered by [Codecov](#). Last update 96b02e8...7e162a8

[codecov/codecov-action@v3](#)

## License scanning

FOSSA Public Index

diktat [home](#)

master [cae03e : chore\(deps\): update dependency io.github.gradle-nexus.publish-plugin to v2](#)

SUMMARY DEPENDENCIES 0 LICENSES 2 SEE MORE

**SCAN SUMMARY**

**License scan passed**  
Last scanned 4 hours ago

**Scan Details**

Issues found	0
License checks performed	3
Dependencies scanned	0
Scan type	Limited
Deepest dependency level	0

<https://app.fossa.com/>

# Что еще идет вместе с CI?



## CodeCoverage

**Codecov Report**

Merging #2159 into master will increase coverage by -1.09%

	Coverage Diff			
@@		@@		
##	master	#2159	+/-	##
- Coverage	52.36%	51.27%	-1.09%	
Files	125	125		
Lines	11447	11449	+2	
- Hits	5994	5871	-123	
- Misses	4706	4832	+126	
+ Partials	747	746	-1	

**Impacted Files**

File	Coverage	Impact
registry/handlers/blobupload.go	45.17%	<75.13%> (+4.17%)
registry/handlers/app.go	48.2%	<15%> (-7.1%)
registry/handlers/basicauth.go	100%	<o> (o)
... and 4 more		

I = absolute <relative> (impact) +  
o = not affected  
? = missing data  
Powered by [Codecov](#). Last update 96b02e8...7e162a8

[codecov/codecov-action@v3](#)

## License scanning

**FOSSA Public Index**

diktat [home](#)

master : cae03e : chore(deps): update dependency io.github.gradle-nexus.publish-plugin to v2

SUMMARY DEPENDENCIES 0 LICENSES 2 SEE MORE

**SCAN SUMMARY**

**License scan passed**  
Last scanned 4 hours ago

**Scan Details**

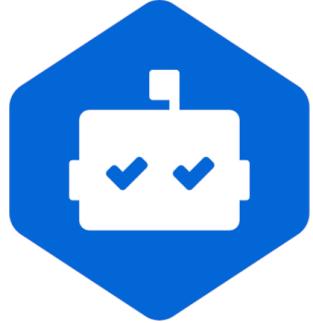
Metric	Value
Issues found	0
License checks performed	3
Dependencies scanned	0
Scan type	Limited
Deepest dependency level	0

<https://app.fossa.com/>

## Кастомизации

- Авто-обновление кода
- Генерация документации
- Работа с внешними API
- Подсчет метрик
- И многое другое...

# DevTools боты: dependencies



## Dependabot



# Renovate

## Dependency Dashboard #197

[Open](#) [7 tasks](#) renovate (bot) opened this issue last week · 0 comments



renovate (bot) commented last week · edited

Contributor ...

This issue lists Renovate updates and detected dependencies. Read the [Dependency Dashboard](#) docs to learn more.

### Awaiting Schedule

These updates are awaiting their schedule. Click on a checkbox to get an update now.

- Update actions/checkout action to v2.7.0
- Update all non-major dependencies (except core Kotlin) ( `org.junit.jupiter:junit-jupiter-engine`, `org.ajoberstar.grgit:grgit-core`, `org.ajoberstar.reckon:reckon-gradle`, `io.github.gradle-nexus:publish-plugin`, `io.gitlab.arturbosch.detekt:detekt-gradle-plugin`, `org.cqfn.diktat:diktat-gradle-plugin` )
- Update dependency gradle to v8
- Update dependency org.ajoberstar.grgit:grgit-core to v5
- Lock file maintenance

### Open

These updates have all been created already. Click a checkbox below to force a retry/rebase of any.

- Update all github actions (major) ( `actions/cache`, `actions/checkout`, `actions/setup-java`, `actions/upload-artifact`, `codecov/codecov-action`, `github/codeql-action` )

### Detected dependencies

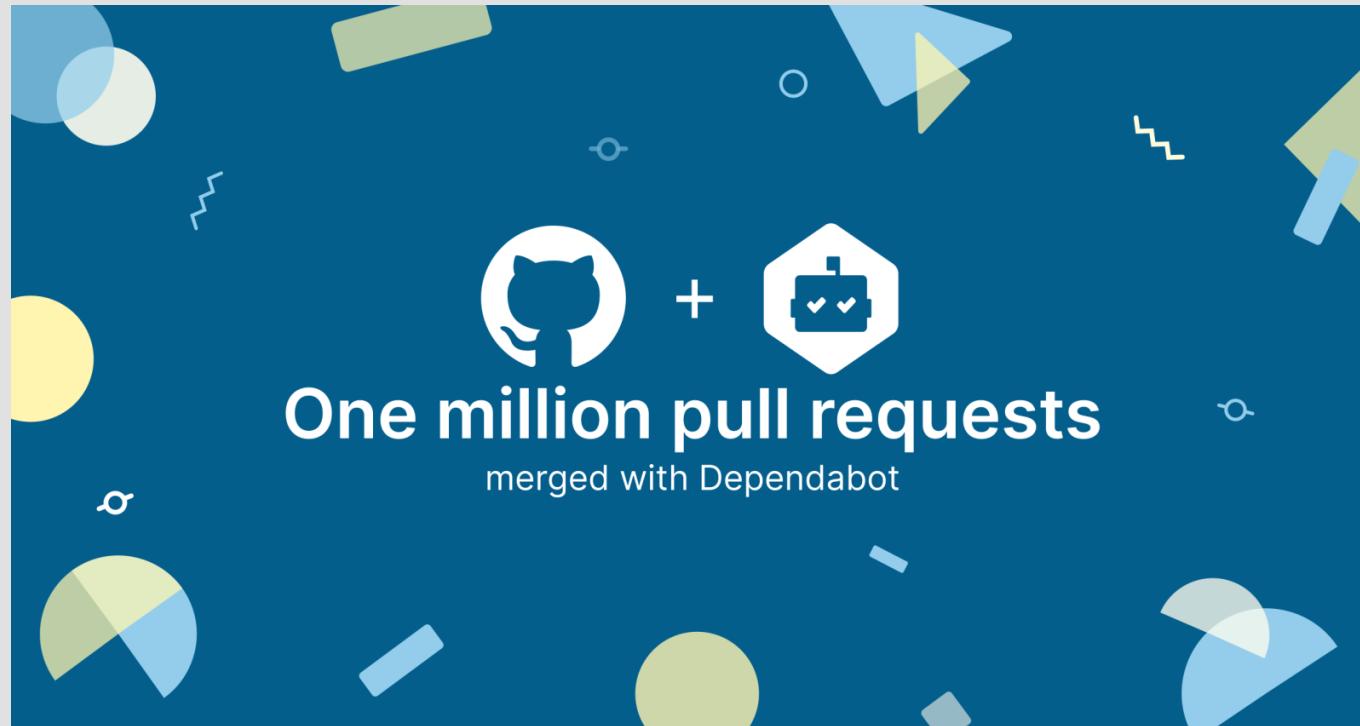
- ▶ `github-actions`
- ▶ `gradle`
- ▶ `gradle-wrapper`

Check this box to trigger a request for Renovate to run again on this repository



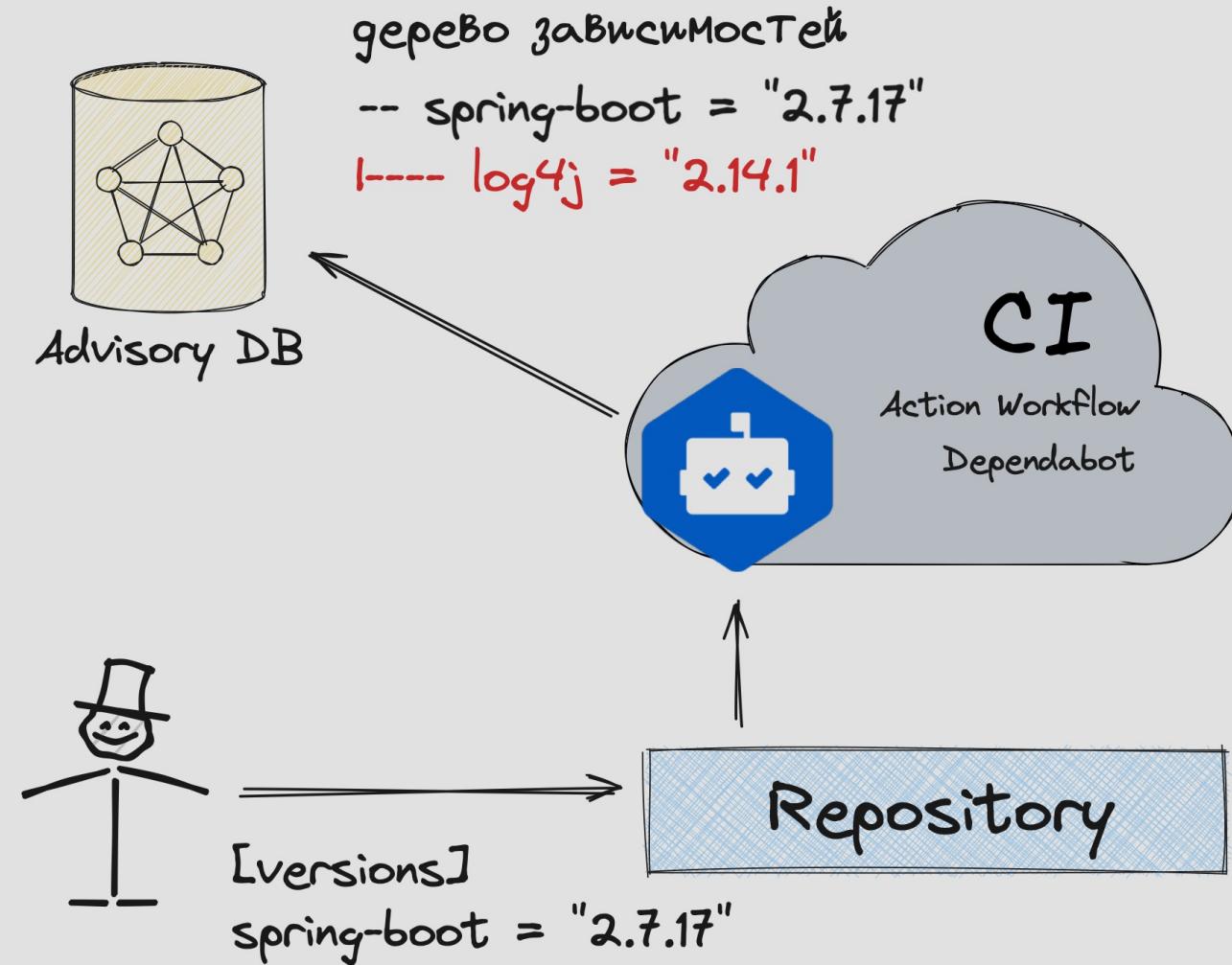
```
{
  "enabled": true,
  "dependencyDashboard": true,
  "schedule": [
    "before 4am on Monday"
  ],
  "lockFileMaintenance": {
    "enabled": true
  },
  "packageRules": [
    {
      "managers": ["github-actions"],
      "groupName": "all github actions",
      "groupSlug": "all-github-actions"
    },
    {
      "managers": ["gradle"],
      "matchPackagePatterns": [
        "*"
      ],
      "excludePackagePatterns": [
        "^org\\\\.jetbrains\\\\.kotlin[.]",
        "^org\\\\.cqfn\\\\.diktat\\{:diktat-gradle-plugin"
      ],
      "matchUpdateTypes": [
        "minor",
        "patch"
      ],
      "groupName": "all non-major dependencies",
      "groupSlug": "all-minor-patch"
    }
  ]
}
```

# Dependabot



July 25, 2019

# Dependabot



# Dependabot

- Граф зависимостей, но **есть нюанс**
- Авто-обновление зависимостей через PR
- Нотификации об уязвимостях



**Dependency graph**  
Understand your dependencies.  
Dependency graph is always enabled for public repos. Disable

---

**Dependabot**  
Keep your dependencies secure and up-to-date. [Learn more about Dependabot](#).

**Dependabot alerts**  
Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull requests to resolve these vulnerabilities. [Configure alert notifications](#). Disable

**Dependabot rules**  
Create your own custom rules and manage alert presets. 0 rules enabled

**Dependabot security updates**  
Enabling this option will result in Dependabot automatically attempting to open pull requests to resolve every open Dependabot alert with an available patch. If you would like more specific configuration options, leave this disabled and use [Dependabot rules](#). Disable

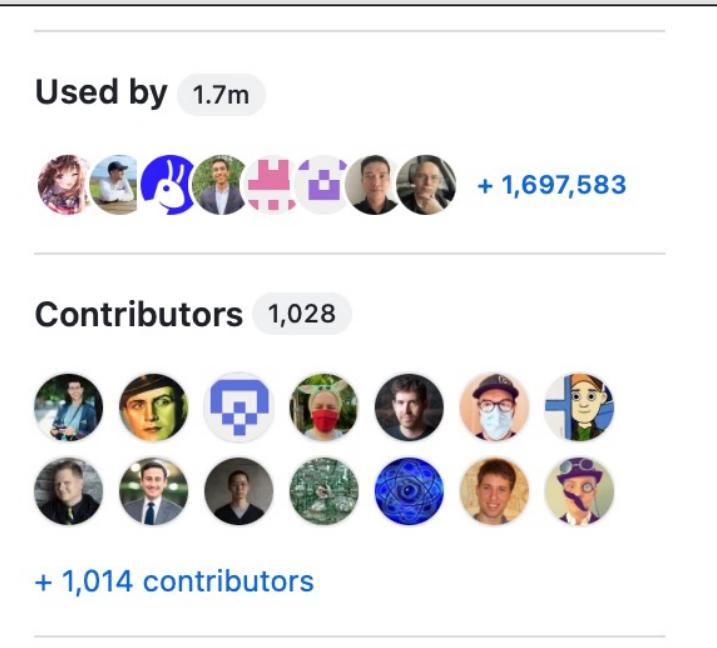
**Grouped security updates Beta**  
Groups all available updates that resolve a Dependabot alert into one pull request (per package manager and directory of requirement manifests). This option may be overridden by group rules specified in dependabot.yml - [learn more here](#) Disable

**Dependabot version updates**  
Allow Dependabot to open pull requests automatically to keep your dependencies up-to-date when new versions are available. [Learn more about configuring a dependabot.yml file](#). Enable

Cargo	Rust
Composer	PHP
NuGet	.NET languages (C#, F#, VB), C++
GitHub Actions	YAML
Go modules	Go
Maven	Java, Scala
npm	JavaScript
pip	Python
pnpm	JavaScript
pub	Dart
Python Poetry	Python
RubyGems	Ruby
Swift Package Manager	Swift
Yarn	JavaScript

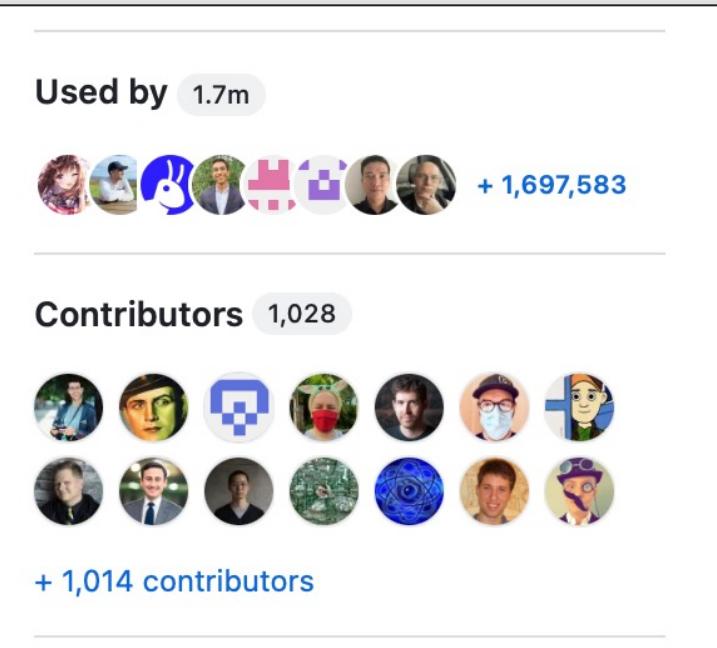
HtOaHC

Gradle?  
SBT?  
Kotlin?



Used by 1.7m

+ 1,697,583



Contributors 1,028

+ 1,014 contributors



Что отдаёт?



Screenshot of the GitHub Dependabot alerts page.

The page title is "Dependabot alerts". On the left sidebar, under the "Dependabot" section, there are two open alerts indicated by the number "2".

The main content area shows a summary of alerts:

- Auto-triage your alerts (Beta)**: A section describing how to control alert handling. It includes a "Configure" button and a diagram illustrating actions like "Generate fix for custom pattern" and "Ignore for manifest".
- A search bar with the query "is:open".
- Filtering options: Open/Closed status, Package, Ecosystem, Manifest, Severity, and Sort.
- A list of two open alerts, both categorized as "Data written to GitHub Actions Cache may expose secrets" (High severity):
  - #8 opened last year • Detected in gradle/gradle-build-action (GitHub Actions) • .github/workflows/kjs-yarn-update.yml
  - #7 opened last year • Detected in gradle/gradle-build-action (GitHub Actions) • .github/workflows/diktat.yml
- A "ProTip!" message: "See auto-dismissed alerts with [resolution:auto-dismissed](#)".

At the bottom, there is a footer with the GitHub logo and copyright information: "© 2024 GitHub, Inc. Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information".

ДОКЛАД Analytics 14.03 / 11:00 – 11:45 (UTC+3)

# Архивы уязвимостей и как их готовить

RU 🎧

Презентация [pdf](#) ⌂

В мире существует множество баз данных и форматов для хранения уязвимостей. Многие из вас знакомы с такими аббревиатурами, как CVE и CWE. Некоторые слышали о NVD и OWASP, а кто-то, возможно, даже умеет рассчитывать векторы атак по CVSS. Однако в глобальном мире, где программистам важно быстро анализировать свой код и узнавать об уязвимых зависимостях, существует множество баз данных для лучшей агрегации и поиска по существующим проблемам безопасности.

Есть целые комитеты, которые разрабатывают форматы – такие, как OSV – для лучшего представления и репортинга проблем с безопасностью в базах GitHub Advisory, Ubuntu Security Notices, Android Vulnerability Database и других. В итоге очень сложно уследить за всеми новыми аббревиатурами и обновлениями, которые появляются почти ежедневно.

Обобщу знания об уже существующих форматах, схемах и репозиториях для уязвимостей. Поделюсь своим опытом создания нового формата для представления и хранения уязвимостей под названием COSV. Кроме того, расскажу про личный опыт разработки базы данных уязвимостей, построенной на основе этого формата, которая стала стандартом для China Computing Federation (CCF).

## Спикеры

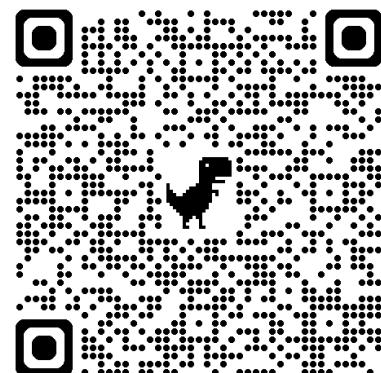


Андрей Кулешов  
Huawei

## Приглашенные эксперты



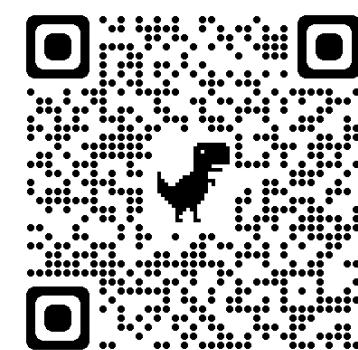
Антон Сысоев  
Независимый разработчик

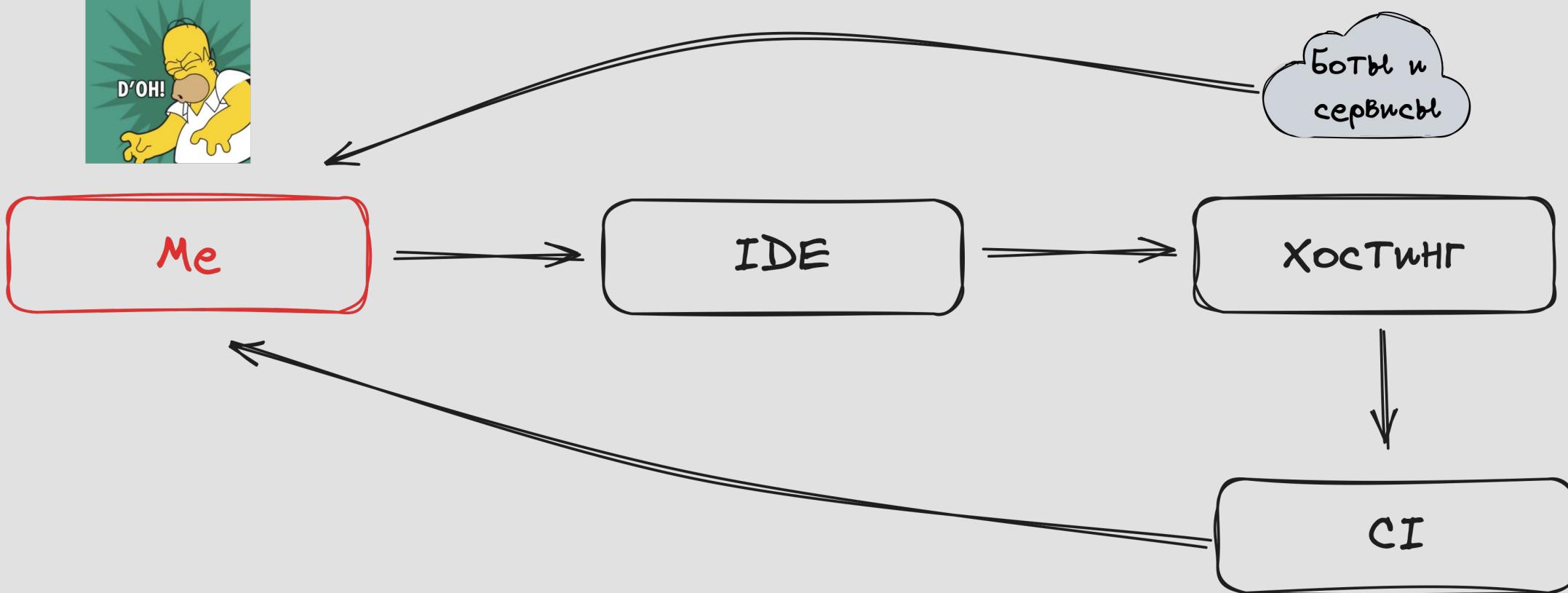


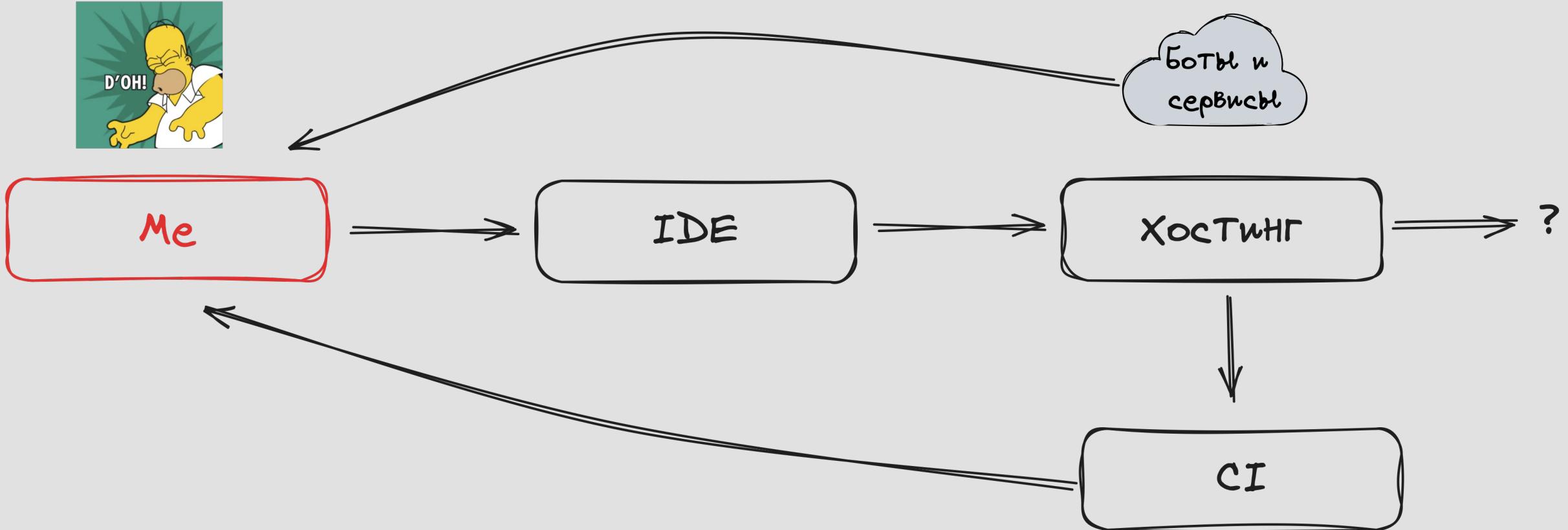
# DevTools боты: CodeQL



```
/**  
 * @id java/examples/tryfinally  
 * @name Try-finally statements  
 * @description Finds try-finally statements without a catch clause  
import java  
  
from TryStmt t  
where  
exists(t.getFinally()) and  
not exists(t.getACatchClause())  
select t
```



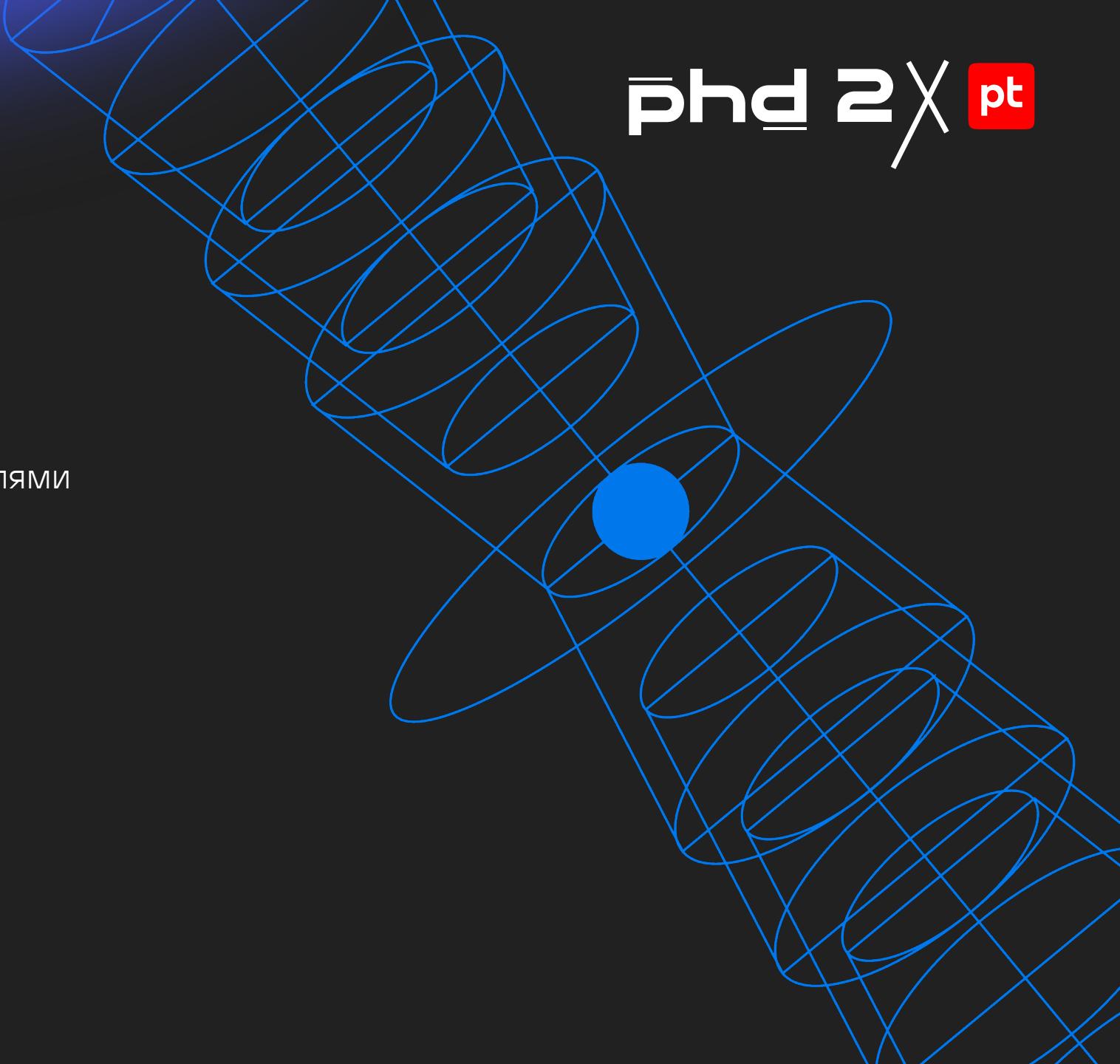




# 03

## *DevTools*

Дело за малым! Поработать с пользователями



# Packages – результат работы

GitHub Packages /

## Working with a GitHub Packages registry

Learn how to use a supported GitHub Packages registry.

- [Working with the Container registry](#)
- [Working with the Docker registry](#)
- [Working with the RubyGems registry](#)
- [Working with the npm registry](#)
- [Working with the Apache Maven registry](#)
- [Working with the Gradle registry](#)
- [Working with the NuGet registry](#)
- [Migrating to the Container registry from the Docker registry](#)

Работает абсолютно как  
и любой другой  
артефакт менеджер

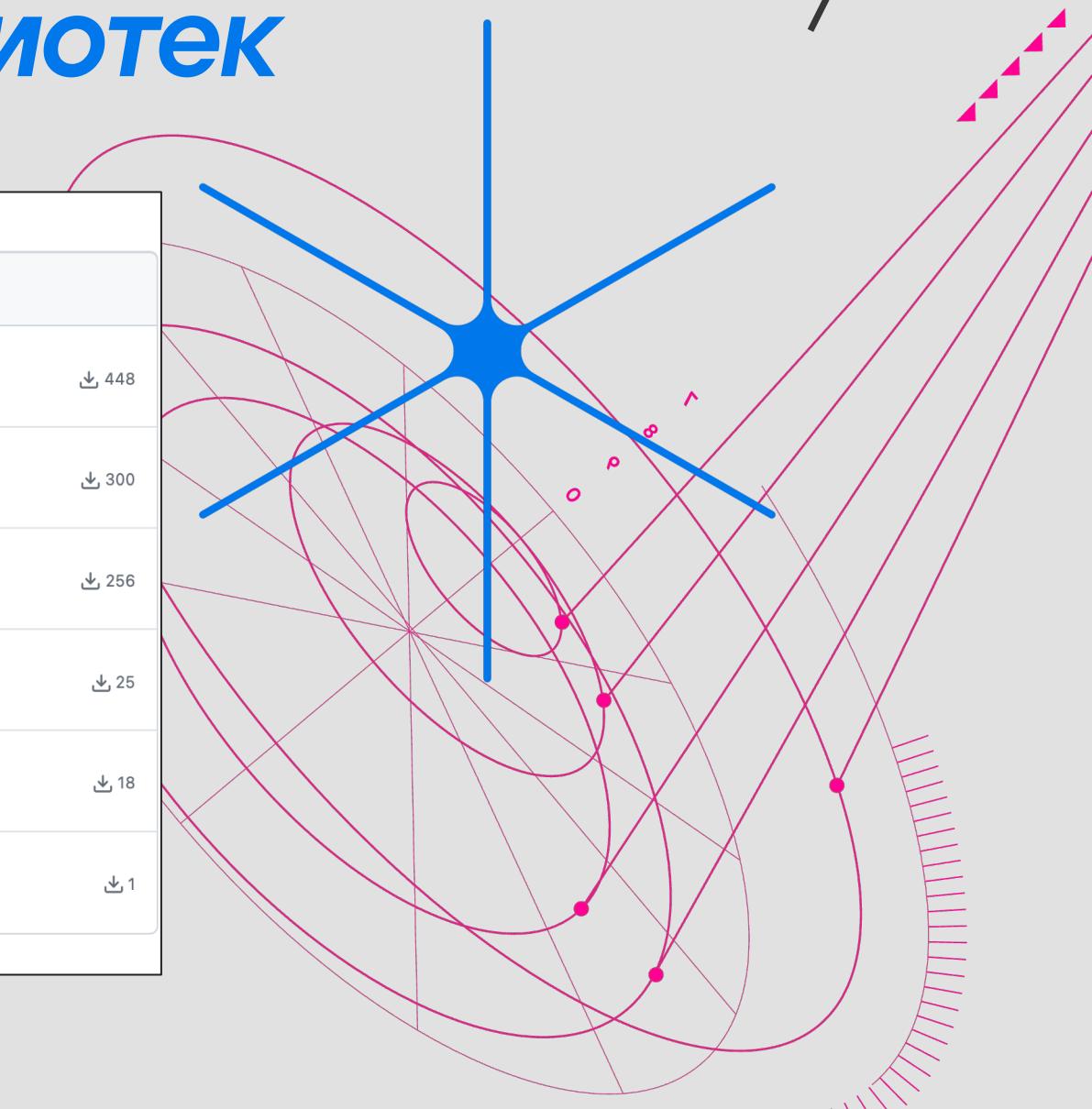


# Packages – для библиотек

Clear current search query, filters, and sorts

**6 packages**

-  **com.saveourtool.okio-extras-jvm**  
Published on Mar 2, 2023 by Save Our Tool! in [com.saveourtool.okio-extras-jvm](#)
-  **com.saveourtool.okio-extras**  
Published on Mar 2, 2023 by Save Our Tool! in [com.saveourtool.okio-extras](#)
-  **com.saveourtool.okio-extras-linuxx64**  
Published on Mar 2, 2023 by Save Our Tool! in [com.saveourtool.okio-extras-linuxx64](#)
-  **com.saveourtool.okio-extras-mingwx64**  
Published on Mar 2, 2023 by Save Our Tool! in [com.saveourtool.okio-extras-mingwx64](#)
-  **com.saveourtool.okio-extras-macosx64**  
Published on May 4, 2023 by Save Our Tool! in [com.saveourtool.okio-extras-macosx64](#)
-  **com.saveourtool.okio-extras-macosarm64**  
Published on May 4, 2023 by Save Our Tool! in [com.saveourtool.okio-extras-macosarm64](#)



# Packages – для приложений

**save-backend**

Install from the command line

```
$ docker pull ghcr.io/saveourtool/save-backend:0.4.0-alpha.0.460-8f62e13
```

Recent tagged image versions

<a href="#">0.4.0-alpha.0.460-8f62e13</a>	↓ 2
Published 12 days ago · Digest	...
<a href="#">0.4.0-alpha.0.459-e101105</a>	↓ 9
Published 23 days ago · Digest	...
<a href="#">0.4.0-alpha.0.458-7e126d4</a>	↓ 13
Published about 1 month ago · Digest	...
<a href="#">0.4.0-alpha.0.457-7501e3e</a>	↓ 33
Published 2 months ago · Digest	...
<a href="#">0.4.0-alpha.0.456-11bdef0</a>	↓ 33
Published 2 months ago · Digest	...
<a href="#">View and manage all versions</a>	

Details

- saveourtool
- save-cloud
- MIT License

Last published **12 days ago**

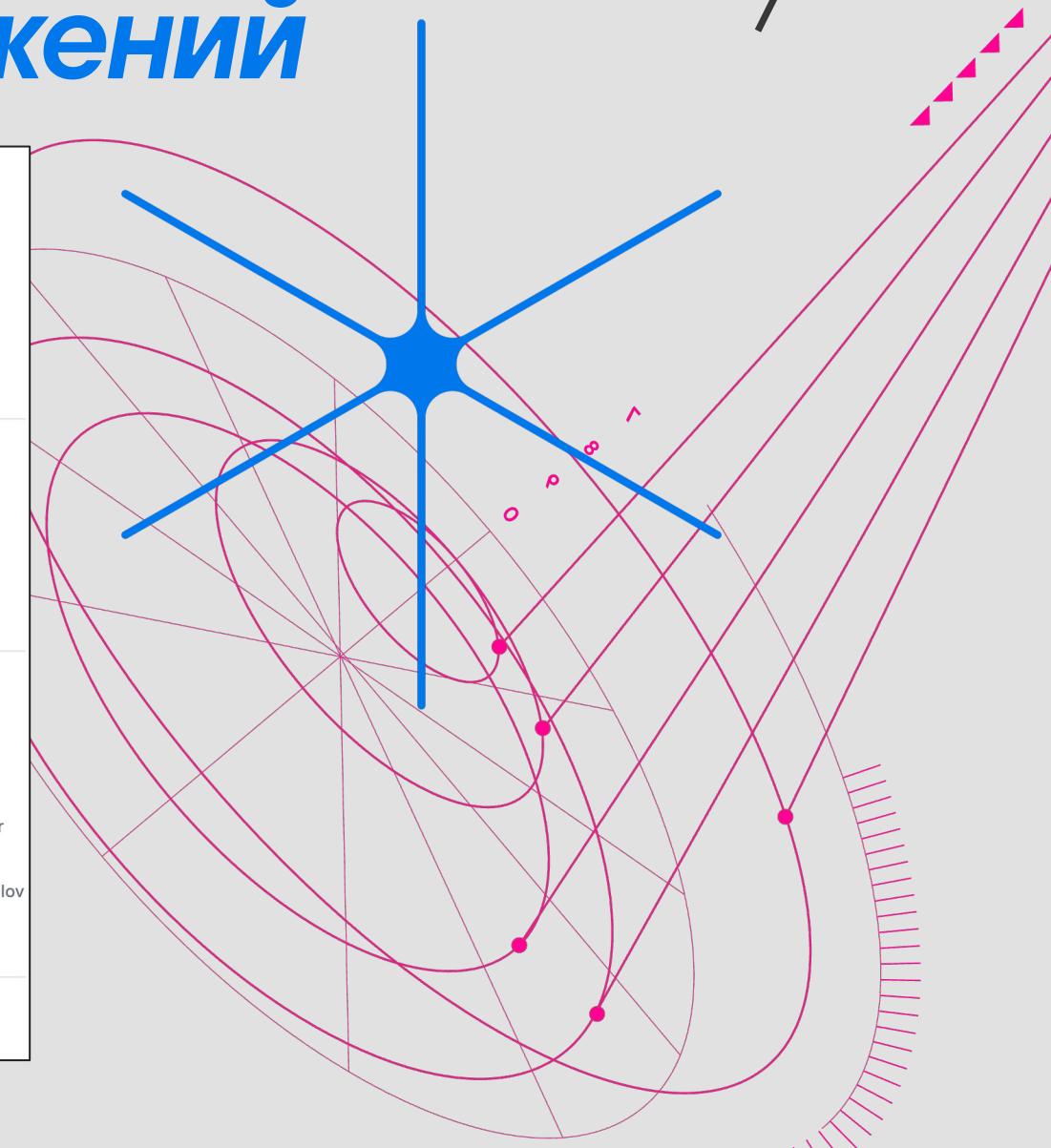
Discussions **6** Issues **201**

Total downloads **222K**

Collaborators **5**

-  **peterrr** Peter Trifanov
-  **nulls** Nariman Abdullin
-  **sanyavertolet** Alexander Frolov
-  **Cheshiriks** Vladislav Frolov
-  **renovate[bot]**

[Start a discussion](#) [Open an issue](#)



# Метрики — завлечем пользователей



CII Best Practices Level:

cii gold

CII Best Practices Tiered Percentage:

cii 107%

CII Best Practices Summary:

cii in progress 94%

<https://bestpractices.coreinfrastructure.org>

total lines 78k

repo size 749 kB

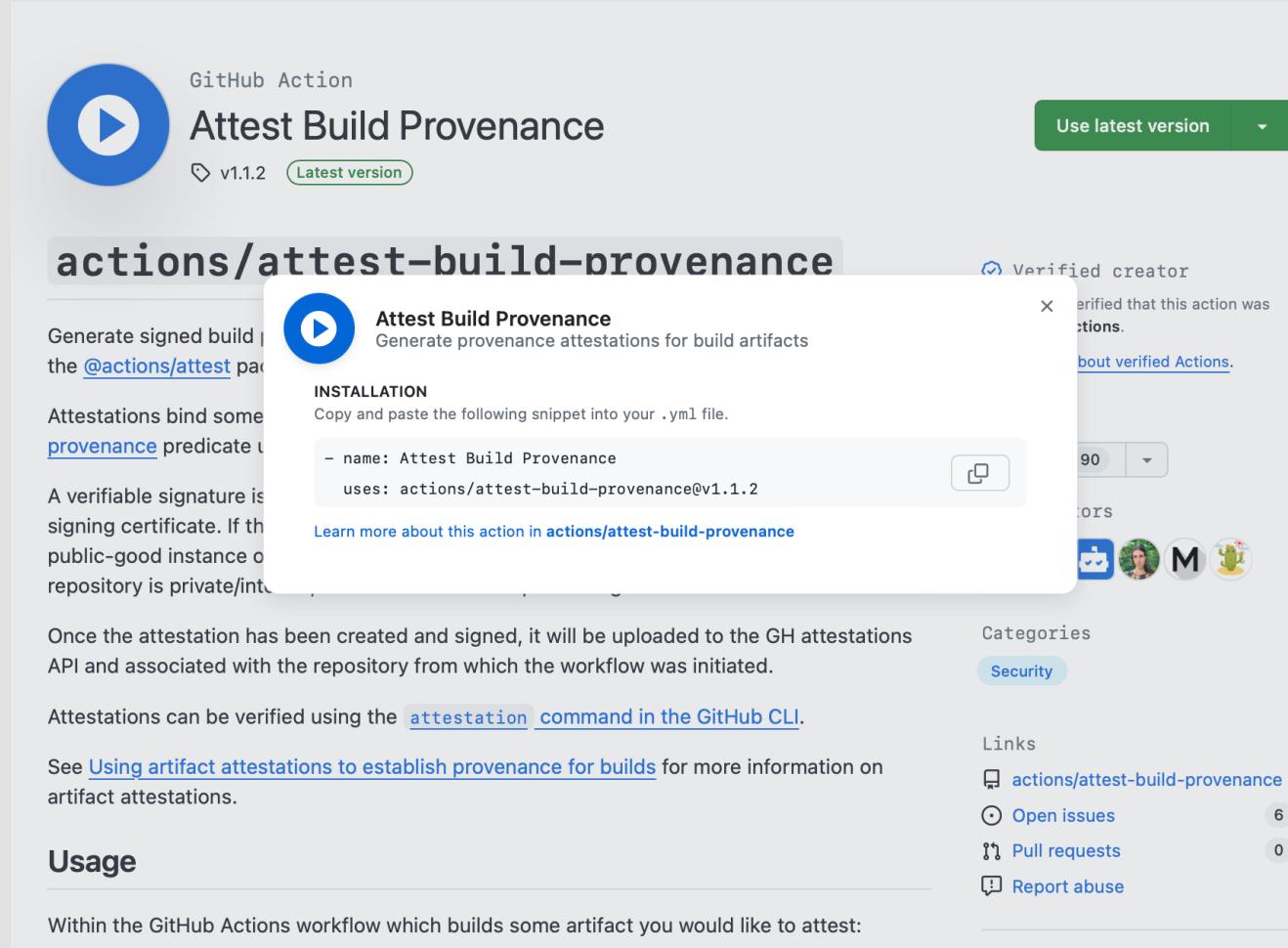
Hits-of-Code 54.7k

<https://hitsofcode.com>

codebeat A

<https://codebeat.co>

# Аттестация и provenance – завлечем пользователей



The screenshot shows the GitHub Action 'Attest Build Provenance' page. At the top, there's a blue play button icon, the action name, its version (v1.1.2), and a 'Latest version' button. A green button says 'Use latest version'. Below this, the repository name 'actions/attest-build-provenance' is shown. The main content area contains a brief description of the action, installation instructions (snippet for .yml file), and a 'Learn more about this action' link. It also includes a note about verifiable signatures and a warning about public-good instances. Further down, it discusses artifact attestations and provides usage examples. On the right side of the page, there's a sidebar with metrics: 90 stars, 3 contributors (one verified), and categories like Security. Below the sidebar are links to the repository, issues, pull requests, and abuse reporting.

GitHub Action

Attest Build Provenance

v1.1.2 Latest version

Use latest version

actions/attest-build-provenance

Attest Build Provenance

Generate provenance attestations for build artifacts

INSTALLATION

Copy and paste the following snippet into your .yml file.

```
- name: Attest Build Provenance
  uses: actions/attest-build-provenance@v1.1.2
```

Learn more about this action in [actions/attest-build-provenance](#)

Once the attestation has been created and signed, it will be uploaded to the GH attestations API and associated with the repository from which the workflow was initiated.

Attestations can be verified using the [attestation command in the GitHub CLI](#).

See [Using artifact attestations to establish provenance for builds](#) for more information on artifact attestations.

Usage

Within the GitHub Actions workflow which builds some artifact you would like to attest:

Verified creator

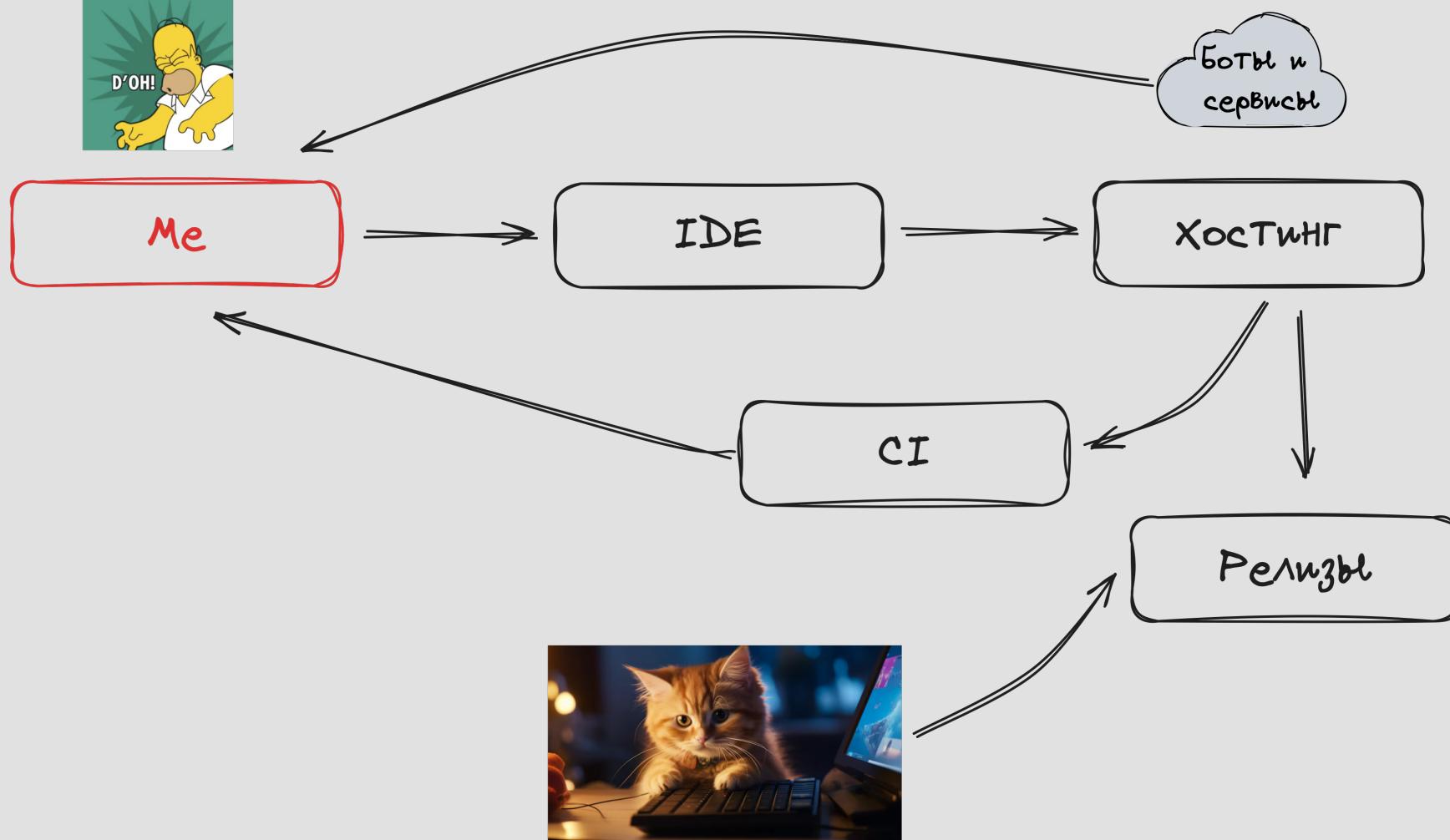
90 stars

3 contributors

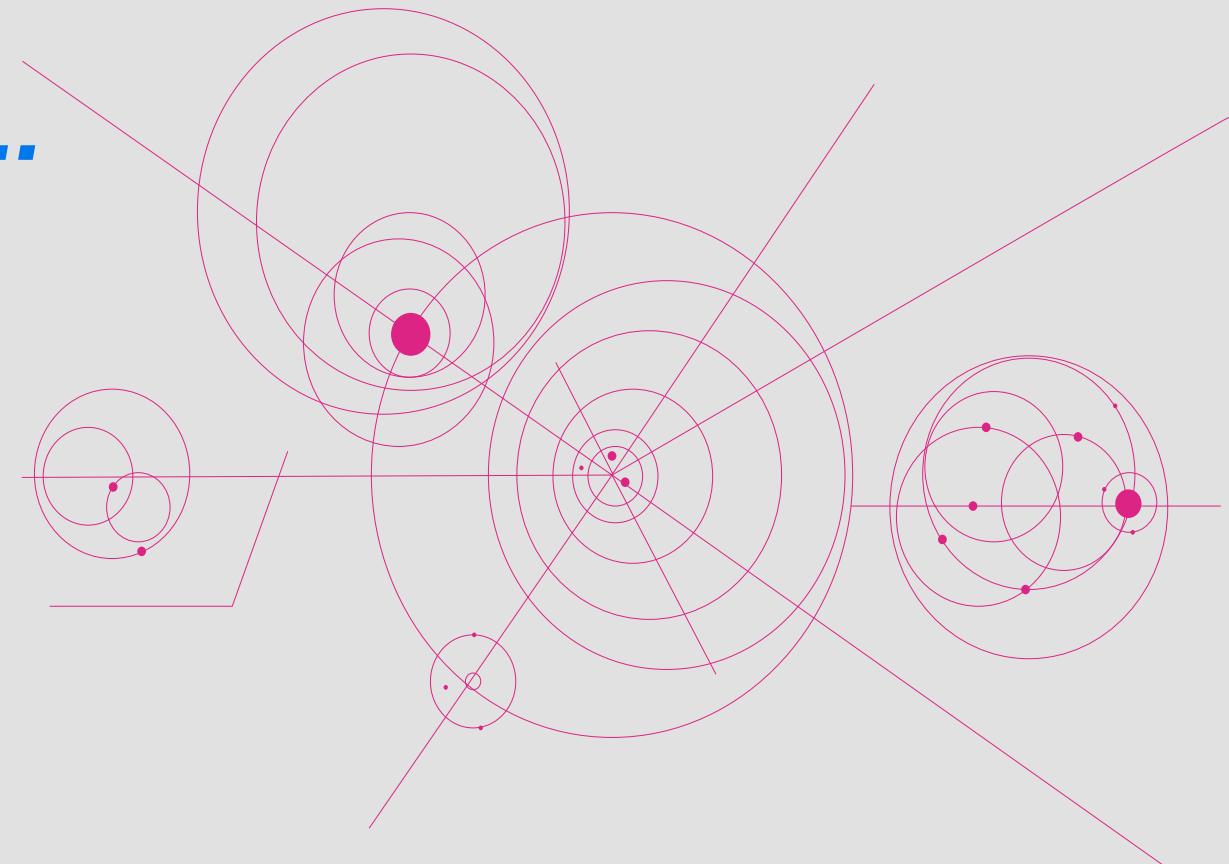
Categories: Security

Links:

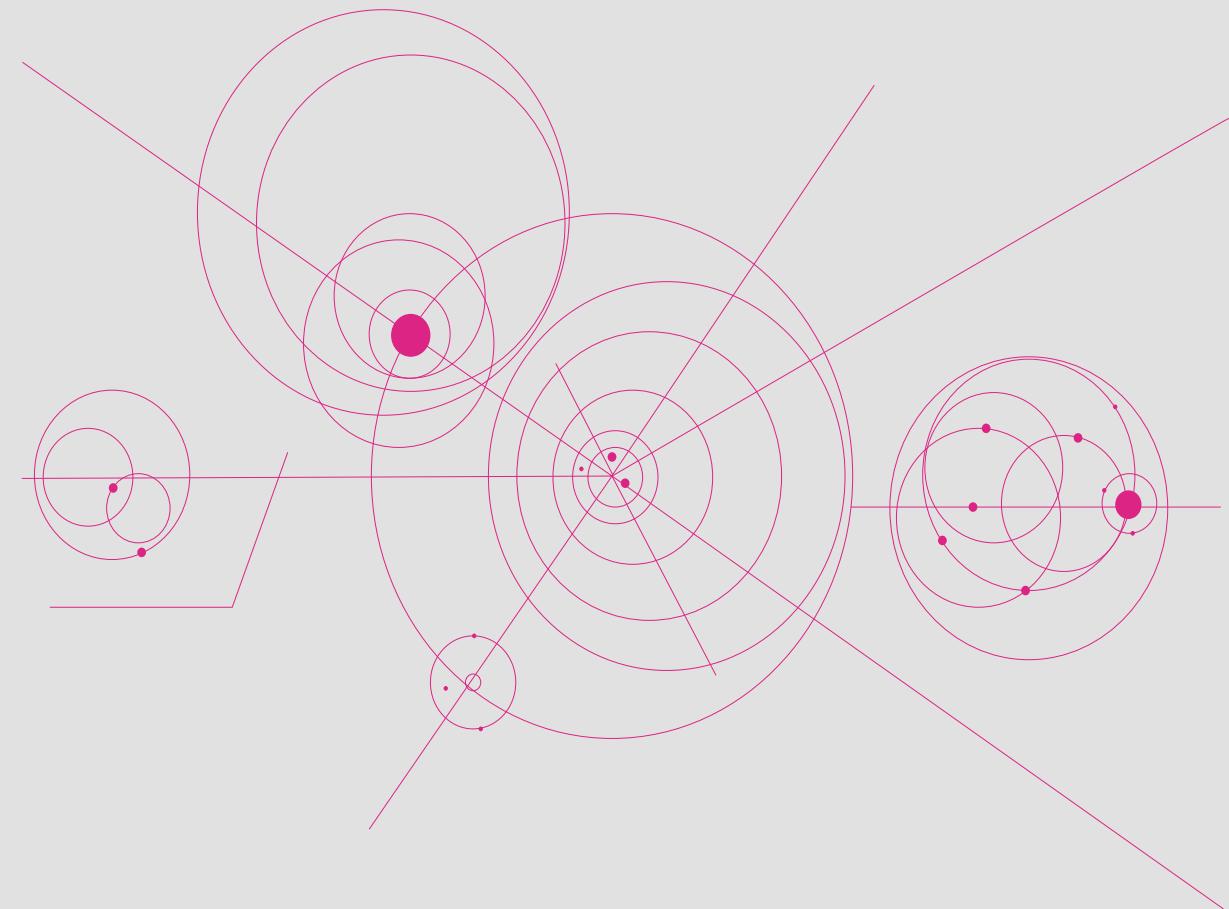
- actions/attest-build-provenance
- Open issues: 6
- Pull requests: 0
- Report abuse

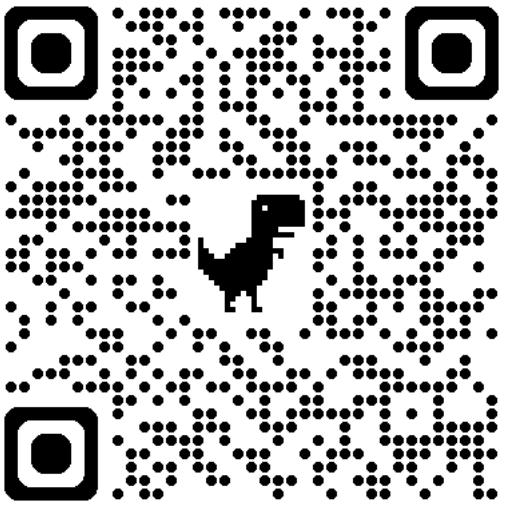


*И вот мы достучались до  
пользователя,  
а впереди еще больше  
плагинов и инструментов...*



И о них мы поговорим на  
следующем Positive Hack  
Days 😊





Подпишись!

Спасибо!

оставь обратную связь

