Безопасность проверенная временем

Будущее уже здесь: РБПО как “Новая линия разлома” безопасной разработки

Немного о боли

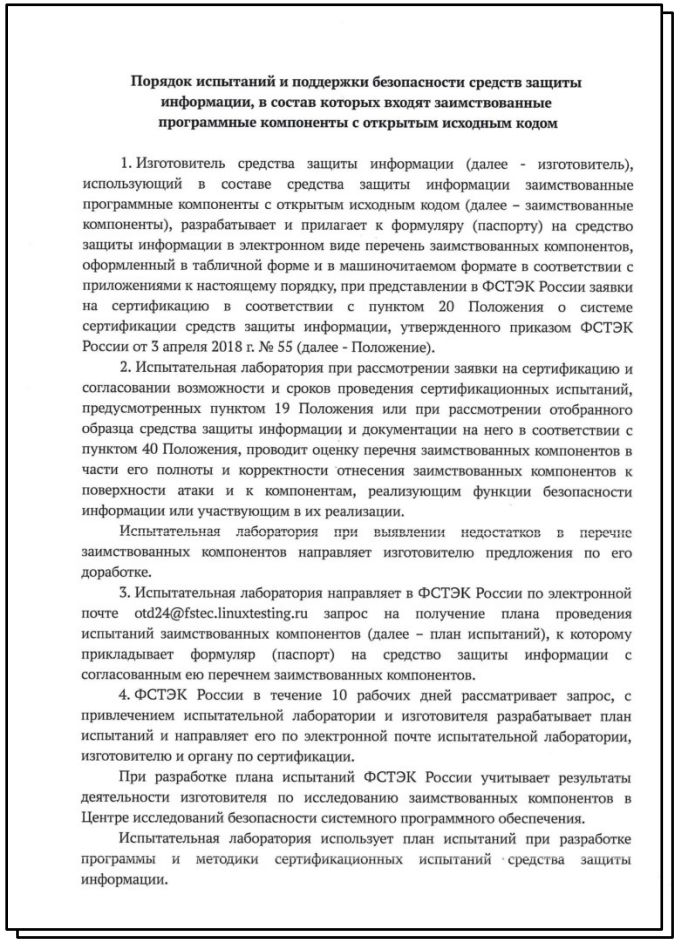
Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

О чем речь?

Информационное сообщение ФСТЭК России от 26 сентября 2024 г. N 240/24/4436

О порядке испытаний и поддержки безопасности средств защиты информации, в состав которых входят заимствованные программные компоненты с открытым исходным кодом



Порядок испытаний и поддержки безопасности средств защиты информации, в состав которых входят заимствованные программные компоненты с открытым исходным кодом

1. Изготовитель средства защиты информации (далее - изготовитель), использующий в составе средства защиты информации заимствованные программные компоненты с открытым исходным кодом (далее – заимствованные компоненты), разрабатывает и прилагает к формуляру (паспорту) на средство защиты информации в электронном виде перечень заимствованных компонентов, оформленный в табличной форме и в машиночитаемом формате в соответствии с приложениями к настоящему порядку, при представлении в ФСТЭК России заявки на сертификацию в соответствии с пунктом 20 Положения о системе сертификации средств защиты информации, утвержденного приказом ФСТЭК России от 3 апреля 2018 г. № 55 (далее - Положение).

2. Испытательная лаборатория при рассмотрении заявки на сертификацию и согласовании возможности и сроков проведения сертификационных испытаний, предусмотренных пунктом 19 Положения или при рассмотрении отобранного образца средства защиты информации и документации на него в соответствии с пунктом 40 Положения, проводит оценку перечня заимствованных компонентов в части его полноты и корректности отнесения заимствованных компонентов к поверхности атаки и к компонентам, реализующим функции безопасности информации или участвующим в их реализации.

Испытательная лаборатория при выявлении недостатков в перечне заимствованных компонентов направляет изготовителю предложения по его доработке.

3. Испытательная лаборатория направляет в ФСТЭК России по электронной почте otd24@fstec.linuxtesting.ru запрос на получение плана проведения испытаний заимствованных компонентов (далее – план испытаний), к которому прикладывает формуляр (паспорт) на средство защиты информации с согласованным ею перечнем заимствованных компонентов.

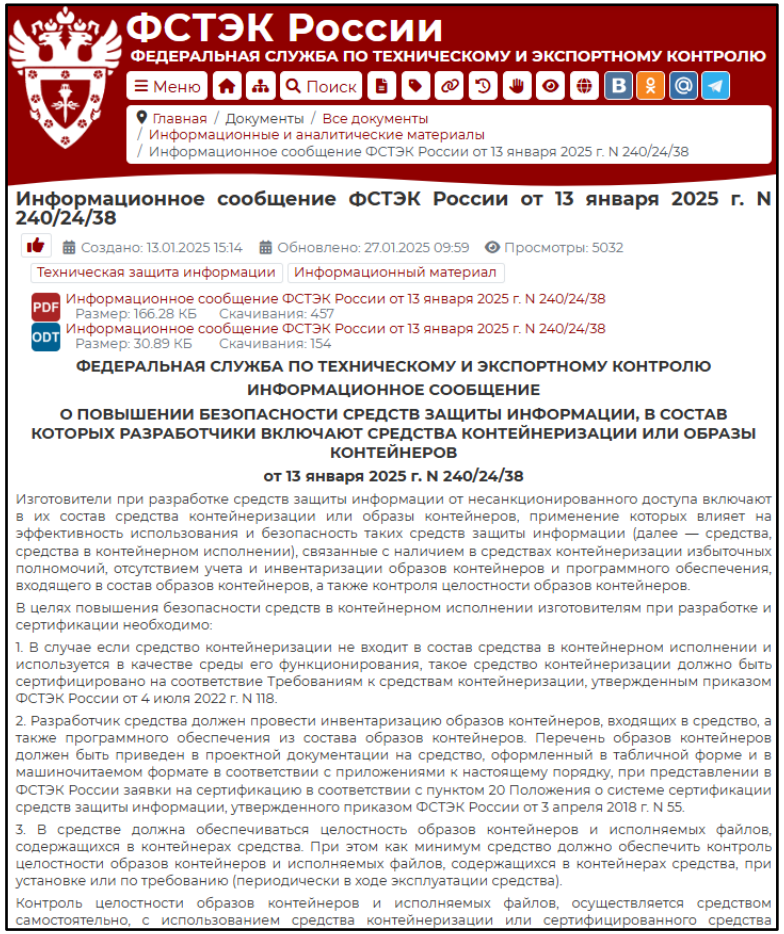
4. ФСТЭК России в течение 10 рабочих дней рассматривает запрос, с привлечением испытательной лаборатории и изготовителя разрабатывает план испытаний и направляет его по электронной почте испытательной лаборатории, изготовителю и органу по сертификации.

При разработке плана испытаний ФСТЭК России учитывает результаты деятельности изготовителя по исследованию заимствованных компонентов в Центре исследований безопасности системного программного обеспечения.

Испытательная лаборатория использует план испытаний при разработке программы и методики сертификационных испытаний средства защиты информации.

Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38

О повышении безопасности средств защиты информации, в состав которых разработчики включают средства контейнеризации или образы контейнеров



ФСТЭК России

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Меню Поиск

Главная / Документы / Все документы / Информационные и аналитические материалы / Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38

Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38

Создано: 13.01.2025 15:14 Обновлено: 27.01.2025 09:59 Просмотры: 5032

Техническая защита информации | Информационный материал

PDF Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38
Размер: 166.28 КБ Скачивания: 457

ODT Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38
Размер: 30.89 КБ Скачивания: 154

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

О ПОВЫШЕНИИ БЕЗОПАСНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, В СОСТАВ КОТОРЫХ РАЗРАБОТЧИКИ ВКЛЮЧАЮТ СРЕДСТВА КОНТЕЙНЕРИЗАЦИИ ИЛИ ОБРАЗЫ КОНТЕЙНЕРОВ

от 13 января 2025 г. N 240/24/38

Изготовители при разработке средств защиты информации от несанкционированного доступа включают в их состав средства контейнеризации или образы контейнеров, применение которых влияет на эффективность использования и безопасность таких средств защиты информации (далее — средства, средства в контейнерном исполнении), связанные с наличием в средствах контейнеризации избыточных полномочий, отсутствием учета и инвентаризации образов контейнеров и программного обеспечения, входящего в состав образов контейнеров, а также контроля целостности образов контейнеров.

В целях повышения безопасности средств в контейнерном исполнении изготовителям при разработке и сертификации необходимо:

1. В случае если средство контейнеризации не входит в состав средства в контейнерном исполнении и используется в качестве среды его функционирования, такое средство контейнеризации должно быть сертифицировано на соответствие Требованиям к средствам контейнеризации, утвержденным приказом ФСТЭК России от 4 июля 2022 г. N 118.

2. Разработчик средства должен провести инвентаризацию образов контейнеров, входящих в средство, а также программного обеспечения из состава образов контейнеров. Перечень образов контейнеров должен быть приведен в проектной документации на средство, оформленный в табличной форме и в машиночитаемом формате в соответствии с приложениями к настоящему порядку, при представлении в ФСТЭК России заявки на сертификацию в соответствии с пунктом 20 Положения о системе сертификации средств защиты информации, утвержденного приказом ФСТЭК России от 3 апреля 2018 г. N 55.

3. В средстве должна обеспечиваться целостность образов контейнеров и исполняемых файлов, содержащихся в контейнерах средства. При этом как минимум средство должно обеспечить контроль целостности образов контейнеров и исполняемых файлов, содержащихся в контейнерах средства, при установке или по требованию (периодически в ходе эксплуатации средства).

Контроль целостности образов контейнеров и исполняемых файлов, осуществляется средством самостоятельно, с использованием средства контейнеризации или сертифицированного средства

[Ссылка на ИС ФСТЭК России № 240/24/38]

О чем речь?

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Информационное сообщение ФСТЭК России от 26 сентября 2024 г. N 240/24/4436

```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "version": 1,
  "metadata": {
    "timestamp": "2025-04-25T00:00:00",
    "component": {
      "type": "application",
      "name": "ТБФорум",
      "version": "2026",
      "manufacturer": {
        "name": "ТБФорум"
      }
    }
  },
  "components": [
    {
      "type": "library",
      "name": "nginx",
      "version": "1.24.4",
      "exernalReferences":
        [{"type": "vcs", "url": "https://github.com/nginx/nginx.git"}],
      "properties": [
        { "name": "GOST:attack_surface", "value": "yes" },
        { "name": "GOST:secutity_function", "value": "yes" }
      ]
    }
  ]
}
```

Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38

```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "version": 1,
  "metadata": {
    "timestamp": "2025-04-25T00:00:00",
    "component": {
      "type": "application",
      "name": "ТБФорум",
      "version": "2026",
      "manufacturer": {
        "name": "ТБФорум"
      }
    }
  },
  "components": [
    {
      "type": "container",
      "name": "nginx-container",
      "version": "1.0",
      "properties": [
        { "name": "GOST:attack_surface", "value": "yes" },
        { "name": "GOST:secutity_function", "value": "yes" }
      ],
      "components": [
        {
          "type": "library",
          "name": "nginx",
          "version": "1.24.4",
          "properties": [
            { "name": "GOST:attack_surface", "value": "yes" },
            { "name": "GOST:secutity_function", "value": "yes" }
          ]
        }
      ]
```

О чем речь?

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Информ::Доверенная Разработка
Методическая рекомендация № 2025-09-012 | Рекомендация

Алгоритм представления перечня заимствованных программных компонентов с открытым исходным кодом (далее - SBOM).

Описание: В соответствии с требованиями информационного письма № 240/24/4436 от 26.09.2024 изготовители средств защиты информации (далее - СЗИ), испытательные лаборатории и органы по сертификации при проведении сертификации СЗИ, включающих в свой состав заимствованные программные компоненты с открытым исходным кодом (далее - заимствованные компоненты), должны проводить сертификационные испытания СЗИ и осуществлять их поддержку безопасности в соответствии с Порядком испытаний и поддержки безопасности СЗИ, в состав которых входят заимствованные компоненты.

На практике значительная часть представленных SBOM возвращается на доработку по причине ошибок, несоответствий или недостатка информации.

Целью данной методической рекомендации является представление алгоритма подготовки SBOM, направленного на минимизацию ошибок.

1. Для проверки SBOM рекомендуется использовать скрипт sbom-checker.py **с включенными опциями:**
`-e ERRORS`, `--errors ERRORS` — максимальное число ошибок для вывода; по умолчанию - **10**; для вывода всех ошибок - **0**.
`--check-vcs` — проверка **url** типа **vcs** на git/svn/hg/fossil-репозиторий (требуется доступ к Интернет и наличие пакетов *git*, *subversion* и *mercurial*).
`--check-source-distribution` — проверка **url** типа **source-distribution**.

- Ошибки типа **ERROR** обязательны к исправлению;

- Большинство ошибок типа **WARNING** являются обязательными к исправлению, но при проверке ссылок могут быть ложные срабатывания. (см. п. 4.1).

2. В соответствии с требованиями к полям объекта, описывающего информацию о продукте (Табл. 3 информационного письма) необходимо:

[Ссылка на методические рекомендации по формированию SBoM]

Ресурсы Центра компетенций ФСТЭК России и ИСП РАН

ALL CHARACTERS AND
EVENTS IN THIS SHOW--
EVEN THOSE BASED ON REAL
PEOPLE--ARE ENTIRELY FICTIONAL.
ALL CELEBRITY VOICES ARE
IMPERSONATED.....POORLY. THE
FOLLOWING PROGRAM CONTAINS
COARSE LANGUAGE AND DUE TO
ITS CONTENT IT SHOULD NOT BE
VIEWED BY ANYONE■

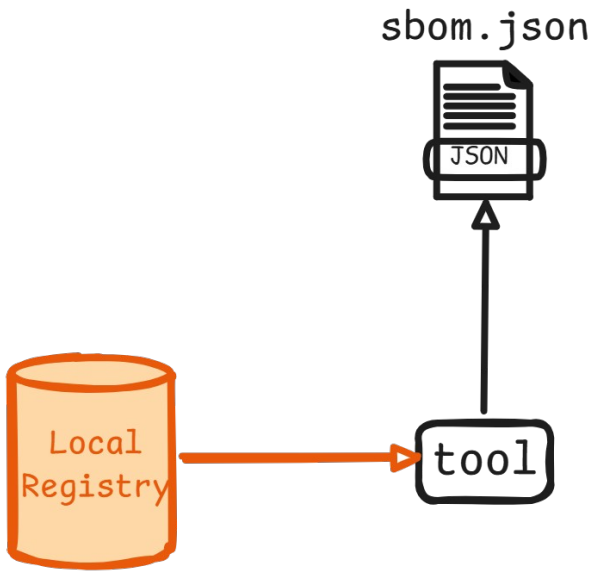
Боли глазами лаборатории. Deepseek

Ожидание

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

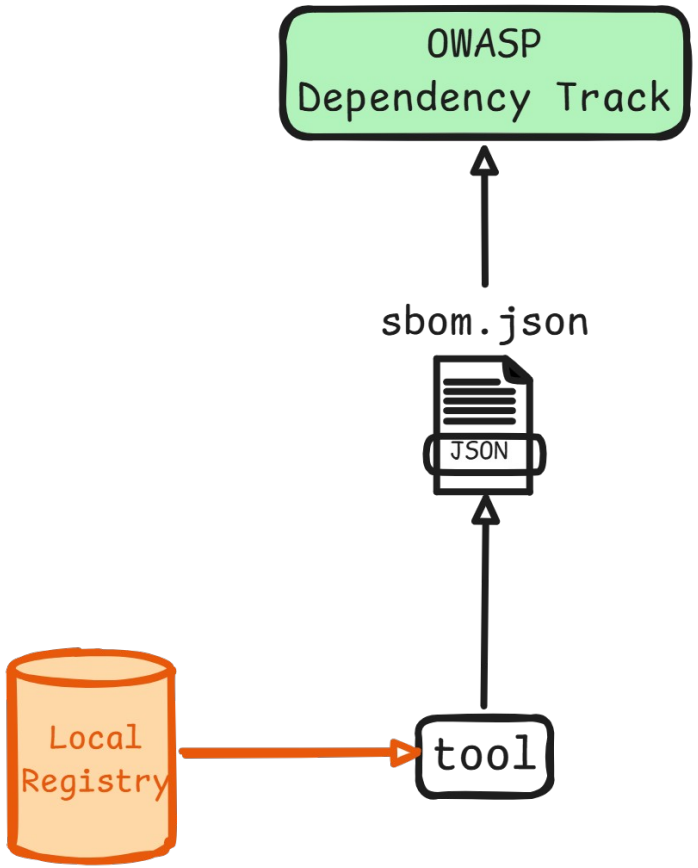
Боли глазами лаборатории. Deepseek

Ожидание



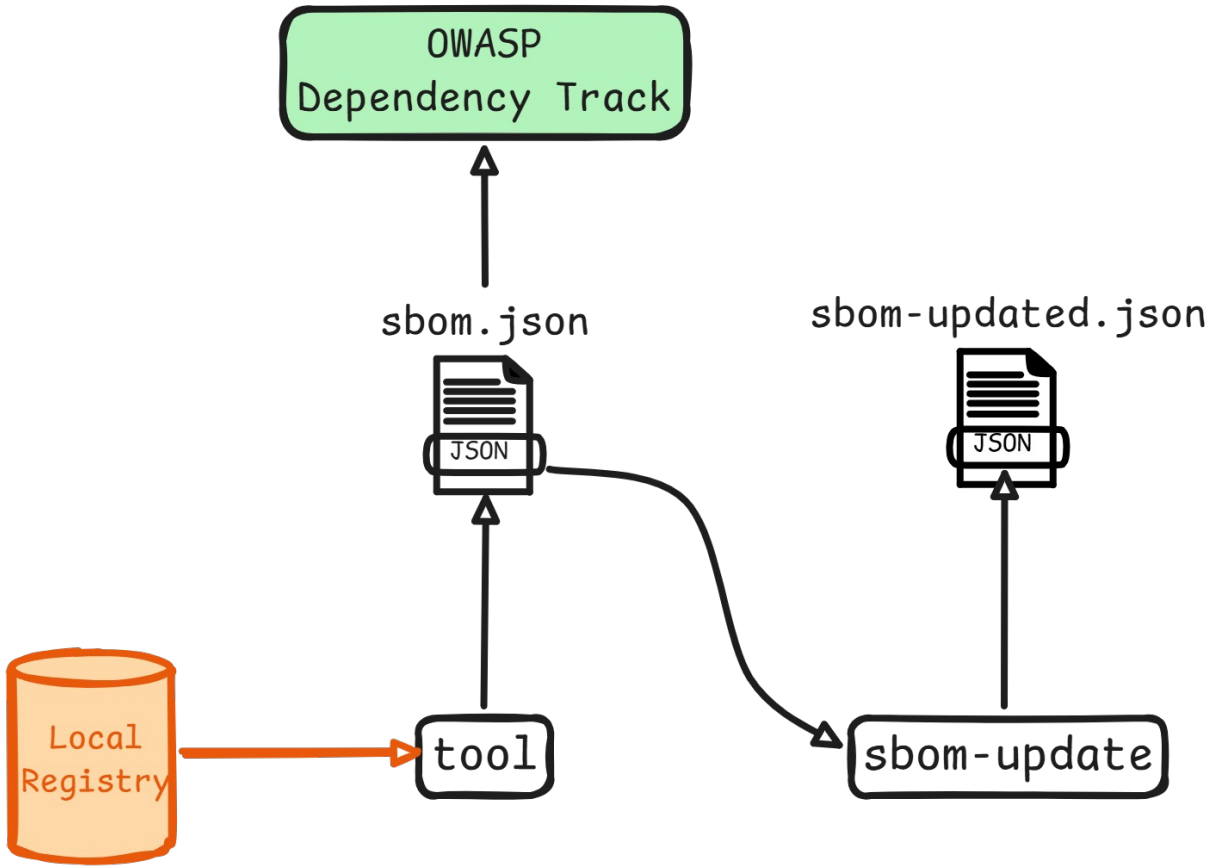
Боли глазами лаборатории. Deepseek

Ожидание



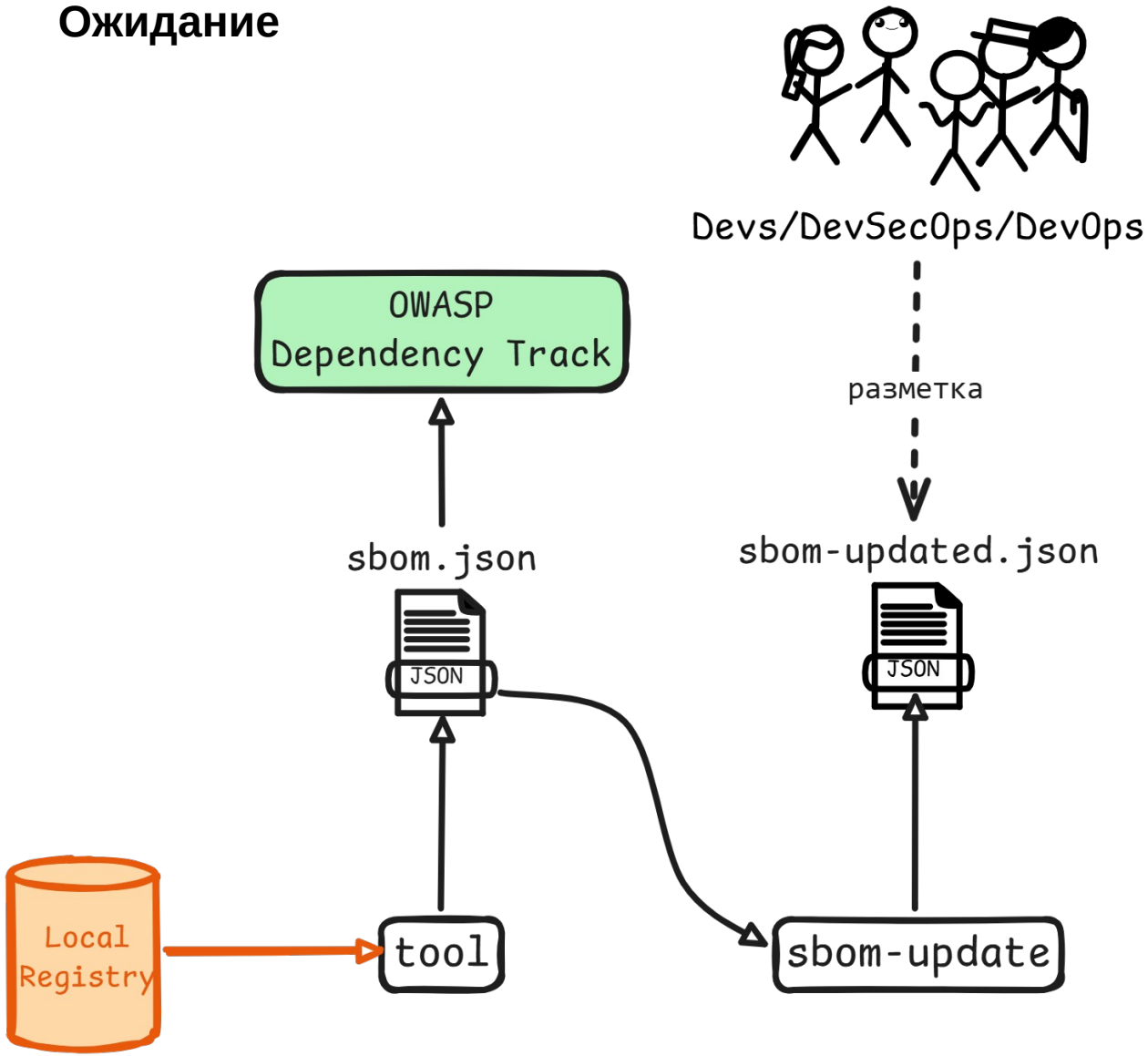
Боли глазами лаборатории. Deepseek

Ожидание



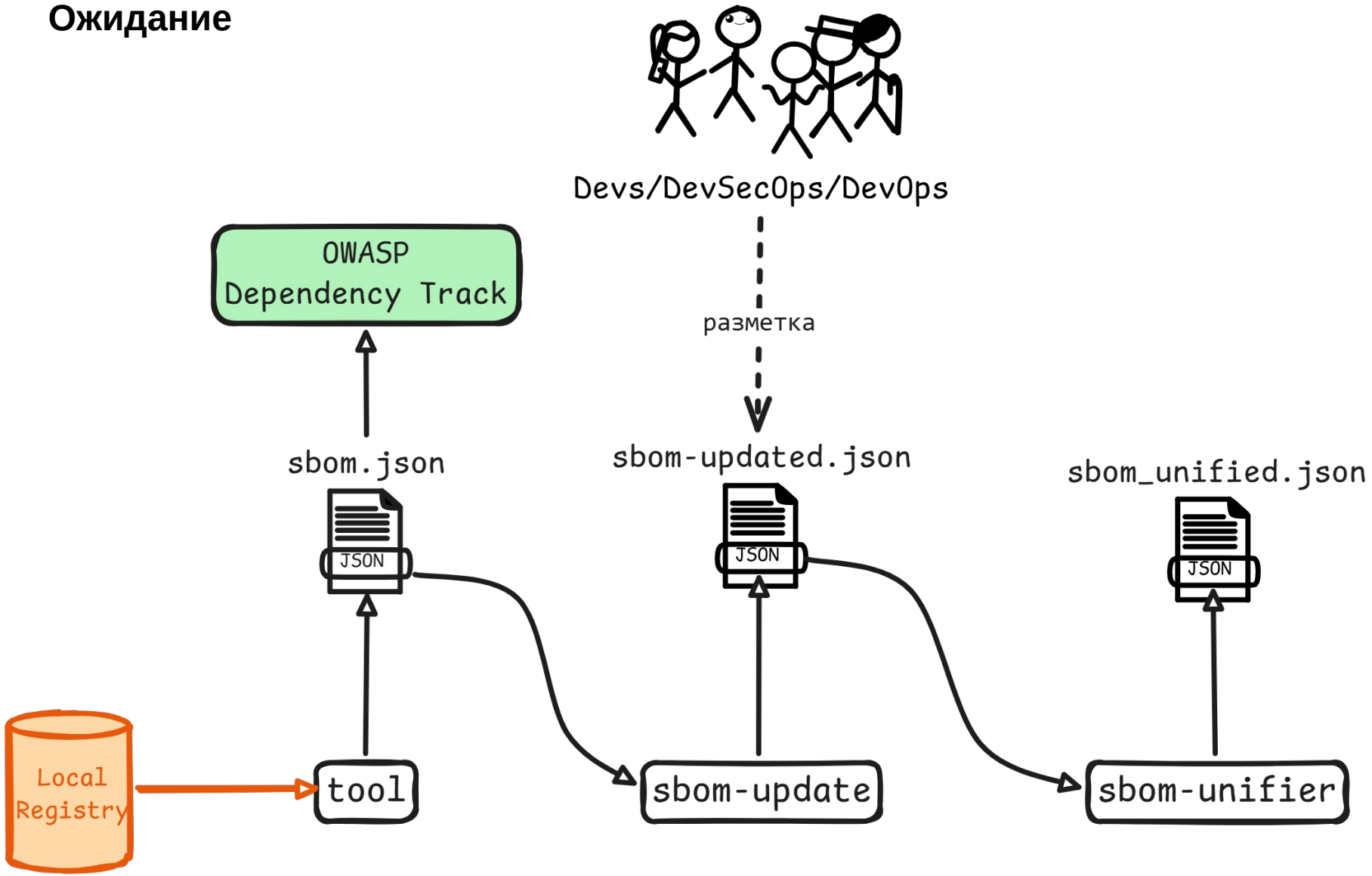
Боли глазами лаборатории. Deepseek

Ожидание



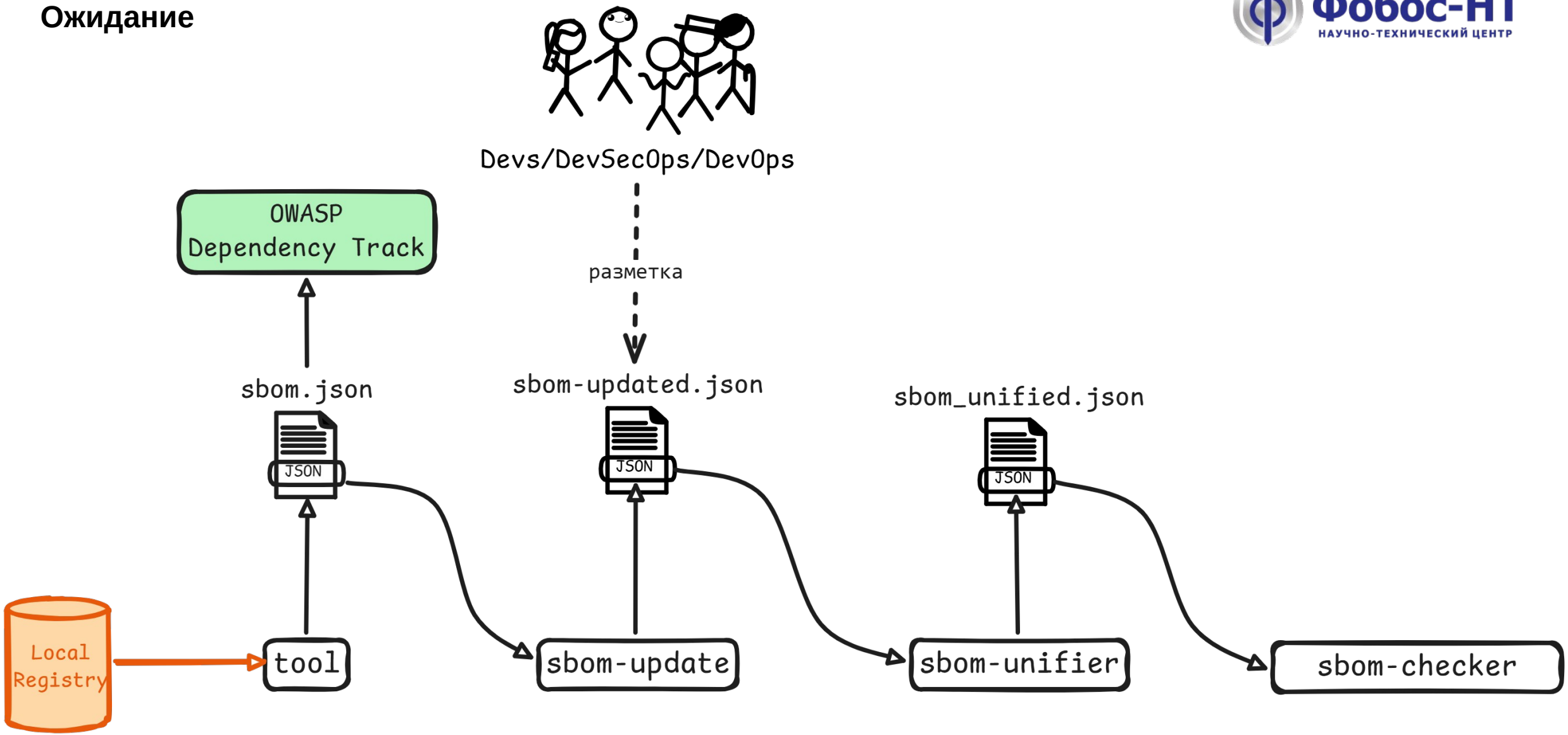
Боли глазами лаборатории. Deepseek

Ожидание



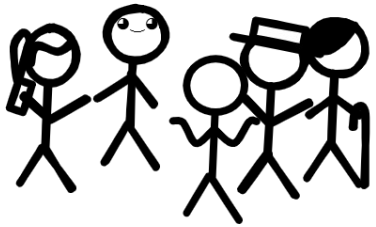
Боли глазами лаборатории. Deepseek

Ожидание



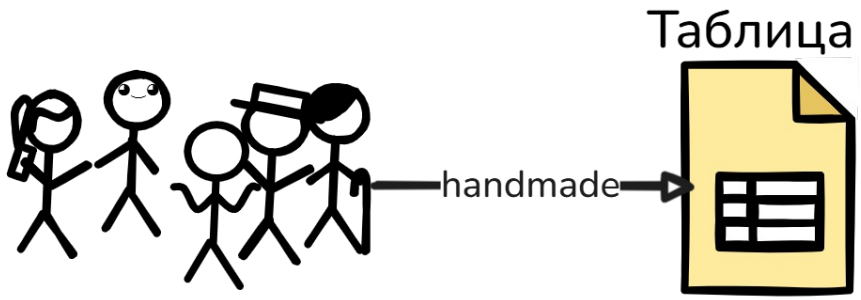
Боли глазами лаборатории. Deepseek

Реальность



Боли глазами лаборатории. Deepseek

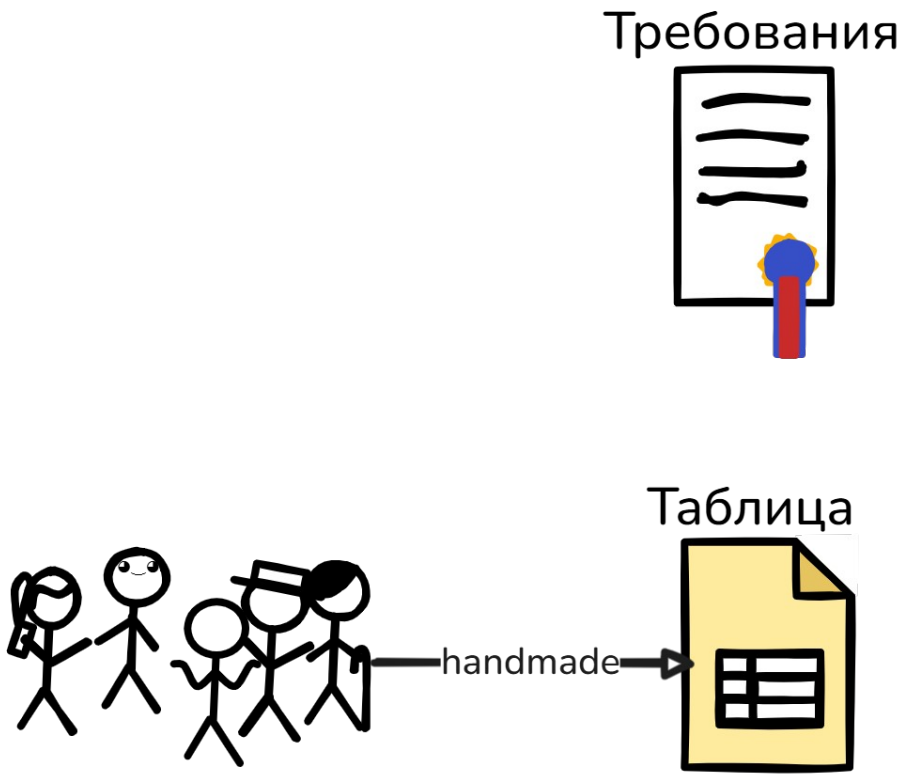
Реальность



Боли глазами лаборатории. Deepseek

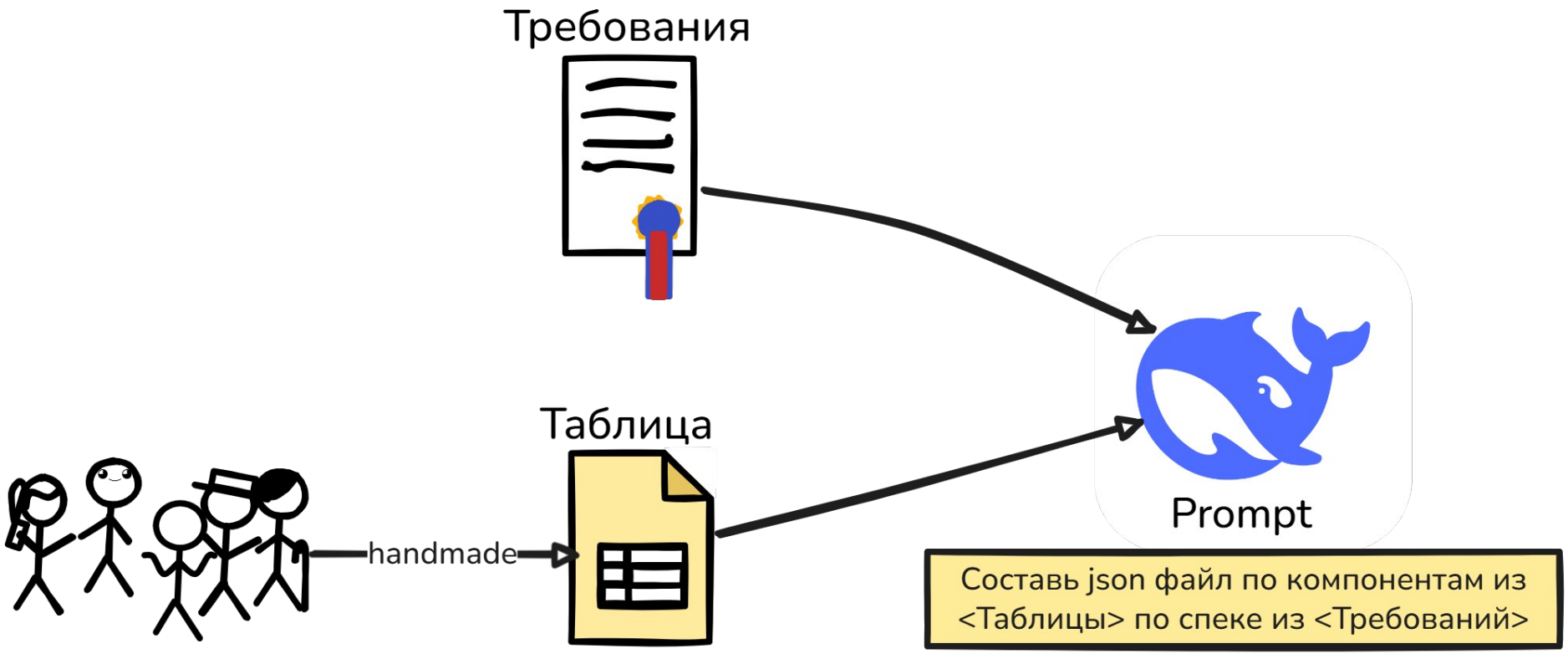
Реальность

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР



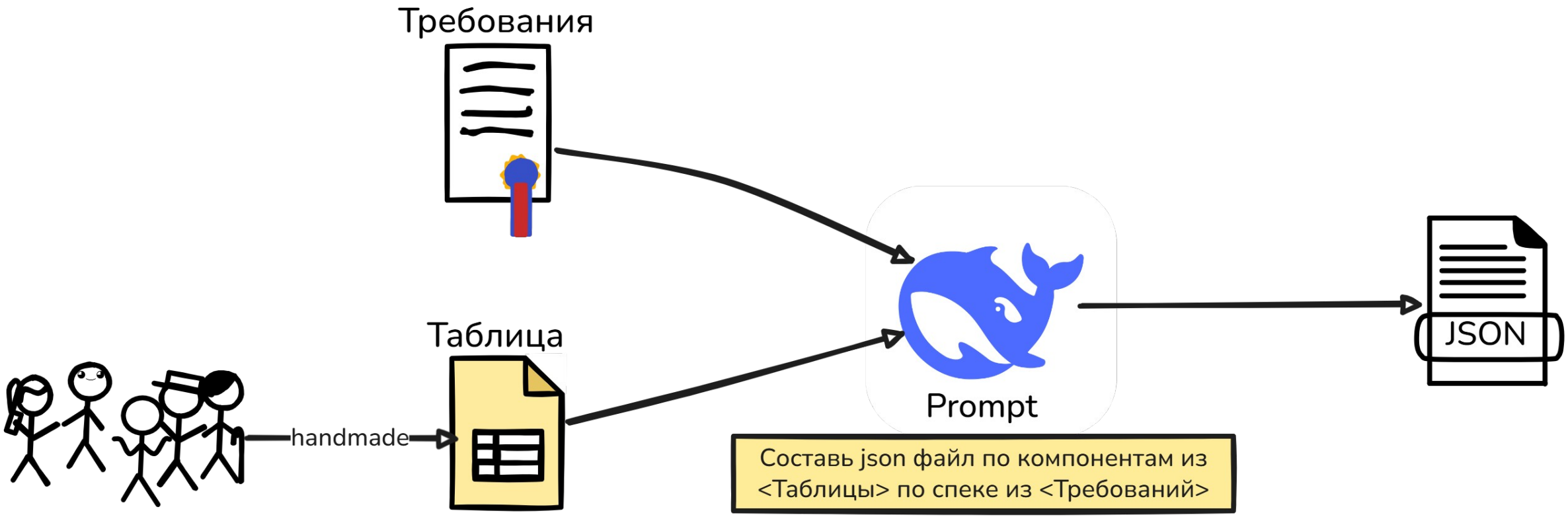
Боли глазами лаборатории. Deepseek

Реальность



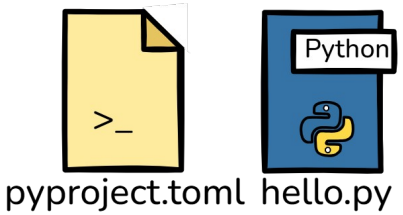
Боли глазами лаборатории. Deepseek

Реальность

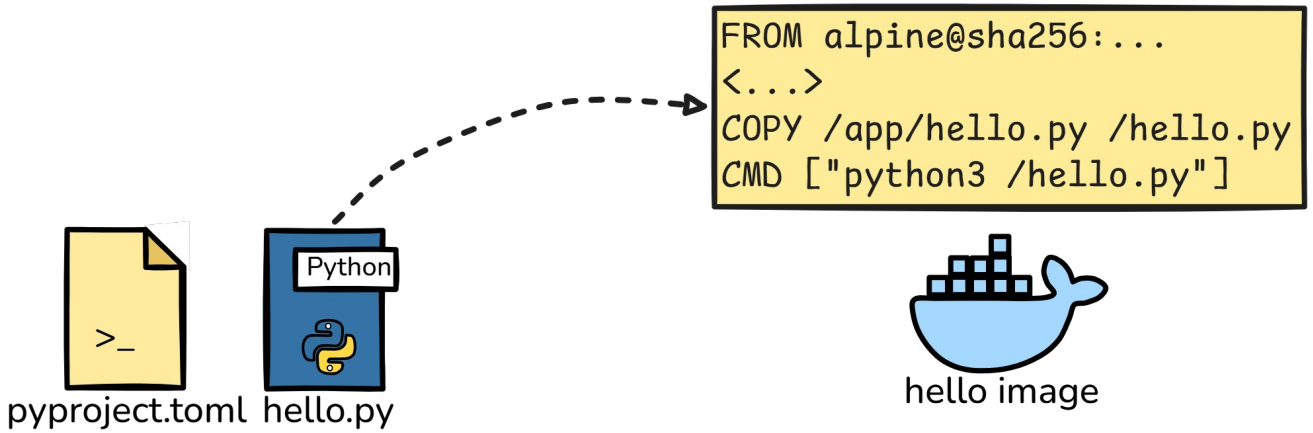


Боли глазами лаборатории и заявителей. Содержание СБоМов

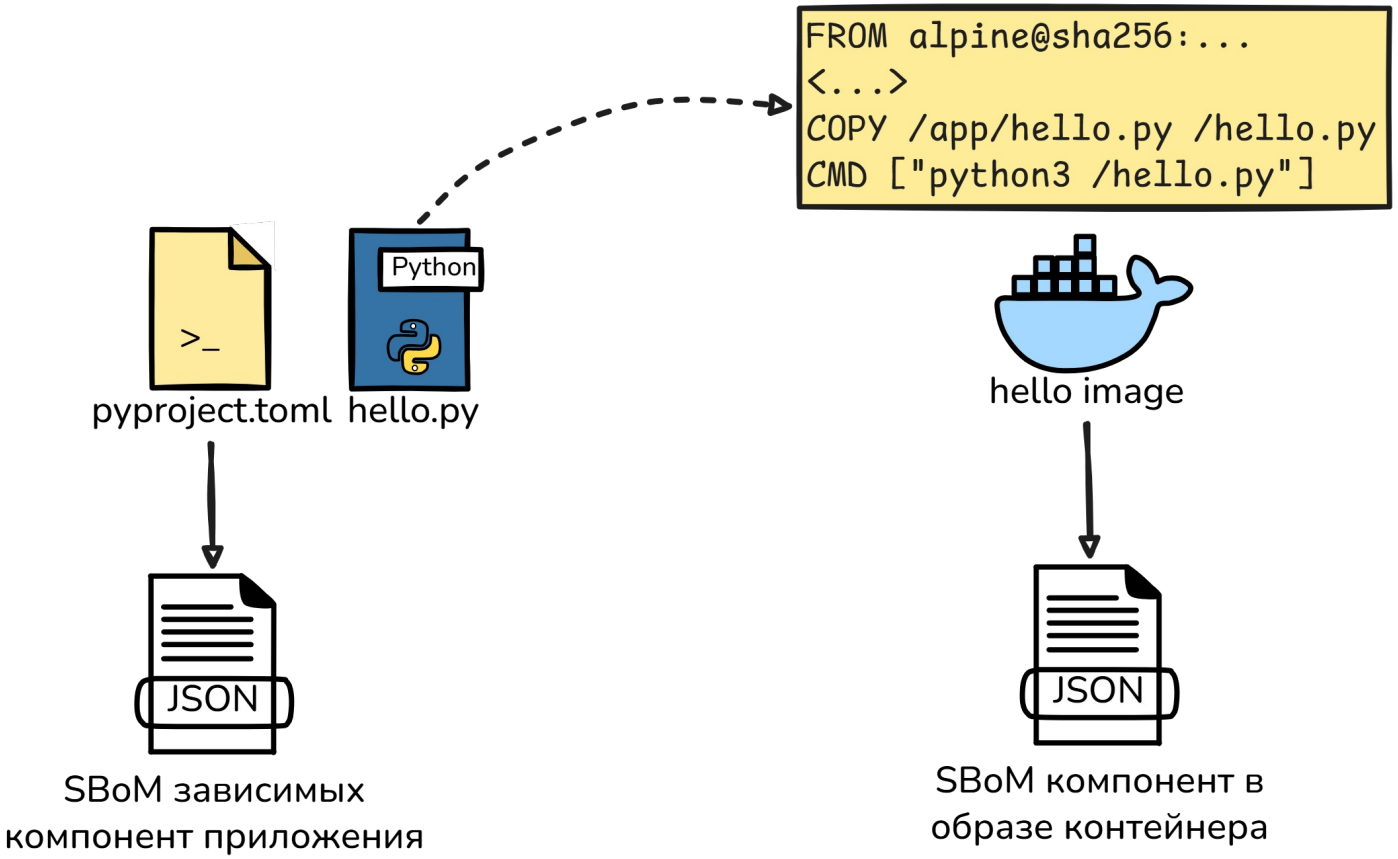
Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР



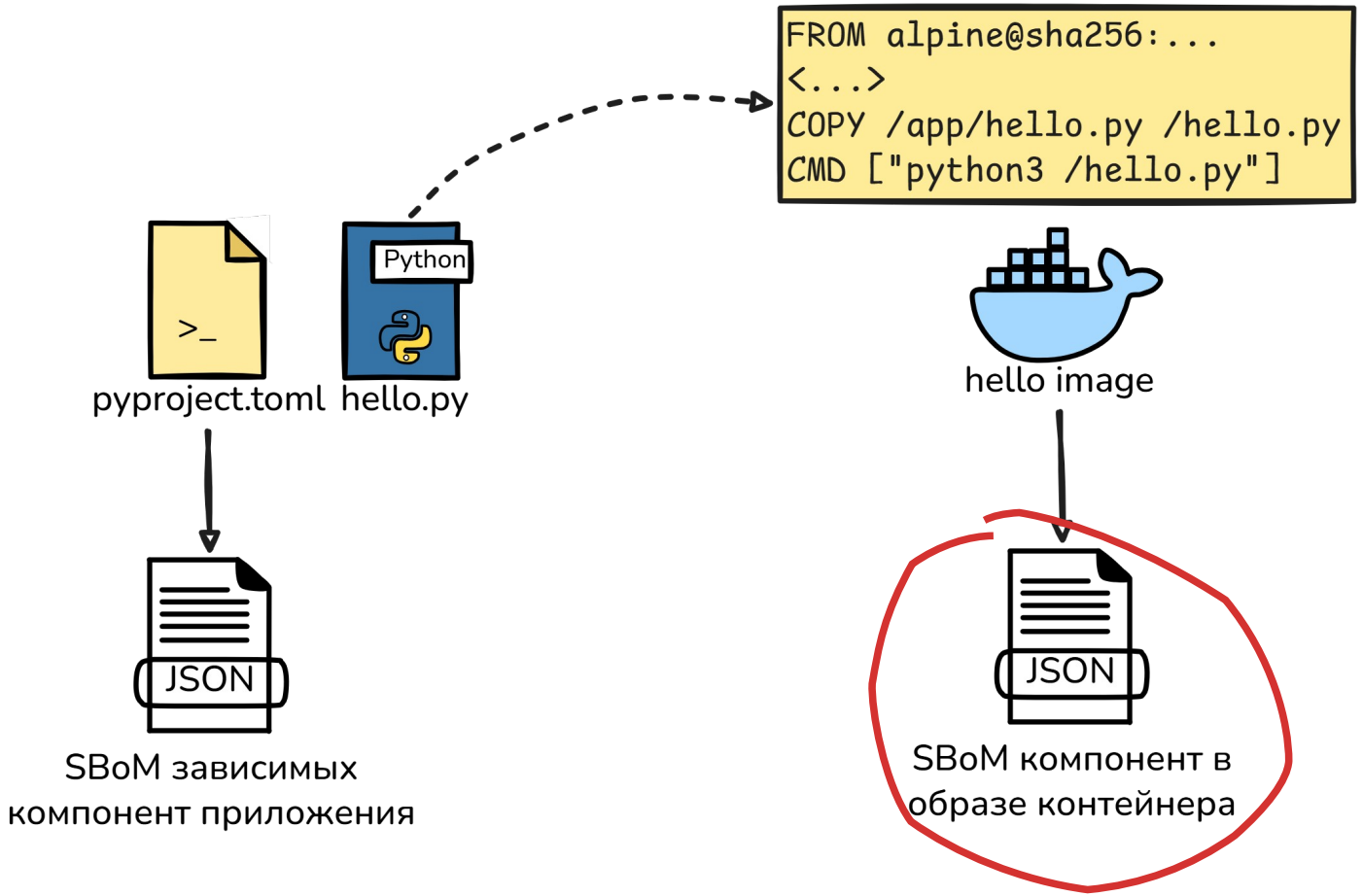
Боли глазами лаборатории и заявителей. Содержание СБоМов



Боли глазами лаборатории и заявителей. Содержание СБоМов



Боли глазами лаборатории и заявителей. Содержание СБоМов



Боли глазами лаборатории и заявителей. Содержание СБоМов

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

alpine:3.23.3 MULTI-PLATFORM

OPERATING SYSTEMS

INDEX DIGEST sha256:25109184c71bdad752c8312a8623239686a9a2071e8825f20acb8f2198c3f659

OS/ARCH

linux/386

COMPRESSED SIZE	LAST PUSHED	TYPE	VULNERABILITIES	MANIFEST DIGEST
3.52 MB	16 days by doijanky	Image	0 0 1 0 0	sha256:a76a5883...

Layers (2)

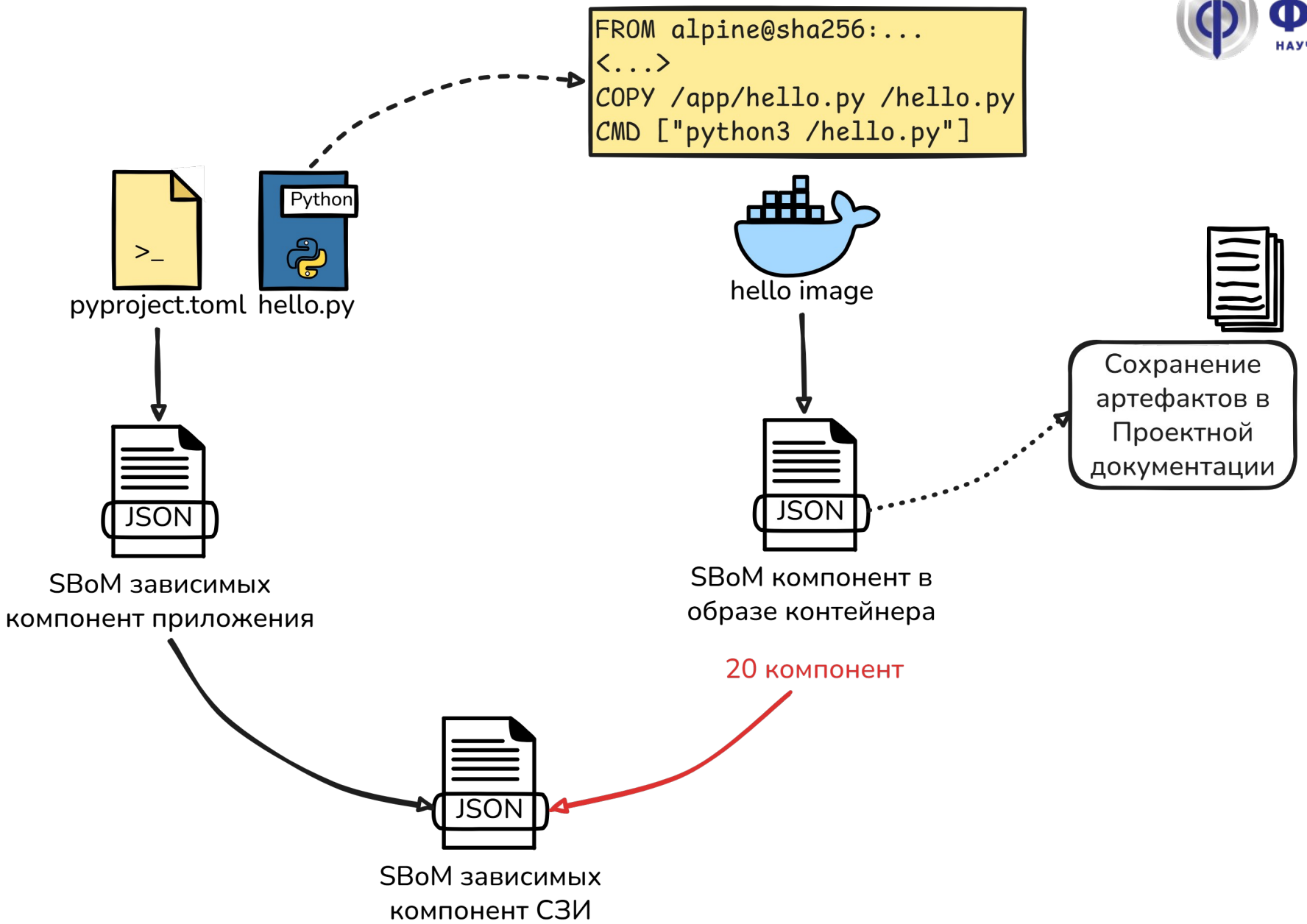
alpine:3.23.3	0 0 1 0 0		
0	ADD alpine-minirootfs-3.23.3-x86.tar.gz / # buildkit	3.69 MB	
1	CMD ["/bin/sh"]	0 B	

Vulnerabilities (1) Packages (20) Give fe

Package or CVE name Vulnerable Show excepted

Package Name	Present in
apk / alpine/busybox / 1.37.0-r30	
apk / alpine/apk-tools / 3.0.3-r1	
apk / alpine/libcrypto3 / 3.5.5-r0	

Боли глазами лаборатории и заявителей. Содержание СБоМов



Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

4000

Боли глазами лаборатории. Нереалистичное распределение

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

10

Боли глазами лаборатории. Нереалистичное распределение

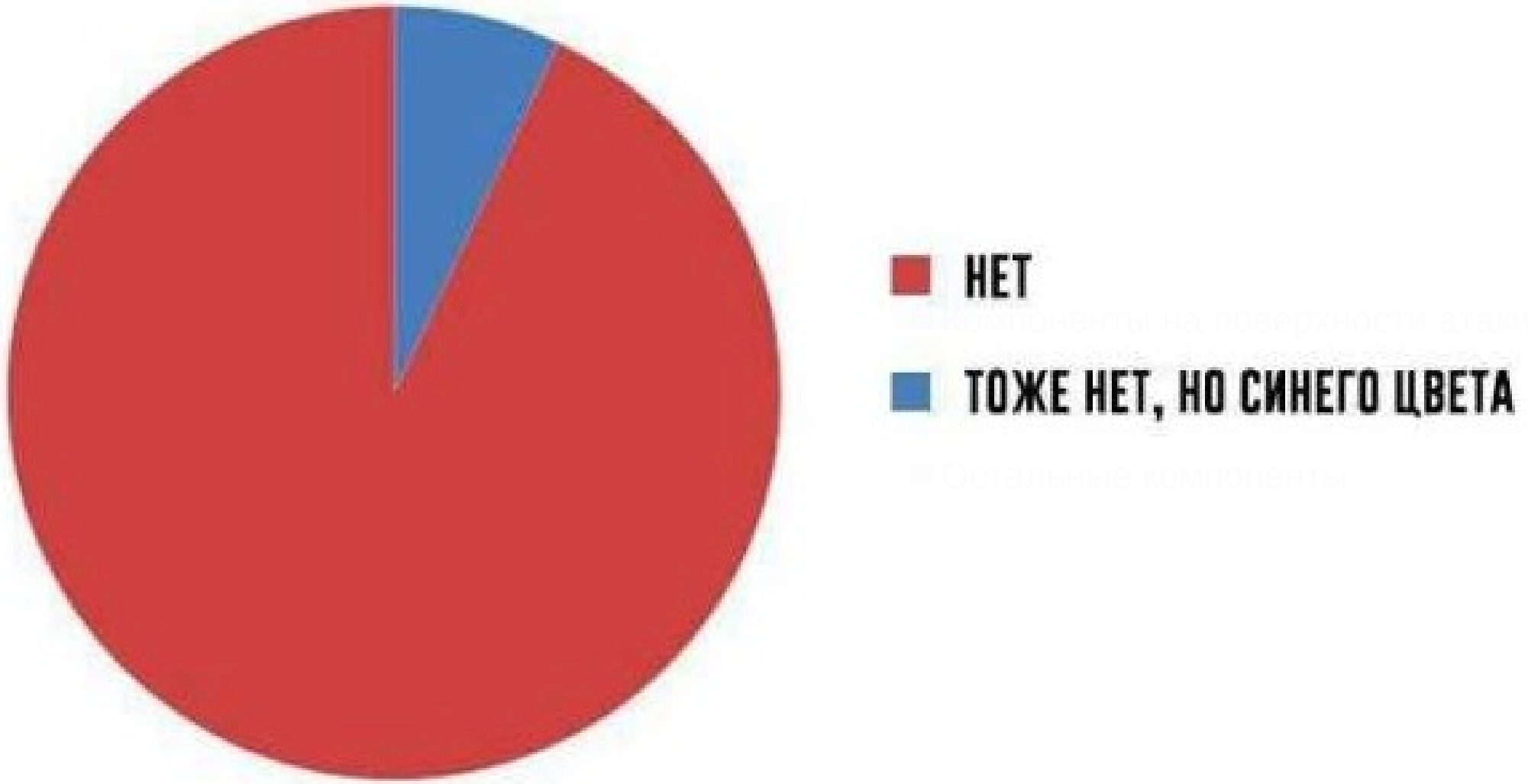
Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

2

Боли глазами лаборатории. Нереалистичное распределение

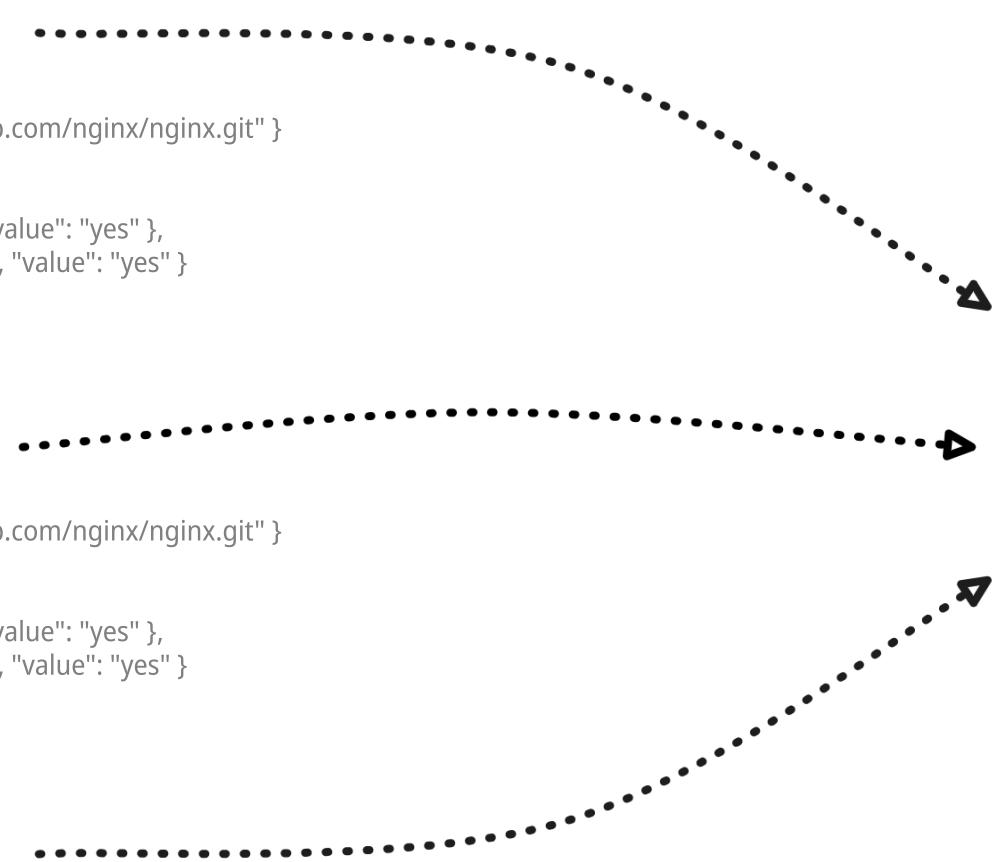
Боли глазами лаборатории. Нереалистичное распределение

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР



Боли глазами лаборатории. Дубликаты


```
"components": [
  {
    "type": "library",
    "name": "nginx",
    "version": "1.21.0",
    "exernalReferences": [
      { "type": "vcs", "url": "https://github.com/nginx/nginx.git" }
    ],
    "properties": [
      { "name": "GOST:attack_surface", "value": "yes" },
      { "name": "GOST:secutity_function", "value": "yes" }
    ]
  },
  {
    "type": "library",
    "name": "nginx",
    "version": "1.24.4",
    "exernalReferences": [
      { "type": "vcs", "url": "https://github.com/nginx/nginx.git" }
    ],
    "properties": [
      { "name": "GOST:attack_surface", "value": "yes" },
      { "name": "GOST:secutity_function", "value": "yes" }
    ]
  },
  {
    "type": "library",
    "name": "nginx",
    "version": "1.18.2",
    "exernalReferences": [
      { "type": "vcs", "url": "https://github.com/nginx/nginx.git" }
    ],
    "properties": [
      { "name": "GOST:attack_surface", "value": "yes" },
      { "name": "GOST:secutity_function", "value": "yes" }
    ]
  }
]
```

Необходимо будет исследовать все версии компоненты:
отслеживание уязвимостей
статический анализ
динамический анализ

Боли глазами лаборатории. dev- и test-инструменты

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР


```
"name": "coverage",
"purl": "pkg:pypi/coverage@7.10.6",
"type": "library",
"scope": "required",
"authors": [
  {
    "name": "Ned Batchelder and 243 others",
    "email": "ned@nedbatchelder.com"
  }
],
"bom-ref": "pkg:pypi/coverage@7.10.6_1",
"version": "7.10.6",
```

Боли глазами лаборатории. dev- и test-инструменты

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР


```
"name": "coverage",
"purl": "pkg:pypi/coverage@7.1
"type": "library",
"scope": "required",
"authors": [
  {
    "name": "Ned Batchelder ar
    "email": "ned@nedbatchelde
  }
],
"bom-ref": "pkg:pypi/coverage@
"version": "7.10.6",
```

```
{
  "name": "eslint",
  "purl": "pkg:npm/eslint@7.32.0",
  "type": "library",
  "scope": "required",
  "authors": [
    {
      "name": "Nicholas C. Zakas",
      "email": "nicholas+npm@nczconsulting.com"
    },
    {
      "name": "eslintbot",
      "email": "contact@eslint.org"
    },
    {
      "name": "openjsfoundation",
      "email": "npm@openjsf.org"
    }
  ],
  "bom-ref": "pkg:npm/eslint@7.32.0",
```

Боли глазами лаборатории. dev- и test-инструменты

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР


```
"name": "coverage",
"purl": "pkg:pypi/coverage@7.1
"type": "library",
"scope": "required",
"authors": [
  {
    "name": "Ned Batchelder ar
    "email": "ned@nedbatchelde
  }
],
"bom-ref": "pkg:pypi/coverage@
"version": "7.10.6",
```

```
{
  "name": "eslint",
  "purl": "pkg:npm/eslint@7.32.0",
  "type": "library",
  "scope": "required",
  "authors": [
    {
      "name": "Nicholas C. Zakas",
      "email": "nicholas+npm@nczcon
    },
    {
      "name": "eslintbot",
      "email": "contact@eslint.org"
    },
    {
      "name": "openjsfoundation",
      "email": "npm@openjsf.org"
    }
  ],
  "bom-ref": "pkg:npm/eslint@7.32.0",
```

```
{
  "name": "opentelemetry-exporter-otlp",
  "purl": "pkg:pypi/opentelemetry-exporter-otlp@1.30",
  "type": "library",
  "scope": "required",
  "authors": [
    {
      "name": "OpenTelemetry Authors",
      "email": "cncf-opentelemetry-contributors@lists.cncf.io"
    }
  ],
  "bom-ref": "pkg:pypi/opentelemetry-exporter-otlp@1.30",
  "version": "1.30.0",
  "licenses": [
    {
      "license": {
        "url": "https://opensource.org/license/apache-2-0",
        "name": "Apache-2.0"
      }
```

Боли глазами лаборатории. dev- и test-инструменты

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР


```
"name": "coverage",
"purl": "pkg:pypi/coverage@7.1
"type": "library",
"scope": "required",
"authors": [
  {
    "name": "Ned Batchelder ar
    "email": "ned@nedbatchelde
  }
],
"bom-ref": "pkg:pypi/coverage@
"version": "7.10.6",
```

```
{
  "name": "eslint",
  "purl": "pkg:npm/eslint@7.32.0",
  "type": "library",
  "scope": "required",
  "authors": [
    {
      "name": "Nicholas C.
      "email": "nicholas+npr
    },
    {
      "name": "eslintbot",
      "email": "contact@esl
    },
    {
      "name": "openjsfounda
      "email": "npm@openjsf
    }
  ],
  "bom-ref": "pkg:npm/eslint
```

```
{
  "name": "opentelemetry-exporter-otlp",
  "purl": "pkg:pypi/opentelemetry-exporter-otlp@1.30",
  "type": "library",
  "scope": "required",
```

```
{
  "name": "nyc",
  "purl": "pkg:npm/nyc@15.1.0",
  "type": "library",
  "scope": "required",
  "authors": [
    {
      "name": "Ben Coe",
      "email": "ben@npmjs.com"
    },
    {
      "name": "bcoe",
      "email": "bencoe@gmail.com"
    },
    {
      "name": "coreyfarrell",
      "email": "git@cfware.com"
    },
    {
      "name": "isaacs",
      "email": "i@izs.me"
    }
  ],
  "bom-ref": "pkg:npm/nyc@15.1.0",
```

Боли глазами лаборатории. dev- и test-инструменты

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР


```
"name": "coverage",
"purl": "pkg:pypi/coverage@7.1
"type": "library",
"scope": "required",
"authors": [
  {
    "name": "Ned Batchelder ar
    "email": "ned@nedbatchelde
  }
],
"bom-ref": "pkg
"version": "7.1
```

```
{
  "name": "eslint",
  "purl": "pkg:npm/eslint@7.32.0",
  "type": "library",
  "scope": "required",
  "authors": [
    {
      "name": "Nicholas C.
      "email": "nicholas+npm
    },
    {
```

```
  "name": "debug",
  "purl": "pkg:npm/debug@4.4.3",
  "type": "library",
  "scope": "required",
  "authors": [
    {
      "name": "Josh Junon"
    },
    {
      "name": "qix",
      "email": "npm@josh.junon.me"
    },
    {
      "name": "tootallnate",
      "email": "nathan@tootallnate.net"
    }
  ],
  "bom-ref": "pkg:npm/debug@4.4.3",
  "version": "4.4.3"
```

```
{
  "name": "opentelemetry-exporter-otlp",
  "purl": "pkg:pypi/opentelemetry-exporter-otlp@1.30",
  "type": "library",
  "scope": "required",
```

```
{
  "name": "nyc",
  "purl": "pkg:npm/nyc@15.1.0",
  "type": "library",
  "scope": "required",
  "authors": [
    {
      "name": "Ben Coe",
      "email": "ben@npmjs.com"
    },
    {
      "name": "bcoe",
      "email": "bencoe@gmail.com"
    },
    {
      "name": "coreyfarrell",
      "email": "git@cfware.com"
    },
    {
      "name": "isaacs",
      "email": "i@izs.me"
    }
  ],
  "bom-ref": "pkg:npm/nyc@15.1.0",
```

Боли глазами лаборатории. dev- и test-инструменты

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР


```
"name": "coverage",
"purl": "pkg:pypi/coverage@7.1
"type": "library",
"scope": "required",
"authors": [
  {
    "name": "Ned Batchelder ar
    "email": "ned@nedbatchelde
  }
],
"bom-ref": "pkg
"version": "7.1
```

```
{
  "name": "eslint",
  "purl": "pkg:npm/eslint@7.32.0",
  "type": "library",
  "scope": "required",
  "authors": [
    {
      "name": "Nicholas C.
      "email": "nicholas+npm
    },
    {
```

```
  "name": "debug",
  "purl": "pkg:npm/debug@4.4.3",
  "type": "library",
  "scope": "required",
  "authors": [
    {
      "name": "Josh Junon"
    },
    {
      "name": "qix",
      "email": "npm@josh.junon.me"
    },
    {
      "name": "tootallnate",
      "email": "nathan@tootallnate.net"
    }
  ],
  "bom-ref": "pkg:npm/debug@4.4.3",
  "version": "4.4.3"
```

```
{
  "name": "opentelemetry-exporter-otlp",
  "purl": "pkg:pypi/opentelemetry-exporter-otlp@1.30",
  "type": "library",
  "scope": "required",
```

```
{
  "name": "nyc",
  "purl": "pkg:npm/nyc@15.1.0",
  "type": "library",
  "scope": "required",
  "authors": [
    {
      "name": "Ben Coe",
      "email": "ben@npmjs.com"
    },
    {
      "name": "bcoe",
      "email": "bencoe@gmail.com
    },
    {
      "name": "coreyfarrell",
      "email": "git@cfware.com"
    },
    {
      "name": "isaacs",
      "email": "i@izs.me"
    }
  ],
  "bom-ref": "pkg:npm/nyc@15.1.0",
```

```
{
  "name": "jest",
  "purl": "pkg:npm/jest@27.5.1",
  "type": "library",
  "scope": "required",
  "authors": [
    {
      "name": "aaronabramov",
      "email": "aaron@abramov.io"
    },
    {
      "name": "cpojer",
      "email": "christoph.pojer@gmail.com"
    },
    {
```

Боли глазами лаборатории. dev- и test-инструменты

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Боли глазами лаборатории. dev- и test-инструменты

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

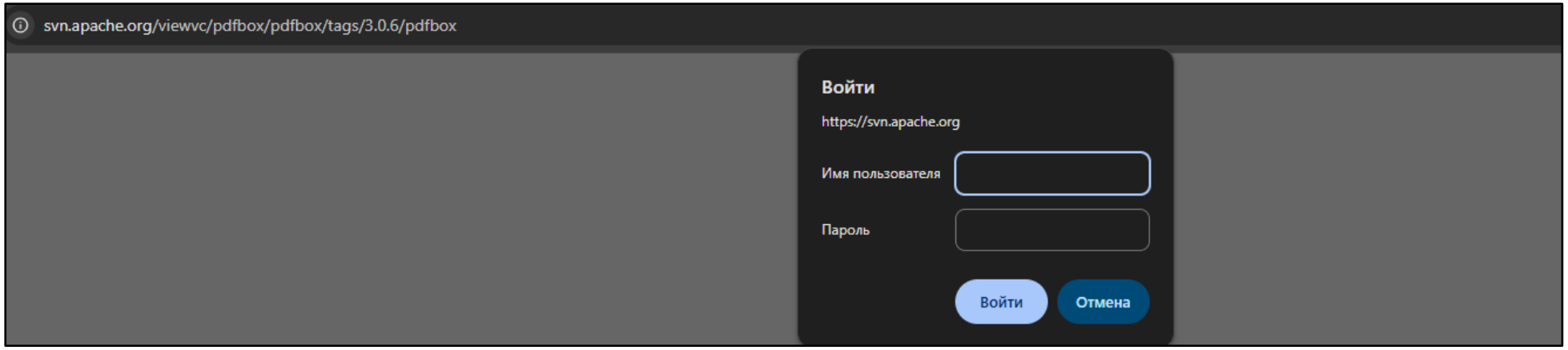
Боли глазами лаборатории. Проблемные ссылки

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Проблема (низкий уровень): некоторые репозитории требуют пройти авторизацию

```
--------------------------------------------------
ERROR/GIT: fatal: could not read Username for 'https://svn.apache.org': terminal prompts disabled

ERROR/SVN: Command 'svn ls https://svn.apache.org/viewvc/pdfbox/tags/3.0.6/pdfbox' timed out after 15 seconds
ERROR/HG: Command 'hg identify https://svn.apache.org/viewvc/pdfbox/tags/3.0.6/pdfbox' timed out after 15 seconds
ERROR/FOSSIL: https://svn.apache.org/viewvc/pdfbox/tags/3.0.6/pdfbox returned code 401
WARNING: https://svn.apache.org/viewvc/pdfbox/tags/3.0.6/pdfbox не подходит под шаблон и не является git/svn/hg/fossil-репозиторием
--------------------------------------------------
```



Боли глазами лаборатории. Проблемные ссылки

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Проблема (низкий уровень): некоторые репозитории требуют пройти авторизацию

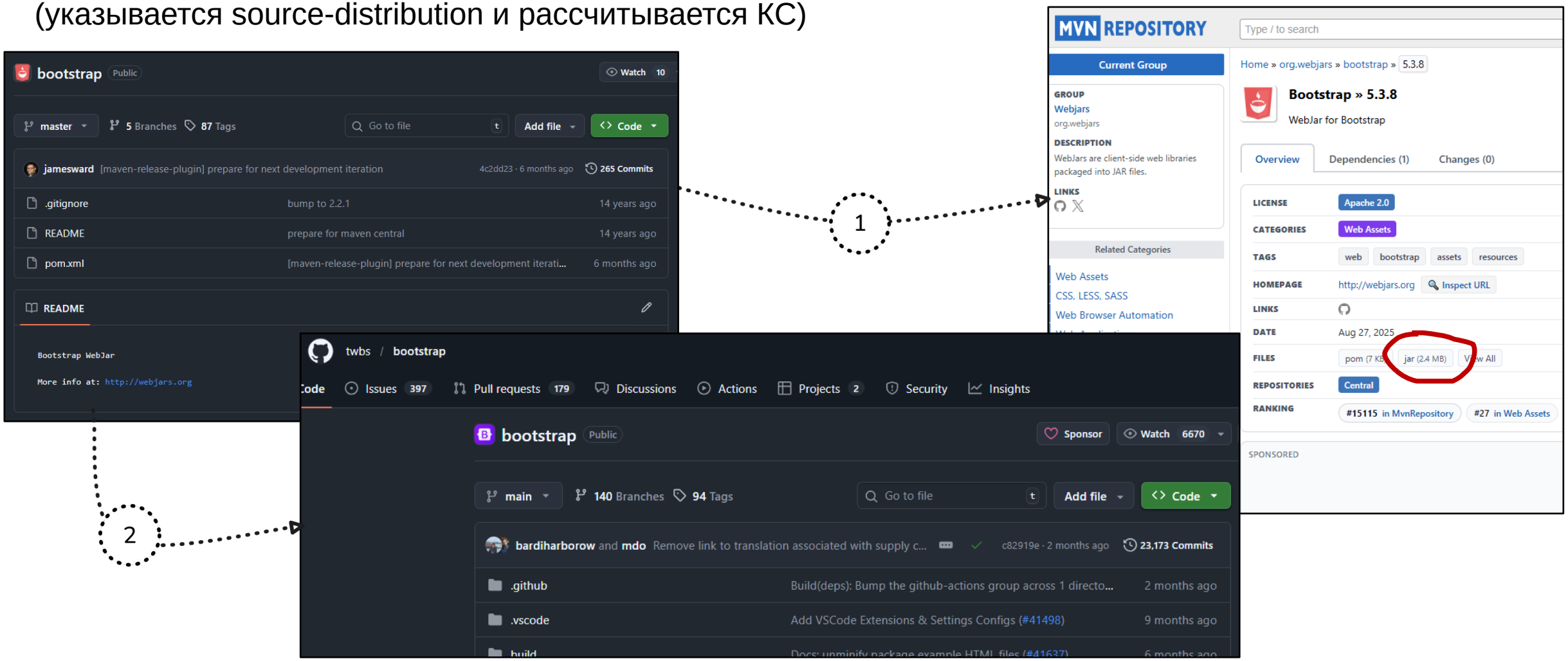
Решение: поиск ссылок на зеркала репозитория или на архив с исходными текстами (указывается source-distribution и рассчитывается КС)

Боли глазами лаборатории. Проблемные ссылки

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Проблема (средний уровень): ссылка на репозиторий, в котором отсутствуют исходные тексты

Решение: поиск ссылок на зеркала репозитория или на архив с исходными текстами (указывается source-distribution и рассчитывается КС)

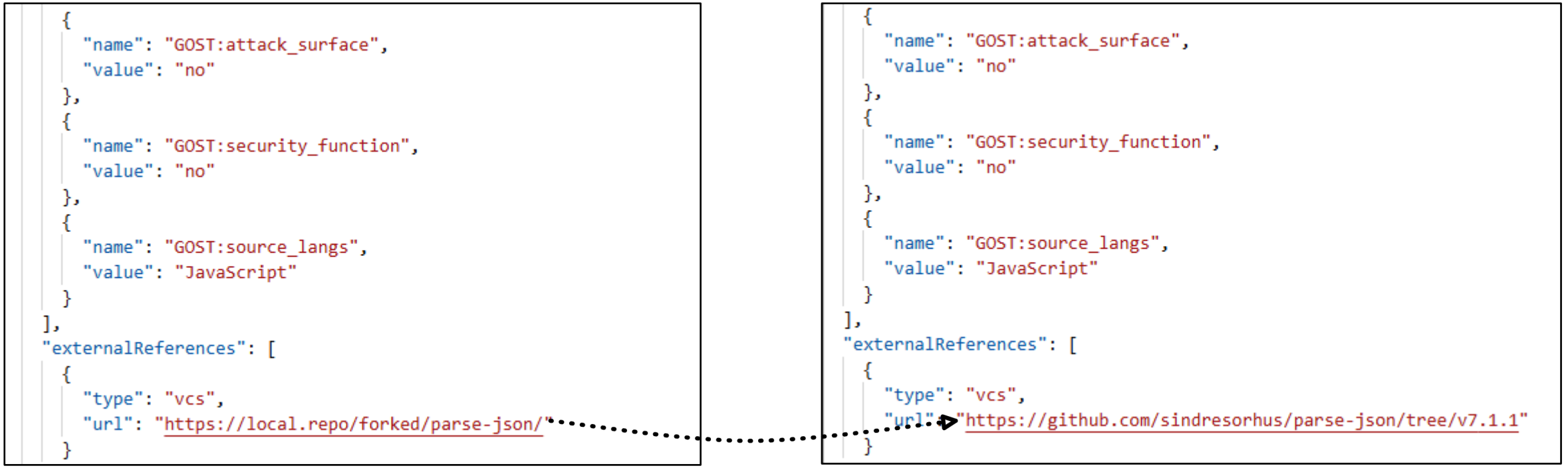


Боли глазами лаборатории. Проблемные ссылки

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Проблема (средний уровень): ссылка на внутренний репозиторий разработчика

Решение: в SBoM файлах необходимо указывать только ссылки на репозитории зависимых компонент с открытым исходным кодом.
В случае форка OSS репозитория и его дальнейшей внутренней поддержки все равно указывается ссылка на репозиторий первоисточника.



Больные выводы

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

- Да, на ПА/ФБ может быть много компонент, но это лучше, чем меньше 1% всех компонент, которые были расставлены случайно и предоставлены для анализа лаборатории
- SBoM файлы следует поддерживать и использовать их для анализа уязвимостей, к ним не следует относится как «к прихоти» лаборатории или Регулятора
- Инструменты сборки и тестирования нужны, но не в составе дистрибутива
- Форки OSS репозиториев с собственными патчами нужно указывать, поскольку это упрощает отслеживание уязвимостей и дает более полную картину (нет понятия «сколько процентов кода репозитория используется»)

Фаззинг это не больно

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

libvirt

- Найдено >10 багов за 2024–2025.
- Критическая ошибка: разбор XML и аллокации происходят до проверки прав доступа.
- Специальный XML → OOM → падение демона → отказ в обслуживании.

Почему обычный подход не работал:

- Рандомный ввод отбрасывался парсером сразу.
- До реальной логики код не доходил.

Что сработало:

- Генерация структурно корректных XML.
- Осмысленные мутации вместо случайных байт.
- Фаззер начал проходить парсер и доходить до глубинных багов.

python

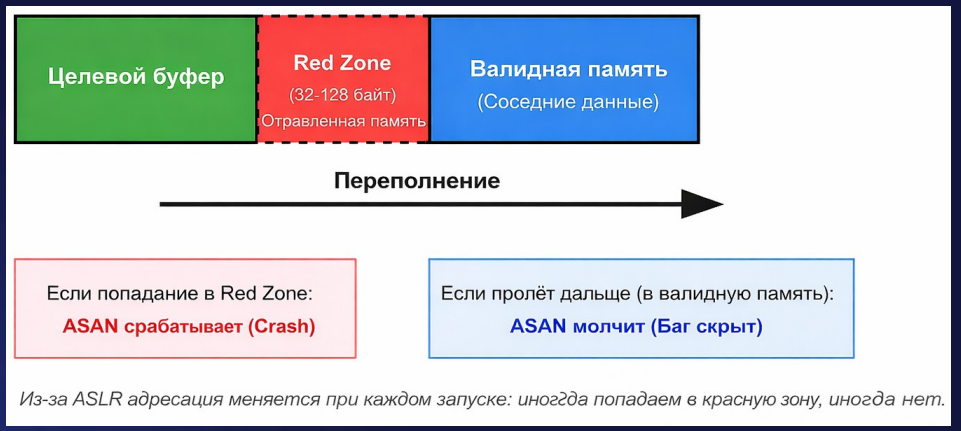
Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Обёртка	Была	Стала
fuzz_builtin_unicode	91.72%	100.00%
fuzz_struct_unpack	57.70%	100.00%
fuzz_timemodule	29.56%	30.77%
fuzz_csv_reader	95.63%	100.00%
fuzz_sre_compile	6.20%	9.16%
fuzz_builtin_float	93.48%	100.00%
fuzz_json_loads	39.12%	100.00%
fuzz_string_find	93.57%	100.00%
fuzz_sre_match	95.28%	100.00%
fuzz_io_textio_read	96.28%	100.00%
fuzz_ll1_ast_parser	53.20%	100.00%

pcre2

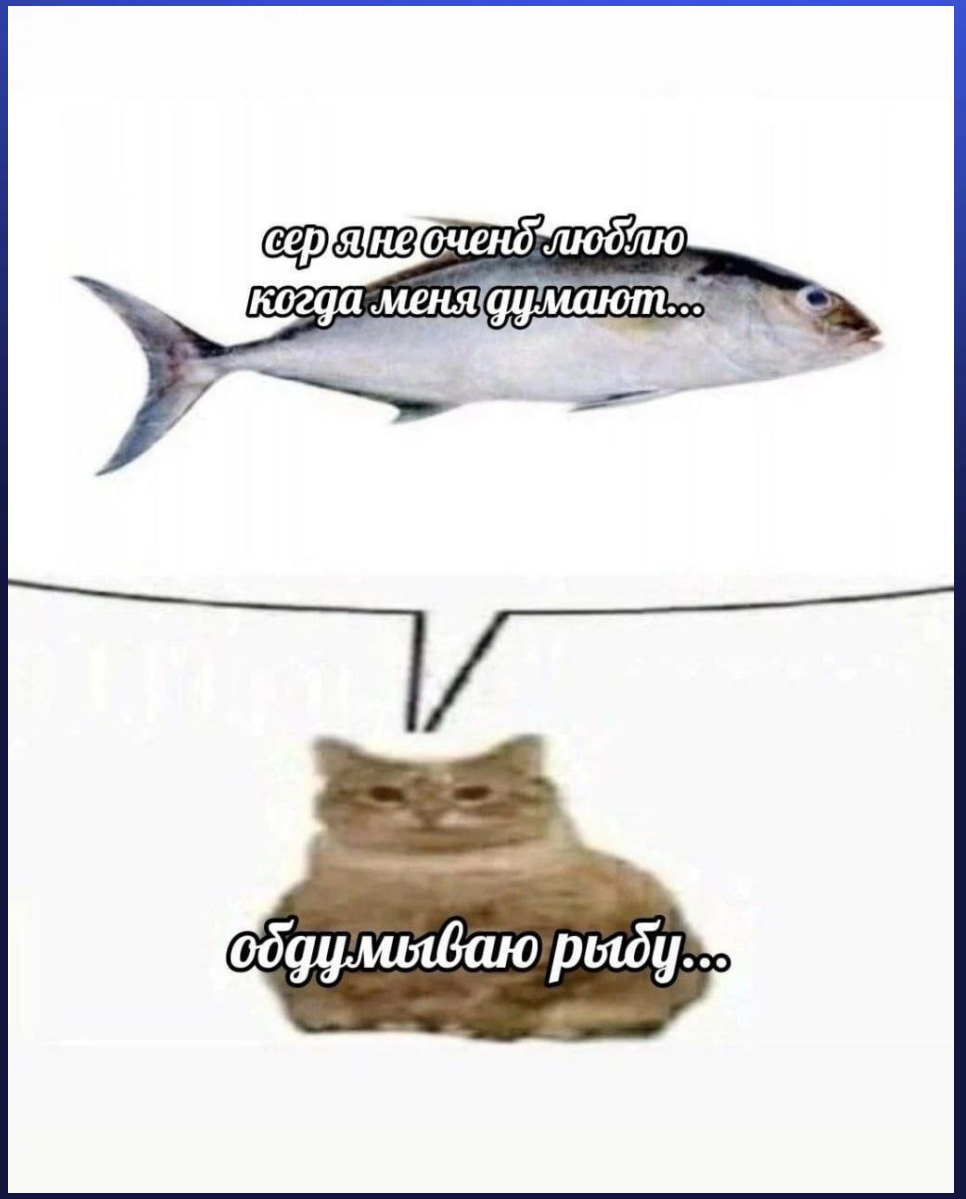
Идеально скрытый баг

ASAN срабатывал время от времени, но при попытке отладить проблему она исчезала: под отладчиком всё «работало», с разными флагами поведение менялось. Мы долго гонялись за версиями и инструментами, пока не поняли простую вещь — переполнение было реальным, но среда тестирования меняла его проявление, и мы по сути отлаживали не баг, а эффект окружения.



Фаззинг - не магия

- Осмысленные мутации > случайность
- Стабильность важнее количества
- Понимание платформы решает



Автоматизируй это

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Зачем делать автоматизацию запуска фаззинга?

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Closed **Запустить фаззинг 3proxy**

Activity

Sort or filter

- **L.reviakin** changed due date to October 18, 2024 5 months ago
- **L.reviakin** added fuzzing label 5 months ago
- **L.reviakin** assigned to @d.fedin 5 months ago

L.reviakin @L.reviakin · 5 months ago Author Owner

@d.fedin, как успехи?

через некоторое время...

Closed **Запустить фаззинг 3proxy**

L.reviakin @L.reviakin · 3 months ago Author Owner

Зависания не удаётся воспроизвести на сервере. Кажется, что проблема в обёртке. Займусь этим на новогодних.

- **L.reviakin** changed due date to January 11, 2025 3 months ago

Зачем делать автоматизацию запуска фаззинга?

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

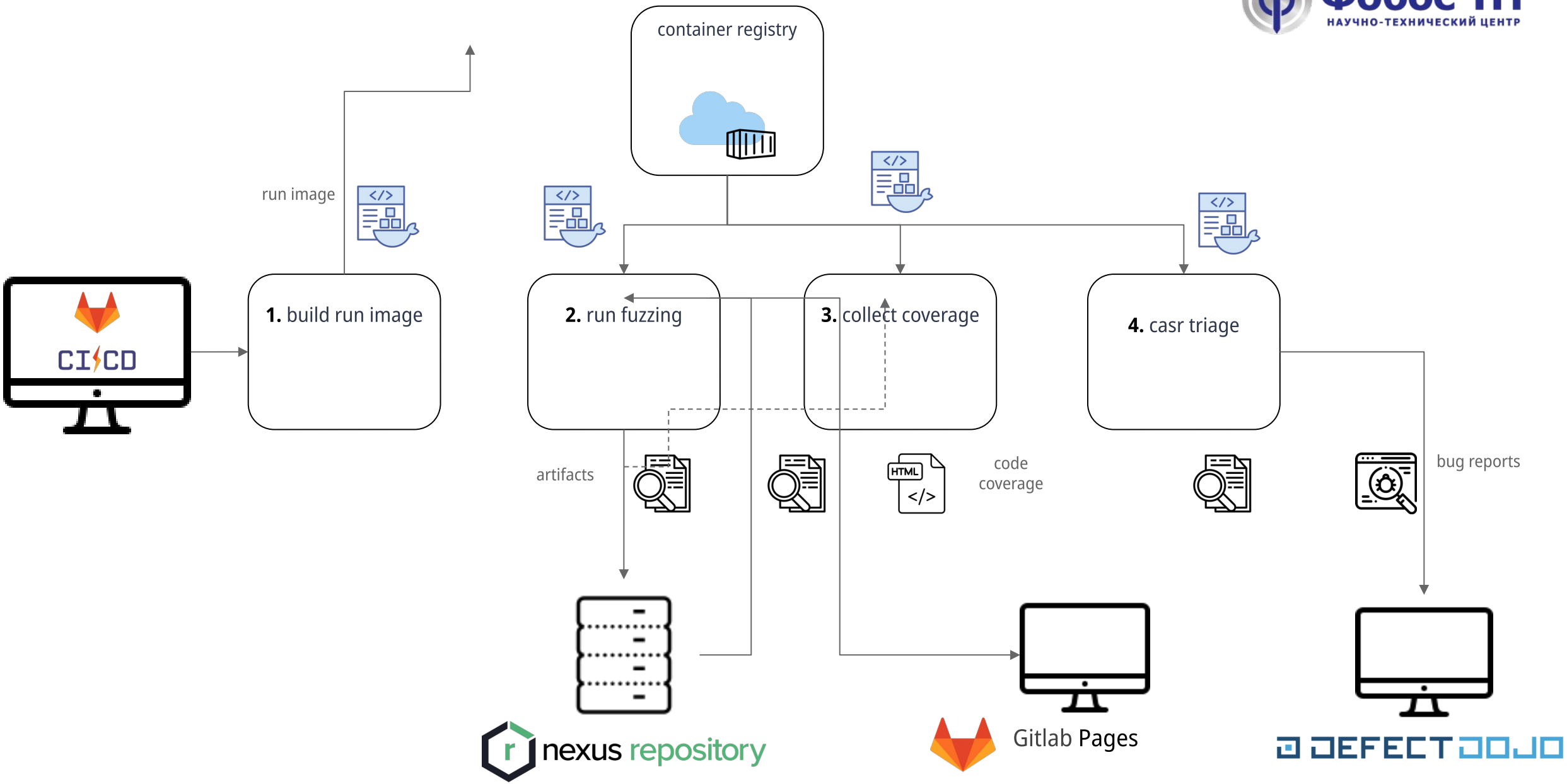
- запускать продолжительные фаззинг-итерации с автоматическим сбором необходимой статистики по результатам фаззинга (наработанное покрытие, найденные падения)
- обеспечить итеративность запуска фаззинг-итераций для фаззинг-проектов
- сократить инженерное время на рутинных задачах, таких как запуск фаззинга и сбор необходимых статистик фаззинг-итераций.

Решение: создаём планировщик фаззинг-итераций

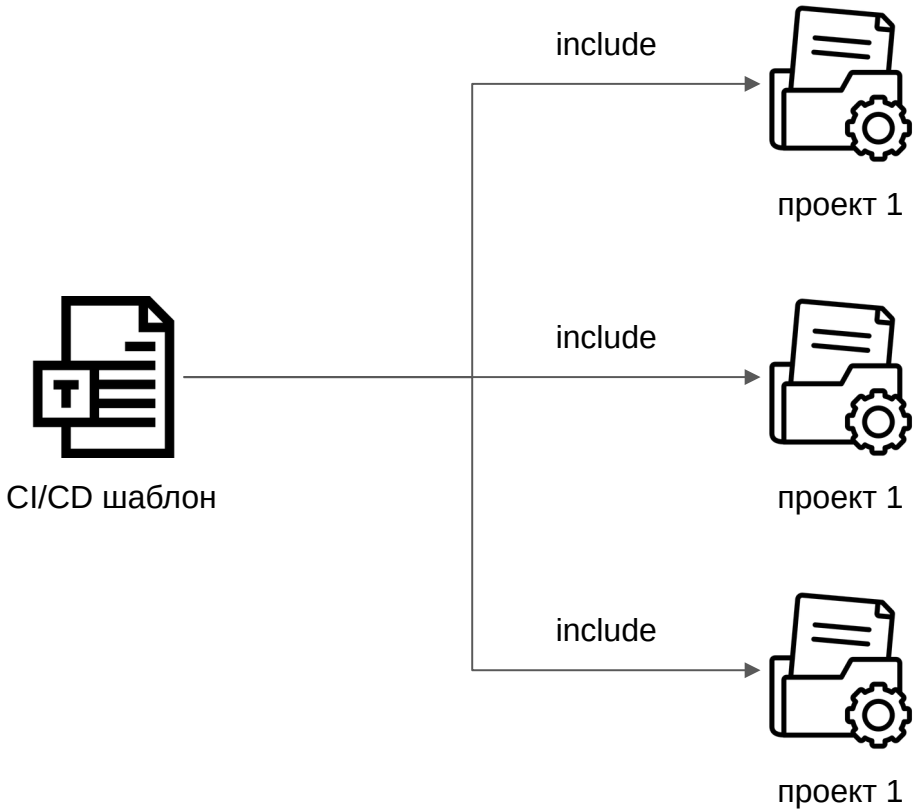
Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Шаг 1: создаём пайплайн фаззинг-итерации для проекта

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР



Шаг 2: создаём шаблон пайплайна фаззинг-итерации



.gitlab-ci.yml 178 B

```yaml
include:
  - project: 'fuzz_group/fuzz-manager'
    ref: main
    file: '/ci_cd_templates/general_docker_exec_ci.yml'

variables:
  FUZZ_TARGET: 'http_parse'
  FUZZ_TIME: '100s'
```

Пример использования шаблона

Шаг 3: создаём планировщик запусков пайплайнов

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

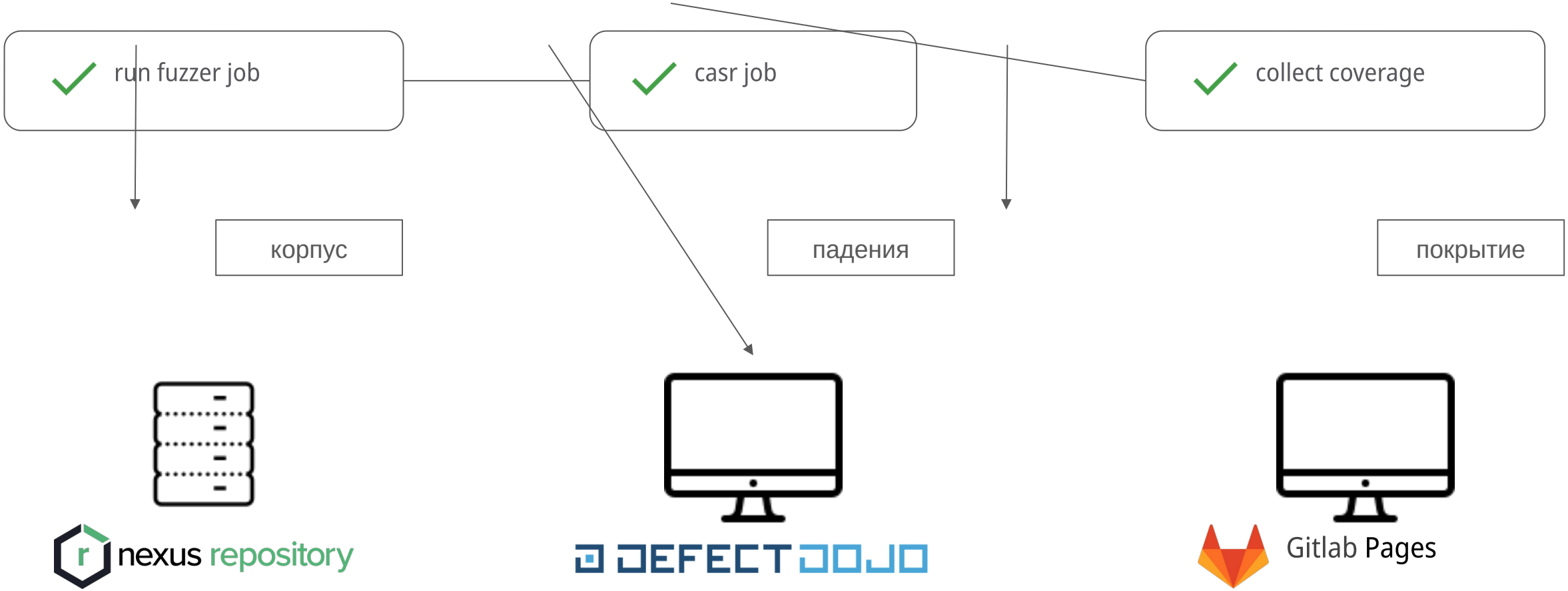
Принцип работы планировщика пайплайнов:

1. приоритизация проектов для фаззинга
2. определение доступных раннеров
3. запуск продолжительной фаззинг-итерации (12 часов)

```
44  Запуск пайплайна для проекта: cups-filters_1.28.17 (kazan_pipe)
45  Ошибка при запуске пайплайна для cups-filters_1.28.17: {'base': ['jobs config should contain at least one visible job']}
46  Запуск пайплайна для проекта: 389-ds-base_2.2.9 (master)
47  Создан пайплайн #3371 https://gitlab.inner.fobos-nt.ru/fuzz_group/basealt/389-ds-base_fuzz/-/pipelines/3371
48  Запуск пайплайна для проекта: networkmanager_1.42.0 (main)
49  Создан пайплайн #3372 https://gitlab.inner.fobos-nt.ru/fuzz_group/basis/networkmanager_1.42.0/-/pipelines/3372
50  Все доступные раннеры заняты, остальные проекты будут запущены позже.
51  Cleaning up project directory and file based variables                                                    00:00
52  Job succeeded
```

Шаг 4: получаем необходимую статистику по результатам фаззинг-итерации

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР



Результаты

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

1. непрерывный запуск фаззинг-итераций для проектов
2. автоматическое распределение фаззинг-итераций в зависимости от количества доступных раннеров
3. упрощение написания пайплайнов для новых проектов за счёт переиспользования шаблонов

Показатель	Без автоматизации	С автоматизацией
Среднее время на запуск разработанной фаззинг-обёртки	от 2-х часов до **нескольких дней**	–
Среднее время на сбор статистик фаззинга (покрытие, падения)	от 2-х часов до **нескольких недель**	–
Среднее время на написание пайплайна	**4 часа**	– (если используется шаблон)

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Елена, сотрудница воспитательной лаборатории

Аудитоконсалтинг

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

ТБ Форум 2025

АРПП лето 2025

Задачи (аудитоконсалтера):

- ***провести проверку*** выстроенных процессов на предмет соответствия требованиям стандартов серии «Безопасная разработка»
- ***помочь*** аудируемым осознать степень несовершенства выстроенных процессов
- ***передать*** аудируемым ***опыт*** и ознакомить с новостями сферы
- ***посчитать*** общую ***экспертную оценку*** и ***подготовить набор рекомендаций*** по развитию процессов разработки

Польза (для тех, кто еще не с нами - welcome):

- наконец-то ***понять, о чём ГОСТ*** РБПО и остальные стандарты по теме
- составить ***маппинг процессов*** ГОСТ на собственные процессы
- ***выделить*** совместно с аудитором ***зоны для оптимизаиии*** и ***системного улучшения***
- здраво ***оценить*** возможность выхода или не ***выхода на сертифиикацию*** процессов РБПО

С нами: Айдеко, *Юзергейт, Код безопасности, Флант, Кейсистемс, Базальт,, Др.Веб, Лукоморье (РТК ИТ +), Гарда Технологии, Яндекс.Облако, БАЗИС, МТС ИИ и 5 компаний, названий которых не приводим*

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Байки аудитоконсалтера

Байка 1: Орган не выдаёт сертификаты

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Сколько артефактов надо подготовить, чтобы Орган выдал сертификат?

1) орган *не выдает* сертификаты
2) выстраивать процессы, а не готовить артефакты

Байка 2: Вынести РБПО на финальный этап?

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Важно ли, чтоб было эффективно? Или можно вынести всё РБПО на заключительный этап релизного цикла?

Тебе нужно сходить на Круглый стол “РБПО. Долгая дорога — эффективный бизнес”, ТБ Форум 20 фев 2026 :)

Байка 3: Моделирование угроз vs поверхность атаки

Можно не выполнять моделирование угроз и получить положительную оценку аудитора, сказав, что строим поверхность атаки?

МУ и ПА части процесса №7, оценка бинарная: либо процесс выполняется (то есть выполняются все требования), либо процесс не выполняется

Байка 4: «У нас не тот статанализатор, но процесс есть»

Итоги испытаний статических анализаторов при поддержке ФСТЭК России 2025

У нас *не тот стат.анализатор*, но автоматизация есть, события запуска определены, ну да, еще *нет регламента*, но стат.анализатор есть, правда ГОСТ Р 71207-2024 не соответствует, да у нас, скорее, *линтер*. Но *процесс №10 у нас есть*, верно?) Ну, да, надо только регламент написать, ну и другой стат.анализатор встроить в пайплайн. Процесс у нас есть :D

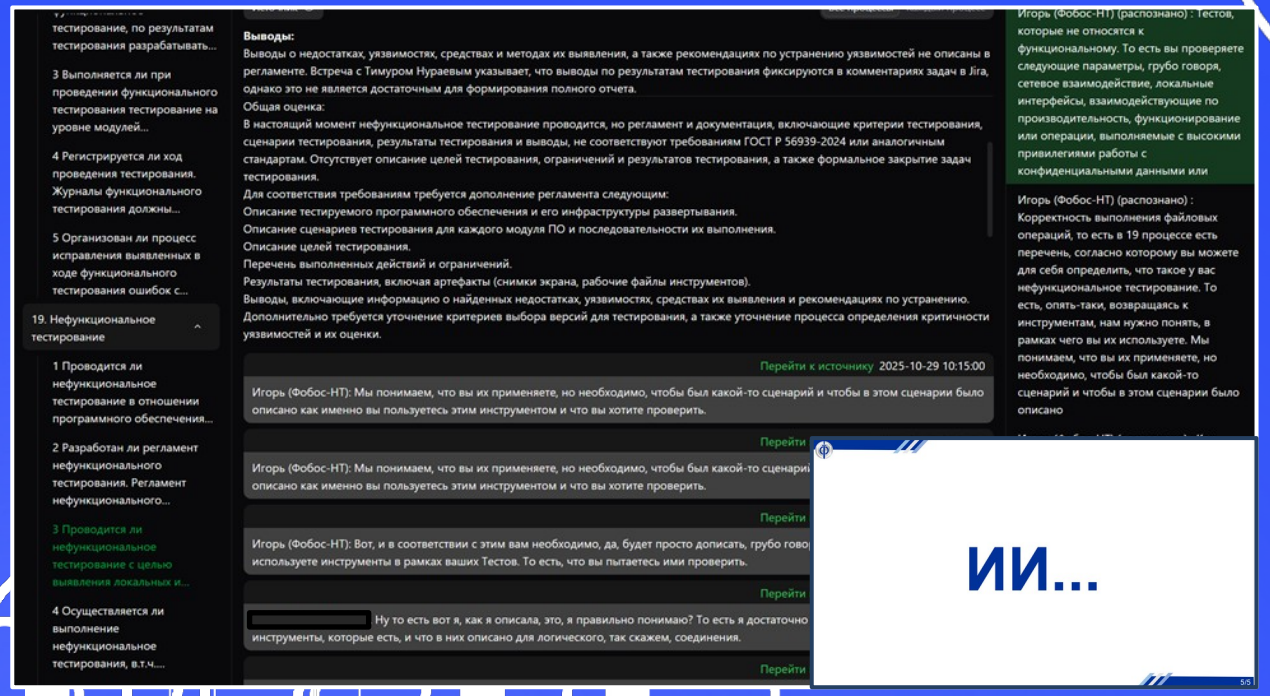
Процесс №10 про статический анализ. Поэтому без стат.анализатора и описанного порядка реализации процесса – процесса нет :)

ИИ-инструмент для аудита

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР

Проблематика:
- На составление отчета уходит больше времени, чем на сам аудит.

Задача:
- Разработать программу, которая будет обрабатывать файлы транскрибации встреч и готовить отчёты по заданным шаблонам.



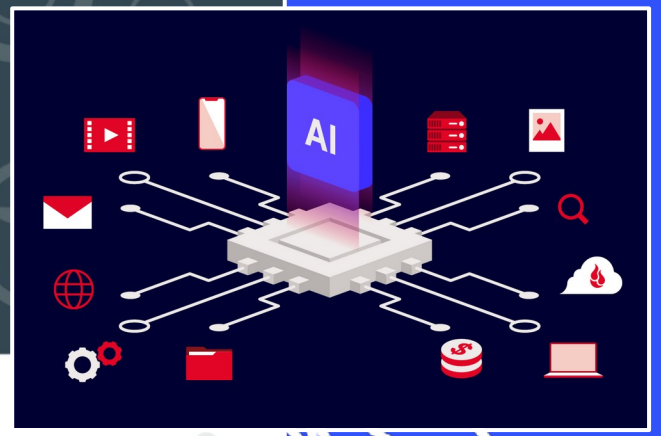
Основная рабочая единица — моделька. Она:
- Анализирует транскрибацию встреч.
- Оценивает выполнение каждого требования ГОСТ.
- Подкрепляет выводы цитатами.
- Позволяет перейти к моменту записи, на основе которого сделан вывод.
- Умеет отвечать на вопросы в интерактивном чате.

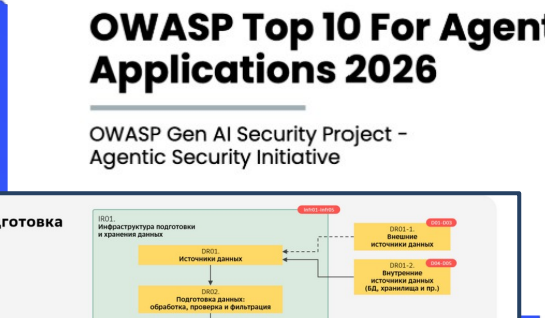
Сложности:
1) Моделька долго думает. Но всё равно не так долго, как аудитор.
2) Моделька искажает информацию.
3) Мы не можем использовать решения, которые не гарантируют конфиденциальность. А это сразу сужает круг мощных моделек.

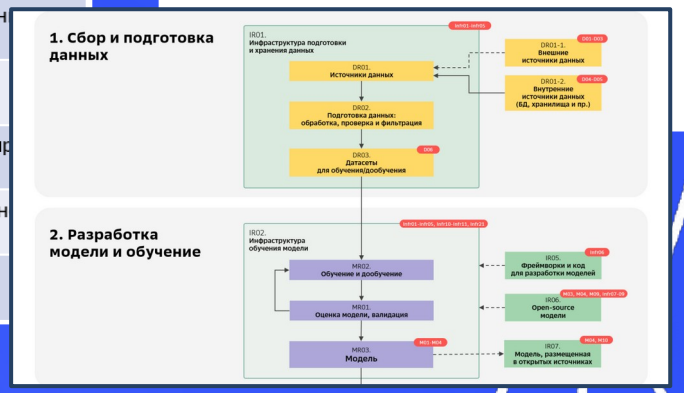
Итог: программа в тестовом режиме, минусов пока больше, чем плюсов. Но проект продолжаем.

Новое направление: ИИ + РБПО

№ п.п	Наименование процесса в соответствии с ГОСТ 56939	№ п.п	Наименование процесса в соответствии с ГОСТ 56939
5.1	Планирование процессов разработки безопасного программного обеспечения	5.14	Управление доступом и контроль целостности кода при разработке программного обеспечения
5.2	Обучение сотрудников	5.15	Обеспечение безопасности используемых секретов
5.3	Формирование и предъявление требований безопасности к программному обеспечению	5.16	Использование инструментов композиционного анализа
5.4	Управление конфигурацией программного обеспечения	5.17	Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок
5.5	Управление недостатками и запросами на изменение программного обеспечения	5.18	Функциональное тестирование
5.6	Разработка, уточнение и анализ архитектуры программного обеспечения	5.19	Нефункциональное тестирование
5.7	Моделирование угроз и разработка описания поверхности атаки	5.20	Обеспечение безопасности при выпуске готовой к эксплуатации версии программного обеспечения
5.8	Формирование и поддержание в актуальном состоянии правил кодирования	5.21	Безопасная поставка программного обеспечения пользователям
5.9	Экспертиза исходного кода	5.22	Обеспечение поддержки программного обеспечен этапе эксплуатации пользователями
5.10	Статический анализ исходного кода	5.23	Обеспечение реагирования на информацию об уязвимостях
5.11	Динамический анализ кода программы	5.24	Поиск уязвимостей в программном обеспечении пр эксплуатации
5.12	Использование безопасной системы сборки программного обеспечения	5.25	Обеспечение безопасности при выводе программн обеспечения из эксплуатации
5.13	Обеспечение безопасности сборочной среды программного обеспечения		







Аудитоконсалтинг & DevDecOps