Ростелеком

Ростелеком
Информационные технологии

Феникс

Доверенный корпоративный репозиторий.

Опыт ПАО «Ростелеком» 2022–2026–...

Кирилл Пихтовников
Заместитель генерального директора
Технический директор Ростелеком
Информационные Технологии

Open Source — основа современного ПО

более

90%

кодовой базы современного ПО — Open Source компоненты

более

18 млрд

скачиваний Open Source компонентов в день

Open Source позволяют сильно сократить время вывода продукта на рынок

На практике...

Новые уязвимости выявляются постоянно

Новые CVE выявляются каждый день — только в 2024 году обнаружено более 30 000 CVE в Open Source.

Реакция замедлена

Исправления уязвимостей применяются с задержкой, а иногда и не применяются вовсе.

Уязвимости уже существуют

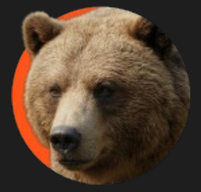
Многие компоненты содержат известные CVE ещё до использования в разработке.

Преднамеренная компрометация

Число обнаруженных вредоносных пакетов к концу Q2 2025 превысило 845 000.

Так, мужики, я заказала шишки из западного леса. И они положили весь прод...

Что такое «прод»?



Клещи что ли с ними приехали...

Ростелеком 2022 год

более
2 000
разработчиков

более
10
самостоятельных репозиториев с собственными проверками

4,5 млн
артефактов в целом по компании

Независимые политики безопасности на проектах

более
200
проектов

Выделенные сотрудники ИБ на критические проекты

Квалификаторы безопасности

*Определение Алексея Смирнова

Зачастую эта терминология применяется к репозиторию артефактов, но также может быть применима и к репозиторию разработки

РТК-Феникс

Доверенный контролируемый репозиторий артефактов разработки ГК «Ростелеком».

РТК-Феникс решает задачу предоставить разработчикам ПО инструменты, позволяющие снизить риски при использовании open-source артефактов, без внесения изменений в существующие процессы разработки.

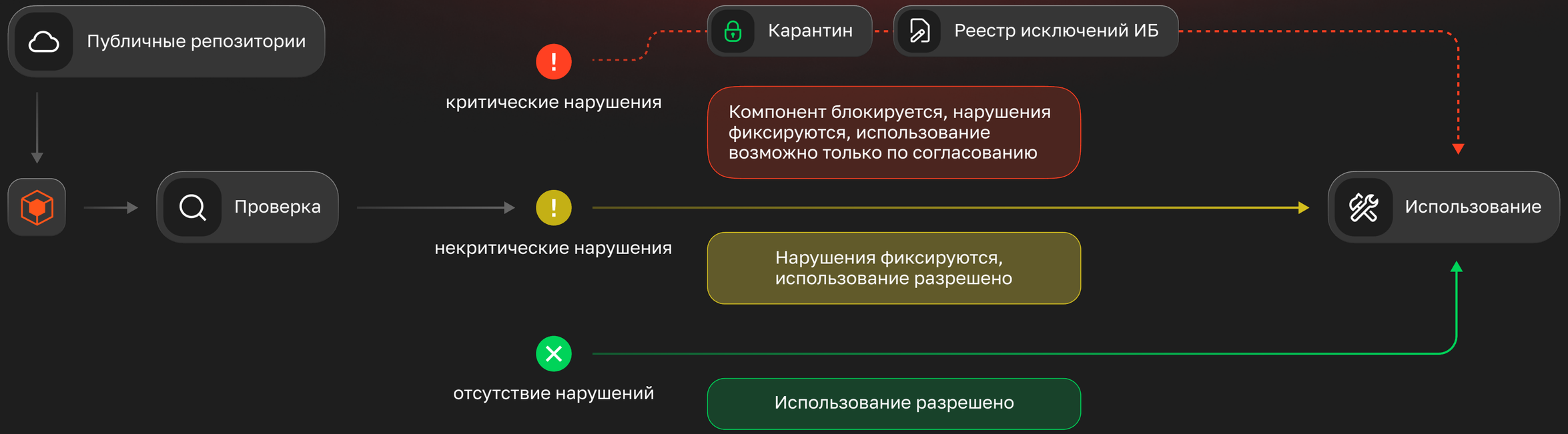
При создании продукта в том числе были использованы уже существовавшие в ГК Ростелеком собственные практики и инструменты в области Безопасной разработки

Ростелеком · Ростелеком Информационные технологии · РТК-ЦОД · БФТ · t2 · TData · bercut · Нетрис · РТК - ЦД Цифровой документооборот

Основные функции Корпоративного репозитория

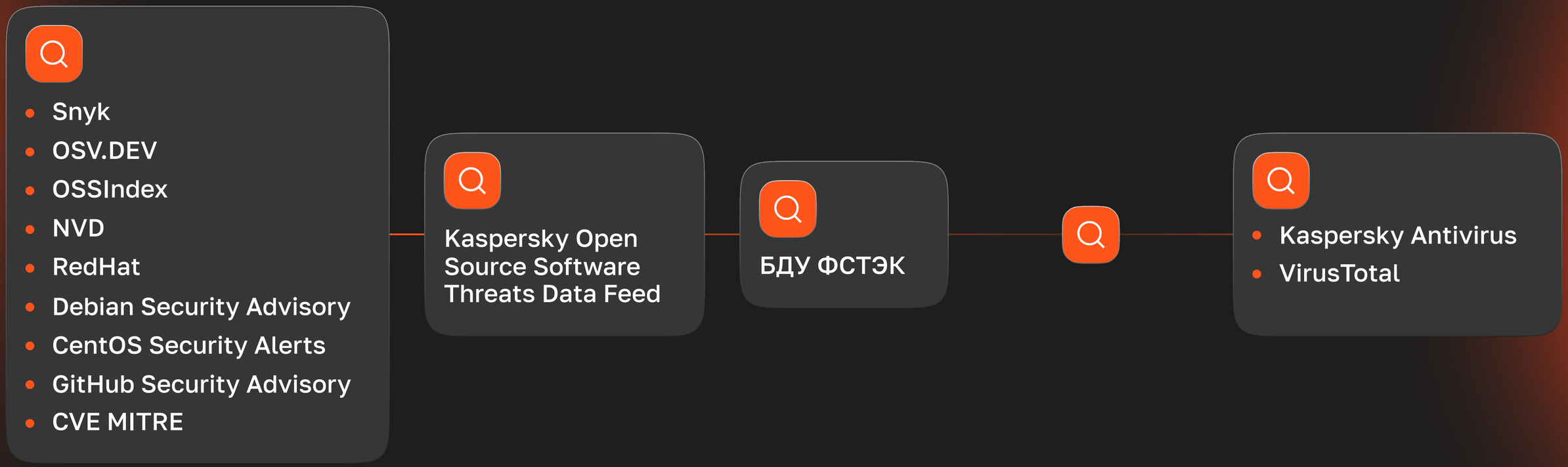
1. Автоматическое скачивание, проверка на вирусы и уязвимости, хранение и предоставление разработчикам запрошенных артефактов
2. Регулярная перепроверка хранимых артефактов по подключенным базам уязвимостей
3. Пользовательский интерфейс не требующего наличия у разработчиков специальных навыков и знаний в области информационной безопасности
4. Предоставление информации об уязвимостях в артефактах разработки и рекомендаций по их устранению
5. Исключение из использования в разработке библиотек, представляющих угрозу безопасности
6. Хранение и проверка SBOM, Vdr-отчеты, уведомление об угрозах

Процесс проверки компонентов



1. Проверка компонентов
2. Классификация нарушений
3. Автоматическая блокировка
4. Согласование исключений
5. Использование компонентов

Проверки


Snyk
OSV.DEV
OSSIndex
NVD
RedHat
Debian Security Advisory
CentOS Security Alerts
GitHub Security Advisory
CVE MITRE
Kaspersky Open Source Software Threats Data Feed
БДУ ФСТЭК
Kaspersky Antivirus
VirusTotal

Правила

Всё сложное — «под капотом». Многоуровневое категорирование уязвимости.

Attack Vector (AV)	Attack Complexity (AC)	Privileges Required (PR)	User Interaction (UI)	Scope (S)	Confidentiality (C)	Integrity (I)	Availability (A)
Physical (P)	Low (L)	None (N)	None (N)	Changed (C)	High (H)	High (H)	High (H)
Physical (P)	High (H)	High (H)	Required (R)	Unchanged (U)	Low (L)	None (N)	None (N)
Local (L)	Low (L)	None (N)	None (N)	Changed (C)	High (H)	High (H)	High (H)
Local (L)	Low (L)	None (N)	None (N)	Unchanged (U)	High (H)	High (H)	High (H)
Local (L)	Low (L)	None (N)	Required (R)	Changed (C)	High (H)	High (H)	High (H)
Local (L)	Low (L)	None (N)	Required (R)	Unchanged (U)	High (H)	High (H)	High (H)
Local (L)	Low (L)	High (H)	Required (R)	Unchanged (U)	Low (L)	Low (L)	Low (L)
Local (L)	High (H)	None (N)	None (N)	Changed (C)	High (H)	High (H)	High (H)
Local (L)	Low (L)	High (H)	None (N)	Changed (C)	High (H)	High (H)	High (H)
Local (L)	Low (L)	None (N)	Required (R)	Changed (C)	High (H)	High (H)	High (H)
Local (L)	High (H)	High (H)	Required (R)	Unchanged (U)	Low (L)	None (N)	None (N)
Adjacent (A)	Low (L)	None (N)	None (N)	Changed (C)	High (H)	High (H)	High (H)
Adjacent (A)	High (H)	None (N)	None (N)	Changed (C)	High (H)	High (H)	High (H)
Adjacent (A)	Low (L)	None (N)	Required (R)	Changed (C)	High (H)	High (H)	High (H)
Adjacent (A)	High (H)	None (N)	Required (R)	Changed (C)	High (H)	High (H)	High (H)
Network (N)	Low (L)	None (N)	None (N)	Changed (C)	High (H)	High (H)	High (H)
Network (N)	High (H)	None (N)	None (N)	Changed (C)	High (H)	High (H)	High (H)
Network (N)	Low (L)	High (H)	None (N)	Changed (C)	High (H)	High (H)	High (H)

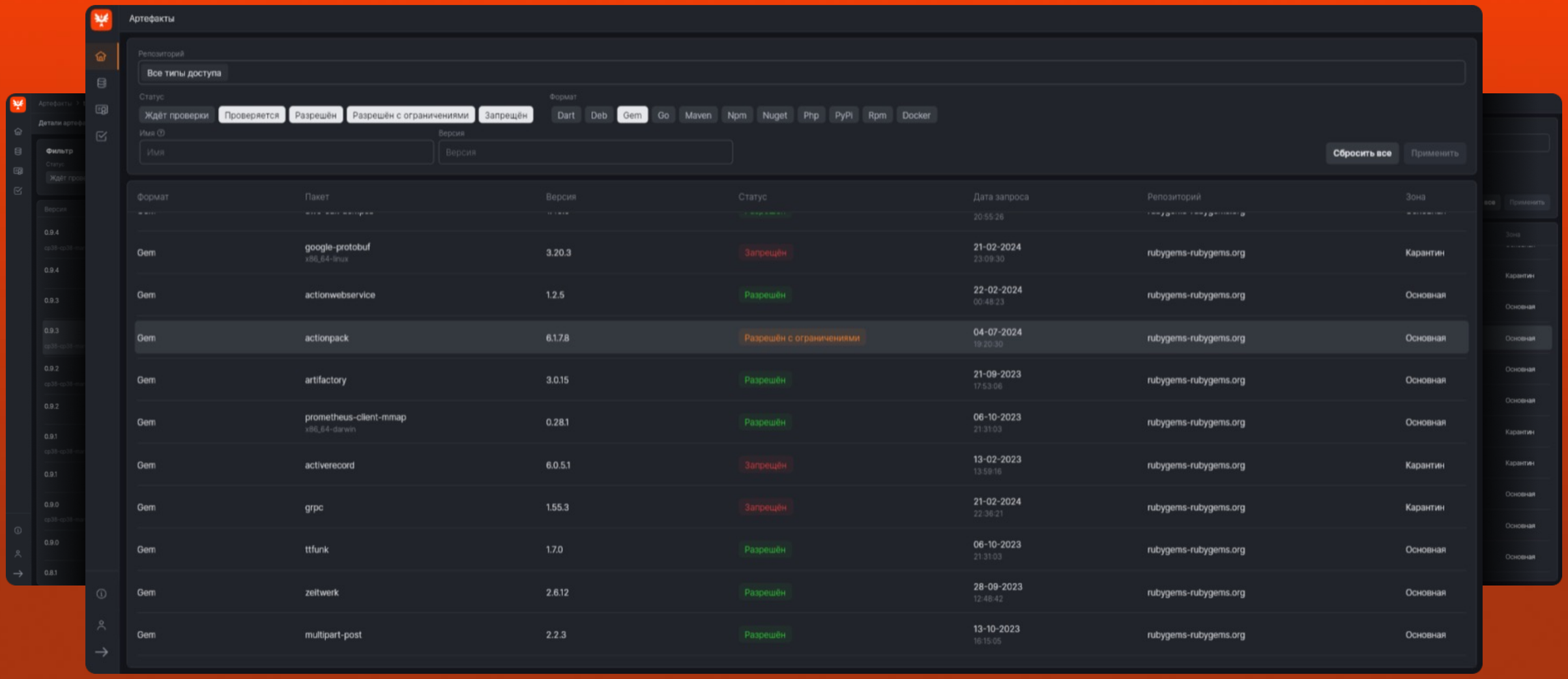
Разработчику — светофор: Можно | Можно с ограничениями | Нельзя

Состояние артефактов на февраль 2026

Формат	«Запрещен»	«Разрешен с ограничением»	«Разрешен»	Общее количество
maven	61 373	13 154	1 151 041	1 225 814
PYRi	9 492	1 492	42 964	54 014
deb	730	63	12 069	12 863
rpm	11 830	1 898	142 856	156 612
gem	3 379	1 514	13 682	18 577
npm	4 946	2 195	212 876	220 136
nuget	519	62	8 625	9 208
php	38	6	2 024	2 068
dart	12	3	1 854	1 881
go	467	25	10 833	11 330
Docker(fat)	1 837	1 120	320	5 518
Docker(manifest)	11 071	6 247	1 812	26 663
Docker (layer)	15 149	13 927	75 025	104 423
Apk	18	3	535	665
	120 861	**41 709**	**1 676 516**	**1 849 772**

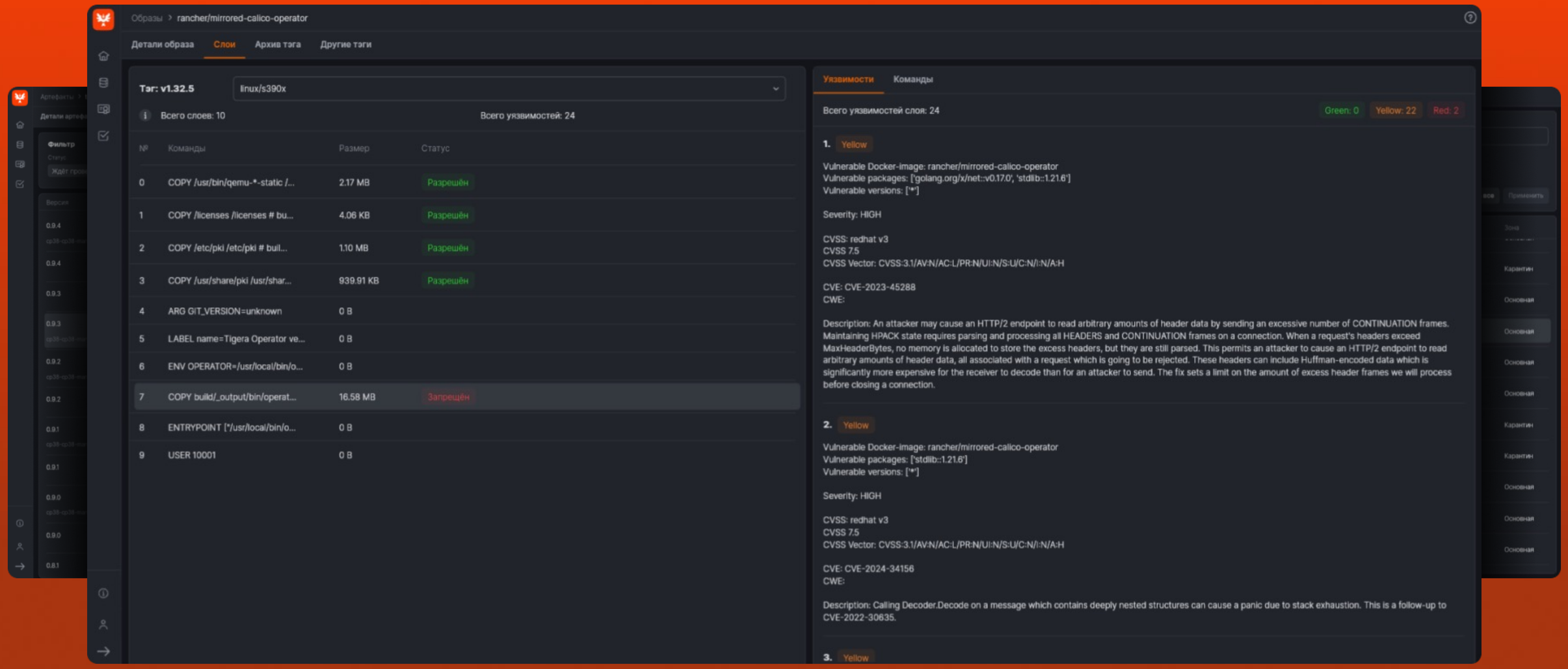
Корпоративный репозиторий в работе

Интерфейс репозитория (1)



Интерфейс репозитория (2)

Интерфейс репозитория (3)

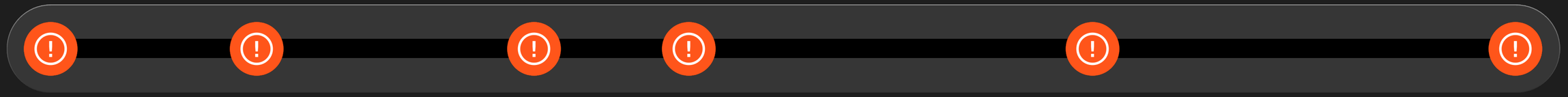


Вызовы

Использование в SBOM библиотек собственной разработки

Отсутствие «безопасных» версий библиотек

Дублирование артефактов из разных репозиториев-зеркал

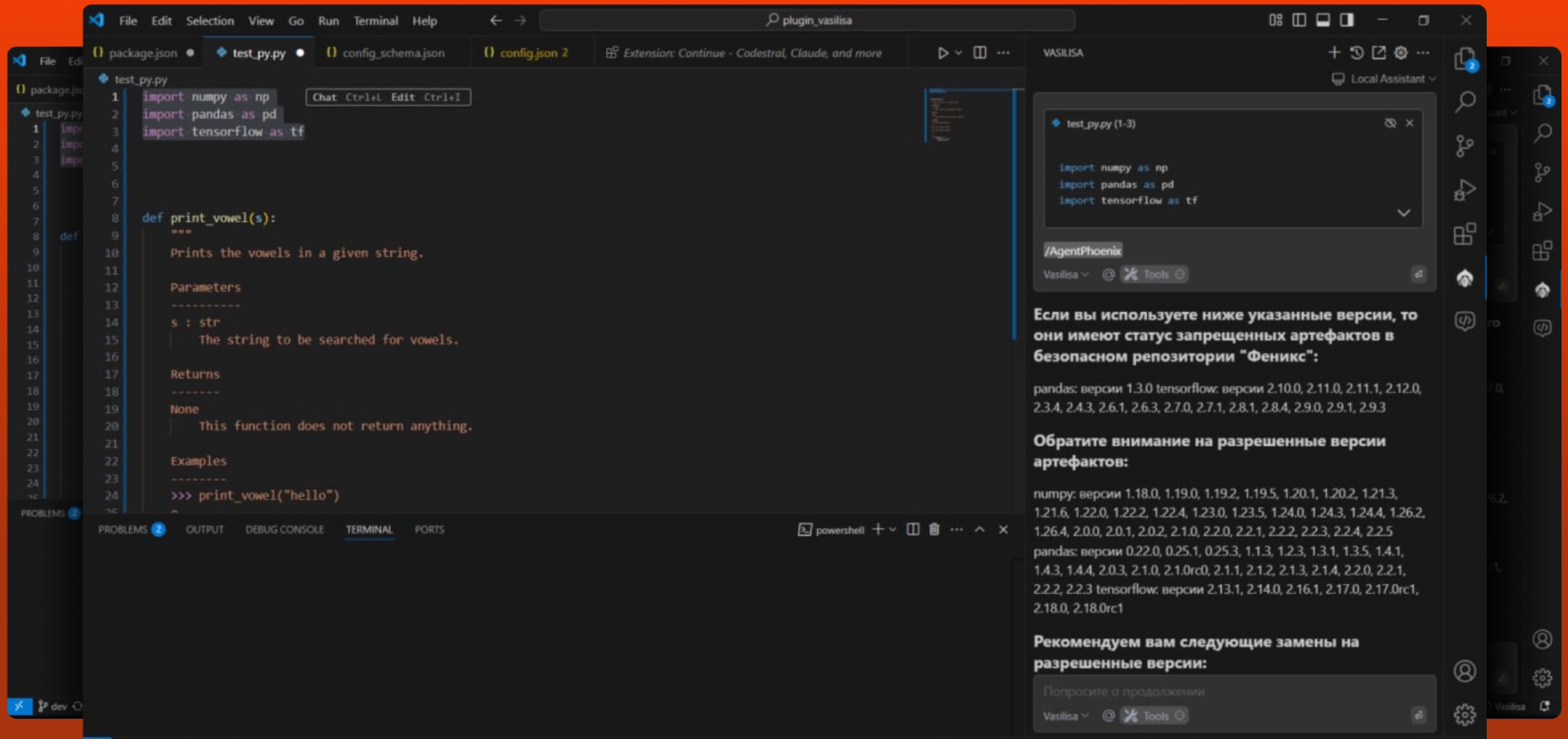


Уязвимости в транзитивных библиотеках

Плагины и транзитивные зависимости, необходимые только для сборки, не попадают в SBOM

Баланс между T2M × стоимость разработки × безопасность ПО

ИИ «Василиса»


File Edit Selection View Go Run Terminal Help
plugin_vasilisa
package.json
test_py.py
config_schema.json
config.json 2
Extension: Continue - Codestral, Claude, and more
Chat Ctrl+L Edit Ctrl+I
import numpy as np
import pandas as pd
import tensorflow as tf
def print_vowel(s):
"""
Prints the vowels in a given string.
Parameters
s : str
The string to be searched for vowels.
Returns
None
This function does not return anything.
Examples
>>> print_vowel("hello")
PROBLEMS 2
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
powershell
VASILISA
Local Assistant
test_py.py (1-3)
/AgentPhoenix
Vasilisa
Tools
Если вы используете ниже указанные версии, то они имеют статус запрещенных артефактов в безопасном репозитории "Феникс":
pandas: версии 1.3.0 tensorflow: версии 2.10.0, 2.11.0, 2.11.1, 2.12.0, 2.3.4, 2.4.3, 2.6.1, 2.6.3, 2.7.0, 2.7.1, 2.8.1, 2.8.4, 2.9.0, 2.9.1, 2.9.3
Обратите внимание на разрешенные версии артефактов:
numpy: версии 1.18.0, 1.19.0, 1.19.2, 1.19.5, 1.20.1, 1.20.2, 1.21.3, 1.21.6, 1.22.0, 1.22.2, 1.22.4, 1.23.0, 1.23.5, 1.24.0, 1.24.3, 1.24.4, 1.26.2, 1.26.4, 2.0.0, 2.0.1, 2.0.2, 2.1.0, 2.2.0, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5
pandas: версии 0.22.0, 0.25.1, 0.25.3, 1.1.3, 1.2.3, 1.3.1, 1.3.5, 1.4.1, 1.4.3, 1.4.4, 2.0.3, 2.1.0, 2.1.0rc0, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.2.0, 2.2.1, 2.2.2, 2.2.3 tensorflow: версии 2.13.1, 2.14.0, 2.16.1, 2.17.0, 2.17.0rc1, 2.18.0, 2.18.0rc1
Рекомендуем вам следующие замены на разрешенные версии:
Попросите о продолжении
Vasilisa
Tools

Ростелеком 2022 год и 2026 год

2022	2026
2+ тыс. разработчиков	3+ тыс. разработчиков
10+ самостоятельных репозиториев	1 централизованный репозиторий и 5 дочерних зависимых
4,5 млн артефактов в целом по компании	1,8 млн уникальных артефактов в централизованном репозитории
Независимые политики безопасности на проектах	Единая политика безопасности на проектах. SBOM на каждый релиз
200+ проектов	300+ проектов

Что мы получили?

Быстрое обнаружение уязвимостей

Уменьшение риска инцидентов и компрометации продуктов благодаря раннему выявлению критических проблем.

Автоматическая фильтрация компонентов

Команде не нужно вручную проверять библиотеки — система сама блокирует опасные артефакты.

Меньше простоев и аварий на продакшене

Снижение числа инцидентов, которые требуют аварийных обновлений или остановки сервисов.

Экономия времени разработчиков

Автоматизация снижает рутину: меньше ручной проверки, поиска CVE, мониторинга зависимостей.

Прозрачность и контроль процессов

Чёткая видимость: какие компоненты безопасны, какие требуют внимания, где риски.

Что мы получили?

Для кого продукт?

Роль / ЦА	Основные боли	Что дал Корпоративный репозиторий
Разработчики / DevOps	Ручная загрузка зависимостей, неизвестные уязвимости, сбои в CI/CD	Безопасные пакеты напрямую из проверенного репозитория, автоматическая блокировка уязвимых компонентов
Инженеры по ИБ / DevSecOps	Отсутствие прозрачности, перегрузка проверками, поздние реакции на CVE	Централизованный контроль, автоматическое сканирование и карантин, отчёты и уведомления
Руководители разработки / CTO	Сложность управления рисками OpenSource, потери времени на аудиты	Снижение рисков и трудозатрат, прозрачная аналитика, единая панель состояния проектов

Статистика Репозитория на февраль 2026

Количество артефактов

1 849 772

1 676 516	Разрешенных без ограничений артефактов
41 709	Разрешенных с ограничениями артефактов
120 861	Запрещенных артефактов

Количество проектов

303

13,88	Среднее количество sbom по проектам
204,37	Среднее количество разрешенных библиотек
2,17	Среднее количество запрещенных библиотек
4,06	Среднее количество исключений по проектам

Статистика Репозитория на февраль 2026

Количество пользователей:

1 482

пользователя

Статистика по исключениям:

1 029

библиотек

83.8

дней — средний срок жизни разрешений

Репозитории библиотек собственной разработки:

30

количество репозиториев в Феникс hub

202

количество артефактов в Феникс hub

Ростелеком

Ростелеком
Технологии возможностей

ПАО «Ростелеком»
company.rt.ru

Крупнейший в России интегрированный провайдер цифровых услуг и решений, который присутствует во всех сегментах рынка и охватывает миллионы домохозяйств, государственных и частных организаций.

«Ростелеком»

Лидер рынка телекоммуникационных услуг для органов государственной власти России и корпоративных пользователей всех уровней.

Признанный технологический лидер

В инновационных решениях в области электронного правительства, кибербезопасности, дата-центров и облачных вычислений, биометрии, здравоохранения, образования, жилищно-коммунальных услуг.

Посмотреть на Корпоративный репозиторий Ростелеком

Публичная демо-зона РТК-Феникс

Система работает на Российских сертификатах безопасности

Решение внесено в реестр Российского ПО:
reestr.digital.gov.ru/reestr/1601290