Ростелеком

Российские решения в области безопасной разработки

Текущая ситуация

Ростелеком- это компания ИТ-разработчик

Все ИТ-разработчики используют решения с открытым кодом.

При использовании готовых продуктов на основе решений с открытым кодом их безопасность, надежность и доступность целиком на производителе конечных продуктов

При создании собственных продуктов с использованием исходных компонент и артефактов с открытым кодом кто даст гарантии безопасности?

При создании собственных продуктов с использованием исходных компонент и артефактов с открытым кодом кто даст гарантии доступности?

Предпосылки к созданию собственного репозитория

Текущая политическая ситуация, риск отключения от централизованных репозиториев

Внесение злонамеренного кода в СПО:
дефекты, шифровальщики, алгоритмические и программные закладки и др.

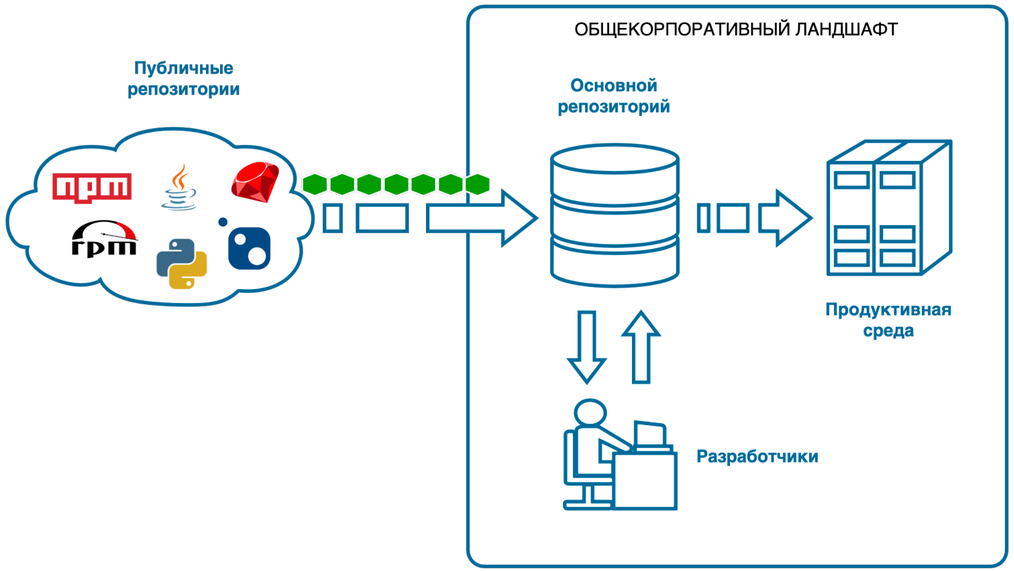
Обеспечение безопасности – необходимость проверки целостности и безопасности артефактов

Риск потери кода в локальных репозиториях в случае отключения от централизованного репозитория

Достижение более высокой управляемости целостностью пользовательского основного репозитория и его безопасностью

В ЧЕМ ПРОБЛЕМА ИТ-РАЗРАБОТКИ?

Так больше не работает:

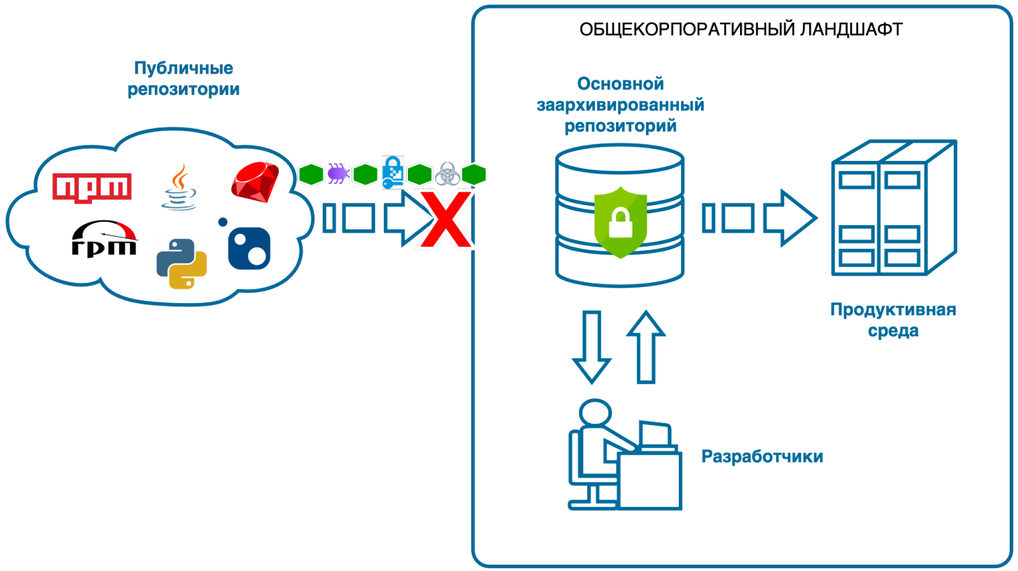


Причина – злонамеренное внесение в СПО:

- дефектов
- шифровальщиков
- вирусов
- алгоритмических и программных закладок и др.

Временное решение

– устранение риска отключения от централизованных репозиториев и злонамеренного кода в СПО:

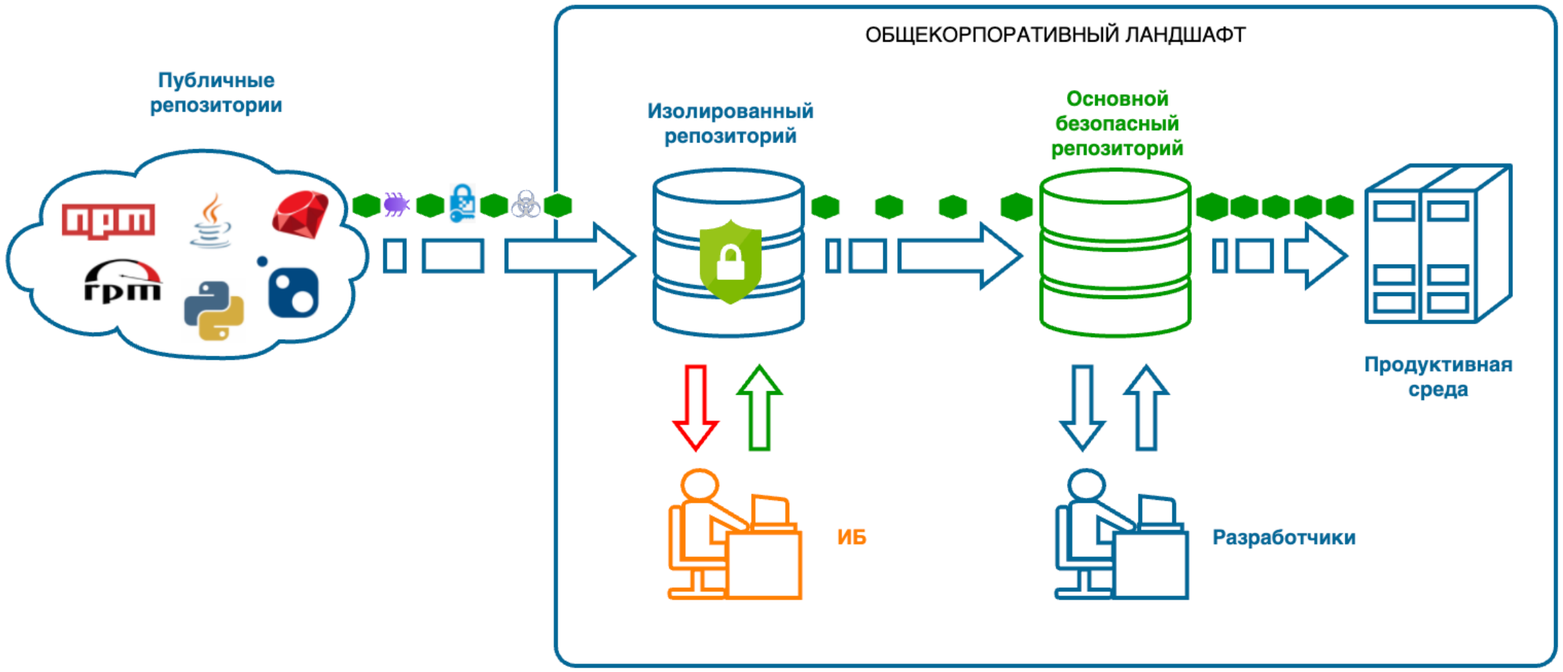


Мы создали архив репозитория для артефактов который содержит:

- **48000+** библиотек/артефактов;
- **15+** типов центральных репозиториев

Безопасный репозиторий Феникс (1/3) - схема

Безопасный репозиторий Феникс– это внутренний доверенный репозиторий артефактов и средств разработки с предварительной проверкой их целостности и безопасности



Назначение

Агрегация, фильтрация, валидация и хранение артефактов

Безопасный репозиторий Феникс (2/3) – ИТ функционал

Реализованный функционал

- Импорт содержимого существующих централизованных репозиториев Ростелеком;
- Создание и обслуживание следующего набора репозиториев:
  - ✓ maven, pypi, deb, rpm, gem, npm, nuget
- Проксирование артефактов между основной и карантинной зоной;
- Скачивание артефактов из репозитория соответствующими клиентами и посредством UI;
- Пользовательский интерфейс для контроля наличия артефакта и статуса его проверки;
- Отслеживание транзитивных зависимостей артефактов при их закачивании на проверку;
- Исключение дублирования одного артефакта скаченного из разных источников

Планы развития

- Реализация поддержки популярных форматов ПО — Docker, raw, go, dart, git, terraform
- Реализация механизмов автозагрузки артефактов при обновлении их в репозитории источнике
- Реализация механизмов подтверждения подлинности проверенного артефакта (хэш сумма, подписание файла)

Безопасный репозиторий Феникс (3/3) – ИБ функционал

Перечень проверяемых уязвимостей

- блокировка работы приложения по IP-адресу / по временной зоне;
- увеличение утилизации ресурсов по IP-адресу / по временной зоне;
- замена содержимого переменных окружения;
- замена изображений и текстов на сайтах (подделка контента);
- внедрение баннеров с политическими лозунгами;
- внедрение вредоносного кода для удалённого управления, доступа к конфиденциальным данным, осуществления DDoS-атак, шифрования систем, уничтожения данных на компьютере пользователя;
- кража конфиденциальной информации о пользователях;
- содержание вирусов, червей, троянов и других видов вредоносных программ

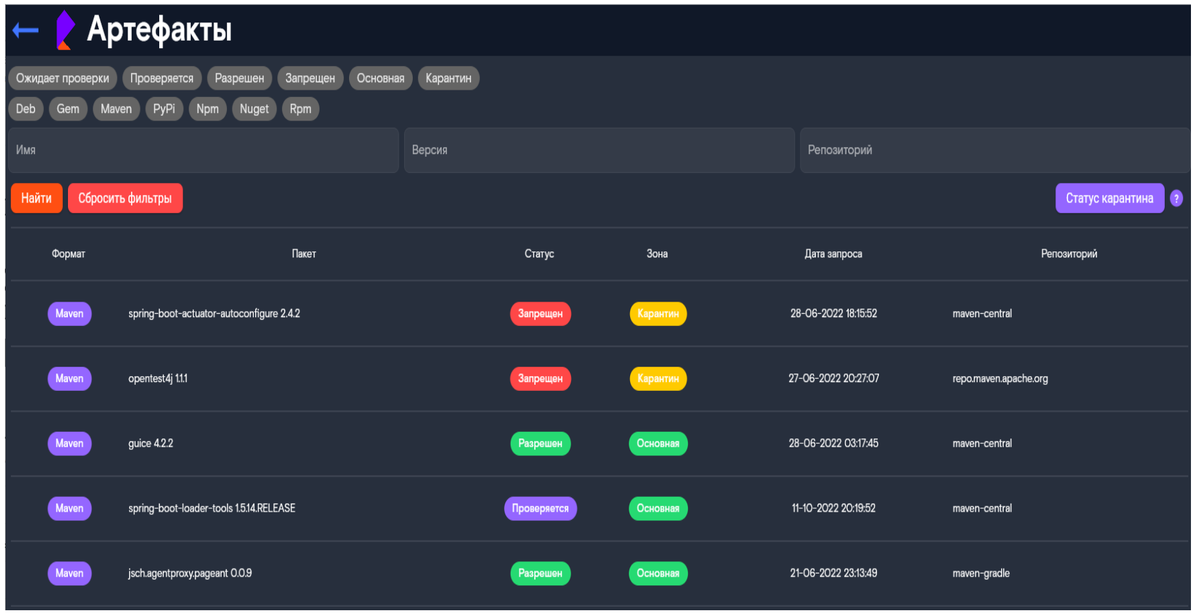
Планы развития

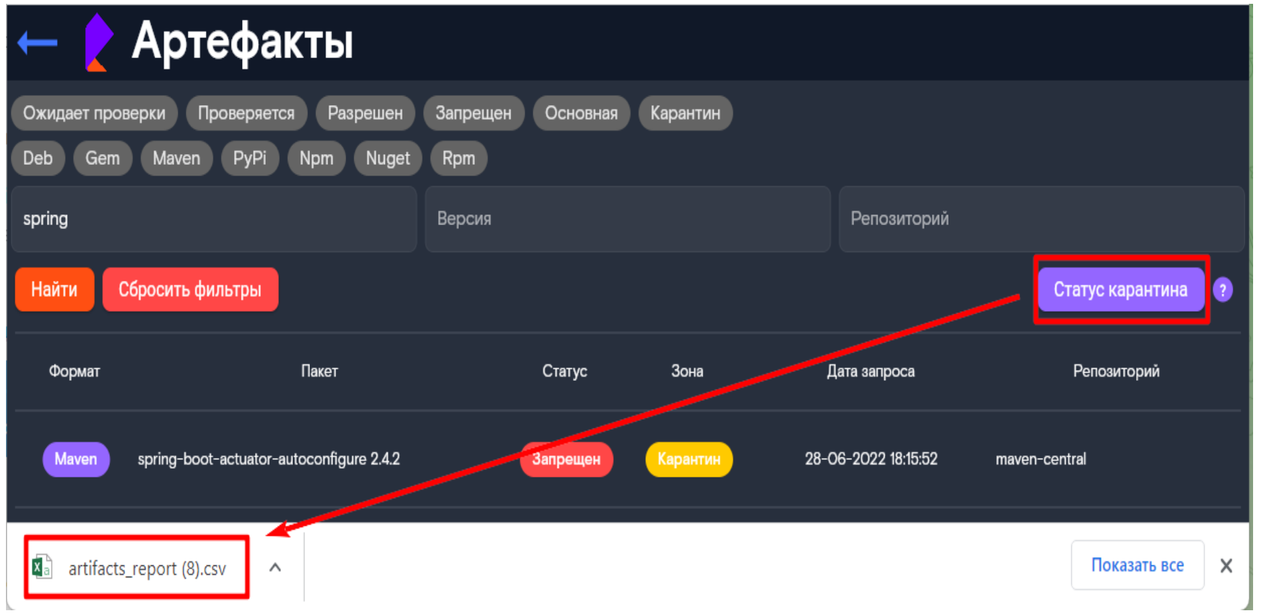
- Запуск расширенного мониторинга профильных новостных ресурсов, социальных сетей,GitHub
- Расширенная проверка бинарного кода артефактов с помощью SAST- и DAST-анализаторов
- Расширенные кастомные конструкции проверки артефактов
- Определение потребителей ‘опасных’ пакетов

Многоуровневое категорирование определяемых уязвимостей в артефактах

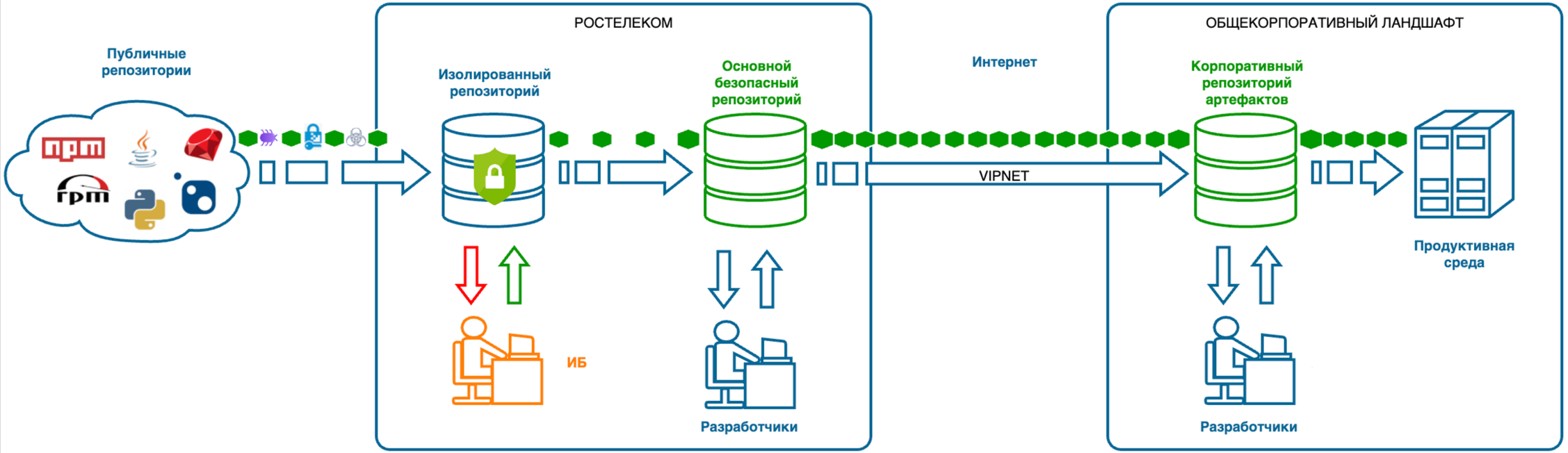
Все сложное – ‘под капотом’. Многоуровневое категорирование уязвимости.

Разработчику - светофор Можно/Можно с ограничениями/Нельзя





Доступ к артефактам репозитория Феникс для ИТ разработчиков ГК Ростелеком



Система работает на Российских сертификатах безопасности

Ростелеком

Кирилл Пихтовников

/ Ростелеком ИТ

Заместитель генерального директора по производству – технический директор
kirill.pikhtovnikov@rt.ru