


РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ.
БЕЗОПАСНЫЙ РЕПОЗИТОРИЙ РТК-ФЕНИКС


Редакция 1.0

2023г.

 Ростелеком <small>Информационные Технологии</small>	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 2 из 18


Оглавление

Глоссарий	3
1 Область применения	4
2 Назначение документа	4
3 Общая информация о системе	5
4 Вход в РЕПО «Феникс»	6
5 Описание интерфейса пользователя-разработчика	8
5.1 Основная страница «Артефакты»	8
5.2 Страница «Детали артефакта»	10
5.3 Страница «Все репозитории»	12
5.4 Страница «Статус артефакта»	13
5.5 Копирование данных формы	15
5.6 Обучение в интерфейсе	16
5.7 Глоссарий элементов интерфейса. Загрузка руководства	17
6 Сценарий проверки артефакта в репозитории	18

 Ростелеком Информационные Технологии	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 3 из 18

Глоссарий

Термин	Определение
Алерт	Угроза. Совокупность условий и факторов, создающих опасность безопасности артефакта.
Артефакт	Определённая версия пакета
Артефакт разрешённый	«Зелёный», безопасный артефакт. Артефакт, признанный безопасным для применения
Артефакт с ограничениями	«Жёлтый», обременённый. Артефакт, с уязвимостями. Такой артефакт возможно безопасно применять при выполнении дополнительных условий.
Артефакт запрещённый	«Красный». Артефакт, содержащий уязвимости, бекдоры, проявляющий вредоносное поведение. Применение такого артефакта не может быть безопасным.
Карантин	Двухнедельный срок, в течение которого запрошенный артефакт проходит проверку на наличие известных уязвимостей, заложенных бекдоров и вредоносность. В течение карантина сотрудниками ЦКиЗ выносится решение о допустимости применения артефакта.
Пакет	Совокупность всех версий одного артефакта
РЕПО «Феникс», Безопасный РЕПО	Безопасный репозиторий РТК-Феникс
ЦКиЗ	Центр кибербезопасности и защиты
MVP	Minimum Viable Product, «минимально жизнеспособный продукт» - самая ранняя версия продукта, у которой есть минимальный набор функций, достаточный для проверки на первых потребителях
JSON	JavaScript Object Notation - текстовый формат обмена данными, основанный на JavaScript


 Ростелеком <small>Информационные Технологии</small>	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 4 из 18

1 Область применения

Безопасный репозиторий РТК-Феникс - это программный комплекс, обеспечивающий возможность безопасного применения open-source библиотек. В данной информационной системе имеются такие функциональные модули, как хранение, проверка на уязвимости и предоставление данных об артефактах различных форматов (maven, rpm, deb, gpm, gem, npm, nuget); хранение и предоставление безопасных артефактов; графический web-интерфейс, средства управления артефактами. В безопасном репозитории предусмотрен алгоритм добавления и обработки текстового файла, содержащего url-списки артефактов, а также загрузки и установки на проверку ранее отсутствующих в Безопасном репозитории артефактов на основании полученного списка, мониторинг статуса, зоны и даты выхода из карантина по существующим и вновь загруженным артефактам.

2 Назначение документа

В данном документе представлено описание руководства пользователя РЕПО «Феникс».

	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 5 из 18

3 Общая информация о системе

Загруженный артефакт проходит проверку актуальных угроз безопасности информации в системе Мониторинга безопасности кода ЦКиЗ. Проверка артефакта на уязвимость выполняется в изолированном репозитории (зона карантина). После успешной проверки артефакт поступает в основной безопасный репозиторий (основная зона). Артефакт может быть взят в работу.

Условно артефакты разделяются на три цветовых статуса:

- *Зеленый* – артефакт безопасен. Может использоваться при разработке проекта;
- *Жёлтый* – артефакт имеет проблемы с безопасностью. Разрешен к использованию с ограничением. Артефакт находится в безопасной зоне репозитория. В комментарии к артефакту приведено описание уязвимости/ограничений использования. На основании анализа описания уязвимости/ограничений использования разработчик принимает решение либо о доработке устранения уязвимости, либо об использовании другого артефакта;
- *Красный* – артефакт заблокирован. Артефакт запрещен для разработки. Если артефакт уже используется в разработке, необходимо предпринять действия по выводу артефакта из разработки проекта. Если артефакт не используется при разработке, его использование запрещено.

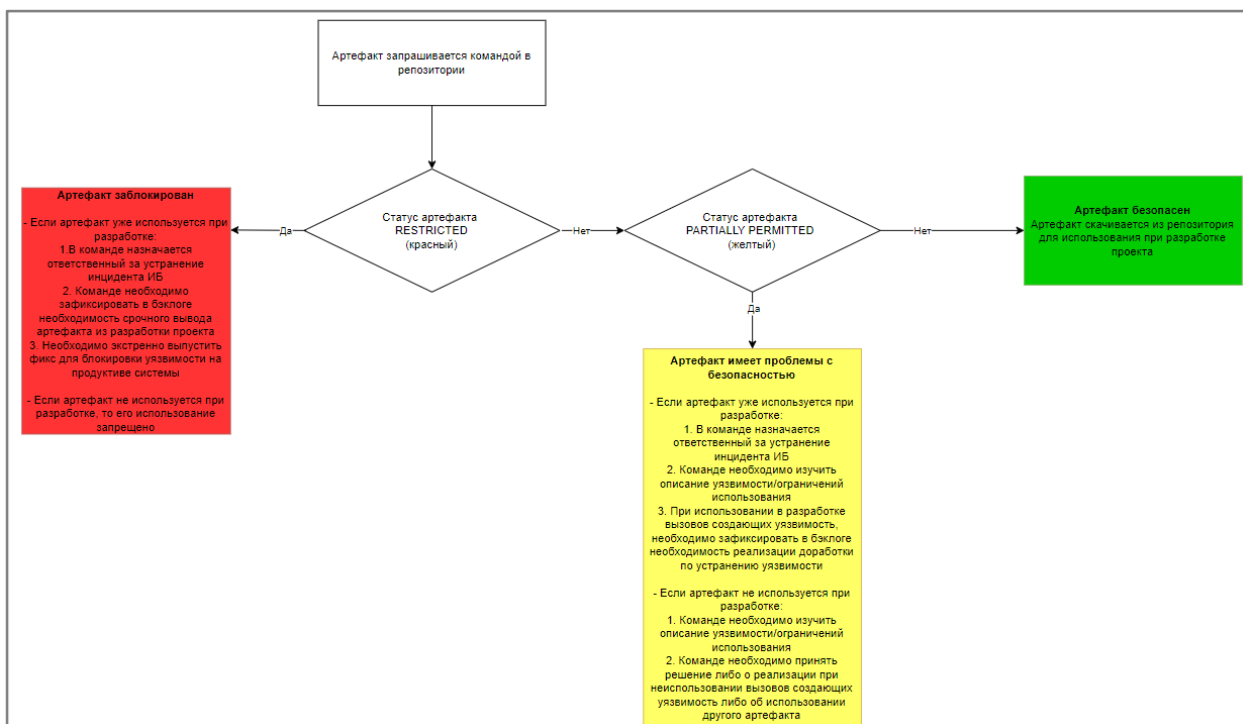



Рисунок 1 - Схема использования РЕПО разработчиком

	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 6 из 18

4 Вход в РЕПО «Феникс»

Интерфейс Безопасного РЕПО выполнен в виде страницы, открывающейся в отдельном окне web-браузера.

Для получения доступа к РЕПО «Феникс» необходимо открыть web-браузер, ввести в адресной строке URL-адрес стартовой страницы <https://repository.rt.ru/#/>.

Открывается окно *Артефакты* – форма для работы в Безопасном репозитории разработчиков ПО

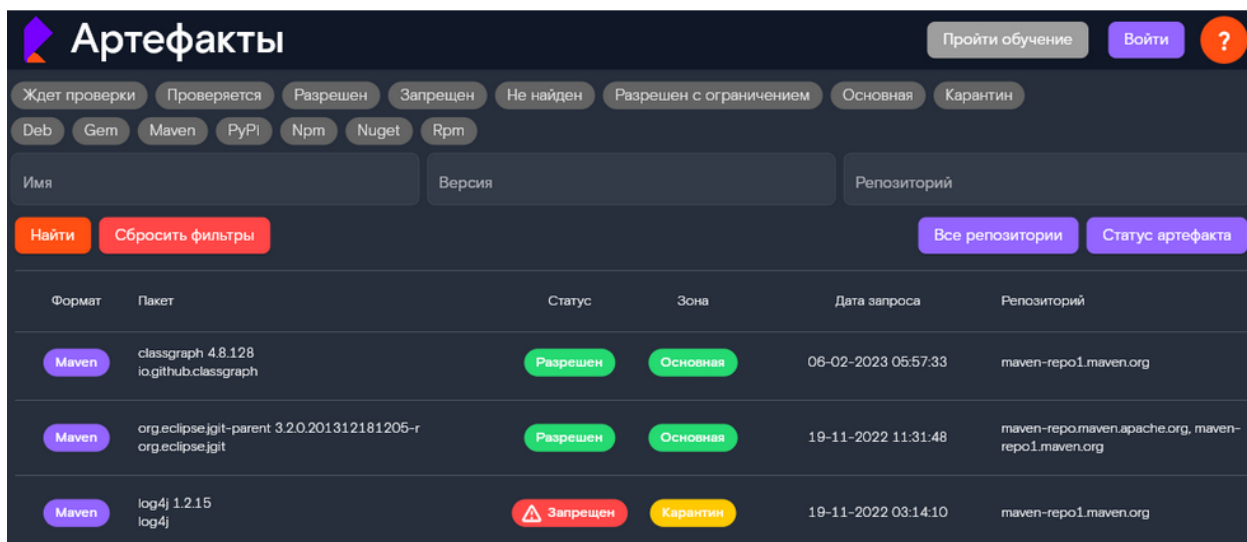

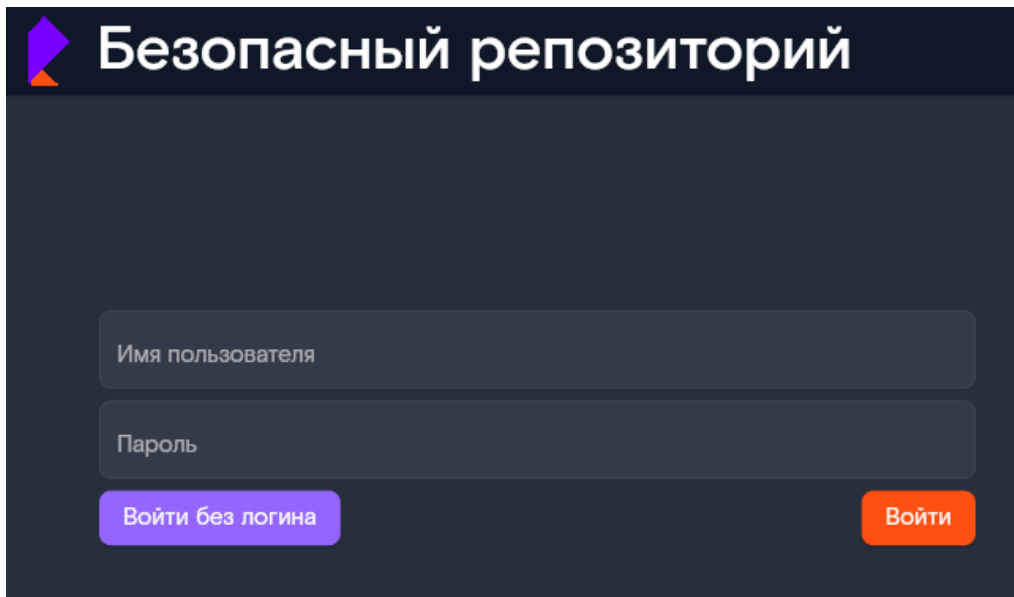


Рисунок 2 – Основной экран РТК-Феникс для разработчика ПО

Интерфейс Безопасного репозитория предназначен для работы как разработчиков ПО, так и сотрудников ЦКиЗ (кнопка **Войти**):

- *Войти без логина* - предназначен для разработчиков ПО, не предполагает заполнение полей *Имя пользователя* и *Пароль*. Разработчик для входа в систему нажимает кнопку *Войти без логина*;
- *Войти* – предназначен для сотрудников ЦКиЗ.
При успешном входе выполняется переход на главную страницу РЕПО – Артефакты.

 Ростелеком <small>Информационные Технологии</small>	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 7 из 18



Безопасный репозиторий

Имя пользователя

Пароль

Войти без логина

Войти

Рисунок 3 – Окно входа пользователя

5 Описание интерфейса пользователя-разработчика

5.1 Основная страница «Артефакты»

Форма **Артефакты** доступна только в режиме просмотра, она информирует разработчика о состоянии (статусе) интересующего его артефакта. Артефакты отсортированы по полю *Дата запроса*.

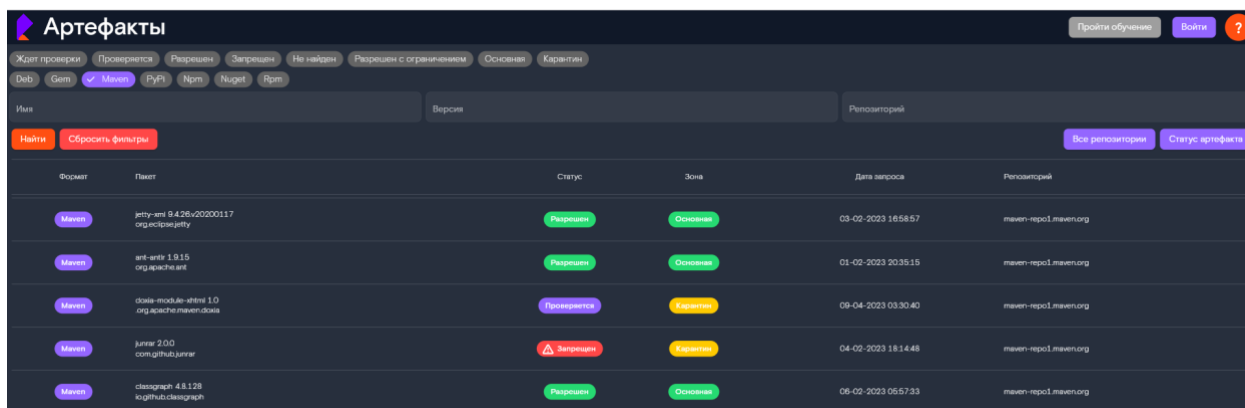


Рисунок 4 – Страница с артефактами

Вкладка *Артефакты* содержит следующие рабочие компоненты:

- 1) *Строка заголовка*. Строка расположена в верхней части окна. В ней сообщается имя открытого приложения, сервисные операции.
- 2) *Параметры поиска*. Параметры поиска представлены набором кнопок-чипсов, отвечающих за формат, статус и зону расположения артефакта. Возможно выбрать одновременно несколько чипсов. Выбранные значения параметров меняют цвет на сиреневый. Повторный выбор снимает выделение.
- 3) *Строка поиска*. Кроме задания в качестве параметров поиска *формата*, *статуса*, *зоны*, допускается произвольный поиск артефакта. Поиск организован в виде текстовых полей: *Имя* (наименование пакета), *Версия* (версия пакета), *Репозиторий* (наименование репозитория). Поиск по полям *Имя*, *Репозиторий* регистронезависимый, по полю *Версия* – регистрозависимый.
- 4) *Операции вкладки*
 - *Найти* – или кнопка *Enter*, нажатая в строке поиска, запускает процесс фильтрации;
 - *Сбросить фильтры* - очищается строка поиска (*Имя*, *Версия*, *Репозиторий*), снимается выделения с чипсов, обновляются данные страницы;
 - *Все репозитории* - открывается страница, на которой представлены веб-ссылки используемых репозиториях. Репозитории сгруппированы по форматам: Deb, Gem, Maven, PyPi, Npm, Nuget, Rpm;
 - *Статус артефакта* – операция позволяет определить статус артефакта, зону и продолжительность нахождения артефакта в зоне карантина и постановку на проверку ранее отсутствующего в Безопасном репозитории артефакта
- 5) *Таблица данных*. Список артефактов


	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 9 из 18







Таблица артефактов представлена графами:


- *Формат* – тип артефакта;
- *Пакет* – составное поле, содержит *Наименование* и *Версию пакета* через пробел.

У форматов есть свои специфичные атрибуты, необходимые для однозначного определения артефакта:

- **Deb**: path, architecture, distributive
- **Gem**: platform
- **Maven**: group
- **Npm**: scope
- **PyPi**: buildInfo
- **Rpm**: path, architecture, distributive, packageRelease
- **Nuget**: -----

Специфические атрибуты артефакта отображаются в графе *Пакет* и в детальной информации по артефакту


-  libxcb-glx0 1.14-2 amd64
ubuntu:20.04 - Пакет Версия Архитектура / Дистрибутив
-  google-protobuf 3.20.0
x86_64-darwin - Пакет Версия / Платформа
-  fontbox 2.0.16
org.apache.pdfbox - Пакет Версия / Группа
-  cryptography 35.0.0
cp36-abi3-win_amd64 - Пакет Версия / buildInfo
-  preset-env 7.7.6
@babel - Пакет Версия / Score
-  zlib 1.2.11 i686
12.el7
redos:7.3 - Пакет Версия Архитектура/Релиз/Дистрибутив
- *Статус* - статус артефакта. Допустимые состояния статуса:
- *Ждет проверки* - не взят в работу ЦКиЗ;
- *Проверяется* – взят в работу ЦКиЗ;
- *Не найден* – артефакт не обнаружен в репозитории;

 Ростелеком Информационные Технологии	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 10 из 18

- *Разрешен с ограничением* - по артефакту обнаружена уязвимость. Такой артефакт возможно безопасно применять при выполнении дополнительных условий;
- *Разрешен* – артефакт может быть взят в работу;
- *Запрещен* - обнаружены угрозы;
- *Зона* - зона размещения артефакта, каждая из зон имеет свою цветовую раскраску:
- **Основная** – артефакт находится в основном безопасном репозитории, артефакт можно использовать в работе;
- **Карантин** – артефакт либо не прошел контроль на безопасность, либо находится на проверке, время карантина 14 дней не истекло. Артефакт находится в изолированном репозитории.
- *Дата запроса* – дата размещения артефакта в репозитории;
- *Репозиторий* – наименование репозитория артефакта

5.2 Страница «Детали артефакта»

По клику левой клавише мыши на текущем артефакте выполняется переход на форму *Детали артефакта*. Форма *Детали артефакта* (см. Рисунок 5) содержит полную информацию об артефакте: специфические атрибуты артефакта, дата выхода из карантина, наличие угроз и их количество, описание уязвимости и пути ее обхода, статус, зону размещения.

	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 11 из 18

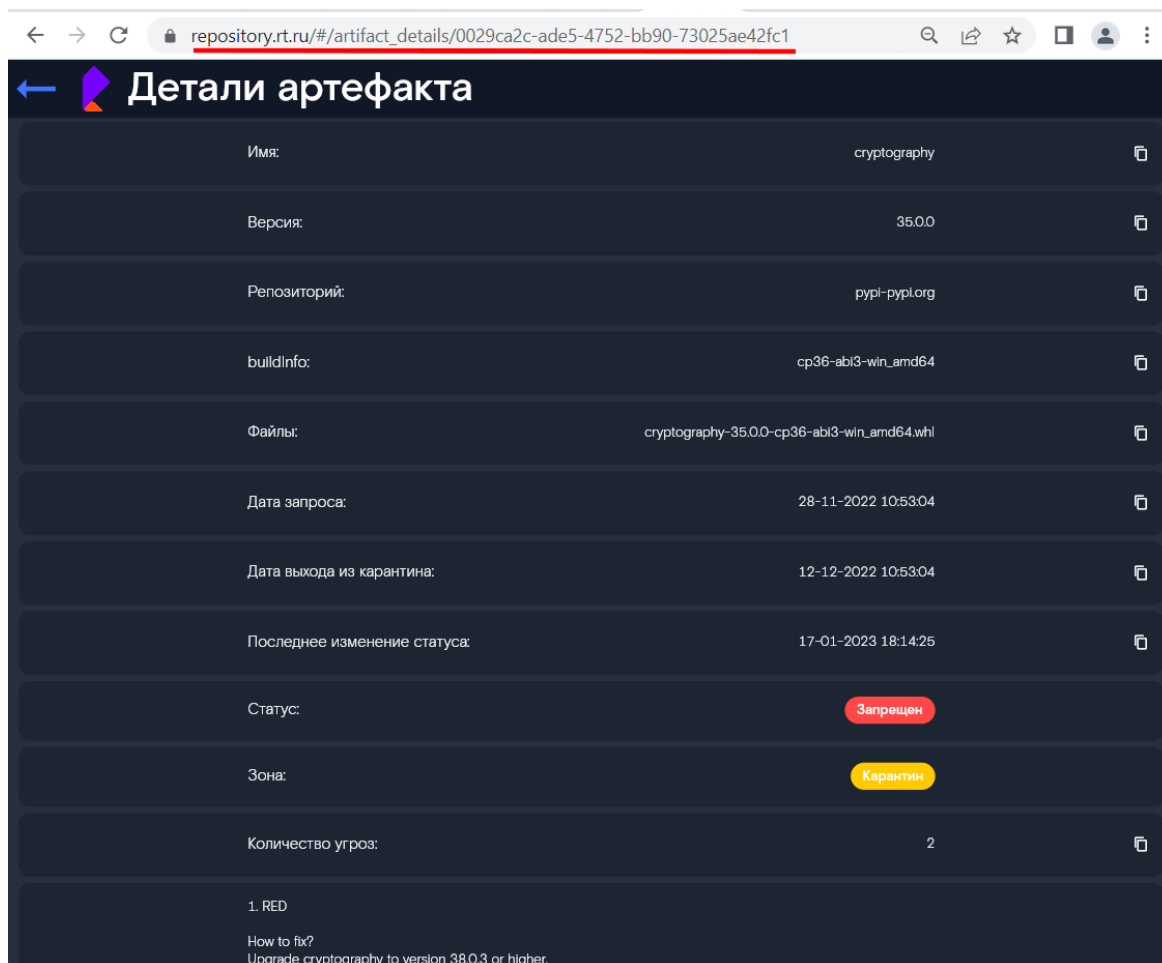


Рисунок 5 – Окно Детали артефакта

Каждая страничка *Детали артефакта* имеет свое уникальное название, которое отображается в адресной строке web-браузера, например: https://repository.rt.ru/#/artifact_details/0029ca2c-ade5-4752-bb90-73025ae42fc1

Отличительным признаком страницы *Детали артефакта*, в ее наименовании, является текст - «*artifact_details*» и ID артефакта - *0029ca2c-ade5-4752-bb90-73025ae42fc1*.

Обратите внимание! Не во всех web-браузерах отображают полное наименование страницы в адресной строке.

Например, в браузер Yandex отображается наименование загрузочной страницы см. Рисунок 6.

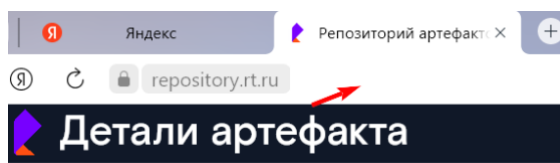



Рисунок 6 – Адресная строка web-браузера Yandex

	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 12 из 18

Для того чтобы увидеть уникальное наименование страницы *Детали артефакта* достаточно кликнуть левой клавишей мыши в пустое пространство адресной строки см. Рисунок 7.



Рисунок 7 – Адресная строка web-браузера Yandex. Полное наименование страницы Детали артефакта


5.3 Страница «Все репозитории»

Операция доступна на вкладке Артефакты. После нажатия [Все репозитории](#) открывается страница, на которой представлены используемые репозитории.

Репозитории сгруппированы по форматам. По мере добавления форматов/репозиториях список репозиториях актуализируется.

Страница Все репозитории имеет уникальное название, которое отображается в адресной строке web-браузера <https://repository.rt.ru/#/repositories>.

Ссылку можно использовать для быстрого перехода на страницу в новом окне web-браузера.

	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 13 из 18

5.4 Страница «Статус артефакта»

При нажатии на кнопку *Статус артефакта* открывается информационное окно *Загрузка артефактов* см. Рисунок 8.

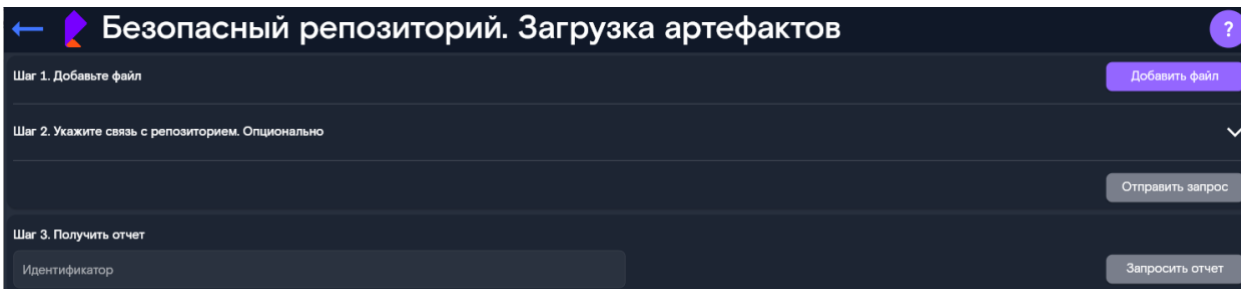

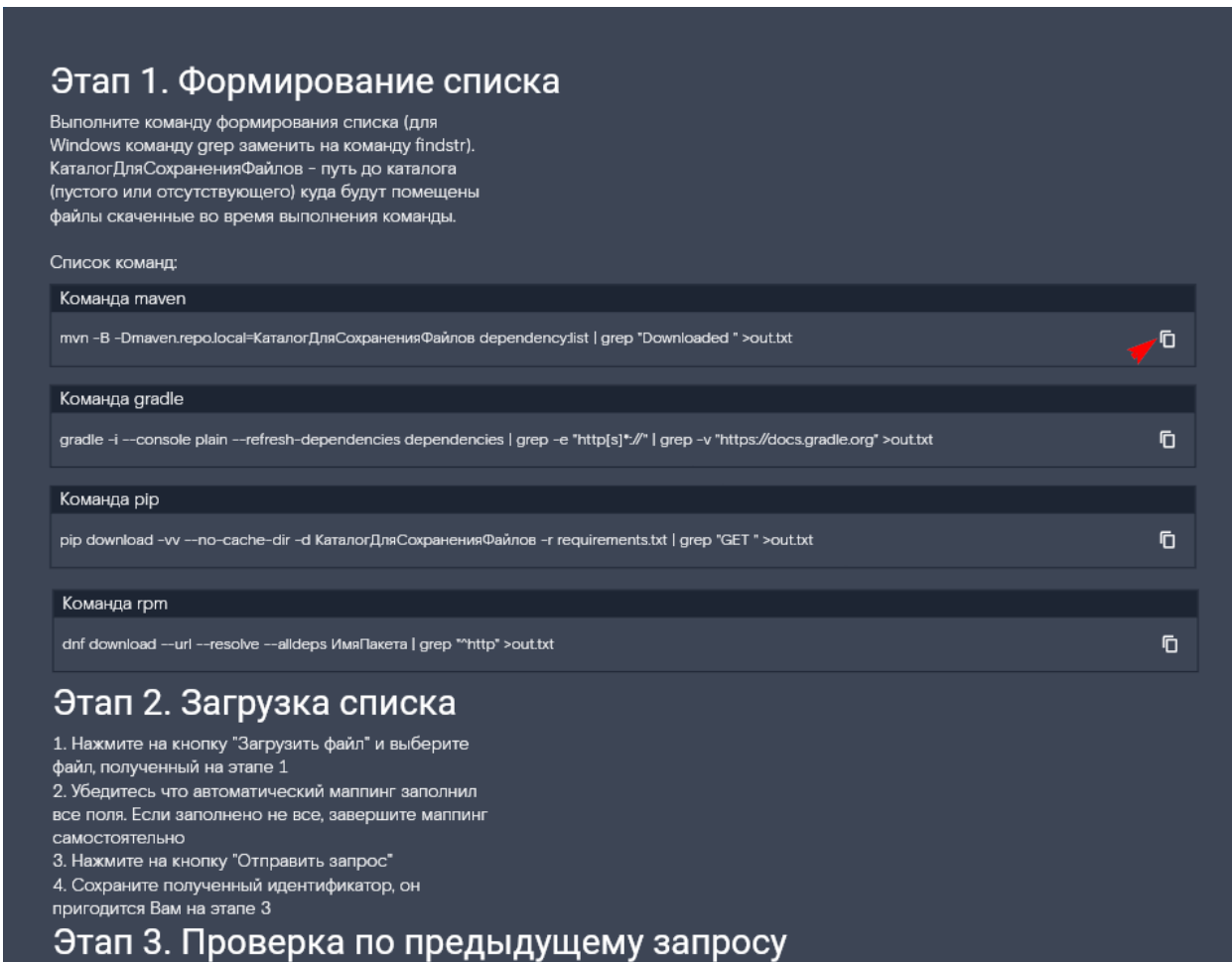


Рисунок 8 – Окно операции Загрузка артефактов

В строке заголовка формы расположена пиктограмма , при нажатии на которую, отображается информационное окно, содержащее этапы операции (см. Рисунок 9).



Этап 1. Формирование списка

Выполните команду формирования списка (для Windows команду `grep` заменить на команду `findstr`). КаталогДляСохраненияФайлов - путь до каталога (пустого или отсутствующего) куда будут помещены файлы скаченные во время выполнения команды.

Список команд:

Команда maven

```
mvn -B -Dmaven.repo.local=КаталогДляСохраненияФайлов dependencylist | grep "Downloaded " >out.txt
```

Команда gradle

```
gradle -i --console plain --refresh-dependencies dependencies | grep -e "http[s]?://" | grep -v "https://docs.gradle.org" >out.txt
```

Команда pip

```
pip download -vv --no-cache-dir -d КаталогДляСохраненияФайлов -r requirements.txt | grep "GET " >out.txt
```

Команда gpm


```
dnf download --url --resolve --alldeps ИмяПакета | grep "http" >out.txt
```

Этап 2. Загрузка списка

1. Нажмите на кнопку "Загрузить файл" и выберите файл, полученный на этапе 1
2. Убедитесь что автоматический маппинг заполнил все поля. Если заполнено не все, завершите маппинг самостоятельно
3. Нажмите на кнопку "Отправить запрос"
4. Сохраните полученный идентификатор, он пригодится Вам на этапе 3


Этап 3. Проверка по предыдущему запросу

Рисунок 9 – Информационное окно операции Статус артефакта

	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 14 из 18

Этап 1 – формирование списка. Формирование текстового файла с url-списком артефактов по проекту.

Текстовый файл формируется вне интерфейса Безопасный РЕПО. Пользователь выполняет команду формирования файла со списком url. В момент выполнения команд программное обеспечение, которое используется для выполнения команд (пакетные менеджеры, инструменты сборки), должно быть настроено на публичные репозитории, а не на Безопасный репозиторий

Команды для поддерживаемых форматов описаны в данном информационном окне этапов загрузки артефактов. Каждая команда информационного окна снабжена пиктограммой  - копирование команды в буфер обмена.

Этап 2 – загрузка списка. Загрузка подготовленного на 1-ом этапе текстового файла с url-списком.

При актуализации кнопки *Добавить файл* выводится диалоговое окно для выбора файла. Необходимо выбрать файл, подготовленный на Этапе 1. После успешной загрузки файла автоматически формируется маппинг репозиторий: левая сторона таблицы сопоставлений соответствует репозиториям Феникс, правая - репозиториям пользователя из файла. Если маппинг выполнен частично, - не удалось сопоставить репозиторию пользователя из списка репозиторий Феникс, - возможно выбрать репозиторий из списка безопасных репозиторий вручную. Если маппинг не указан, то строки, для которых не найден репозиторий, не будут поставлены на проверку, записи об этих строках отображаются в отчете о загрузке в разделе ошибок загрузки.

Обратите внимание! Для формата deb маппинг должен быть указан обязательно, даже при использовании публичного репозитория.

Отправить запрос – это завершающая операция Этапа 2. В ходе исполнения операции *Отправить запрос*:


- формируется идентификатор запроса, однозначно идентифицирующий загруженный файл (последний сгенерированный идентификатор запроса сохраняется и отображается при открытии формы операции *Статус артефакта*);
- выводится информация о количестве строк в обработке;
- выводятся список строки файла с неизвестным репозиторием

Этап 3 – получить отчет. Формирование отчета по статусам артефактов загруженного файла.

В результате исполнения операции *Запросить отчет* формируется файл предварительно выбранного формата (pdf/csv).

По артефактам в отчете представлена информация о статусе, зоне размещения, времени выхода из карантина, специфических атрибутах.

Новые артефакты ставятся в очередь на загрузку через механизм task. Время выполнения task может быть продолжительным и зависит от количества артефактов,

	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 15 из 18

скорости обработки. Поэтому новые артефакты могут отображаться в интерфейсе с задержкой по времени.

Рекомендуется выдерживать интервал времени между операциями *Отправить запрос* и *Запросить отчет* порядка минуты.

Пользователь может повторно запросить отчет по существующим и вновь загруженным артефактам с целью мониторинга статуса, зоны и даты выхода из карантина. Для этого достаточно сохраненный идентификатор запроса указать в одноименном поле без загрузки исходного текстового файла.

Обратите внимание! Вновь загруженные в Безопасный репозиторий артефакты находятся на проверке в карантинной зоне, время карантина 14 дней.

Дальнейшая работа происходит в привычном для команд процессе сборки проектов. Достаточно просто перенастроить среду разработки на использование безопасного репозитория. РТК-Феникс не позволит собрать проект, если среди зависимостей проекта имеются запрещенные артефакты. Замените запрещенные артефакты на разрешенную версию, сборка выполнится успешно.

5.5 Копирование данных формы

Чтобы скопировать любой элемент на форме *Артефакты/Детали артефакта / Все репозитории* необходимо подвести указатель мыши к выбранной точке, затем нажать левую кнопку и тянуть мышь до выделения нужного фрагмента (см. Рисунок 10). Скопировать значение в буфер обмена любым возможным способом (Копировать, Ctrl+C)

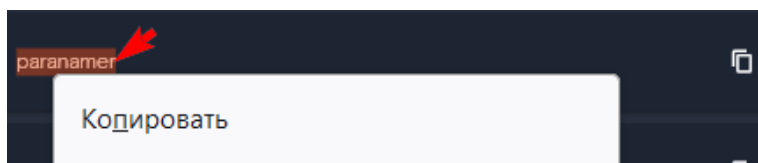



Рисунок 10 – Операция Копировать элемент формы

На форме *Детали артефакта/ Все репозитории* для быстрого копирования элемента формы предусмотрена пиктограмма  см.Рисунок 11.

	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 16 из 18

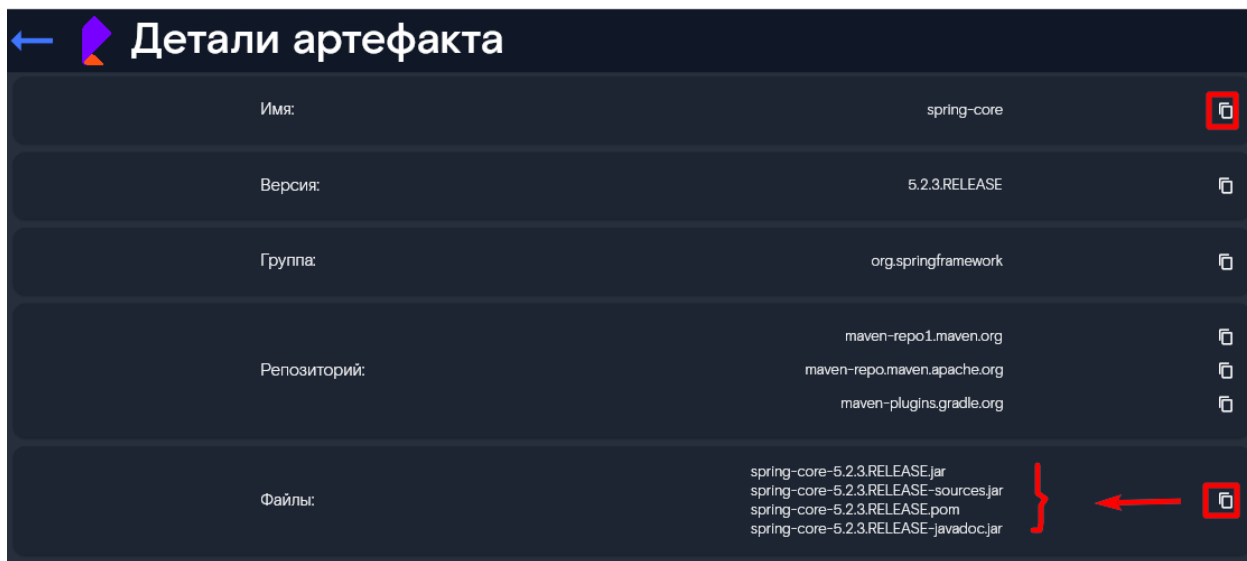



Рисунок 11 – Операция быстрого копирования элемента

Обратите внимание! на форме *Детали артефакта* пиктограмма относится к каждому копируемому элементу, для элемента *Файлы* с помощью пиктограммы  будут скопированы сразу все файлы.


5.6 Обучение в интерфейсе

При нажатии на кнопку *Пройти обучение* запускается автоматическая депо-версия по значимым полям и операциям формы.


Последовательность перехода по полям формы задается автоматически: Информация → Поле поиска → Таблица артефактов → операция *Статус артефакта* → операция *Все репозитории*.

Экран темнеет, выделяется конкретный элемент интерфейса, появляется текст, описывающий, что выполняет этот элемент в Системе. Система останавливается на элементе формы, для дальнейшего продвижения достаточно кликнуть по любому полю формы левой клавишей мыши.

В любой момент можно завершить демонстрационное обучение, нажав кнопку *Пропустить обучение*.

	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 17 из 18

5.7 Глоссарий элементов интерфейса. Загрузка руководства

В строке заголовка, которая расположена в верхней части окна *Артефакты* расположена пиктограмма , при нажатии на которую, открывается информационное окно (см. Рисунок 12), содержащее обозначения, принятые в репозитории. По кнопке *Скачать руководство* можно загрузить руководство пользователя РТК-Феникс.

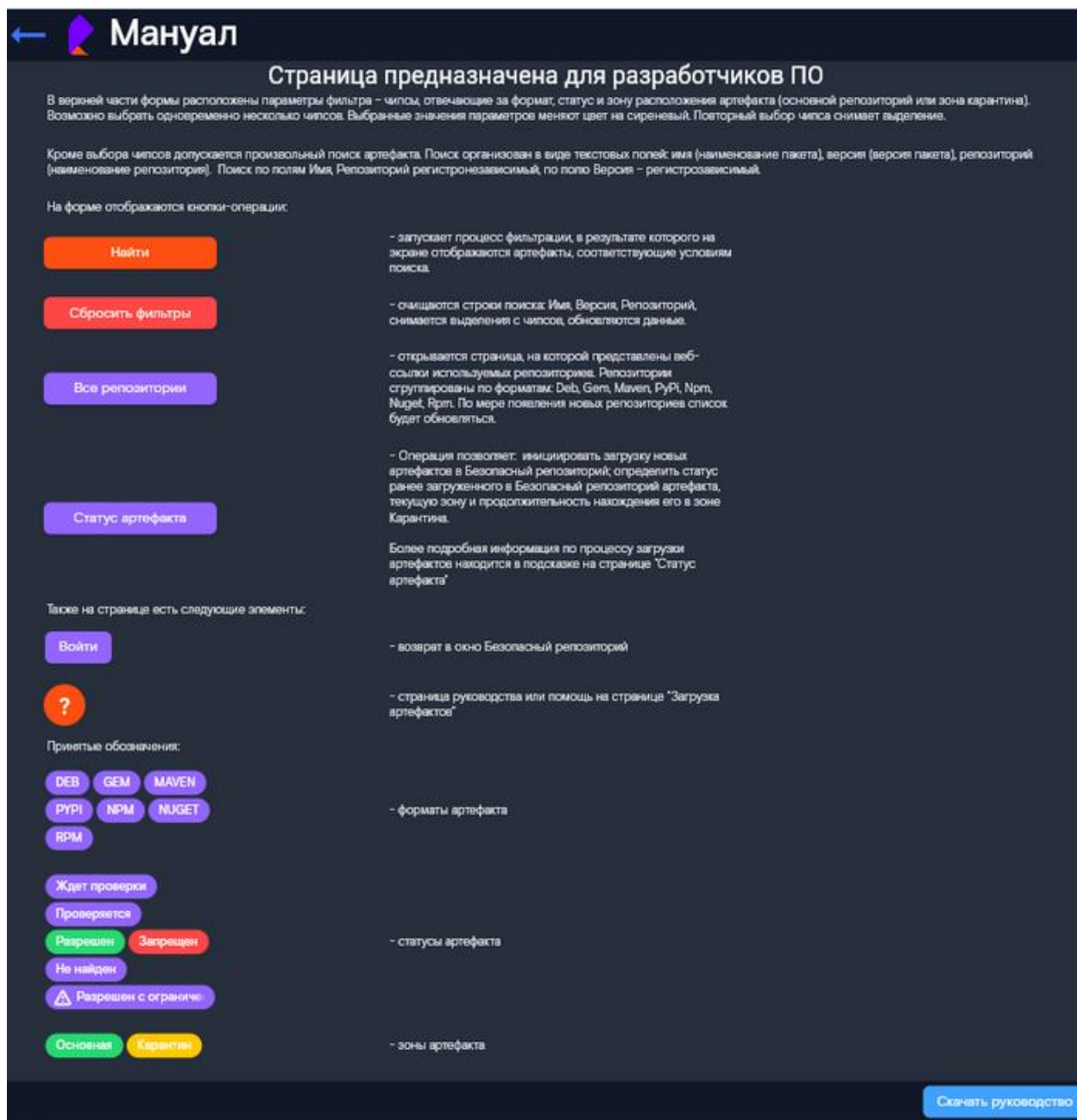



Рисунок 12 – Информационное окно обозначений

 Ростелеком Информационные Технологии	Руководство пользователя. Безопасный репозиторий РТК-Феникс	
	Версия 1.2	Стр. 18 из 18

6 Сценарий проверки артефакта в репозитории

Сценарий проверки артефакта в репозитории РЕПО «Феникс» описан в Руководстве администратора.