SORCA

Комплексный анализ происхождения и рисков программного обеспечения

Руководство администратора и пользователя

Версия 0.3.4-beta

(Листов – 41)

ООО «СОРКА»
Москва
2026

Содержание

1 Основные характеристики

1.1 Назначение программы

Программное обеспечение «SORCA» (далее – SORCA) разработано с целью автоматизации процесса композиционного анализа программного обеспечения, выявления заимствованных компонентов, уязвимостей, секретов и формирования отчётных материалов по результатам анализа.

SORCA предназначено для:

- автоматизированного анализа исходных текстов программного обеспечения, архивов с исходными текстами, репозиториев и SBOM-файлов;
- автоматизированного формирования перечня компонентов программного обеспечения с указанием наименований, версий, экосистем, типов зависимостей и областей применения;
- выявления компонентов с открытым исходным кодом и сопоставления компонентов со ссылками на репозитории или архивы исходных текстов;
- расчёта контрольных сумм архивов исходных текстов компонентов;
- анализа зависимостей компонентов, включая прямые и транзитивные зависимости, с учётом анализа и данных пакетных менеджеров;
- выявления уязвимостей компонентов программного обеспечения по BDU, NVD, GHSA и др.;
- сопоставления уязвимостей с компонентами и их версиями;
- отображения уязвимостей по уровням критичности с возможностью фильтрации, сортировки, разметки статусов и добавления экспертных комментариев;
- поиска секретов, ключей, паролей, токенов и иных чувствительных данных в анализируемых исходных текстах;
- разметки найденных секретов по статусам с сохранением экспертных комментариев;
- определения языков программирования компонентов по репозиториям и архивам исходных текстов;
- формирования и хранения структуры проектов и подпроектов с наследованием настроек анализа;
- запуска анализа отдельных проектов, подпроектов и групп подпроектов в том числе повторного анализа с переносом ранее выполненной экспертной разметки, где это применимо;
- ведения общего справочника компонентов и связанных с ними репозиториев или архивов исходных текстов;
- исключения компонентов из состава учитываемого SBOM по ручной разметке или на основании шаблонов фильтрации;
- формирования списков доверенных компонентов с указанием источника поставки;
- разметки компонентов по признакам поверхности атаки и функций безопасности;
- формирования SBOM в формате CycloneDX, включая SBOM по требованиям ФСТЭК России;
- импорта SBOM и результатов анализа с сохранением состава компонентов, уязвимостей, секретов, ссылок на исходные тексты и экспертной разметки;
- формирования HTML, PDF, CSV, XLSX и JSON отчётов по уязвимостям, секретам, компонентам и SBOM;

- настройки состава экспортируемых отчётов с учётом фильтров по уязвимостям, компонентам и секретам;
- формирования сводных представлений по проектам, подпроектам, запускам, компонентам, уязвимостям и секретам.

1.2 Условия выполнения программы

SORCA предназначено для использования на технических средствах под управлением операционных систем семейства Linux и Windows, обеспечивающих запуск контейнеров Docker. Рекомендуемой средой эксплуатации является Linux x64, в том числе Astra Linux Special Edition.

Серверная часть поставляется и эксплуатируется в контейнере Docker. Для корректной работы требуется поддержка архитектуры x64.

Веб-интерфейс доступен через браузер и может использоваться с любого устройства, имеющего доступ к серверу. Для работы с веб-интерфейсом на клиентском устройстве достаточно современного браузера.

Применение ПО рассчитано на персонал, имеющий опыт работы с анализом состава программного обеспечения, управлением проектами анализа, интерпретацией сведений об уязвимостях, SBOM и результатах проверки исходных текстов.

1.3 Среда функционирования

Минимальные характеристики технических средств, для функционирования программного обеспечения представлены в таблице 1.

Таблица 1 – Минимальные характеристики технических средств для развёртывания сервера

Параметр	Значение
Процессор	архитектура x64
Оперативная память	16 ГБ
Хранилище (SSD)	100 ГБ
Система контейнеризации	Docker

Рекомендуемые характеристики технических средств, для функционирования программного обеспечения представлены в таблице 2.

Таблица 2 – Рекомендуемые характеристики технических средств для развёртывания сервера

Параметр	Значение
Процессор	архитектура x64, 3.7 ГГц и выше
Оперативная память	64 ГБ
Хранилище (SSD NVMe)	600 ГБ
Система контейнеризации	Docker

Для работы пользователей с веб-интерфейсом SORCA достаточно любого технического средства, имеющего сетевой доступ к серверу и установленный современный веб-браузер. Специальные требования к процессору, объёму оперативной памяти и хранилищу клиентского устройства не предъявляются.

2 Развёртывание

Развёртывание выполняется на сервере с установленной и настроенной контейнерной средой Docker. Перед установкой необходимо убедиться, что техническое средство соответствует минимальным требованиям, имеет доступ к образу в реестре контейнеров и располагает достаточным объёмом свободного дискового пространства для хранения базы данных, рабочих каталогов анализа, кэша и отчётных материалов.

Поставка включает контейнерный образ программного обеспечения, файл конфигурации окружения, файл описания сервисов Docker Compose, скрипт первичной инициализации и файл лицензии. В конфигурации задаются параметры запуска контейнера, порт веб-интерфейса, имена томов Docker, параметры подключения к встроенной базе данных, путь к лицензии и иные эксплуатационные настройки, в том числе логин и пароль первого пользователя в системе.

Для развёртывания необходимо выполнить перечисленные ниже действия.

1 Установить Docker и Docker Compose на сервере развёртывания.
2 Получить контейнерный образ SORCA из реестра контейнеров.
3 Подготовить файл конфигурации окружения .env.
4 Запустить сервис SORCA с использованием Docker Compose.
5 Выполнить скрипт «init» для первичной инициализации ПО.
6 Проверить состояние контейнера и доступность веб-интерфейса.
7 Перейти в веб-интерфейс SORCA через браузер по адресу сервера и указанному порту.
8 Выполнить первичную настройку: загрузить лицензию, проверить параметры анализа, состояние баз уязвимостей и учётные записи пользователей.

Данные должны храниться в постоянных Docker-томах. К таким данным относятся база данных, лицензия, рабочие файлы анализов, кэш анализатора, локальные базы уязвимостей и служебные материалы. При обновлении версии контейнер может быть заменён, однако постоянные тома должны сохраняться, так как в них содержатся пользовательские проекты, результаты анализов и настройки системы.

После запуска – веб-интерфейс доступен пользователям с клиентских устройств через современный браузер при наличии сетевого доступа к серверу.

Пример команд для развёртывания:

```
docker pull qwer.sorca.ru/sorca:0.3.4-beta
docker compose --env-file .env up -d
chmod +x ./init.sh
./init.sh (.\init.ps1 – для windows)
```

Пример команд для обновления установленного ПО:

```
docker pull qwer.sorca.ru/sorca:0.3.4-beta
docker stop sorca
docker rm sorca
# поменять версию ПО в .env
docker compose --env-file .env up -d
```

После успешного обновления и проверки, можно удалить docker образ с устаревшей версией ПО.

ВНИМАНИЕ! Не удаляйте .env файл, полученный для развёртывания ПО.

3 Веб-интерфейс

3.1 Начало работы

Перед началом работы необходимо авторизоваться в веб-интерфейсе SORCA (рисунок 1) по заданному URL (URL по умолчанию – localhost:18080), используя учетные данные администратора, содержащиеся в полученном .env файле в ключах ADMIN_NAME и ADMIN_PASS.

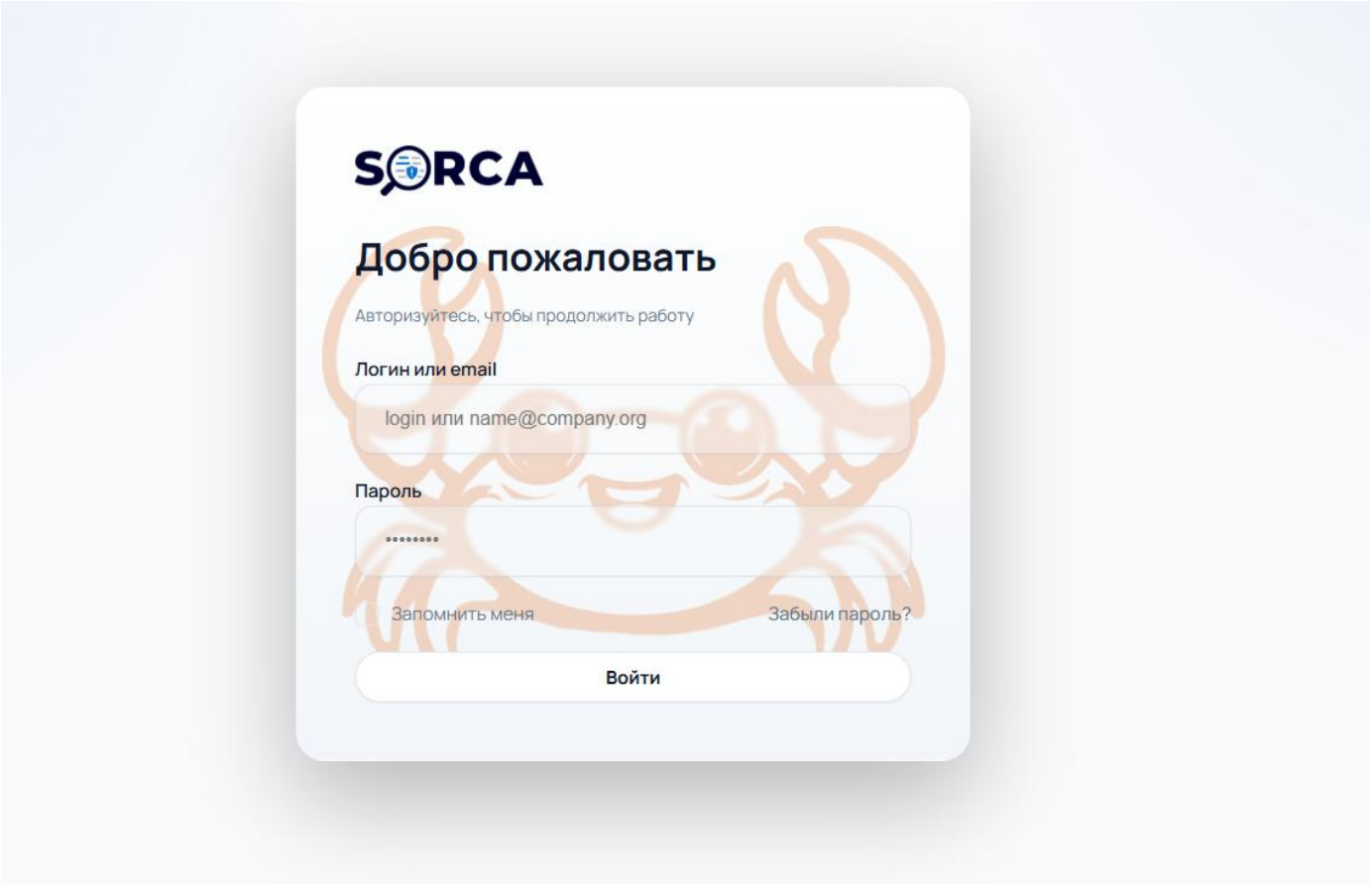

Рисунок 1 – Поле авторизации

Далее следует перейти во вкладку «Параметры» – «Лицензия» (рисунок 2) и загрузить полученный файл лицензии, после чего функции SORCA станут доступны.

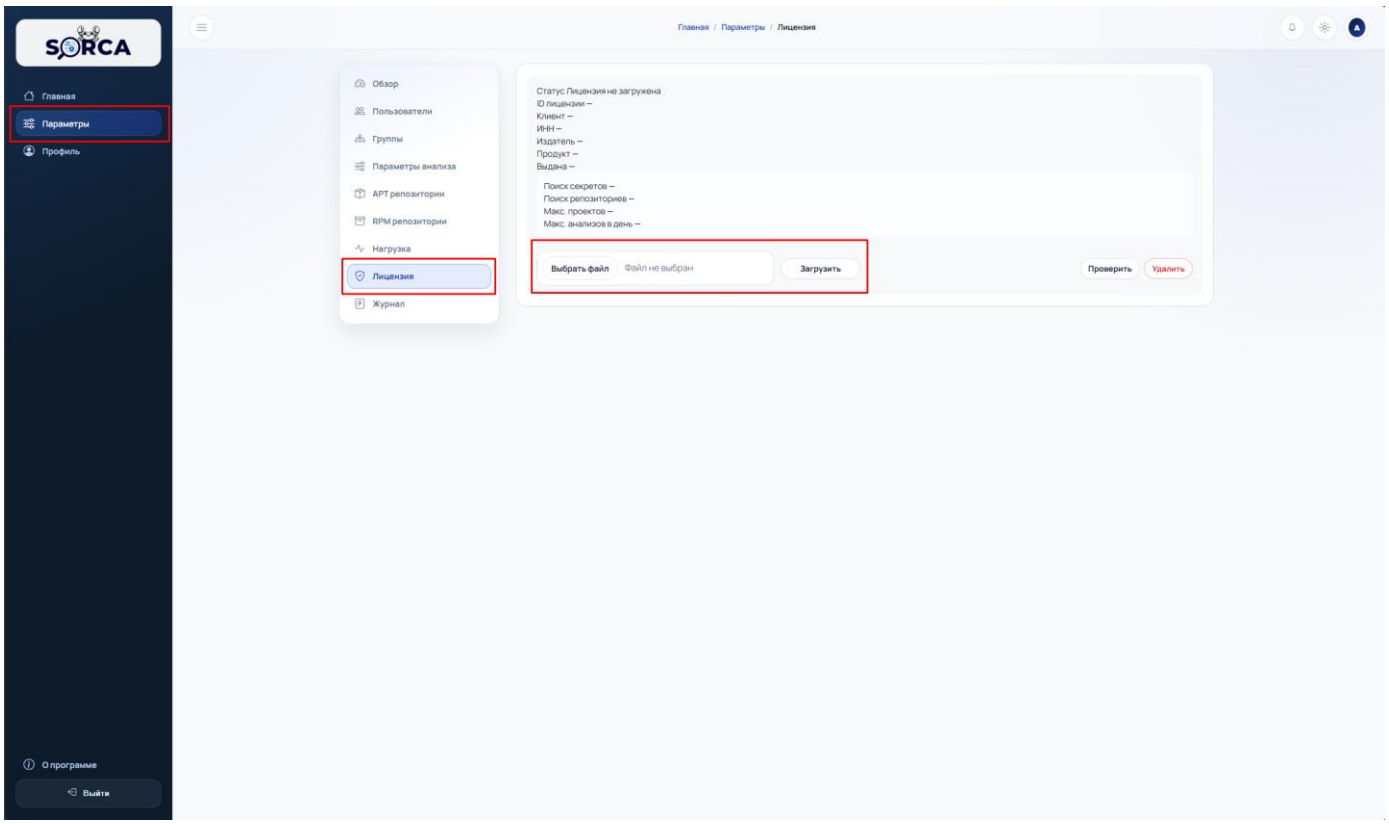

Рисунок 2 – Добавление лицензии

3.2 Вкладка «Главная»

Данная вкладка содержит общую информацию по приложению и проведенным анализом доступных проектов (рисунок 3):

- общее количество активных проектов (подпроектов);
- общее количество запусков проектов (подпроектов);
- общее количество найденных заимствованных компонентов в активных проектах (подпроектах);
- общее количество найденных уязвимостей в активных проектах (подпроектах);
- сводка по анализам:
  - количество выявленных критических и высоких уязвимостей без разметки;
  - общее количество уязвимостей без разметки;
  - количество секретов без разметки;
  - количество ошибок анализов за последние 7 дней;
- статус актуальности базы уязвимостей;
- срок действия лицензии;
- список последних созданных проектов;
- список наиболее частых выявленных уязвимостей;
- график с распределением по языкам активных проектов (подпроектов);
- график с распределением по лицензиям активных проектов (подпроектов).

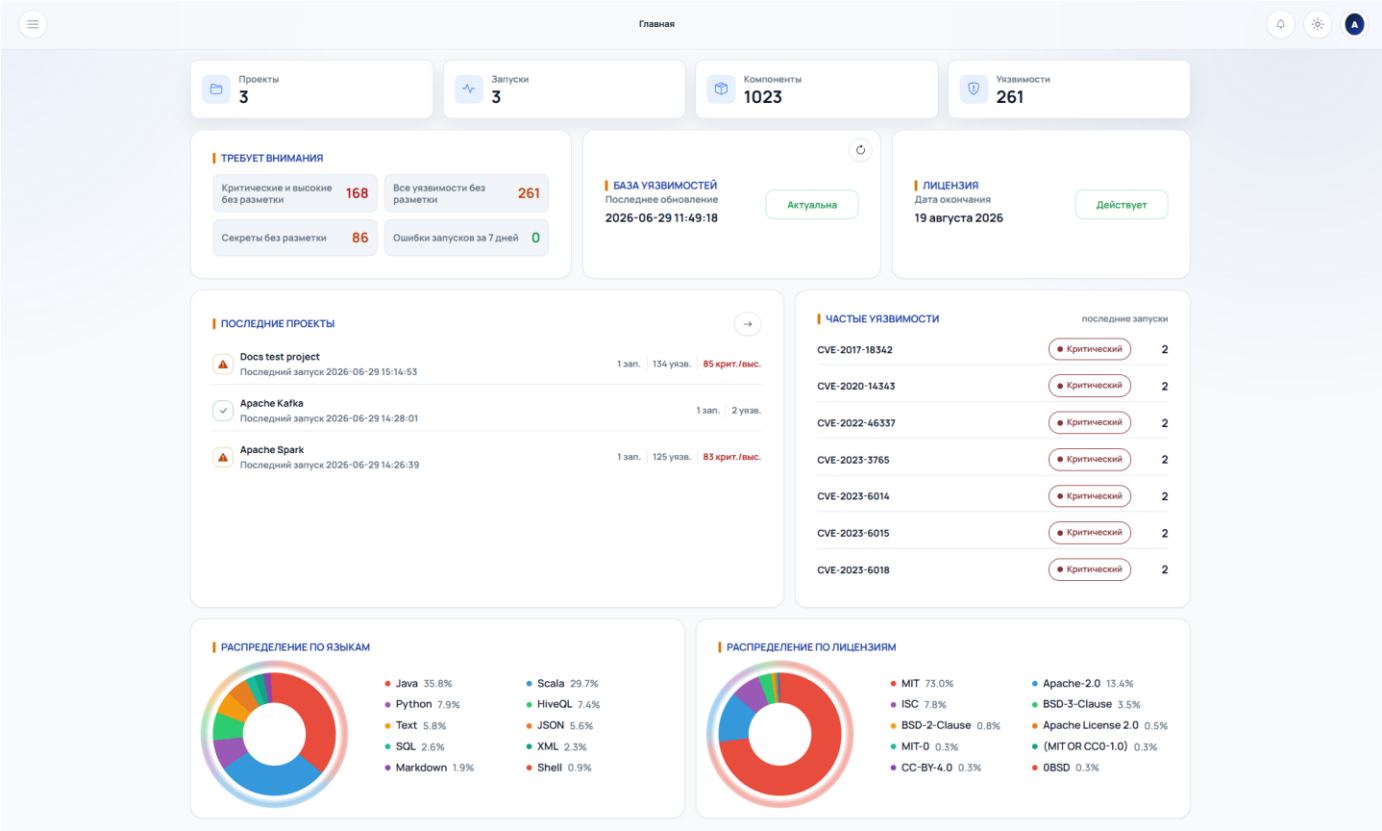

Рисунок 3 – Вкладка «Главная»

3.3 Вкладка «Проекты»

3.3.1 Создание и настройка проекта

По нажатии кнопки «Создать проект» открывается модальное окно, позволяющее произвести предварительную настройку проекта.

Окно содержит следующие настройки:

– Вкладка «Проект» (рисунок 4):
  – поле «Название проекта» – при вводе названия в первую строку поля создается проект, при вводе названия в строки 2–n создаются подпроекты проекта из первой строки;
  – выпадающий список «Родительский проект» – позволяет присвоить создаваемому проекту уже существующий «родительский» проект;
  – выпадающий список «Подпроекты» – позволяет присвоить создаваемому проекту уже существующий подпроект.

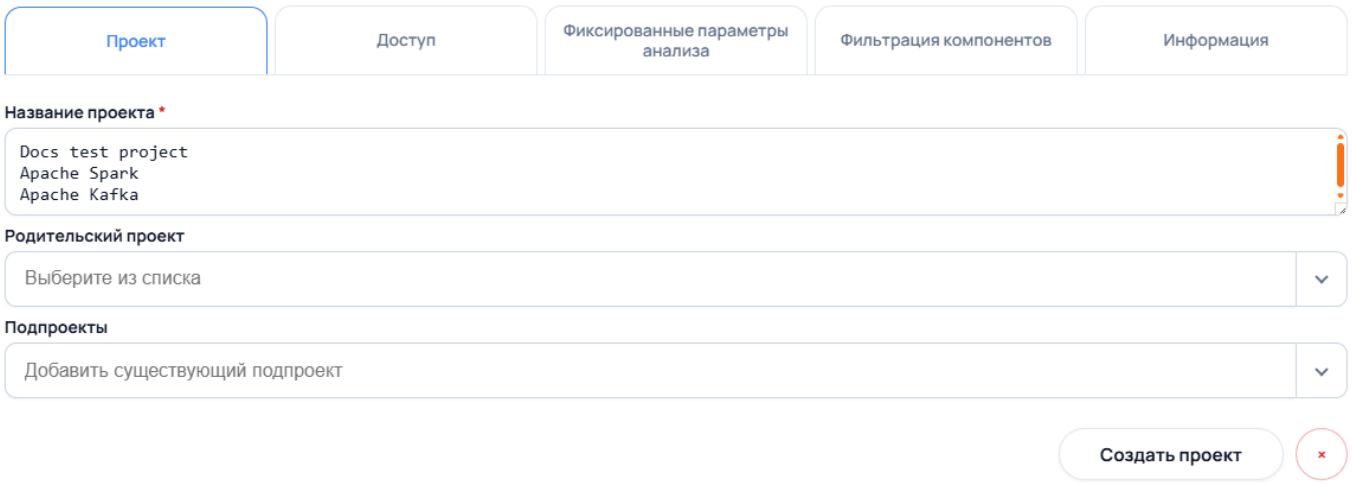

Рисунок 4 – Модальное окно создания проекта, вкладка «Проект»

– Вкладка «Доступ» (рисунок 5):
  – выпадающий список «Группы доступа» – позволяет присвоить группе пользователей доступ к создаваемому проекту;
  – выпадающий список «Пользователи доступа» – позволяет присвоить конкретному пользователю доступ к создаваемому проекту.

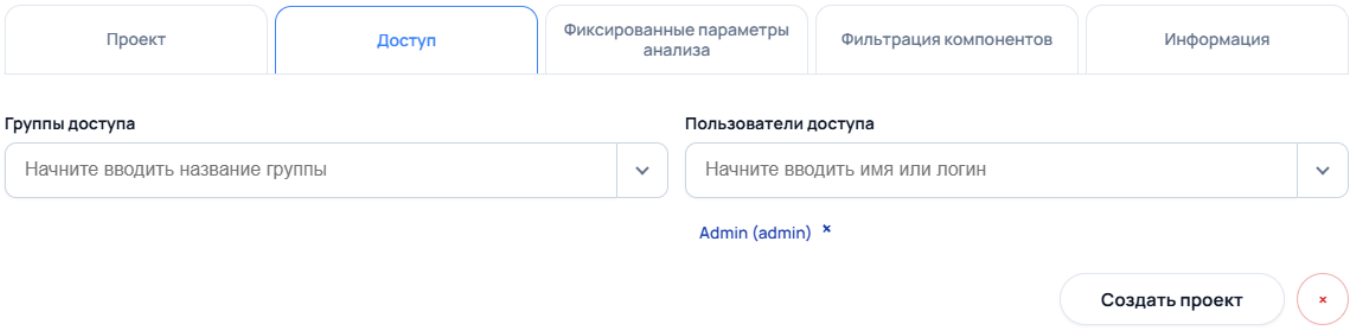

Рисунок 5 – Модальное окно создания проекта, вкладка «Доступ»

– Вкладка «Фиксированные параметры анализа» (рисунок 6):
  – позволяет жестко фиксировать параметры анализа проекта для обычных пользователей. Описание параметров анализа представлено в п. 3.3.2 настоящего руководства;
  – позволяет жестко задавать анализируемые манифесты компонентов проекта. Правило задаётся в формате `целевой_манифест=файл_проекта`. Например, `conanfile.py=project.build.py` скажет анализу считать `project.build.py` Conan-рецептом. Правила проекта наследуются подпроектами.

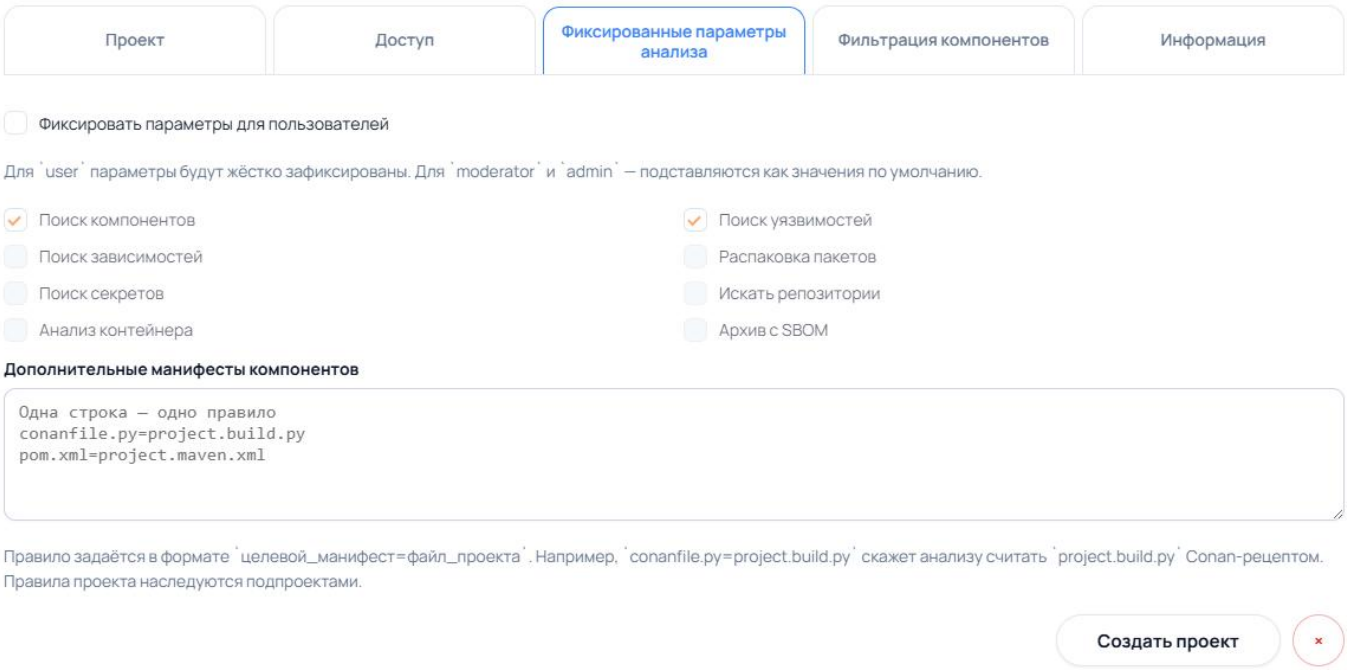

Рисунок 6 – Модальное окно создания проекта, вкладка «Фиксированные параметры анализа»

- Вкладка «Фильтрация компонентов» (рисунок 7);
  - позволяет исключать компоненты из анализа по заданным шаблонам. Поддерживаются правила `name=` и `purl=` для поиска по подстроке, а также `name~=` и `purl~=` для регулярных выражений. Без `*` используется поиск по подстроке. Правила проекта наследуются всеми подпроектами;
  - позволяет задавать правила для разметки доверенных компонентов («provided_by» в рамках SBOM-файла). Каждый список задаёт значение `GOST:provided_by` и правила компонентов, к которым оно применяется. Списки наследуются подпроектами.

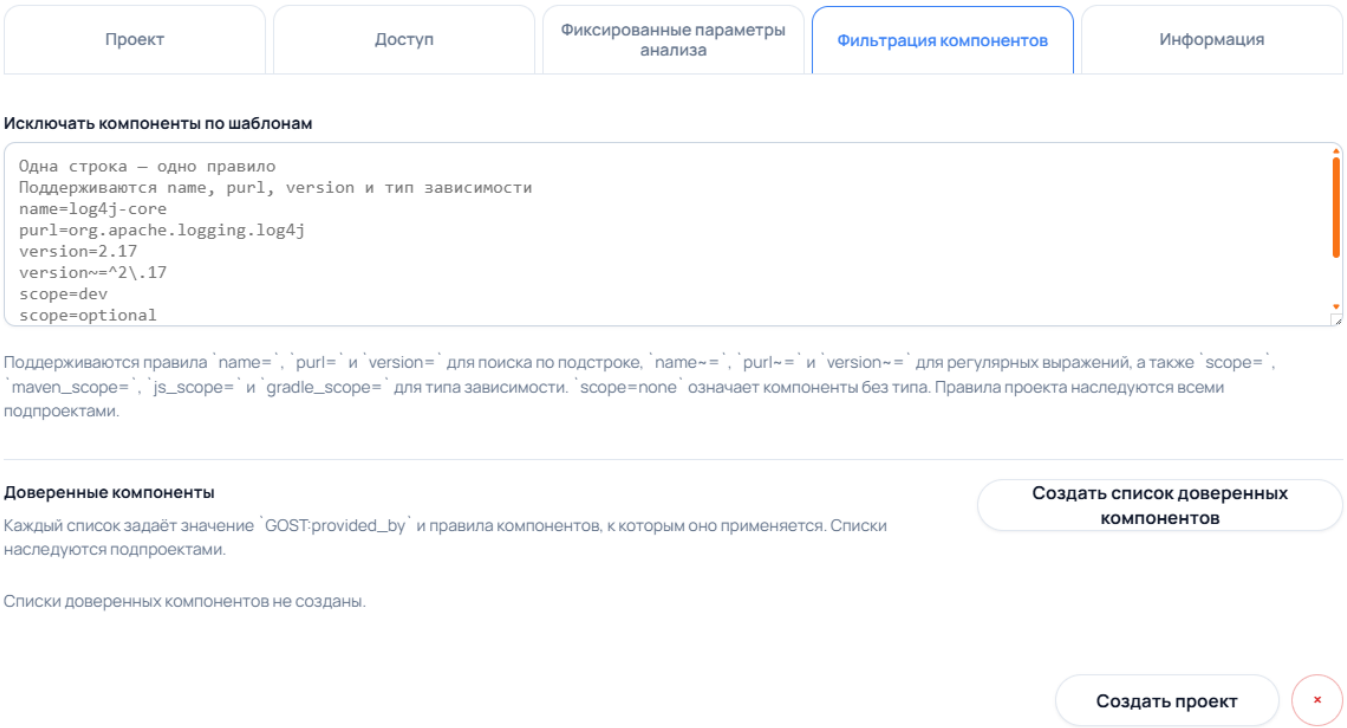

Рисунок 7 – Модальное окно создания проекта, Вкладка «Фильтрация компонентов»

– Вкладка «Информация» (рисунок 8) – позволяет фиксировать информацию о проекте, которая в дальнейшем будет отображаться в формируемых SBOM-файлах:
  – поле «Название продукта»;
  – поле «Версия продукта»;
  – поле «Репозиторий проекта»;
  – поле «Версия SBOM»;
  – поле «Тип компонента проекта»;
  – поле «Заявитель» – название организации, разрабатывающей продукт.

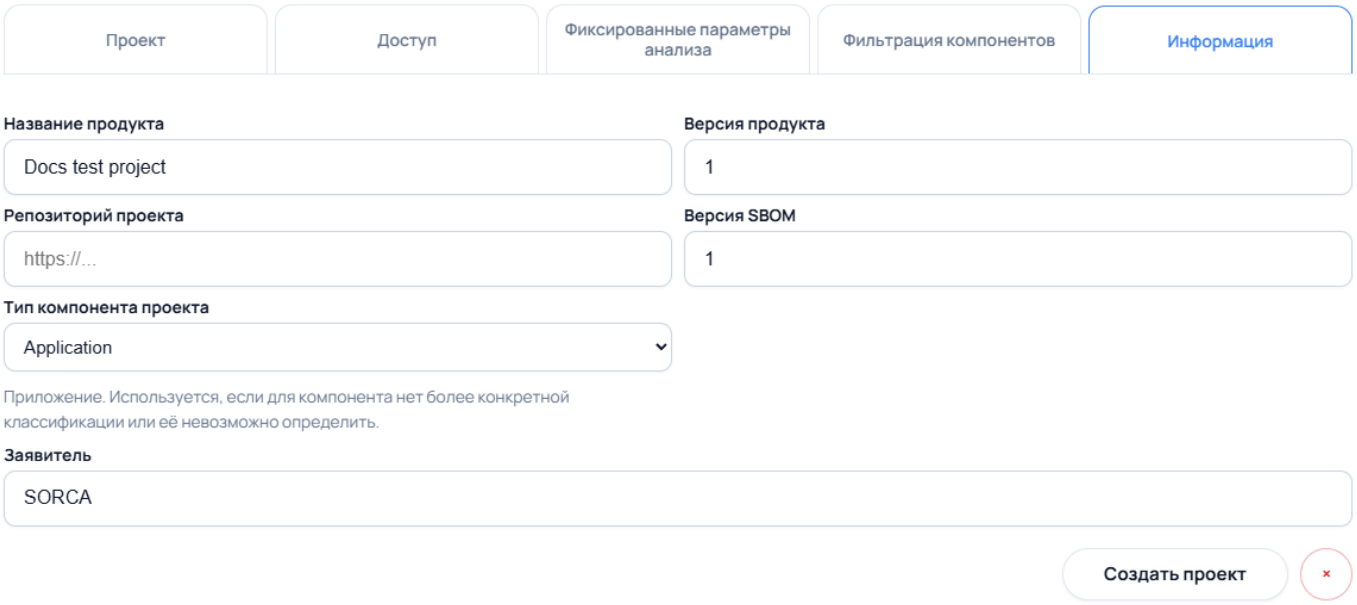

Рисунок 8 – Модальное окно создания проекта, вкладка «Информация»

После настройки и сохранения проект появится в общем списке проектов во вкладке «Проекты» (рисунок 9).

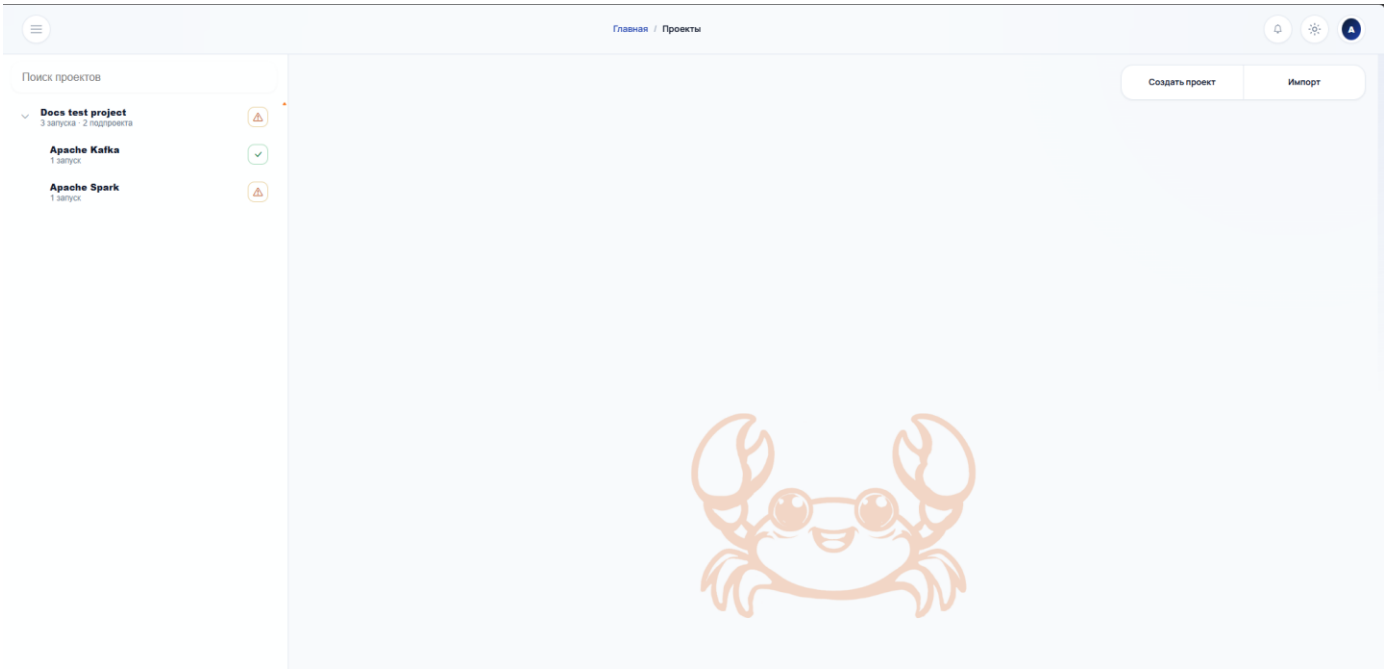

Рисунок 9 – Список проектов

Также страница с проектами содержит кнопку «Импорт», которая позволяет импортировать целые проекты или отдельные запуски/подпроекты из другого экземпляра SORCA.

3.3.2 Настройка и запуск анализа

По нажатии кнопки «Новый анализ» открывается модальное окно (рисунок 10), позволяющее произвести предварительную настройку анализа перед запуском:

- выбор проекта из общего списка проектов;
- выбор источника анализа, а именно:
  - по ссылке на репозиторий (Github/Gitlab) с проектом:
    - с возможностью рекурсивной загрузки submodule (после git clone выполняется git submodule update -init -recursive);
  - через загрузку архива с проектом;
- настройка анализа:
  - параметры анализа:
    - чекбокс «Поиск компонентов» – формирует список заимствованных компонентов проекта;
    - чекбокс «Поиск уязвимостей» – проверяет заимствованные компоненты проекта на предмет наличия в них известных уязвимостей;
    - чекбокс «Поиск зависимостей» – ищет зависимости проекта через системы сборки и менеджеры пакетов;
    - чекбокс «Распаковка пакетов» – Извлекает содержимое пакетов (.rpm/, .apk/, .nupkg/, .whl/, .deb) и Java-архивов (.jar/, .war/, .ear) внутри архива проекта;
    - чекбокс «Поиск секретов» – ищет ключи, токены и пароли в файлах проекта;
    - чекбокс «Искать репозитории» – поиск ссылок на репозитории и архивы с исходными кодами заимствованных компонентов проекта;
  - режимы анализа:
    - чекбокс «Анализ контейнера» – анализирует установленные пакеты в контейнерах без учета транзитивности;
    - чекбокс «Архив с SBOM» – анализ архива с несколькими SBOM JSON (каждый файл анализируется отдельно).

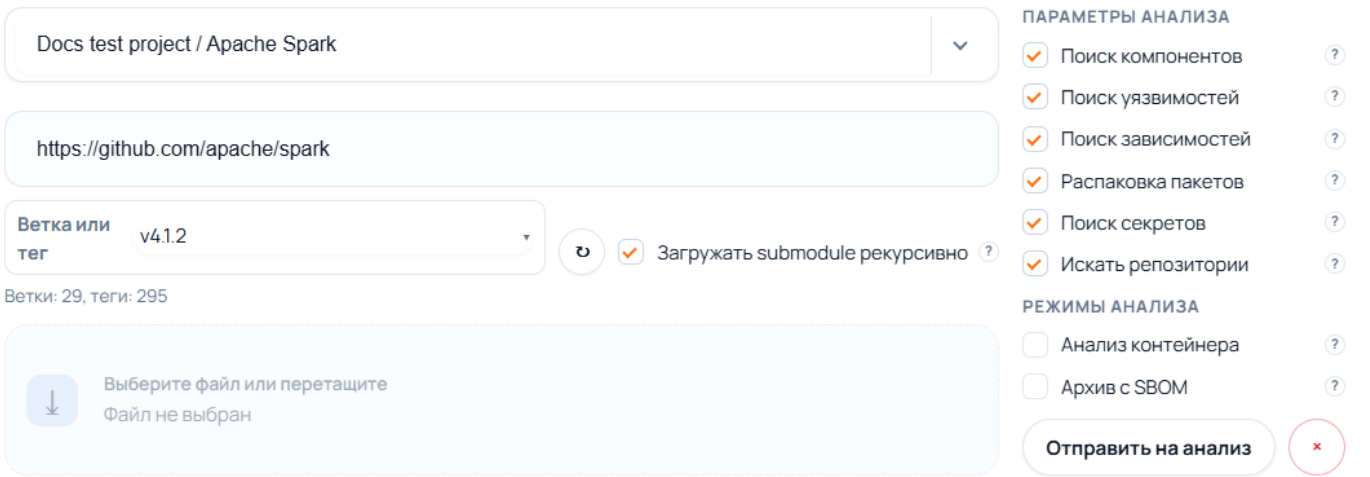

Рисунок 10 – Новый анализ

3.3.3 Запуск анализа

После запуска анализа откроется страница со статусом (рисунок 11). Страница со статусом анализа содержит следующую информацию:

– наименование загруженного архива/репозитория:
– время старта анализа;
– продолжительность анализа в реальном времени;
– сконфигурированные ранее параметры анализа;
– статус-бары с этапами анализа;
– кнопка «Нагрузка» – позволяет отслеживать затрачиваемые ресурсы сервера на проведение анализа;
– кнопка «К результатам анализа» – позволяет сразу перейти на страницу с результатами анализа проекта.

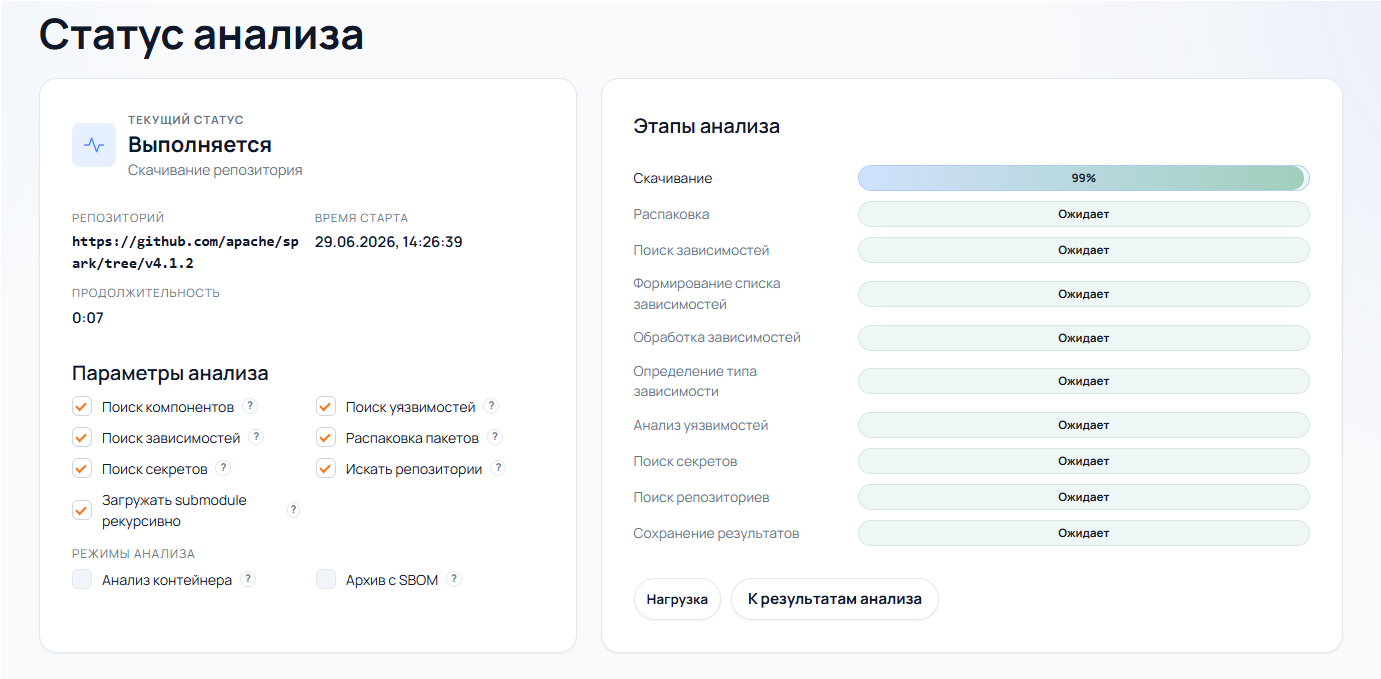

Рисунок 11 – Статус анализа

3.3.4 Работа с проектом

3.3.4.1 Общие сведения о проекте

На странице родительского проекта отображаются модули, содержащие список «головных» запусков самого родительского проекта и список подпроектов, а также модуль, содержащий основную статистику всего проекта (рисунок 12).

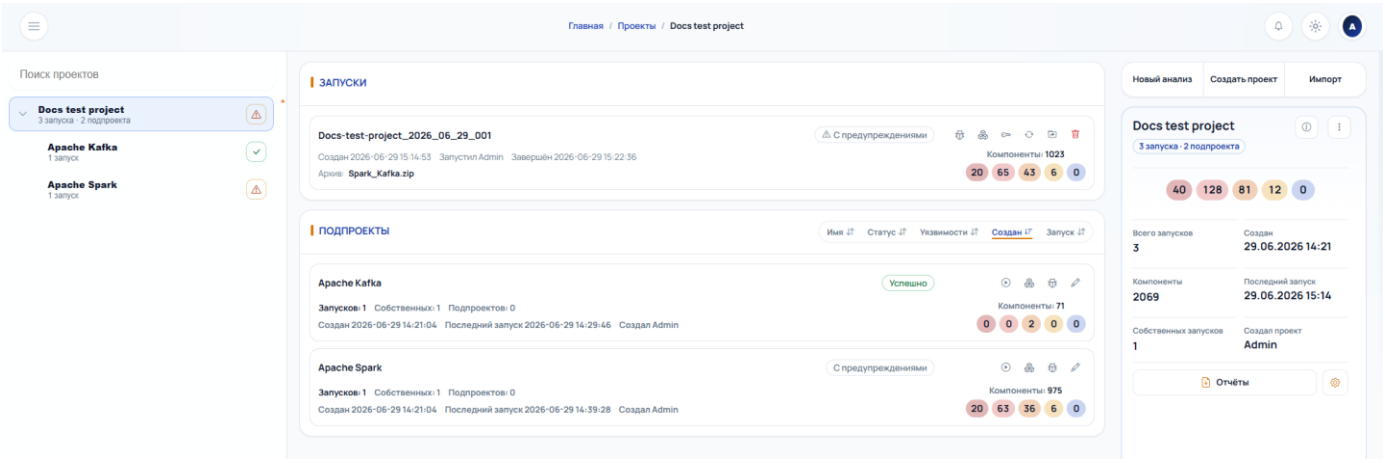

Рисунок 12 – Сведения о проекте

Модуль «Запуски» содержит:

– Кликабельные карточки запусков (рисунок 13), которые содержат:
  – даты создания и завершения анализа;
  – имя пользователя, запустившего анализ;
  – наименование загруженного архива/репозитория;
  – количество найденных компонентов внутри анализа;
  – количество и критичность выявленных уязвимостей после анализа;
  – поле, уведомляющее об успешности/неуспешности/предупреждении проведенного анализа;
  – кнопка «Уязвимости» ( ), переводящая в карточку анализа на страницу с подробной информацией о выявленных уязвимостях;
  – кнопка «Компоненты» ( ), переводящая в карточку анализа на страницу с подробной информацией о выявленных компонентах;
  – кнопка «Секреты» ( ), переводящая в карточку анализа на страницу с подробной информацией о выявленных секретах;
  – кнопка «Повторить анализ» ( ), позволяющая провести повторный анализ (после получения результатов анализа, информация о них сохраняется в СУБД в формате SBOM-файла, который можно автоматически повторно анализировать для обнаружения новых уязвимостей);
  – кнопка «Переместить запуск» ( ), позволяющая переместить анализ в другой проект;
  – кнопка «Удалить запуск» ( ).

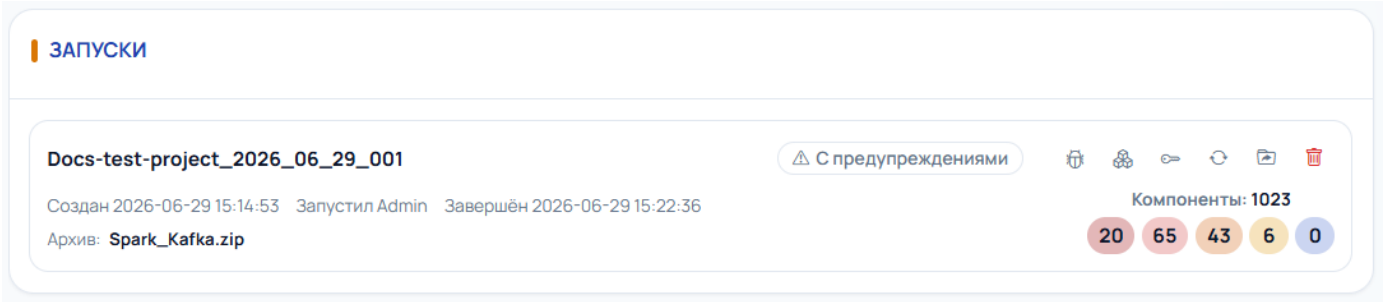

Рисунок 13 – Карточка запуска анализа

Модуль «Подпроекты» содержит:

– Кликабельные карточки подпроектов (рисунок 14), которые содержат:

- количество общих запусков внутри подпроекта (в том числе его подпроектов);
- количество собственных запусков подпроекта;
- количество подпроектов подпроекта;
- дату создания подпроекта;
- дату последнего запуска внутри подпроекта;
- имя пользователя, создавшего подпроект;
- поле, уведомляющее об успешности/неуспешности/предупреждении проведенных анализов внутри подпроекта;
- количество найденных компонентов после выполненных анализов внутри подпроекта;
- количество и критичность выявленных уязвимостей после выполненных анализов внутри подпроекта;
- кнопка «Новый анализ» ( ), позволяющая провести новый анализ внутри подпроекта
- кнопка «Уязвимости» ( ), переводящая на страницу с подробной информацией о выявленных уязвимостях по всем запускам внутри подпроекта;
- кнопка «Компоненты» ( ), переводящая на страницу с подробной информацией о выявленных компонентах по всем запускам внутри подпроекта;
- кнопка «Редактировать проект».

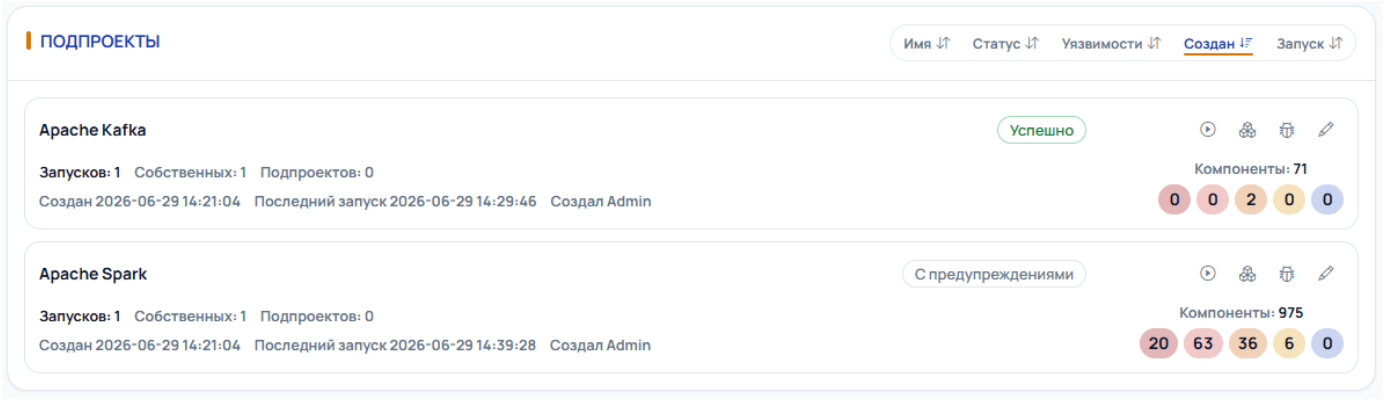

Рисунок 14 – Карточки подпроектов

Модуль статистики проекта (рисунок 15) содержит:

- количество запусков и подпроектов проекта;
- количество и критичность выявленных уязвимостей после выполненных анализов внутри проекта;
- дату создания проекта;
- дату последнего запуска внутри проекта;
- имя пользователя, создавшего проект;
- кнопка «Информация о продукте» ( ), позволяющая изменять информацию о проекте, добавленную на этапе создания проекта;
- кнопка «Действия проекта» ( ), которая позволяет осуществлять следующие действия:
  - экспортировать проект путем формирования файла формата JSON с метаданными о проекте (полезно, когда нужно перенести работу над проектом на другой экземпляр SORCA);
  - переместить проект в другой проект в качестве подпроекта;
  - объединить проект с другим проектом;

  - копировать данные проекта в другой проект;
  - выполнить поиск репозиториев/архивов с исходными текстами заимствованных компонентов для последнего выполненного анализа;
  - просмотреть компоненты проекта (полезно, когда в проекте много подпроектов и нужно получить общую сводку по всем компонентам проекта);
  - просмотреть уязвимости проекта (полезно, когда в проекте много подпроектов и нужно получить общую сводку по всем уязвимостям проекта);
  - сравнить выполненные анализы;
  - сравнить подпроекты внутри проекта;
  - удалить проект.
- Кнопка «Отчёты» (рисунок 16), которая позволяет формировать отчеты:
  - об уязвимостях (в форматах HTML, PDF, CSV, XLSX);
  - о секретах (в форматах HTML, PDF, CSV, XLSX);
  - SBOM:
    - «Сырой» SBOM JSON;
    - SBOM JSON по формату требований ФСТЭК России;
    - единый SBOM JSON по формату требований ФСТЭК России по формату требований ФСТЭК России (полезно, когда в проекте много подпроектов и нужно получить общий SBOM по всему проекту, фиксируются только последние анализы подпроектов);
    - SBOM odt по формату требований ФСТЭК России
    - единый SBOM odt по формату требований ФСТЭК России (полезно, когда в проекте много подпроектов и нужно получить общий SBOM по всему проекту, фиксируются только последние анализы подпроектов);
    - SBOM JSON с фиксацией уязвимостей в компонентах.
- Кнопка «Настройки экспорта» ( ) (рисунок 17), которая позволяет проводить предварительную настройку критериев экспорта для сохраняемых отчетов в части:
  - уязвимостей:
    - по уровню критичности;
    - по типу зависимости;
    - по статусу разметки;
  - компонентов:
    - по версии;
    - по источнику;
    - по исключениям;
    - по доверенным источникам;
    - по поверхности атаки;
    - по функциям безопасности;
    - по типу зависимости;
    - по типу компонента;
  - секретов:
    - по статусу разметки.

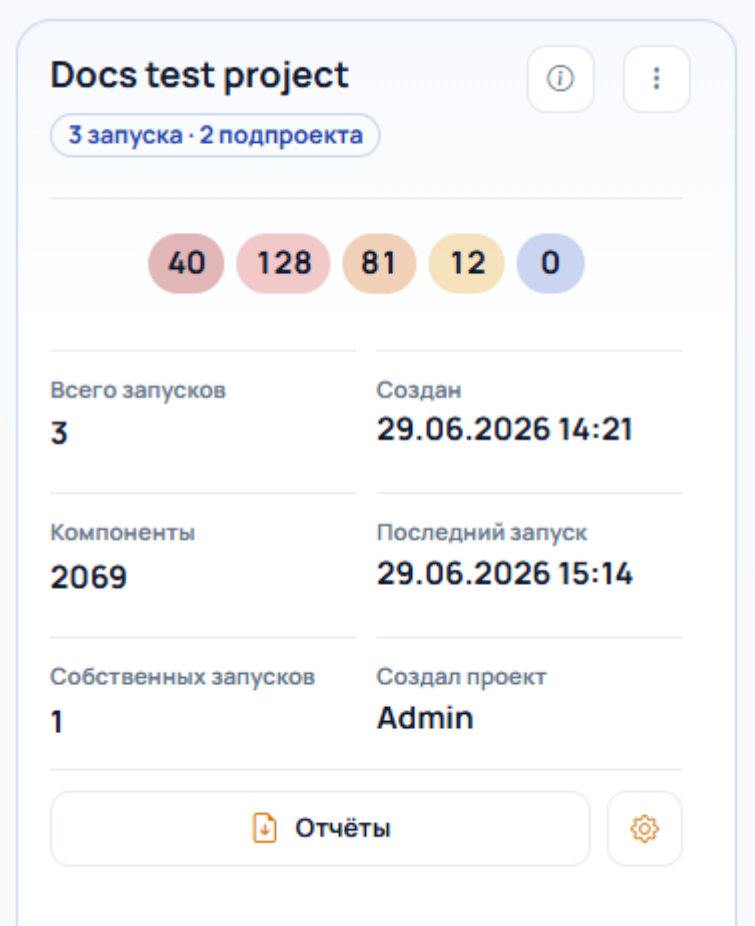

Рисунок 15 – Модуль статистики проекта

Рисунок 16 – Экспорт отчетов

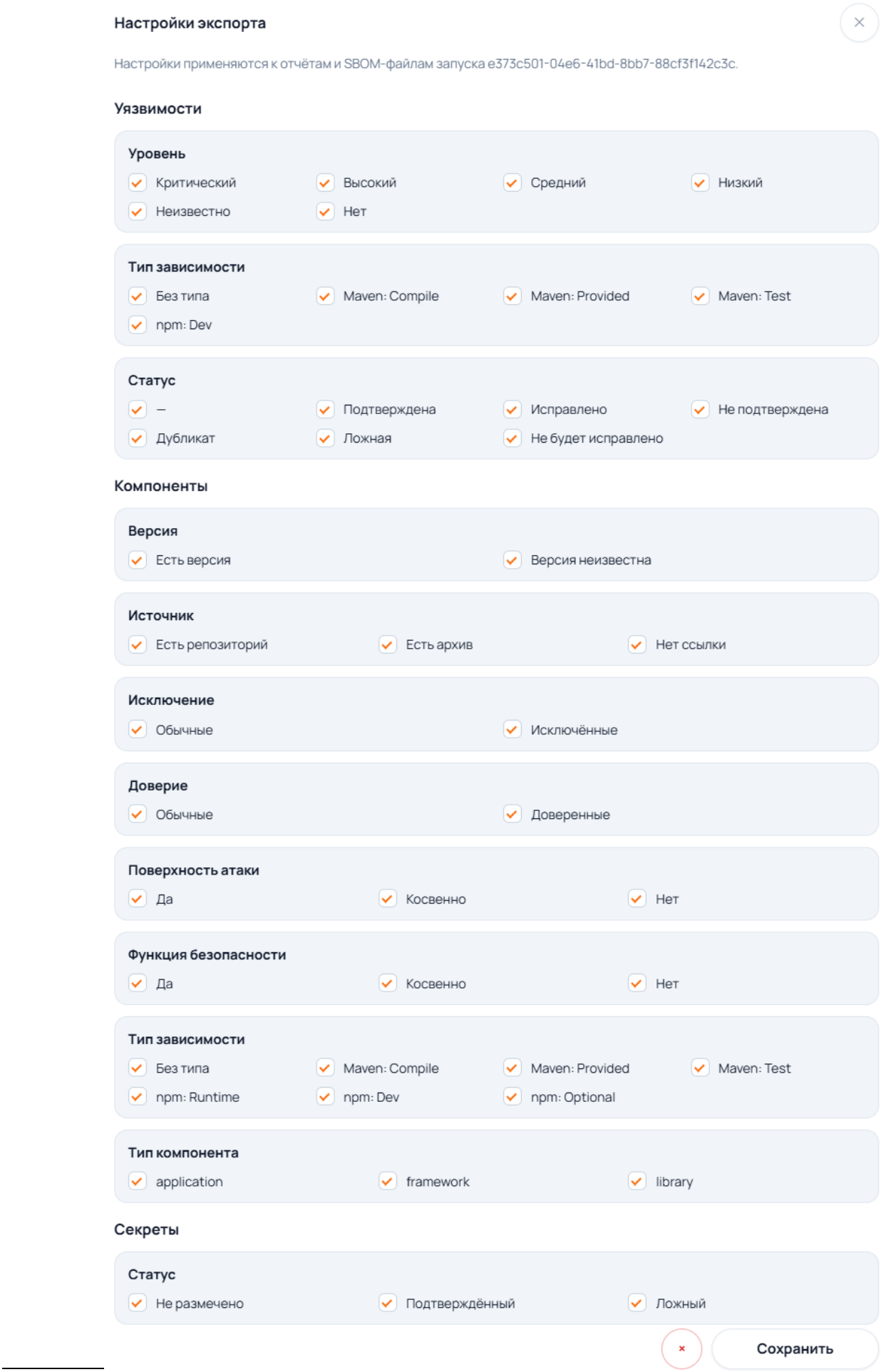
Настройки экспорта
Настройки применяются к отчётам и SBOM-файлам запуска e373c501-04e6-41bd-8bb7-88cf3f142c3c.
Уязвимости
Уровень
Критический
Высокий
Средний
Низкий
Неизвестно
Нет
Тип зависимости
Без типа
Maven: Compile
Maven: Provided
Maven: Test
npm: Dev
Статус
—
Подтверждена
Исправлено
Не подтверждена
Дубликат
Ложная
Не будет исправлено
Компоненты
Версия
Есть версия
Версия неизвестна
Источник
Есть репозиторий
Есть архив
Нет ссылки
Исключение
Обычные
Исключённые
Доверие
Обычные
Доверенные
Поверхность атаки
Да
Косвенно
Нет
Функция безопасности
Да
Косвенно
Нет
Тип зависимости
Без типа
Maven: Compile
Maven: Provided
Maven: Test
npm: Runtime
npm: Dev
npm: Optional
Тип компонента
application
framework
library
Секреты
Статус
Не размечено
Подтверждённый
Ложный
Сохранить

Рисунок 17 – Настройки экспорта

3.3.4.2 Общие сведения об анализе

При переходе по карточке запуска откроется страница с подробной информацией об анализе (рисунок 18):

- Общая информация:
  - статус анализа;
  - наименование архива/репозитория проекта;
  - количество файлов в проекте;
  - размер проекта;
  - дата и время начала анализа;
  - дата и время завершения анализа;
  - график выявленных уязвимостей проекта;
  - график выявленных секретов проекта;
  - график распределения проекта по языкам программирования;
  - график распределения лицензий в заимствованных компонентах проекта.

Основную часть страницы занимает рабочее пространство с выявленным уязвимостями, перечнем заимствованных компонентов, выявленным секретами и выявленными лицензиями заимствованных компонентов.

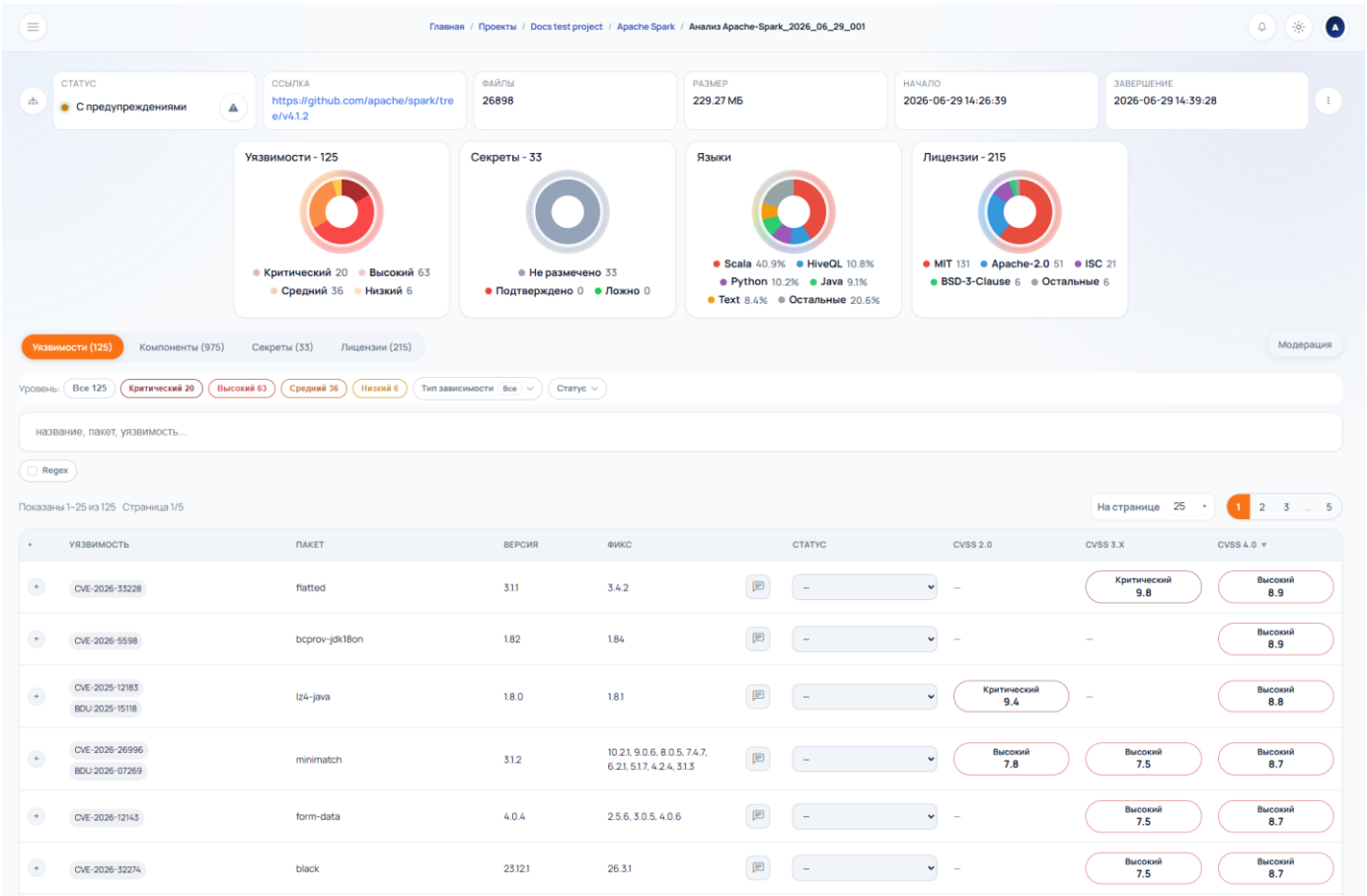

Рисунок 18 – Информация о проекте после анализа

3.3.4.3 Работа с уязвимостями

При переходе на вкладку с уязвимостями открывается список выявленных уязвимостей. Для работы с уязвимостями доступно 2 режима:

- Разметка (рисунок 19) – позволяет проводить анализ и разметку выявленных уязвимостей, и содержит следующую информацию:
  - ID уязвимости – выводятся идентификаторы BDU (при наличии, имеет приоритетный вывод) и CVE;
  - наименование уязвимого компонента;
  - версия уязвимого компонента;
  - версия уязвимого компонента с исправленной уязвимостью;
  - поле «Статус», которое содержит:
    - поле «Комментарий» – для проведения разметки уязвимостей;
    - выпадающий список «Статус», который содержит:
      - статус «Подтверждена»;
      - статус «Исправлена»;
      - статус «Не подтверждена»;
      - статус «Дубликат»;
      - статус «Ложная»;
      - статус «Не будет исправлено».
    - стандарт критичности уязвимости CVSS 2.0;
    - стандарт критичности уязвимости CVSS 3.x;
    - стандарт критичности уязвимости CVSS 4.0.

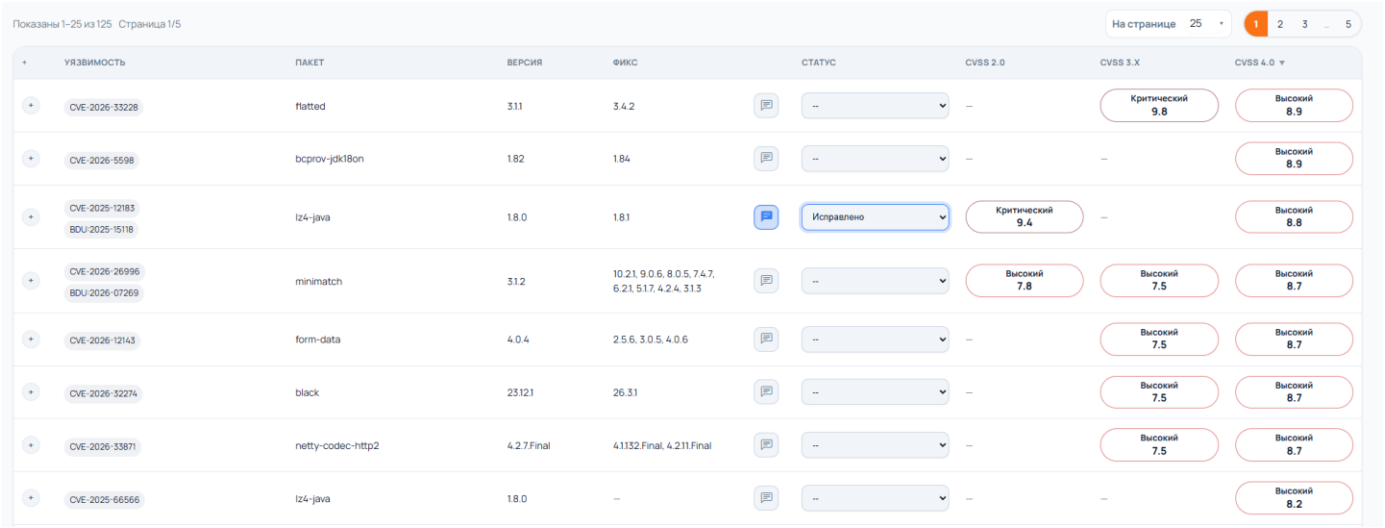

Рисунок 19 – Режим разметки уязвимостей

- модерация (рисунок 20) – позволяет проводить анализ и модерацию размеченных уязвимостей, и содержит следующую информацию:
  - ID уязвимости – выводятся идентификаторы BDU (при наличии, имеет приоритетный вывод) и CVE;
  - наименование уязвимого компонента;
  - версия уязвимого компонента;
  - критичность уязвимости по высшей планке подсчета на основе каждого стандарта CVSS.

– статус уязвимости;
– комментарий к уязвимости после проведения разметки.

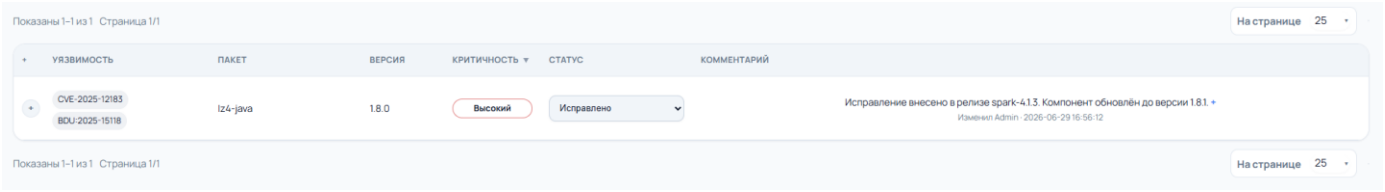

Рисунок 20 – Режим модерации разметки

В каждом режиме также доступна кнопка «Больше» (+) (рисунок 21), являющаяся кнопкой раскрытия модального окна, которое содержит следующую информацию:

– поле «Описание» – содержит основную информацию об уязвимости;
– поле «Даты» – содержит даты публикации уязвимости и обновления информации о ней;
– поле «Тип зависимости» (при наличии) – содержит информацию о типе зависимости (применимо для Java и JavaScript);
– поле «Цель» – указывает на используемый при анализе пакетный менеджер
– поле «Ссылки» – содержит ссылки на все возможные источники с информацией об уязвимости;
– поле «CVSS» – содержит числовой рейтинг (CVSS) и вектор атаки уязвимости;
– поле «Файл» – указывает на путь к файлу, в котором был обнаружен уязвимый компонент.
– поле «Комментарий» – содержит комментарий разметки уязвимости.

Рисунок 21 – Подробная информация об уязвимости

Для удобного анализа уязвимостей представлена фильтрация по:

- уровню критичности;
- типу зависимости:
  - для Maven:
    - compile – По умолчанию. Зависимости с этим scope доступны на всех этапах и упаковываются в финальный артефакт (JAR, WAR и другие форматы).
    - provided – Используется на этапе сборки и тестирования проекта. Предполагается, что зависимость предоставит среда выполнения (например, контейнер сервлетов или сервер приложений).
    - runtime – Зависимости с этим scope нужны для выполнения исходного кода, но не для компиляции.
    - test – Зависимости с этим scope нужны только для компиляции и запуска тестов, а не для производственного кода.
    - system – Зависимости с этим scope не извлекаются из репозитория Maven, а ссылаются на локальную систему. Этот scope обычно не рекомендуется, так как он обходит управление зависимостями Maven.
    - import – Используется только в Maven 2.0.9 и выше. Применяется в разделе dependency Management файла pom для импорта информации об управлении зависимостями из других файлов POM в текущий проект.
  - для JavaScript:
    - runtime – Основные зависимости, необходимые для работы приложения в продакшене. Включают библиотеки и модули, на которые приложение полагается во время выполнения.
    - dev – Зависимости, необходимые только для разработки. Обычно включают фреймворки тестирования, инструменты сборки, линтеры и другие утилиты, используемые на этапе разработки.
    - optional – Зависимости, которые не критичны для работы приложения, но могут быть использованы, если доступны. Если установка одной из этих зависимостей не удалась, это не приведёт к ошибке.
    - peer – Зависимости, которые должны быть установлены разработчиком совместно с пакетом. Указывают, что нужные зависимости уже должны быть установлены на стороне разработчика, либо они должны быть доступны в рабочем окружении, чтобы пакет мог корректно функционировать.
- статусу разметки уязвимостей.

3.3.4.4 Работа с компонентами

При переходе на вкладку с компонентами (рисунок 22) открывается список выявленных заимствованных компонентов. Вкладка содержит следующую информацию:

- наименование компонента;
- версия компонента;
- язык программирования, на котором написан компонент;
- поле «Поверхность атаки» – для определения компонента, как лежащего на поверхности атаки;
- поле «Функции безопасности» – для определения компонента, как выполняющего функции безопасности;

– поле «Репозиторий» – для фиксации ссылок репозиториев и архивов (с функцией подсчета контрольных сумм по алгоритму STREEBOG-256), которые ведут к исходным текстам компонента;
– поле «Пакет» – для отображения ссылок на ресурсы, содержащие информацию о компоненте;
– Поле «Файл» – указывает на путь к файлу, в котором был обнаружен компонент.

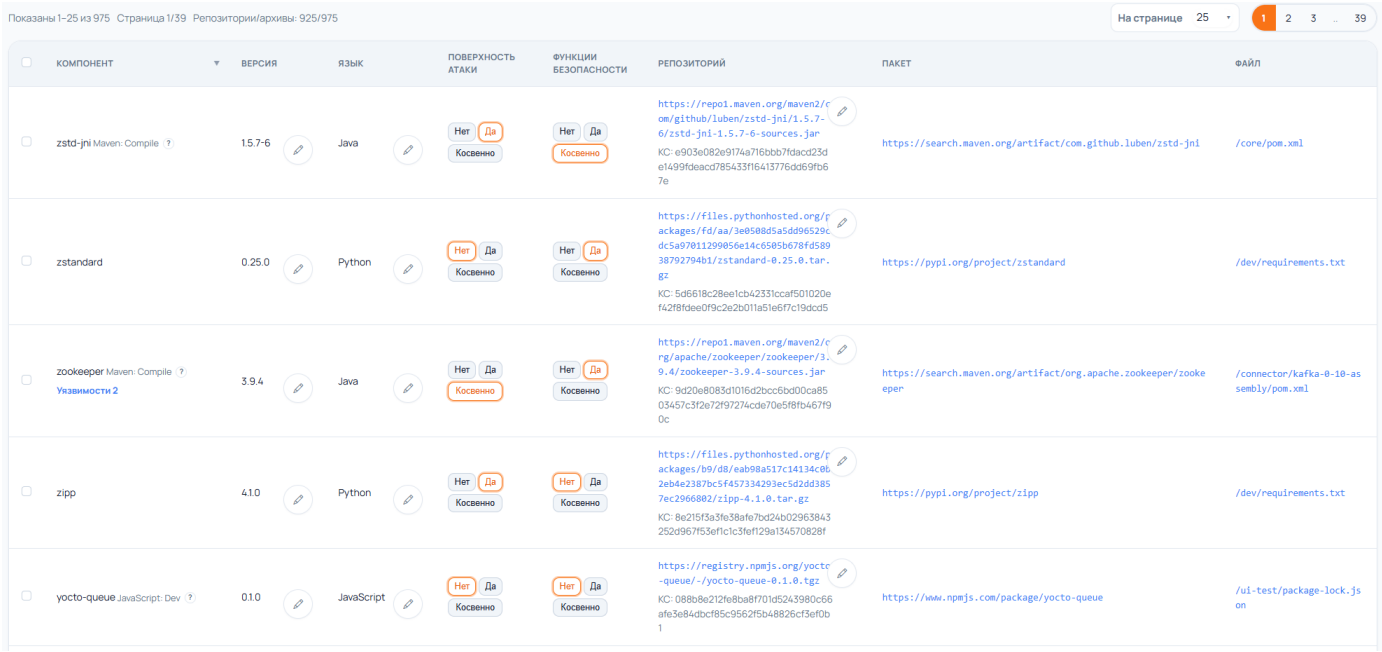

Рисунок 22 – Информация о выявленных заимствованных компонентах

Для анализа транзитивности выявленных компонентов представлена кнопка «Дерево зависимостей» ( ), которая ведет к графу зависимостей анализа (рисунок 23).

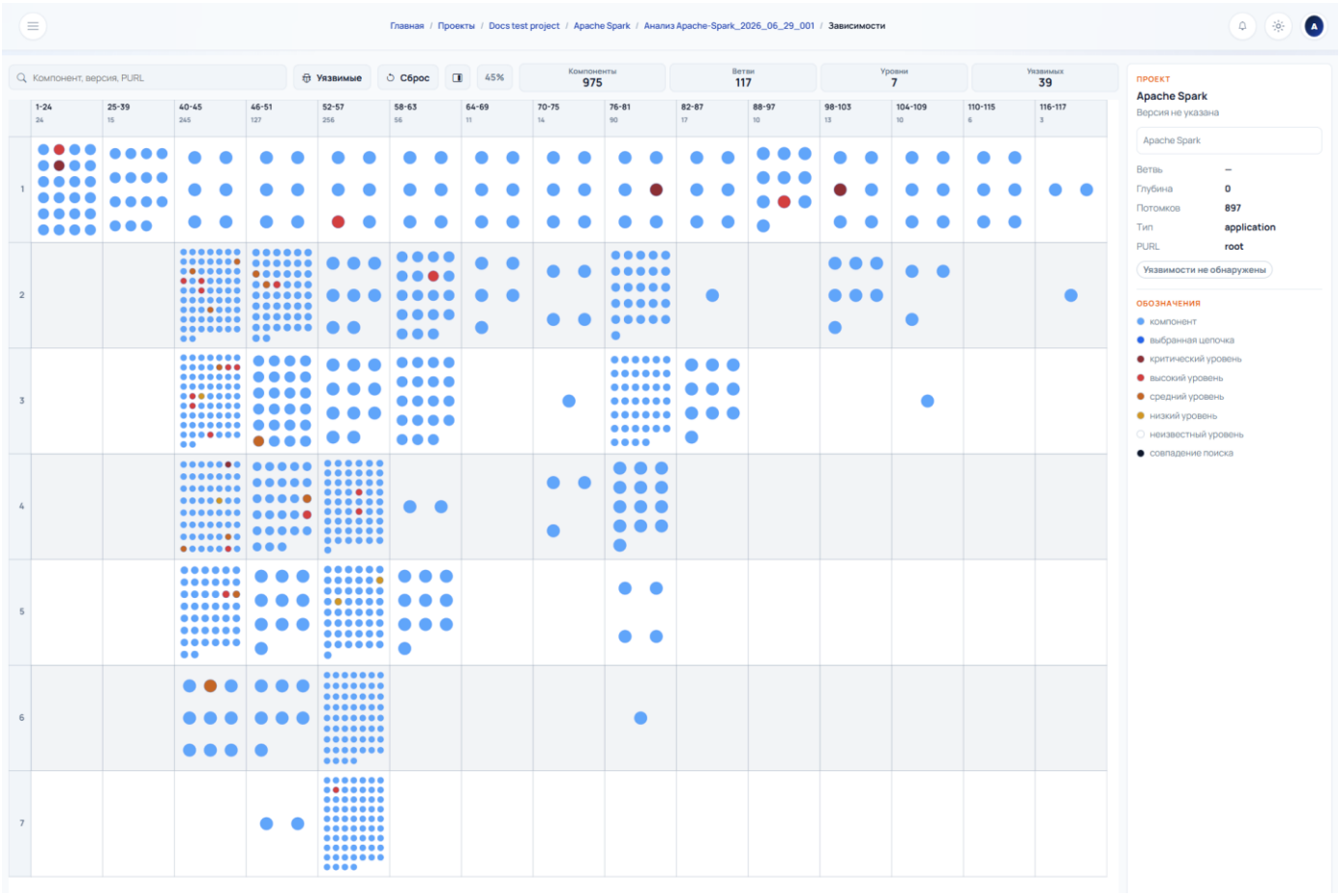

Рисунок 23 – График зависимостей

Для удобного анализа компонентов представлена фильтрация по:

- компонентам, версия которых неизвестна;
- компонентам, для которых не был найден репозиторий/архив с исходными текстами;
- компонентам, для которых был найден репозиторий/архив с исходными текстами;
- компонентам, отмеченным, как лежащим на поверхности атаки;
- компонентам, отмеченным, как реализующим функции безопасности;
- типу зависимости:
  - для Maven:
    - compile – По умолчанию. Зависимости с этим scope доступны на всех этапах и упаковываются в финальный артефакт (JAR, WAR и другие форматы).
    - provided – Используется на этапе сборки и тестирования проекта. Предполагается, что зависимость предоставит среда выполнения (например, контейнер сервлетов или сервер приложений).
    - runtime – Зависимости с этим scope нужны для выполнения исходного кода, но не для компиляции.
    - test – Зависимости с этим scope нужны только для компиляции и запуска тестов, а не для производственного кода.
    - system – Зависимости с этим scope не извлекаются из репозитория Maven, а ссылаются на локальную систему. Этот scope обычно не рекомендуется, так как он обходит управление зависимостями Maven.

- import – Используется только в Maven 2.0.9 и выше. Применяется в разделе dependency Management файла pom для импорта информации об управлении зависимостями из других файлов POM в текущий проект.

– для JavaScript:
  – runtime – Основные зависимости, необходимые для работы приложения в продакшене. Включают библиотеки и модули, на которые приложение полагается во время выполнения.
  – dev – Зависимости, необходимые только для разработки. Обычно включают фреймворки тестирования, инструменты сборки, линтеры и другие утилиты, используемые на этапе разработки.
  – optional – Зависимости, которые не критичны для работы приложения, но могут быть использованы, если доступны. Если установка одной из этих зависимостей не удалась, это не приведёт к ошибке.
  – peer – Зависимости, которые должны быть установлены разработчиком совместно с пакетом. Указывают, что нужные зависимости уже должны быть установлены на стороне разработчика, либо они должны быть доступны в рабочем окружении, чтобы пакет мог корректно функционировать.

3.3.4.5 Работа с секретами

При переходе на вкладку с секретами (рисунок 24) открывается список выявленных секретов. Вкладка содержит следующую информацию:

– поле «Правило» – указывает на правило, по которому найден секрет;
– поле «Файл» – указывает на путь к файлу, в котором был обнаружен секрет;
– поле «Строка» – указывает на строку в файле, в которой был обнаружен секрет;
– поле «Статус» – для указания статуса секрета:
  – ложный;
  – подтвержденный;
– поле «Комментарий» – для проведения разметки уязвимостей.

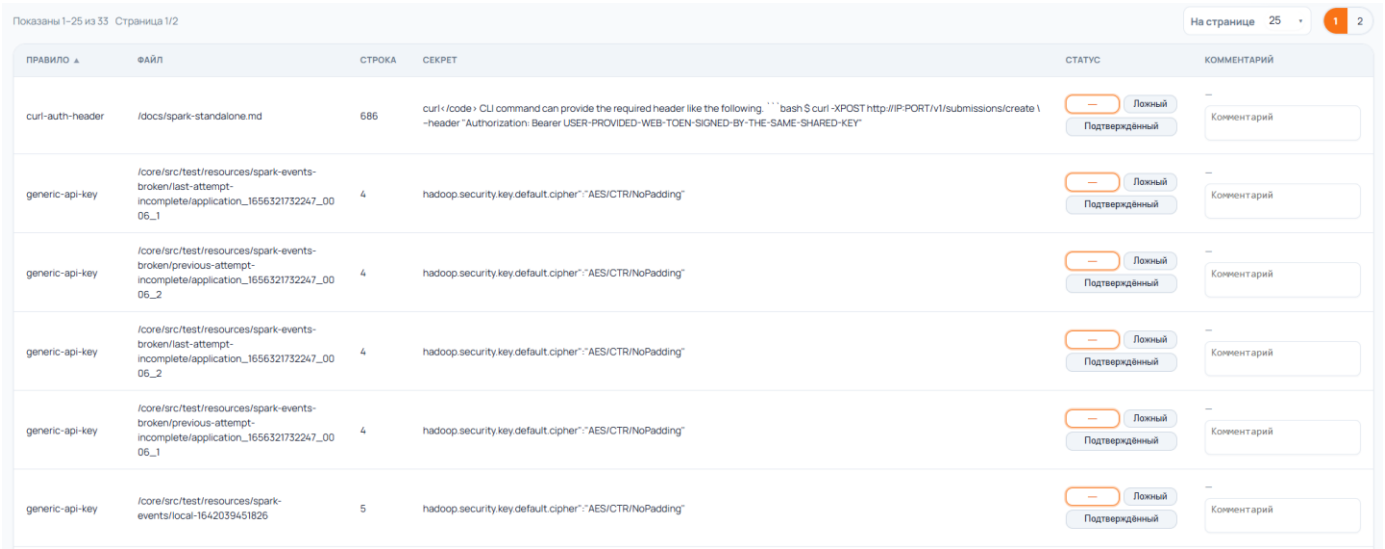

Рисунок 24 – Информация о выявленных секретах

3.3.4.6 Дополнительные действия с анализом

Кнопка «Параметры» (⋮) позволяет:

- провести повторный анализ;
- провести поиск репозиториев/архивов с исходными текстами компонентов в случае, если при запуске анализа данный параметр выставлен не был;
- получить языки программирования компонентов в случае, если при запуске анализа данный параметр выставлен не был;
- скопировать разметку анализа в другой анализ;
- импортировать разметку (полезно, когда нужно перенести разметку анализа на другой экземпляр SORCA).

3.3.4.7 Экспорт анализа

Кнопка «Настройка экспорта» (⚙) позволяет провести предварительную гибкую настройку отчетов анализа перед выгрузкой (рисунок 17).

После настройки экспорта можно формировать отчеты:

- об уязвимостях (в форматах HTML, PDF, CSV, XLSX);
- о секретах (в форматах HTML, PDF, CSV, XLSX);
- SBOM:
  - «Сырой» SBOM JSON;
  - SBOM JSON по формату требований ФСТЭК России;
  - единый SBOM JSON по формату требований ФСТЭК России по формату требований ФСТЭК России (полезно, когда в проекте много подпроектов и нужно получить общий SBOM по всему проекту, фиксируются только последние анализы подпроектов);
  - SBOM odt по формату требований ФСТЭК России
  - единый SBOM odt по формату требований ФСТЭК России (полезно, когда в проекте много подпроектов и нужно получить общий SBOM по всему проекту, фиксируются только последние анализы подпроектов);
  - SBOM JSON с фиксацией уязвимостей в компонентах.

3.4 Вкладка «Параметры»

Данная вкладка является панелью администратора с функцией управления всем приложением в целом.

Вкладка содержит в себе следующие вкладки:

- вкладка «Обзор» (рисунок 25) – содержит общую информацию о приложении:
  - серверное время;
  - информация о базе данных;
  - информация о свободном месте на сервере;
  - версия приложения;
  - количество репозиториев/архивов с исходными текстами компонентов, сохраненных в базе данных;
  - статус актуальности базы уязвимостей;
  - количество и список запущенных задач;
  - срок действия лицензии.

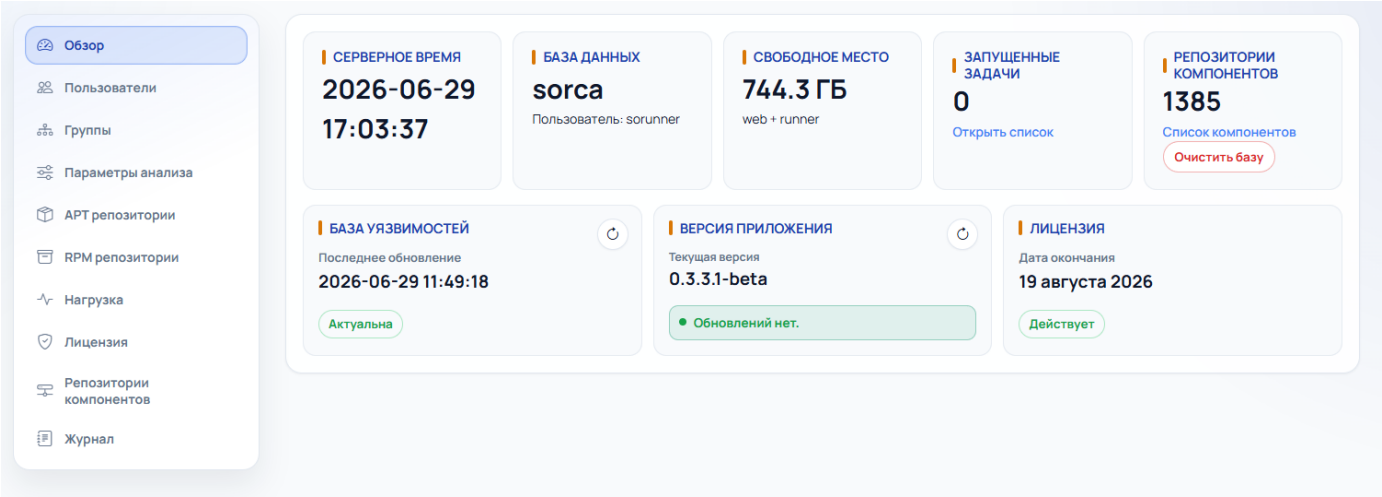

Рисунок 25 – Вкладка «Обзор»

– вкладка «Пользователи» (рисунки 26, 27) – отвечает за создание и обзор пользователей;

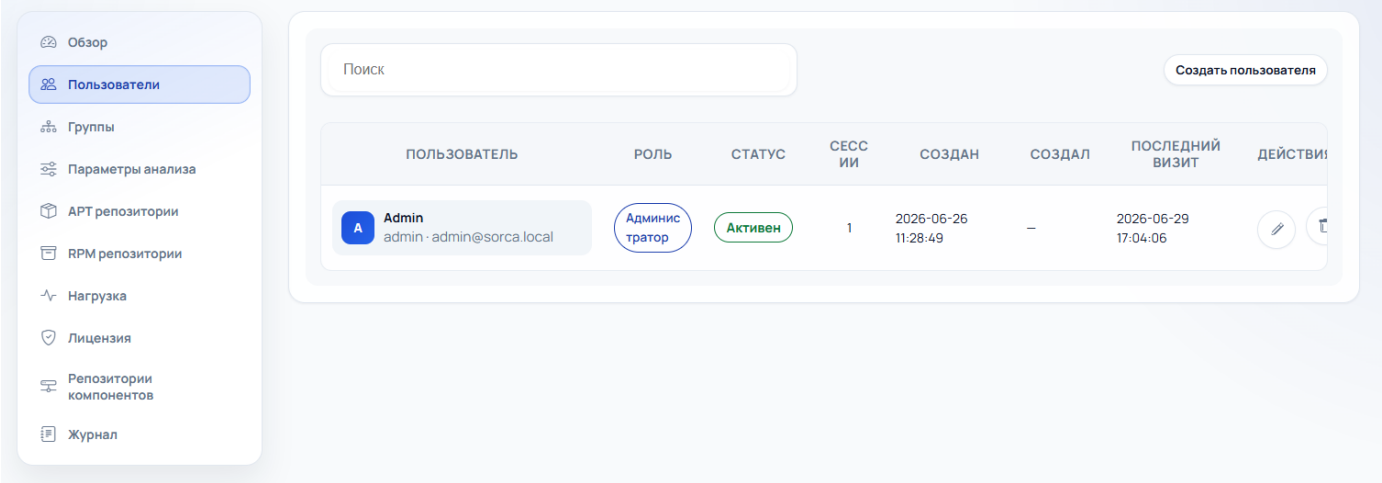

Рисунок 26 – Вкладка «Пользователи»

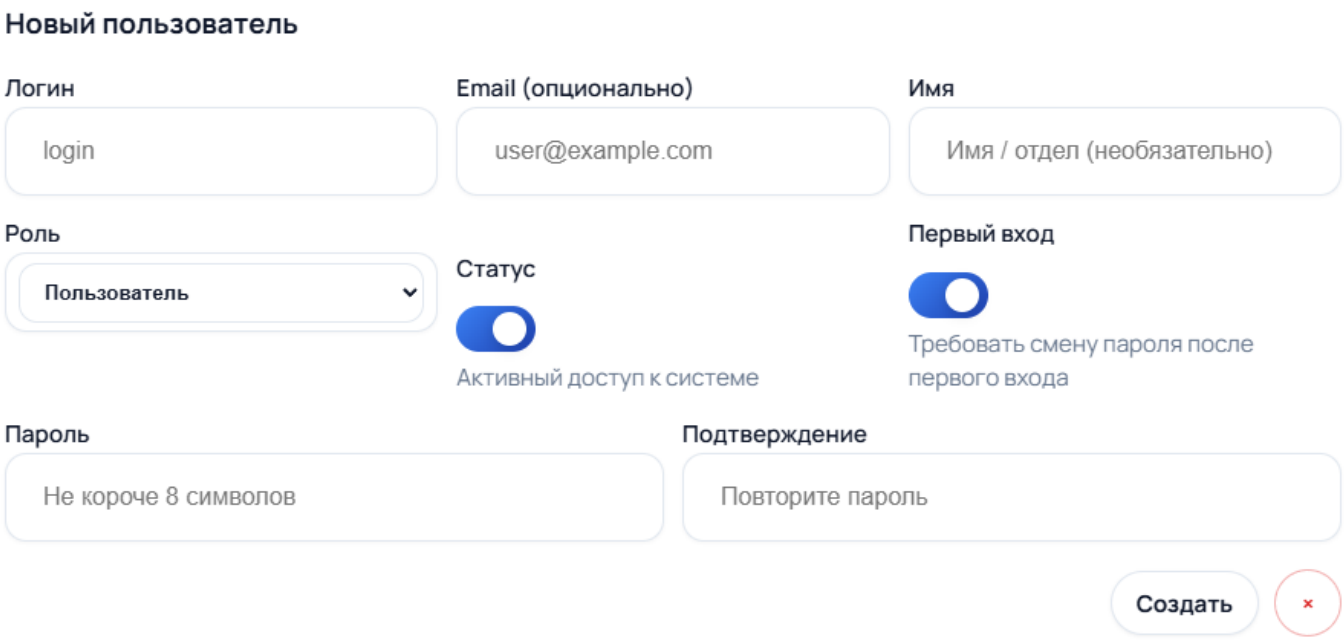

Рисунок 27 – Создание пользователя

– вкладка «Группы» (рисунки 28, 29) – отвечает за создание и обзор групп пользователей;

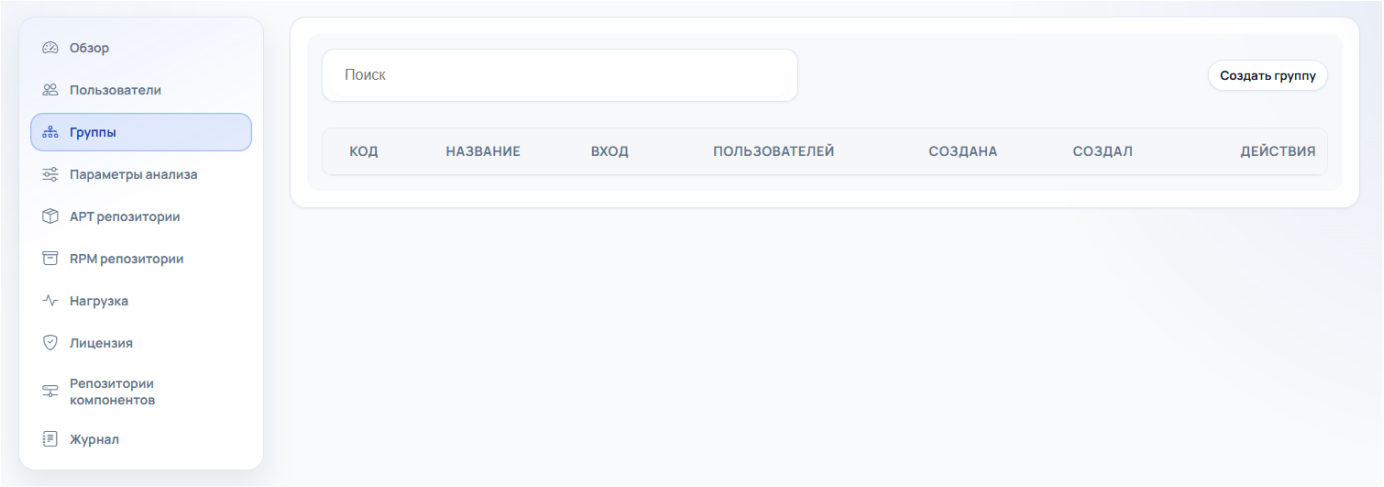

Рисунок 28 – Вкладка «Группы»

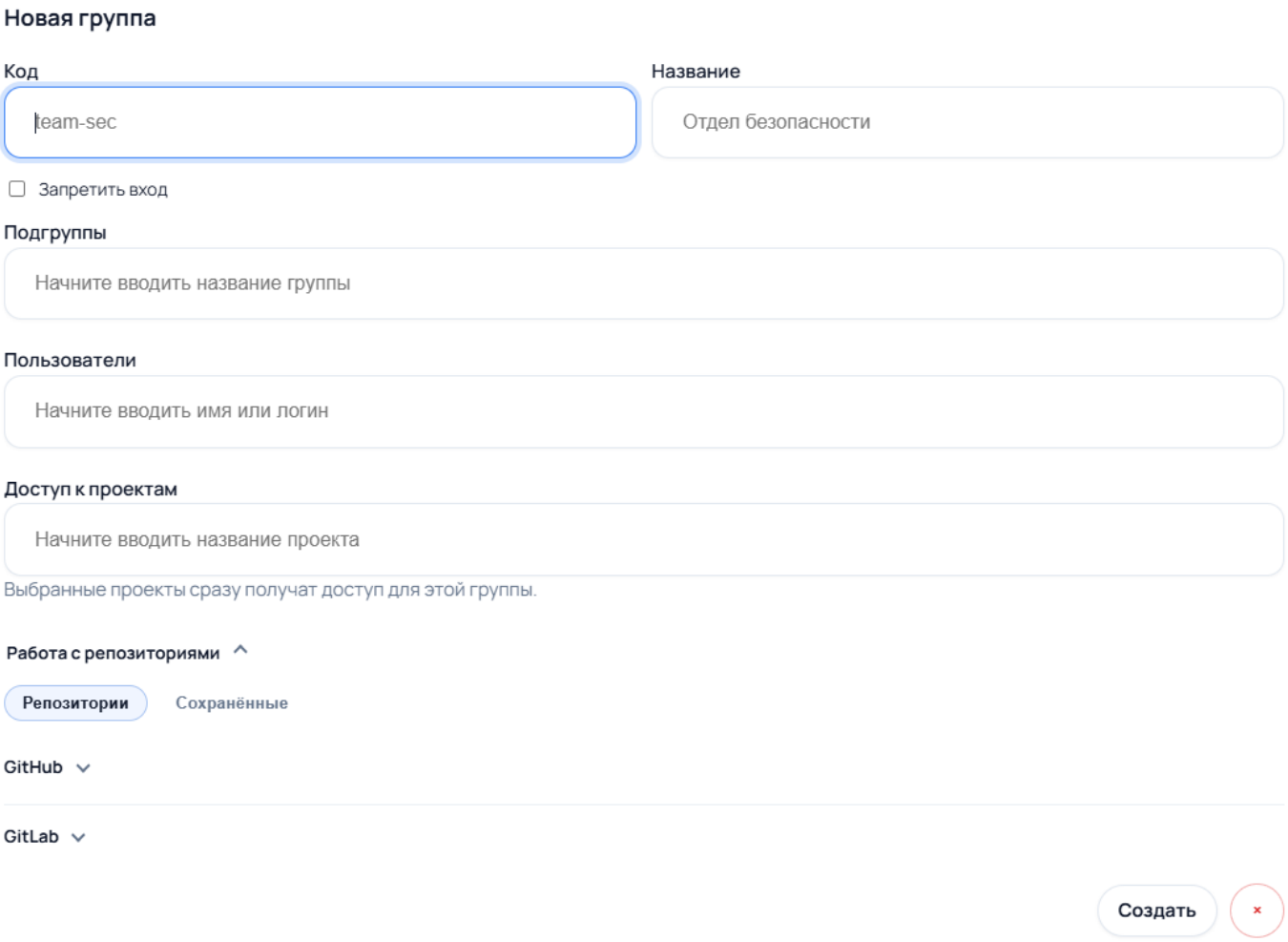

Рисунок 29 – Создание группы

– вкладка «Параметры анализа» (рисунок 30) – содержит параметры:
  – модуль «Глубина распаковки»:
    – параметр «Каталоги» – Устанавливает глубину анализа каталогов после распаковки.
    – параметр «Архивы» – Устанавливает возможное количество распаковываемых архивов в процессе анализа.

- модуль «Производительность»:
  - параметр «Потоки анализа» – По умолчанию — половина доступных потоков CPU.
  - параметр «Потоки поиска репозиториев» – По умолчанию — 8 потоков.
- модуль «Время»:
  - параметр «Ожидание решения по базе уязвимостей, мин» – Если пользователь не ответил, анализ продолжится без обновления (только при наличии локальной БД).
  - параметр «Часовой пояс интерфейса» – Время хранится в UTC, отображается в выбранной зоне. По умолчанию — системная зона: UTC+00:00 · Etc/UTC.
- модуль «Поиск репозиториев во время анализа»:
  - параметр «Поиск репозиториев» – Если выключено, новые repo URL берутся только из локальной БД.
  - параметр «Поиск архивов» – Если выключено, новые ссылки на архивы берутся только из локальной БД.
- модуль «Сохранение»:
  - параметр «Сохранять бинарные файлы, как компоненты» – Отключите, чтобы не сохранять компоненты с непонятным purl.
  - параметр «Исключать доверенные» – Не учитывать компоненты из доверенных источников при поиске уязвимостей.
  - параметр «Исключать исключенные» – Не учитывать исключённые компоненты при поиске уязвимостей.
  - параметр «Подсчёт КС загружаемого архива» – Выберите алгоритмы (STREEBOG-256, MD5, SHA-1, SHA-256, SHA-512), чтобы сохранять контрольные суммы исходного файла.
- модуль «Автоматическое обновление» – Если включено, SORCA в фоне проверяет обновления БД и запускает скачивание, когда доступны новые данные.

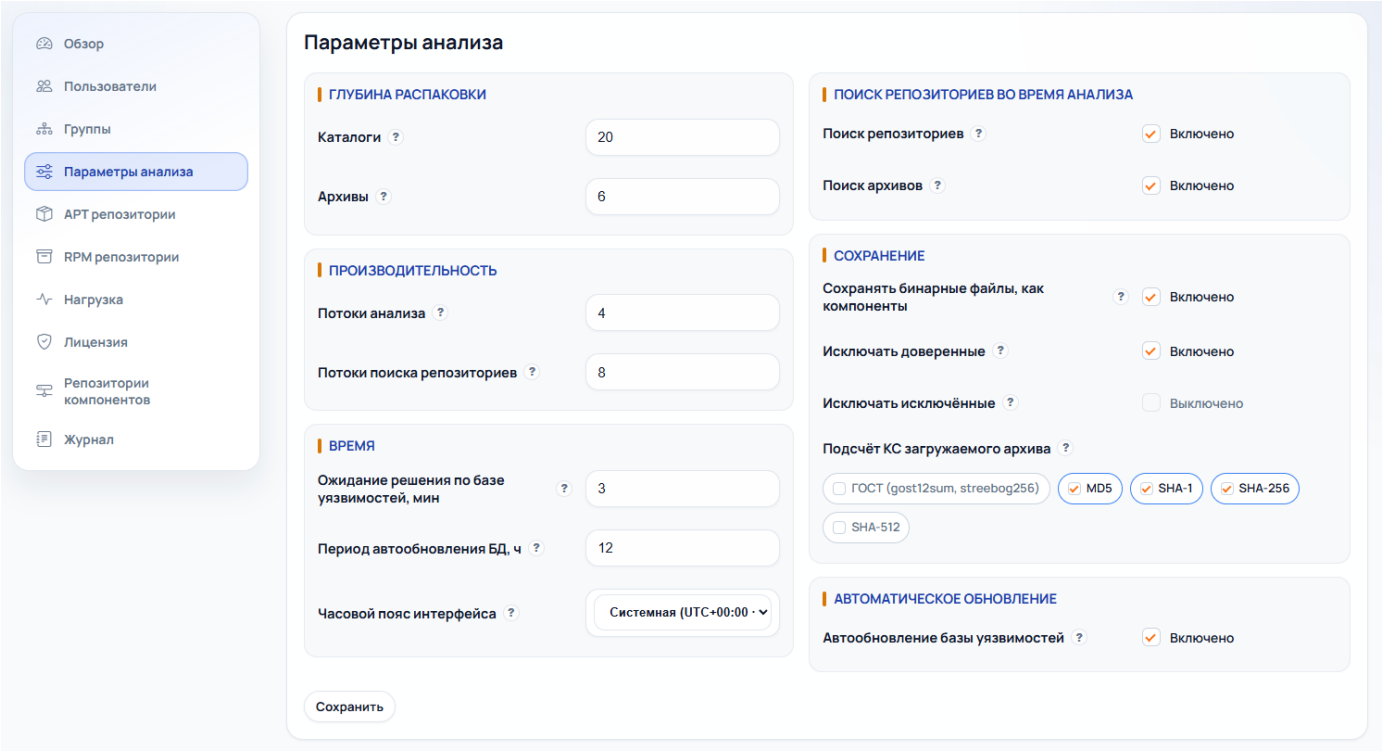

Рисунок 30 – Вкладка «Параметры анализа»

– вкладка «APT репозитории» (рисунок 31) – позволяет вносить в конфигурацию анализов репозитории, которые используются для получения информации о пакетах операционных систем на базе пакетного менеджера APT.

Рисунок 31 – Вкладка «APT репозитории»

– вкладка «RPM репозитории» (рисунок 32) – позволяет вносить в конфигурацию анализов репозитории, которые используются для получения информации о пакетах операционных систем на базе пакетного менеджера RPM.

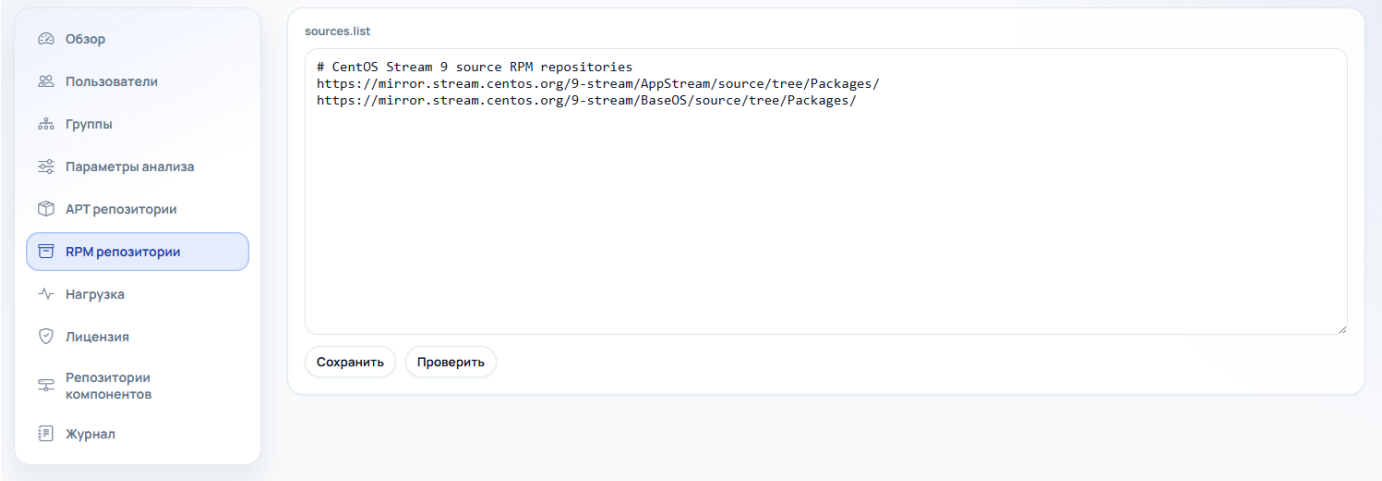

Рисунок 32 – Вкладка «RPM репозитории»

– вкладка «Нагрузка» (рисунок 33) – позволяет отслеживать затрачиваемые ресурсы сервера на проведение анализов.

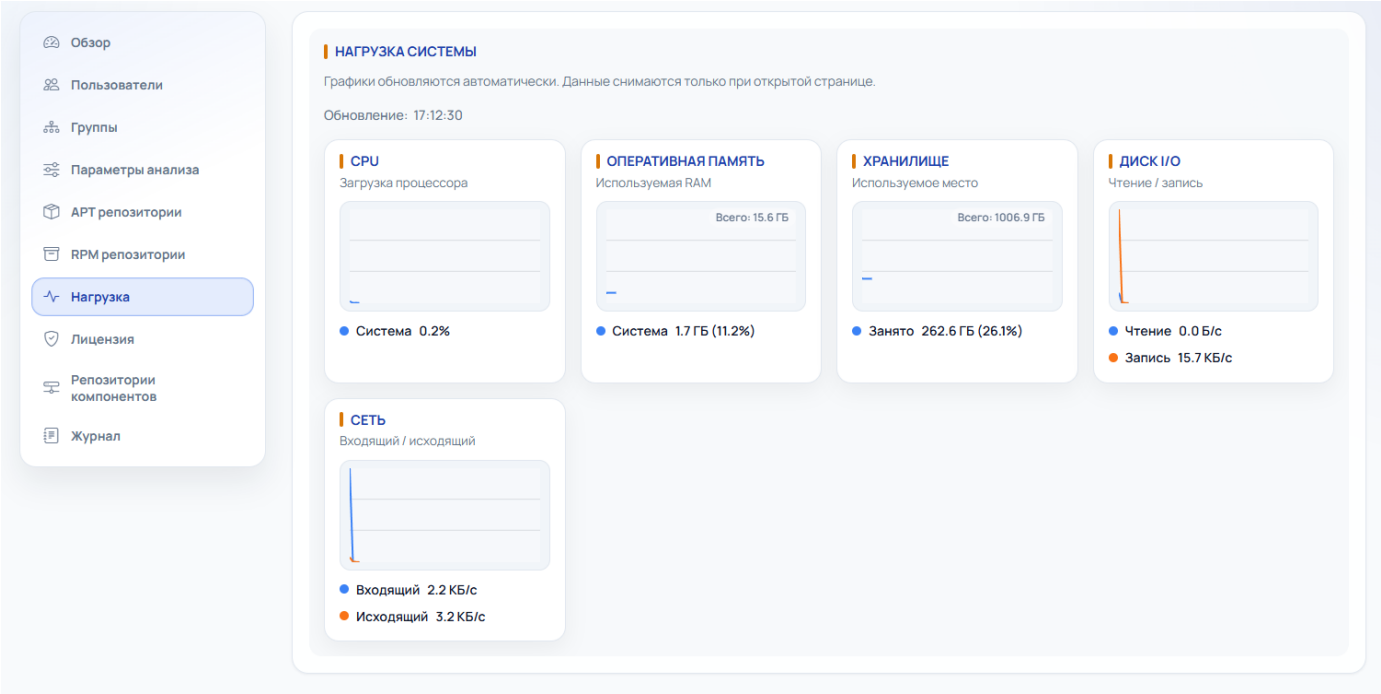

Рисунок 33 – Вкладка «Нагрузка»

– вкладка «Лицензия» (рисунок 34) – позволяет добавлять лицензию для активации функционала приложения.

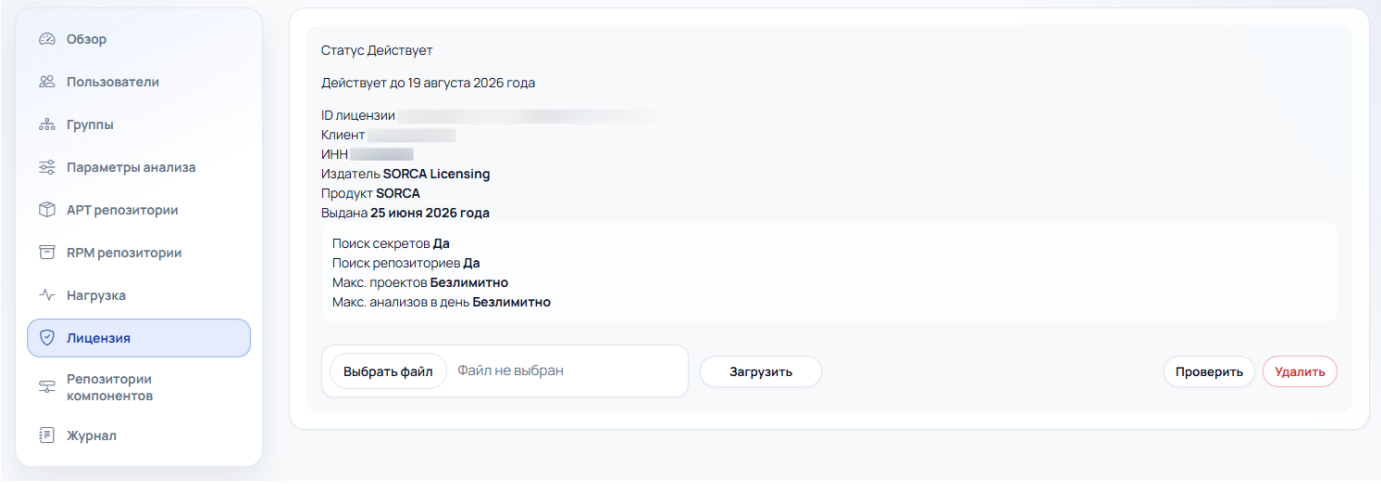

Рисунок 34 – Вкладка «Лицензия»

– вкладка «Репозитории компонентов» (рисунок 35) – позволяет отслеживать и управлять базой данных репозиториев/архивов с исходными текстами компонентов.

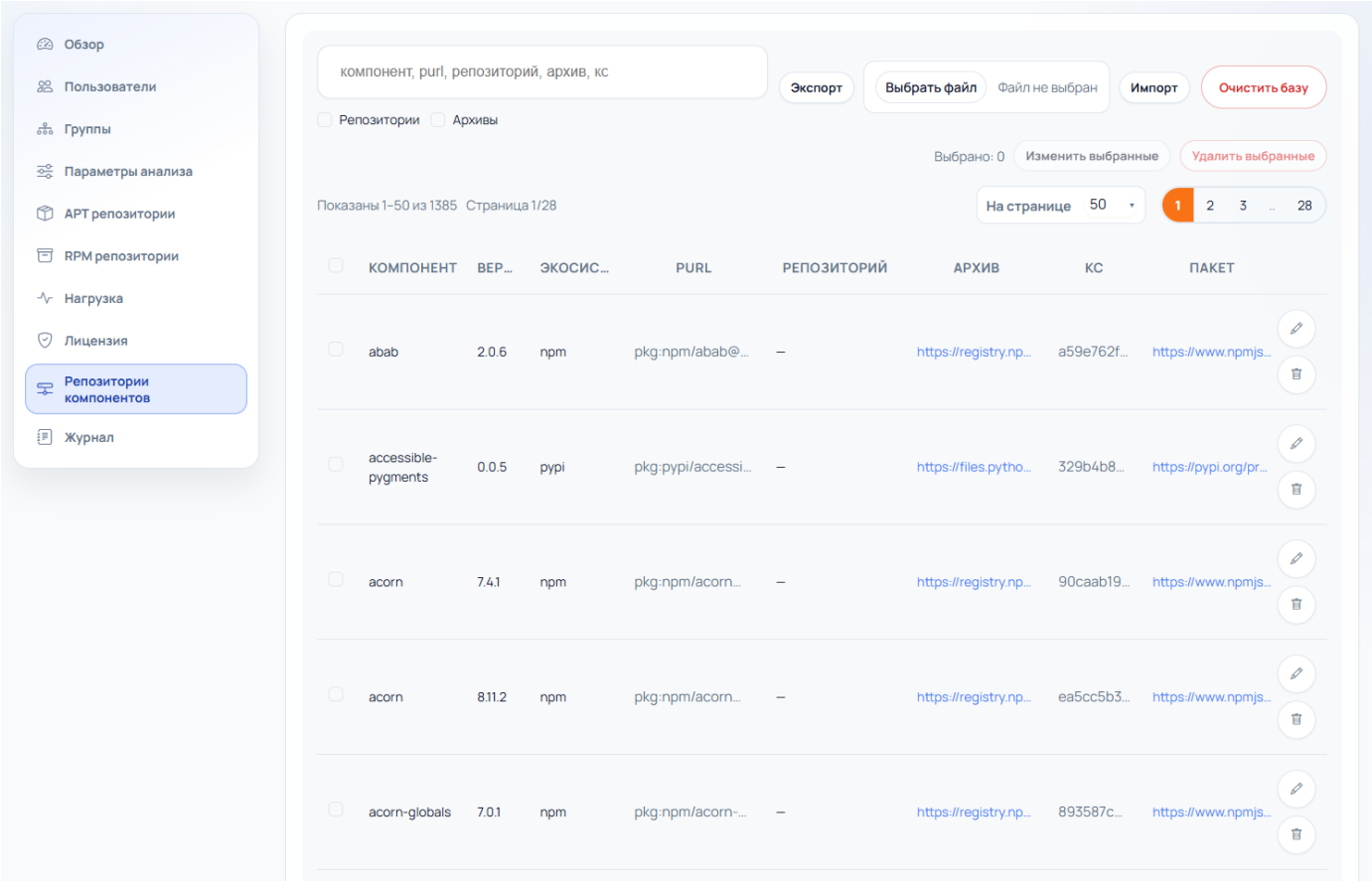

Рисунок 35 – Вкладка «Репозитории компонентов»

– вкладка «Журнал» (рисунок 36) – позволяет отслеживать действия в приложении.

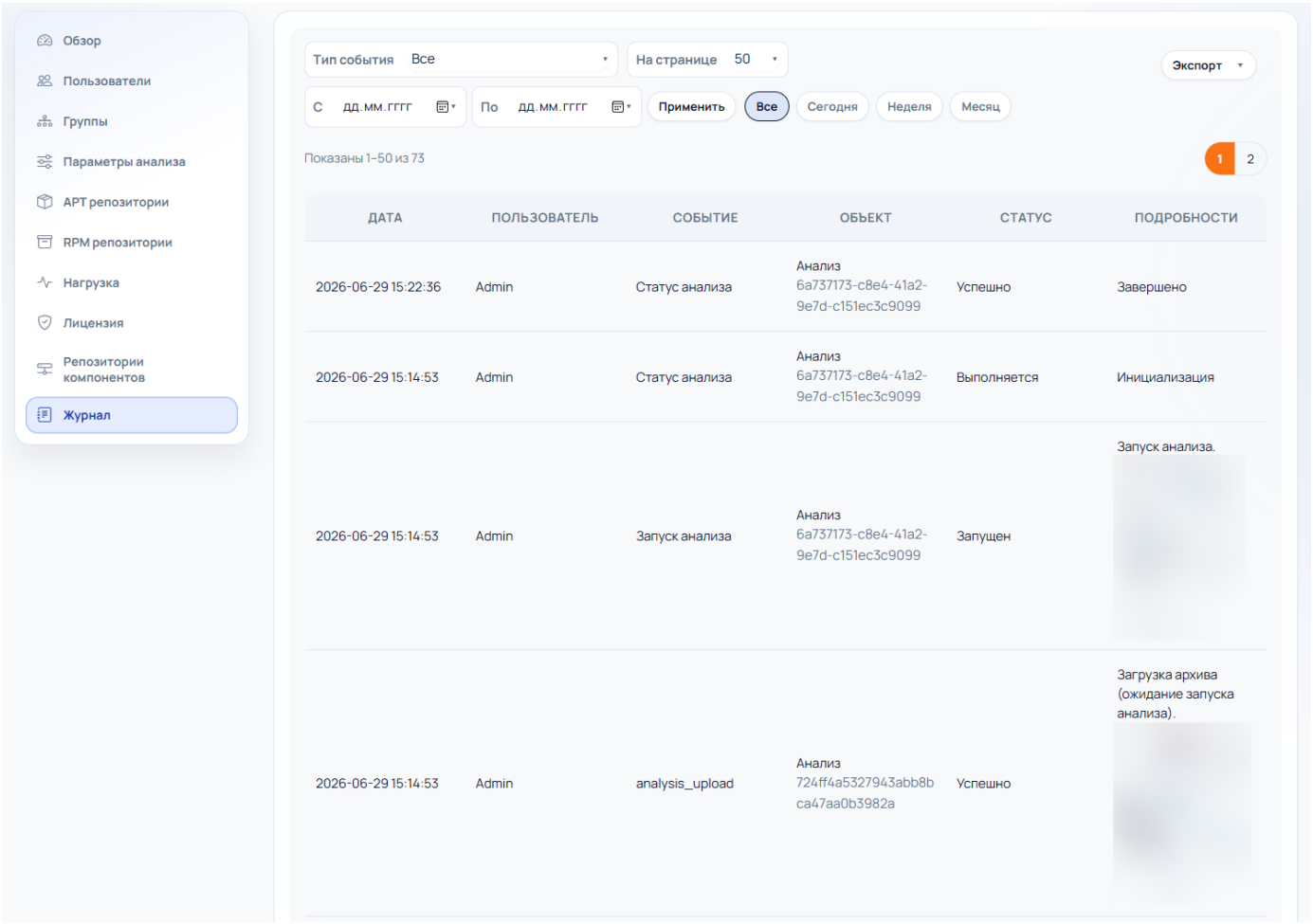

Рисунок 36 – Вкладка «Журнал»

3.5 Вкладка «Профиль»

Вкладка содержит основную информацию о профиле пользователя (рисунок 37), а также позволяет:

- редактировать профиль (рисунок 38);
- менять пароль (рисунок 39);
- добавлять доступ к закрытым репозиториям Github и Gitlab (рисунок 40);
- генерировать API-ключ для доступа консольного агента к основному приложению, а также скачивать конфигурационный файл для консольного агента и непосредственно сам консольный агент (рисунок 41).

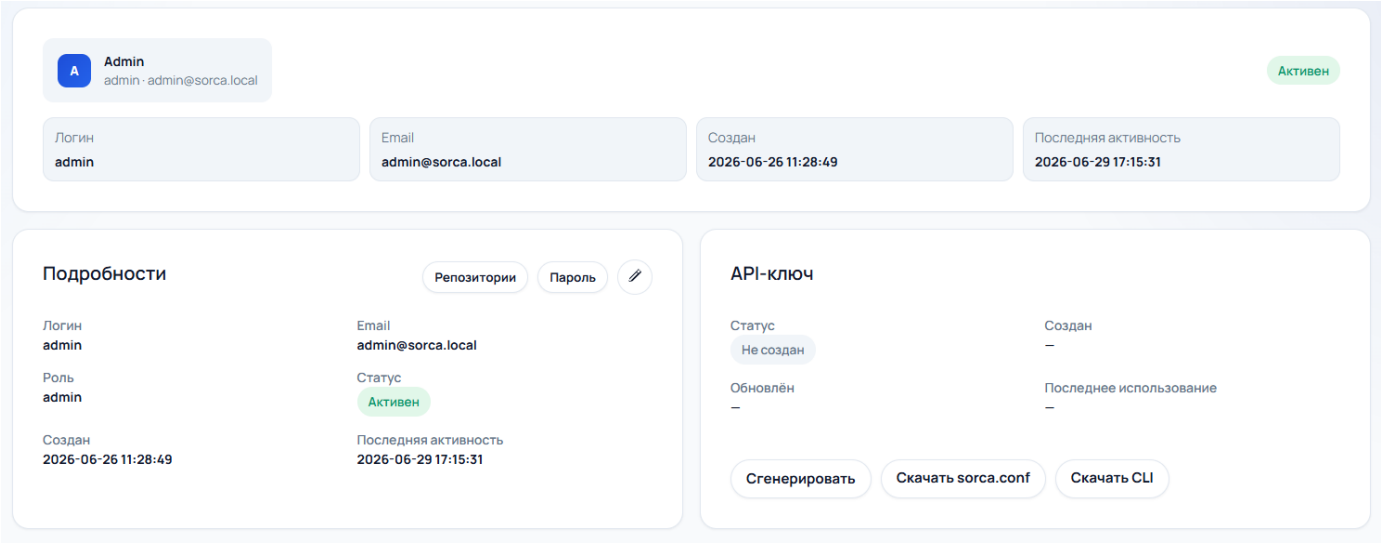

Рисунок 37 – Основная информация о профиле пользователя

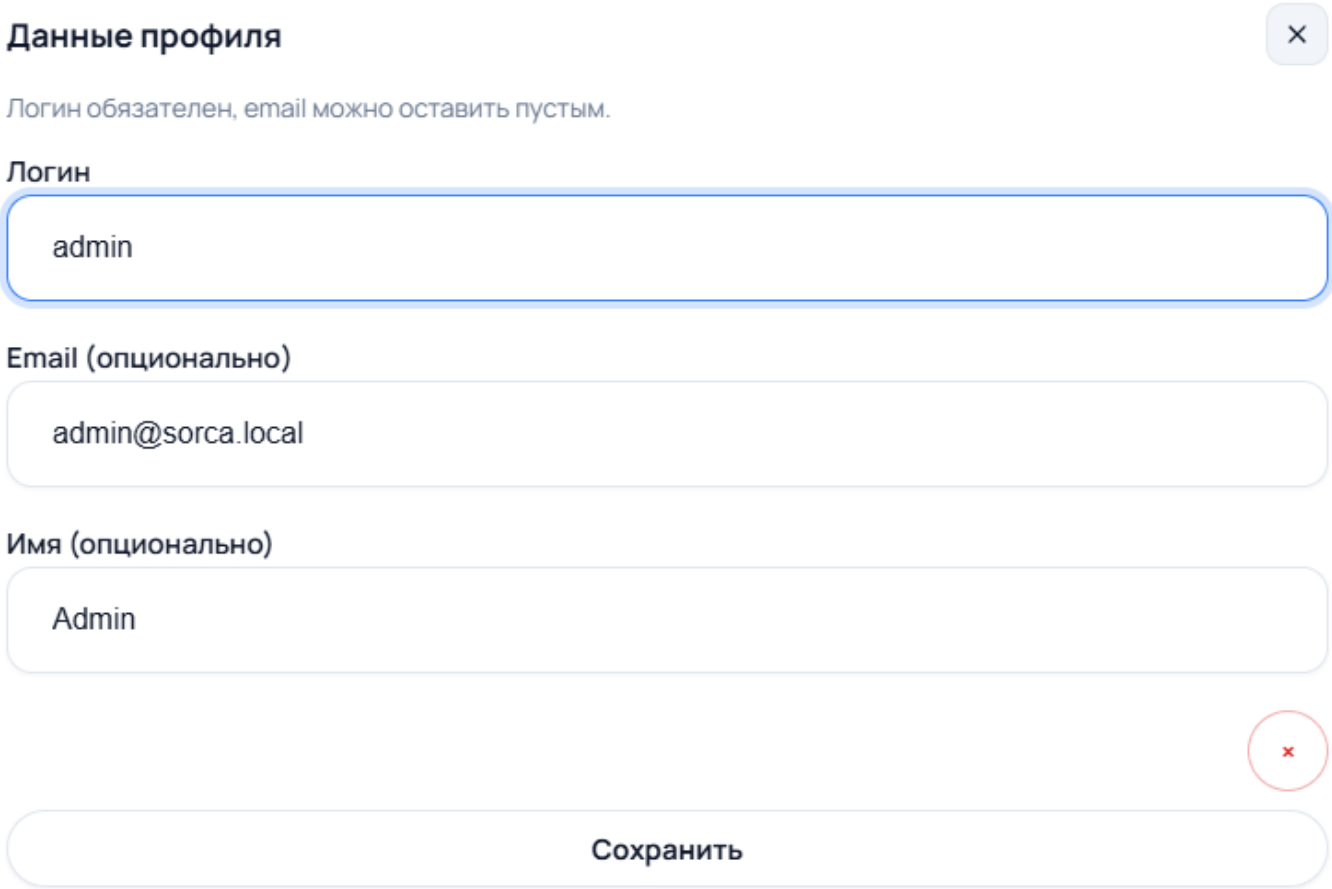

Рисунок 38 – Редактирование профиля

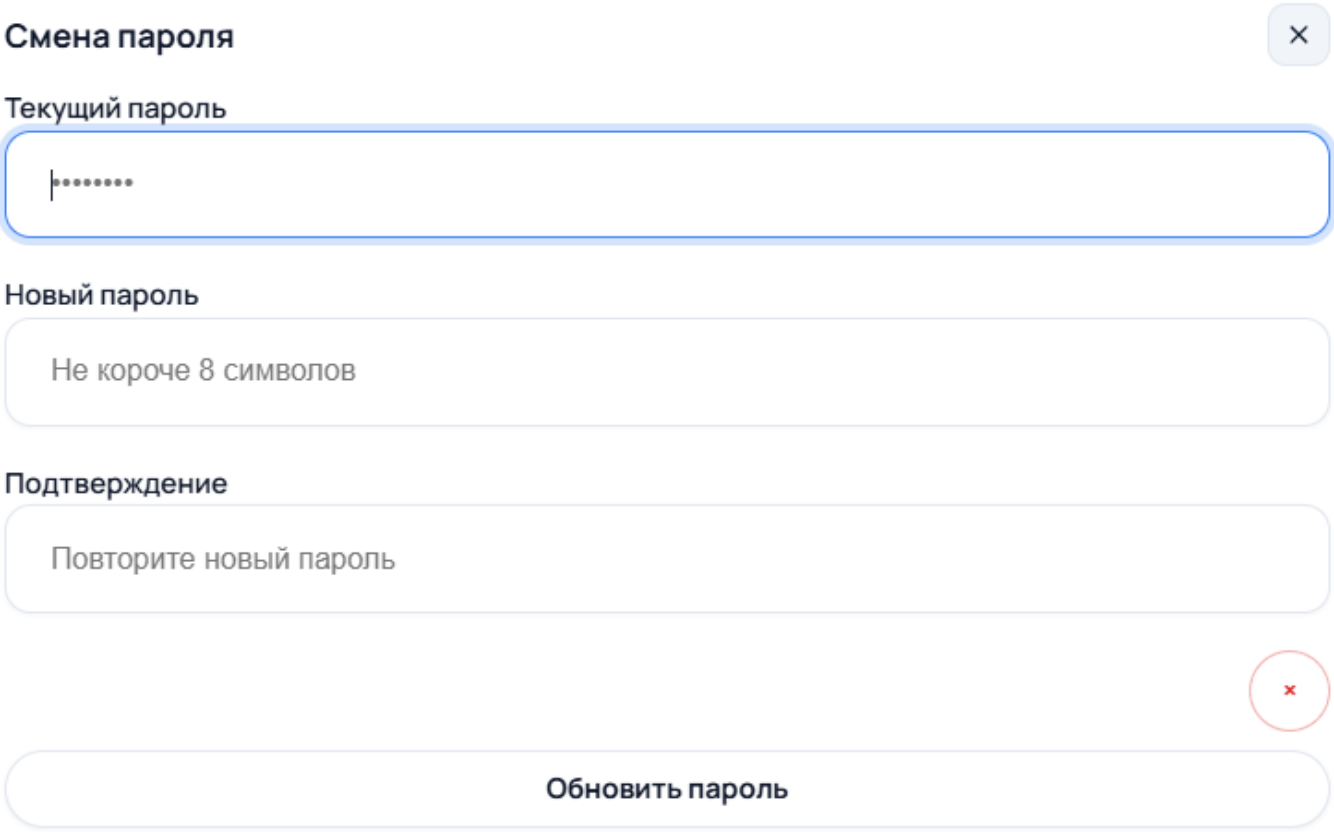

Рисунок 39 – Смена пароля

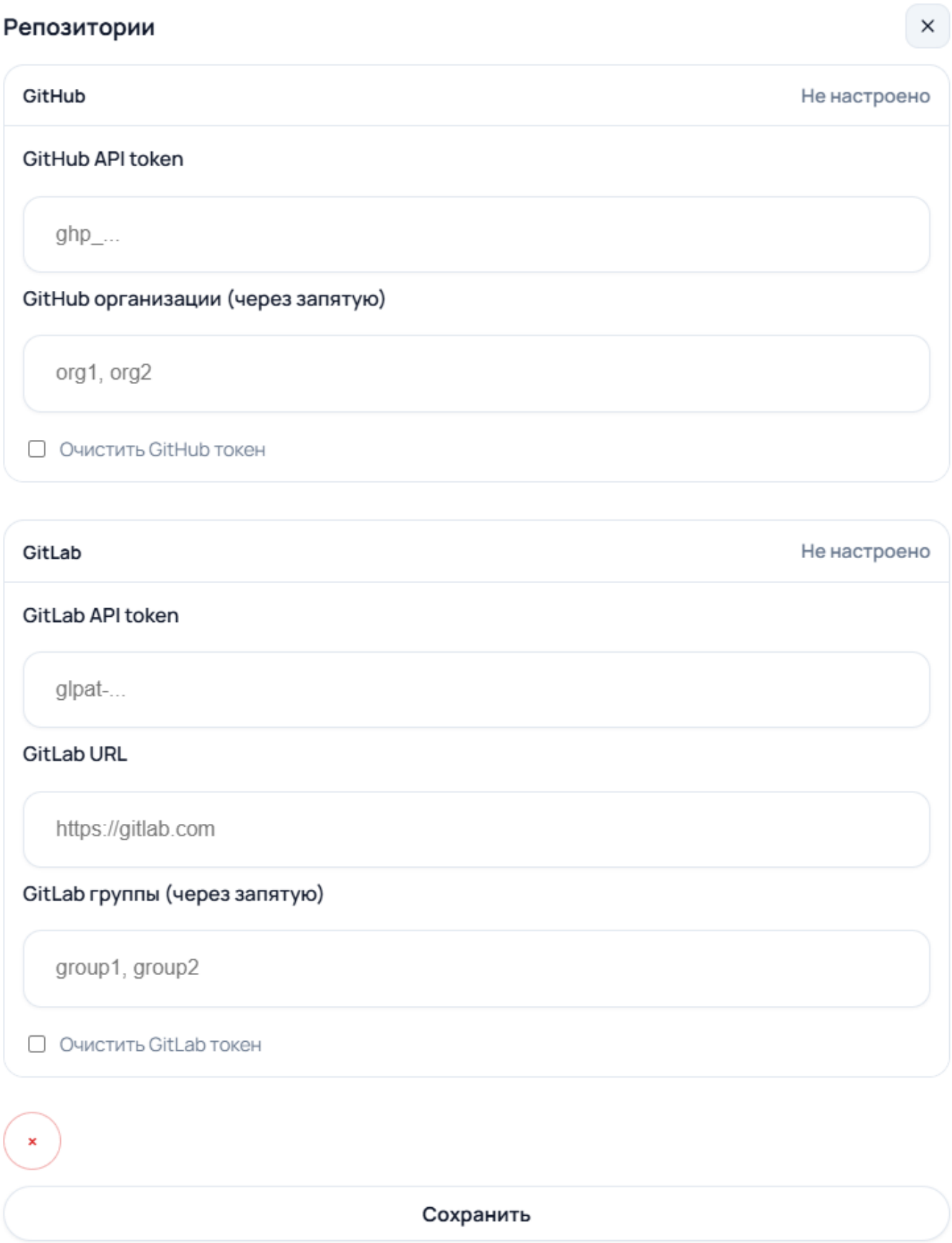

Рисунок 40 – Работа с репозиториями

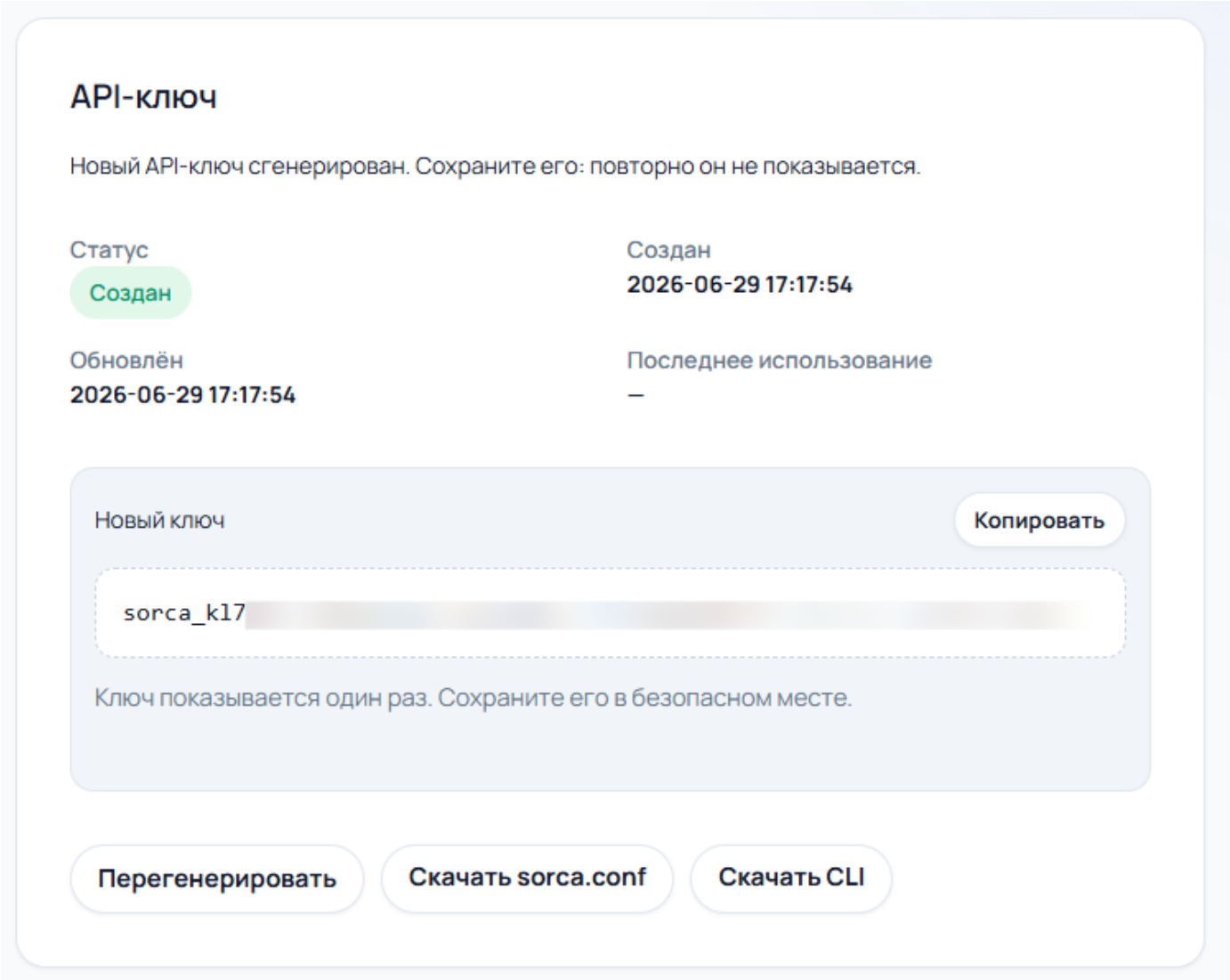

Рисунок 41 – Работа с API

4 Консольный агент

Перед началом работы с консольным агентом требуется произвести конфигурацию файла sorca.conf. Пример содержимого конфигурационного файла представлен в таблице 3.

Таблица 3 – Средства контроля и тестирования

Ключ	Описание	Пример значения
server_url=	Адрес сервера приложения, к которому будет обращаться агент	http://localhost:18080
api_key=	API ключ (рисунок 33) для обращения к серверу приложения	sorca_eIuWxYU2ghpf HbsDEkHiEEjwpnkgndT ZEYE87462V6Xkqp5gIJ
project_id=	ID проекта	55bad7f6-d236-432a-b7d6-08d57a594da2
project_name=	Название проекта	console-demo
default_mode=	watch – запускает анализ и ждёт завершения, периодически опрашивая статус раз в poll_interval_sec=, также выводит текущий статус в консоль =sumbit – запускает и не ждёт ничего, возвращает task_id	watch/submit
poll_interval_sec=	Интервал опроса сервера в процессе ожидания результатов анализа	2
components_scan=	Формирует список заимствованных компонентов проекта	true/false
vuln_scan=	Проверяет заимствованные компоненты проекта на предмет наличия в них известных уязвимостей	true/false
deps_pull=	Ищет зависимости проекта через системы сборки и менеджеры пакетов	true/false
jar_unpack=	Извлекает содержимое Java-архивов (.jar/, .war/, .ear) внутри архива проекта	true/false
pkg_unpack=	Извлекает содержимое пакетов (.rpm/, .apk/, .nupkg/, .whl/, .deb) внутри архива проекта	true/false
container_scan=	Анализирует установленные пакеты в контейнерах без учета транзитивности	true/false
sbom_archive=	Анализ архива с несколькими SBOM JSON (каждый файл анализируется отдельно)	true/false
repo_lookup=	Поиск ссылок на репозитории и архивы с исходными кодами заимствованных компонентов проекта	true/false
secret_scan=	Ищет ключи, токены и пароли в файлах проекта	true/false

ВНИМАНИЕ! project_id и project_name одновременно не задаются.

Параметры конфигурации:

- По умолчанию sorca.conf ищется рядом с бинарным файлом, затем в /srv/sorca.
- Если файл не найден, агент предложит создать его интерактивно.

– Если проект не задан, сервер создаст проект вида console-<индекс>.

Короткие опции (флаги) представлены в таблице 4. Команды для использования консольного агента представлены в таблице 5.

Таблица 4 – Опции

Опция	Описание
-c, --conf, --config <path>	Путь к sorca.conf
-u, --url, --server <url>	Адрес сервера SORCA
-k, --key, --api-key <key>	API-ключ пользователя
-p, --project <name>	Имя проекта
-i, --pid, --project-id <uuid>	Идентификатор проекта
-a, --aid, --analysis-id <uuid>	Использовать конкретный анализ
-t, --type <kind>	Тип отчёта: vulns|secrets
-o, --out, --output <path>	Путь для сохранения файла отчёта
-s, --severity <level>	Фильтр уровня: critical|high|medium|low|unknown
-n, --limit <count>	Ограничить число строк вывода
-w, --watch	Следить за прогрессом после запуска
-q, --submit-only	Только отправить анализ и вернуть task_id
-D, --param <key>=<bool>	Переопределить параметр анализа

Таблица 5 – Команды

Команда	Описание	Доступные опции
sorca <архив>	Запустить анализ по умолчанию и следить за прогрессом	
sorca run <архив> [опции]	То же, что и запуск по умолчанию	Принимают архив как позиционный аргумент и опции -c/-u/-k/-p/-i/-w/-q/-D
sorca submit <архив> [опции]	Только отправить анализ и вернуть task_id	
sorca status <task_id> [опции]	Получить текущий статус задачи	Принимают task_id как позиционный аргумент и опции -c/-u/-k
sorca watch <task_id> [опции]	Следить за статусом существующей задачи	
sorca projects [опции]	Показать доступные проекты	Показывает корневые проекты, доступны опции -c/-u/-k
sorca subprojects [опции]	Показать подпроекты проекта	Требует -p <имя> или -i <uuid>, доступны опции -c/-u/-k
sorca summary [опции]	Показать сводку последнего анализа проекта	Показывает сводку по -a <analysis_id> либо по последнему анализу проекта из -p/-i
sorca vulns [опции]	Показать уязвимости последнего анализа проекта	Показывает уязвимости по -a <analysis_id> либо по последнему анализу проекта из -p/-i. Дополнительно поддерживает -s <severity> и -n <limit>
sorca report [опции]	Скачать HTML-отчёт	Скачивает HTML-отчёт по -a <analysis_id> либо по последнему анализу проекта из -p/-i. Требует -t vulns|secrets.

Команда	Описание	Доступные опции
		-o может указывать директорию или полный путь к файлу. Если задана директория, имя файла выбирается автоматически
sorca init [опции]	Создать или обновить sorca.conf	Создаёт или обновляет sorca.conf, доступна опция -c <path>
sorca -h | --help	Показать справку	