

Платформа для управления  
уязвимостями и обеспечения  
безопасности в процессах разработки и  
DevSecOps “TRON.ASOC v.1.0”

Руководство пользователя

Октябрь 2024

## Содержание

|   |    |
|---|----|
| 1. Введение   | 3  |
| 2. Термины и определения  | 4  |
| 3. Общие сведения   | 6  |
| 4. Установка решения  | 8  |
| 5. Начало работы в системе  | 9  |
| 6. Интерфейс  | 10 |
| 7. Главное меню   | 11 |
| 8. Информационная панель  | 12 |
| 9. Проекты  | 12 |
| 9.1. Создание нового проекта  | 13 |
| 9.2. Редактирование проекта   | 13 |
| 9.3. Раздел Обзор   | 15 |
| 9.4. Конвейеры безопасности и проверки безопасности                                   | 15 |
| 9.4.1. Создание конвейера безопасности  | 16 |
| 9.4.2. Создание проверки безопасности   | 17 |
| 9.4.3. Редактирование проверки безопасности   | 20 |
| 9.4.4. Запуск конвейера безопасности  | 20 |
| 9.4.5. Запуск проверки безопасности   | 21 |
| 9.4.6. Остановка сканирования   | 21 |
| 9.4.7. Загрузка отчета  | 21 |
| 9.4.8. Использование CLI-инструментов   | 22 |
| 9.5. Результаты сканирований  | 23 |
| 9.6. Контроли качества  | 24 |
| 9.7. Проблемы безопасности  | 26 |
| 10. Контроли качества   | 27 |
| 11. Правила безопасности  | 29 |
| 12. Правила дедупликации  | 32 |
| 13. Отчеты  | 33 |
| 14. Требования к аппаратным и программным характеристикам рабочего места пользователя | 34 |

# 1. Введение

Настоящий документ представляет собой руководство пользователя программного комплекса TRON.ASOC.

## 2. Термины и определения

| Термин/сокращение   | Определение  |
|---|--|
| ПО  | Программное обеспечение  |
| ASOC (Application Security Orchestration and Correlation)   | платформы или решения, предназначенные для управления и координации безопасностью приложений. ASOC позволяет автоматизировать процессы обнаружения, анализа и реагирования на угрозы безопасности, связанные с приложениями.   |
| DAST (Dynamic Application Security Testing)   | Динамический анализ кода — анализ программного обеспечения без доступа к исходному коду, реализуемый при помощи выполнения программ. Процесс тестирования приложений, имитирующий вредоносные внешние атаки, пытающиеся использовать распространенные уязвимости.              |
| DevSecOps   | методология разработки программного обеспечения, которая интегрирует практики безопасности (Sec) в процессы разработки и поставки программного обеспечения (DevOps).   |
| Анализ открытого программного обеспечения (OSA, Open Source Analysis) / Анализ структуры программного обеспечения (SCA, | Анализ библиотек и компонентов с открытым исходным кодом, которые входят в периметр разработки программного обеспечения, а также уже используются в качестве артефактов в приложении. Анализ проводится с точки зрения известных уязвимостей безопасности и нарушений лицензий |

|  |  |
|--|--|
| Software Composition Analysis)             |  |
| SAST (Static Application Security Testing) | это процесс тестирования приложения на наличие ошибок и уязвимостей в исходном коде с применением статического анализа. Статический анализ может применяться для поиска кода, потенциально содержащего уязвимости  |
| IaC (инфраструктура как код)               | это подход к созданию и управлению инфраструктурой через использование кода, например, конфигурационных файлов или скриптов.   |
| Container Security                         | подход к защите и безопасной настройке систем контейнеризации, общее понятие, охватывающее набор различных инструментов и методов для защиты контейнеров от возможных угроз и атак.  |
| Проект                                     | это сущность, которая создается авторизованным пользователем, чтобы логически объединить весь набор связанных приложений или компонентов, которые разрабатываются или поддерживаются в рамках одной команды или организации, и который нужно проверять на соответствие политикам безопасности компании и качество. |
| AST (Application Security Testing)         | Тестирование безопасности приложений   |
| Интеграция                                 | обмен данными между системами с возможной последующей обработкой.  |

### 3. Общие сведения

- «TRON.ASOC» - программный продукт, платформа для обнаружения и управления уязвимостями, а также обеспечения безопасности в процессах разработки и DevSecOps.
- Продукт позволяет осуществлять всесторонний контроль безопасности разрабатываемых проектов, обеспечивая надежную защиту на всех этапах разработки.
- Есть возможность интеграции с Git-репозиториями, реестром образов Nexus и различными инструментами анализа безопасности разрабатываемых продуктов (PT Application Inspector, Kaspersky Container Security, Solar AppScreener, CodeScoring и OWASP Dependency Track), а также возможность принимать и анализировать отчеты от инструментов Trivy, Grupte, KICS для дальнейшей обработки полученных от них результатов.
- Программа управляет проверками исходного кода и образов контейнеров на уязвимости и помогает управлять результатами этих проверок. Интеграция с этими инструментами позволяет настроить сканирование, запускать проверки и консолидировать результаты.
- Платформа упрощает работу с найденными при помощи инструментов AST проблемами и уязвимостями, проводя их анализ и группировку для более эффективного управления.
- Система осуществляет консолидацию и визуализацию данных, предоставляя пользователям наглядную информацию о состоянии безопасности их проектов.
- «TRON.ASOC» предлагает удобный пользовательский интерфейс, доступный в современных браузерах на движке Chromium (Google Chrome, Яндекс Браузер, Edge, Safari и т.д.) и Firefox.

- Система предоставляет возможности для управления сканированиями, включая настройку параметров сканирования, планирование запусков и мониторинг выполнения сканирований.
- Решение позволяет выгружать отчеты по проектам в форматах JSON, CSV, PDF, что обеспечивает удобство интеграции с другими системами и инструментами анализа данных.

## 4. Установка решения

Решение поставляется в виде образов контейнеров. Установка состоит из следующих этапов:

### 1. Установка компонентов.

Скачать архив `docker-compose`

Запустить скрипт `show.sh` - он выведет значения переменных из файла `docker-compose.yaml` для проверки `./show.sh`

Задать значения переменной для `ASOC_DOMAIN`

Актуализировать значения переменных: `ASOC_IMG_FRONT`,  
`ASOC_IMG_CORE`, `ASOC_IMG_PSQL`, `ASOC_IMG_NGINX`,  
`ASOC_PROXY_PORT`

Выполнить `docker login <адрес реестра>` (адрес будет предоставлен вендором)

Выполнить `docker-compose up -d`

Проверить статус контейнеров `docker ps`

### 2. Первый запуск консоли управления.

3. Настройка. После завершения установки нужно подготовить решение к работе:

- Настроить интеграцию с инструментами безопасности
- Настроить интеграцию с источниками

## 5. Начало работы в системе

Ссылка для входа в систему предоставляется администратором. При переходе по ссылке пользователь попадает на страницу авторизации. Чтобы войти в систему, введите логин и пароль и нажмите кнопку **“Войти”** (Рис.1).

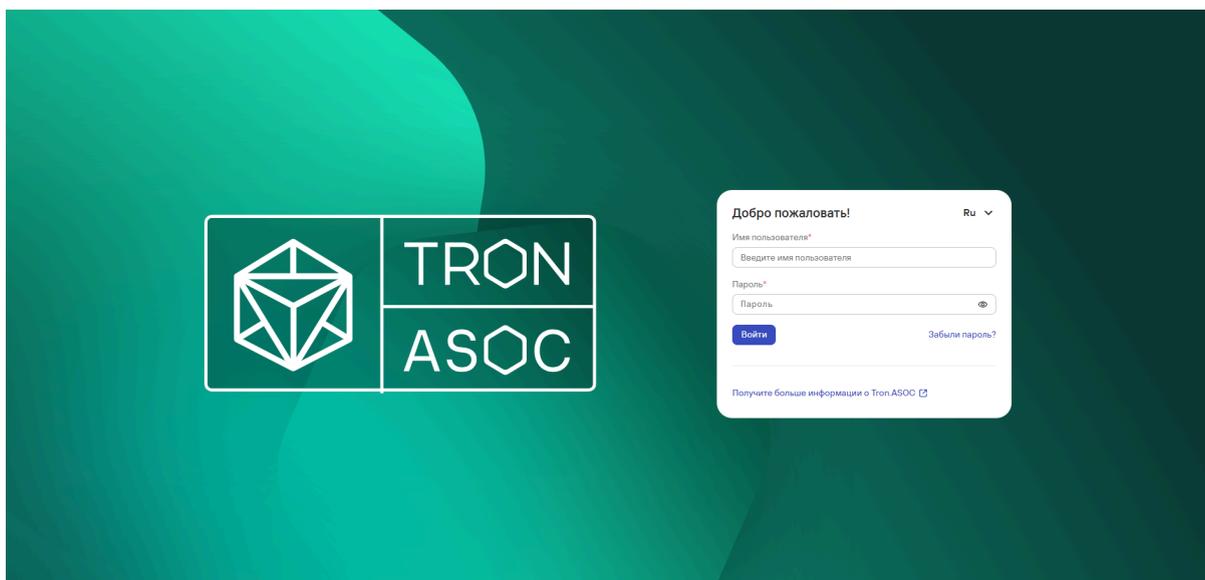


Рис. 1

По запросу измените текущий пароль учетной записи: укажите новый пароль и подтверждение пароля и нажмите на кнопку **“Изменить”**. При вводе неверных учетных данных на экране отобразится сообщение **“Неверный логин и/или пароль”**. При превышении числа попыток аутентификации с неверным паролем ваш аккаунт будет временно заблокирован. Количество попыток аутентификации и продолжительность блокировки устанавливается администратором системы (по умолчанию лимит попыток входа — 3, срок блокировки — 1 минута). После успешного входа в систему отображается домашняя страница с [Информационной панелью](#).

## 6. Интерфейс

Консоль управления реализована в виде веб-интерфейса и состоит из следующих элементов:

- Главное меню: разделы и подразделы главного меню обеспечивают доступ к основным функциям решения.
- Рабочая область: информация и элементы управления в рабочей области зависят от раздела или подраздела, выбранного в главном меню.

### Некоторые способы настройки отображения данных

Для табличных представлений в интерфейсе TRON.ASOC предусмотрены следующие способы настройки отображения данных:

- Фильтрация.

Поля фильтра расположены над таблицами данных. Состав полей фильтра и способы управления фильтром зависят от специфики данных, отображаемых в разделе. В некоторых разделах для открытия полей фильтра требуется нажать на значок фильтра (рис 2).

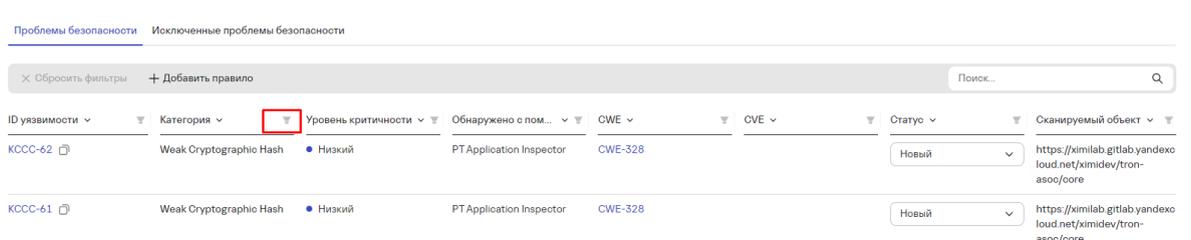


Рис.2

- Сортировка по возрастанию или убыванию.

В некоторых разделах вы можете сортировать список данных по выбранному столбцу с помощью значков в заголовке столбца (рис. 3)

Проблемы безопасности | Исключенные проблемы безопасности

✕ Сбросить фильтры + Добавить правило

| ID уязвимости | Категория               | Уровень критичности | Обнаружено с пом...      | CWE     | CVE | Статус | Сканируемый объект  |
|---------------|-------------------------|---------------------|--------------------------|---------|-----|--------|---|
| KCCC-62       | Weak Cryptographic Hash | Низкий              | PT Application Inspector | CWE-328 |     | Новый  | https://ximilab.gitlab.yandexo<br>loud.net/ximidev/tron-<br>asoc/core |
| KCCC-61       | Weak Cryptographic Hash | Низкий              | PT Application Inspector | CWE-328 |     | Новый  | https://ximilab.gitlab.yandexo<br>loud.net/ximidev/tron-<br>asoc/core |

Рис. 3

## ● Поиск.

Вы можете выполнять поиск по отображаемым данным с помощью поля Поиск, расположенного над таблицей. (рис. 4)

Проблемы безопасности | Исключенные проблемы безопасности

✕ Сбросить фильтры + Добавить правило

| ID уязвимости | Категория               | Уровень критичности | Обнаружено с пом...      | CWE     | CVE | Статус | Сканируемый объект  |
|---------------|-------------------------|---------------------|--------------------------|---------|-----|--------|---|
| KCCC-62       | Weak Cryptographic Hash | Низкий              | PT Application Inspector | CWE-328 |     | Новый  | https://ximilab.gitlab.yandexo<br>loud.net/ximidev/tron-<br>asoc/core |
| KCCC-61       | Weak Cryptographic Hash | Низкий              | PT Application Inspector | CWE-328 |     | Новый  | https://ximilab.gitlab.yandexo<br>loud.net/ximidev/tron-<br>asoc/core |

Рис. 4

## 7. Главное меню

В левой части страницы расположено сайд-бар меню, которое предоставляет доступ к следующим разделам продукта: [Проекты](#), Проблемы безопасности, Администрирование: Управление доступом, Интеграции, Контроль качества, Отчеты, Правила исключения, Правила дедупликации, Параметры подключения, О программе. Видимость разделов меню зависит от набора привилегий и прав роли пользователя.

## 8. Информационная панель

Информационная панель (рис.5) - дает возможность отследить наиболее важные метрики по доступным пользователю проектам в разработке.

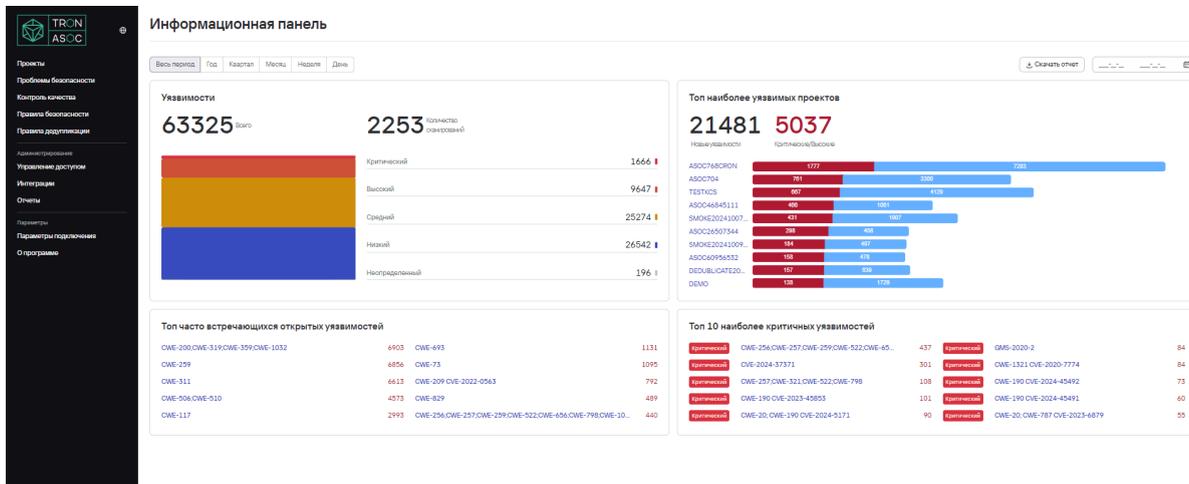


Рис. 5

## 9. Проекты

Проекты - это раздел, который содержит информацию о всех доступных проектах, а также меню для управления проектами. Все созданные и доступные пользователю проекты представлены в виде списка.

**Проекты**

[Создать отчет](#) [+ Добавить проект](#) [X Сбросить фильтры](#)

| Имя проекта                          | Дата добавления  | Дата обновления  | Теги          | Код проекта      | Действия |
|--------------------------------------|------------------|------------------|---------------|------------------|----------|
| PROJECTNAME                          | 23/10/2024 09:38 | 23/10/2024 09:38 | NOTAGS        | PROJECTCODE      |          |
| zzzz                                 | 21/10/2024 18:31 | 21/10/2024 18:31 | fuzzz         | Z324             |          |
| oock11                               | 21/10/2024 18:30 | 21/10/2024 18:30 |               | 10000000F        |          |
| test 21 oot                          | 21/10/2024 18:28 | 21/10/2024 18:28 | newtag, новый | MYPROJ21         |          |
| 234234324234234                      | 18/10/2024 18:36 | 18/10/2024 18:36 | test          | 43423423424      |          |
| DEMO                                 | 07/08/2024 12:29 | 07/08/2024 12:29 |               | DEMO             |          |
| ASOC22072024PTAI_2024-07-22 14:50:46 | 22/07/2024 17:50 | 22/07/2024 17:50 |               | ASOC22072024PTAI |          |
| KCCC                                 | 22/07/2024 17:31 | 22/07/2024 17:31 |               | KCCC             |          |
| 12345                                | 08/07/2024 18:29 | 08/07/2024 18:29 |               | 12345            |          |
| TEST                                 | 14/06/2024 16:55 | 08/07/2024 13:16 |               | TEST             |          |

Всего 11 / Выбрано 0 < 1 2 > 10 / страница

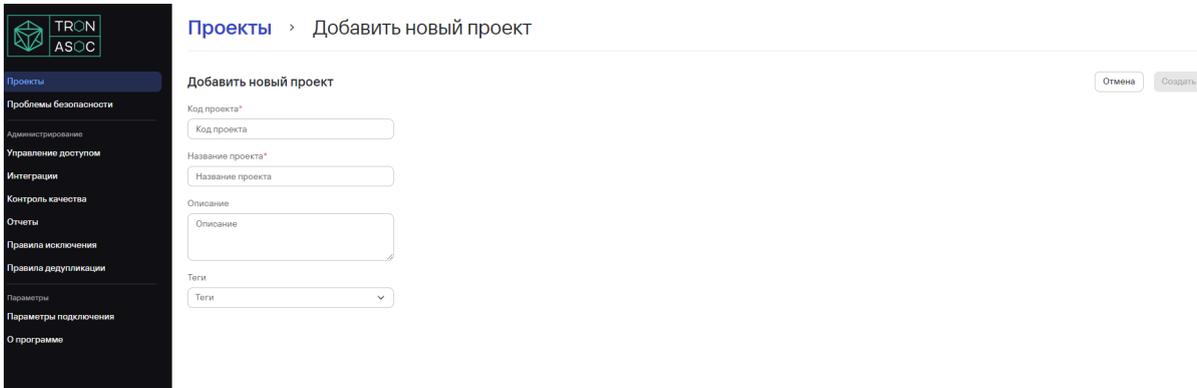
Рис.6

Для каждого проекта отображаются следующие данные: имя проекта, теги, код проекта, доступные действия. В меню действий можно удалить (архивировать) проект и перейти на страницу редактирования проекта. В списке вы можете выполнять следующие действия:

- Выполнять поиск по названию проекта.
- Фильтровать список по тегам.
- Сортировать список по имени, тегу или коду проекта.
- Просмотреть подробную информацию о проекте при нажатии на имя проекта

## 9.1. Создание нового проекта

Чтобы создать новый проект, нажмите кнопку **“Добавить проект”** на странице Проекты. На странице создания проекта (рис.7) заполните поля Код проекта, Имя проекта, Тег, Описание и нажмите кнопку **“Создать”**.



The screenshot shows the 'Добавить новый проект' (Add New Project) form in the TRON ASOC application. The interface includes a dark sidebar menu on the left with the TRON ASOC logo and various navigation options. The main content area has a breadcrumb trail 'Проекты > Добавить новый проект' and a title 'Добавить новый проект'. The form contains the following fields: 'Код проекта\*' (Project Code) with a text input, 'Название проекта\*' (Project Name) with a text input, 'Описание' (Description) with a larger text area, and 'Теги' (Tags) with a dropdown menu. At the top right of the form area, there are two buttons: 'Отмена' (Cancel) and 'Создать' (Create).

Рис. 7

## 9.2. Редактирование проекта

Редактирование проекта доступно по кнопке меню действий в списке проектов (рис.8).

## Проекты

| Имя проекта     | Теги | Код проекта | Действия |
|-----------------|------|-------------|----------|
| 1233455         |      | 1233455     |          |
| 12345           |      | 12345       |          |
| 234234324234234 | test | 43423423424 |          |

Рис. 8

Также, чтобы отредактировать проект, можно перейти на страницу проекта, нажав на имя проекта и затем во вкладке Настройки (рис.9) перейти к редактированию проекта. Форма редактирования проекта аналогична форме создания проекта.

Проекты > 1233455 > Настройки

Обзор Конвейеры безопасности Результаты сканирования Контроль качества Проблемы безопасности Виртуальный помощник **Настройки**

### Настройки проекта

Отмена Редактировать проект

Название проекта  
Name

Описание  
Web store

Теги  
Option1 Option2

Менеджер  
Jake O.

Security champion  
Albert O.

Рис. 9

Можно отредактировать Код проекта, Имя проекта, Описание и Теги. После завершения редактирования, нажмите кнопку “**Сохранить**”. По нажатию на наименование проекта можно перейти к разделам внутри Проекта.

## 9.3. Обзор

Раздел Обзор (рис.10) предоставляет возможность просмотра Дашборда с информацией по часто встречающимся уязвимостям с разбивкой по критичности, источникам обнаружения и рейтингом наиболее критичных уязвимостей.

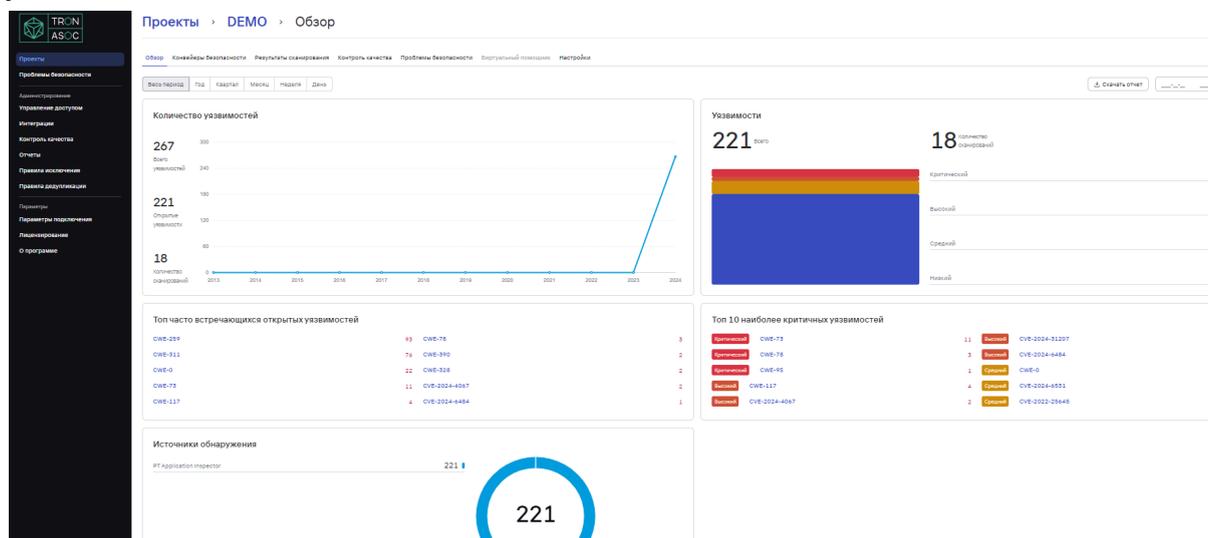


Рис. 10

## 9.4. Конвейеры безопасности и проверки безопасности

Работа с Конвейерами безопасности (пайплайнами) начинается на вкладке меню Конвейеры безопасности внутри каждого проекта.

В TRON.ASOC каждый Конвейер безопасности привязан к проекту. Конвейер безопасности- это группирующая сущность для Проверок безопасности. У пользователя есть возможность создания новых и настройки доступных ему уже созданных Конвейеров безопасности.

Чтобы начать работу с Конвейерами безопасности, перейдите на страницу Проекты, Имя проекта и откройте вкладку Конвейеры безопасности (рис.11). Каждый Конвейер безопасности представлен отдельной строкой, которая содержит название и описание конвейера, ссылку на результаты сканирования, содержащиеся внутри конвейера проверки безопасности.

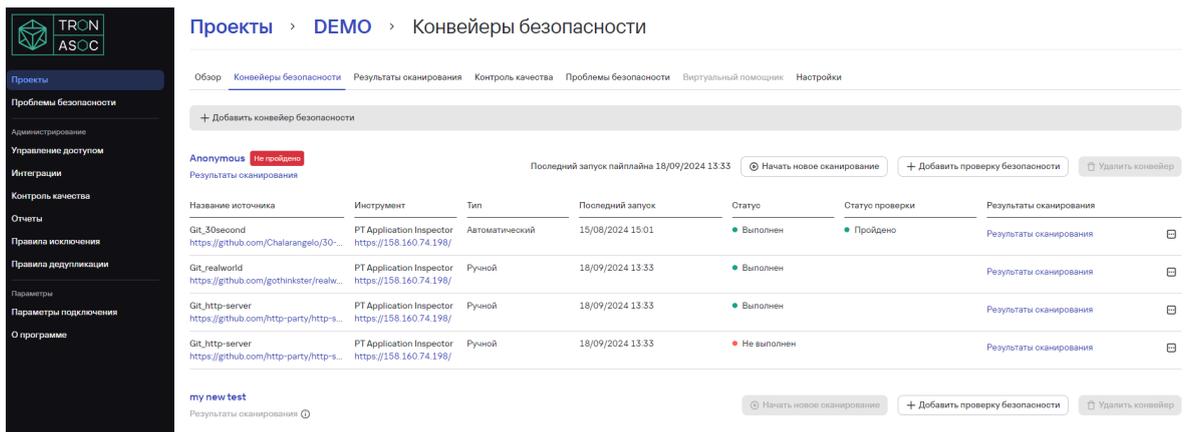


Рис. 11

### 9.4.1. Создание конвейера безопасности

Чтобы создать новый Конвейер безопасности, нажмите на кнопку “Добавить конвейер безопасности” (рис.12).

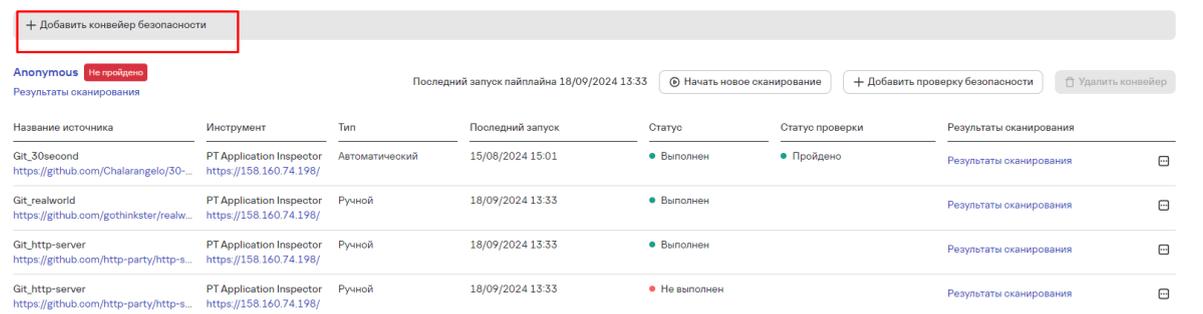


Рис. 12

На странице создания конвейера безопасности (рис.13) заполните поля **Имя** и **Описание** (обязательные поля отмечены звездочкой) и нажмите кнопку “Создать”.

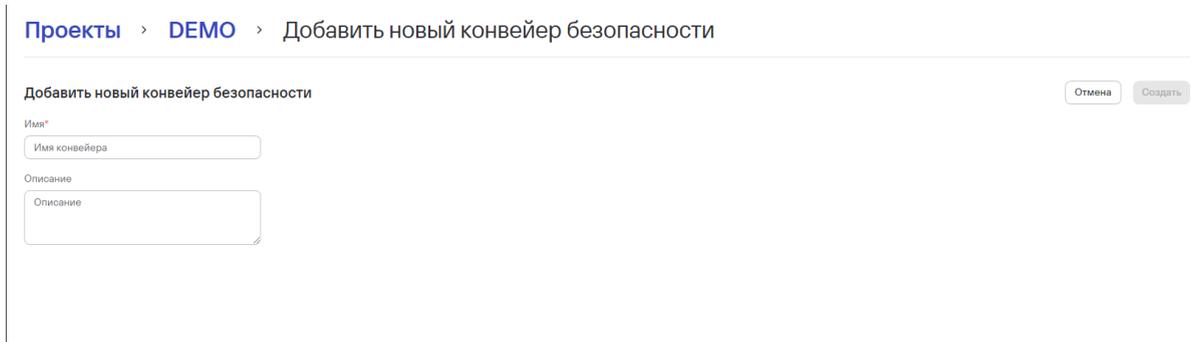
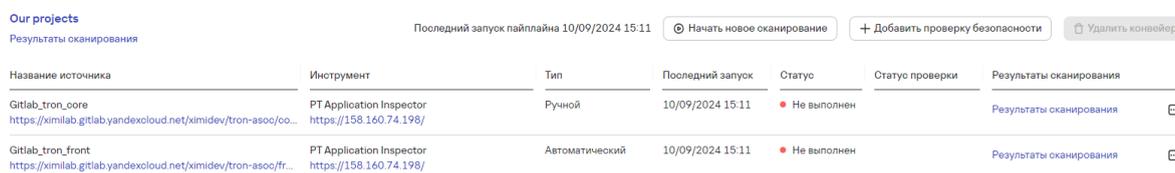


Рис. 13

После создания Конвейера безопасности нужно добавить к нему Проверку безопасности. Проверка безопасности - это сущность, которая может объединять в себе связку инструмента сканирования и источника. Она используется для запуска сканирования безопасности, а также для получения результатов сканирований. На странице Конвейеров безопасности можно увидеть название каждой проверки безопасности в конвейере, используемые в проверке инструменты безопасности и источники, тип проверки (ручной или автоматический), время последнего запуска, статус, ссылку на результаты сканирования (рис.14).



| Название источника   | Инструмент  | Тип            | Последний запуск | Статус        | Статус проверки | Результаты сканирования                 |
|--|---|----------------|------------------|---------------|-----------------|---|
| Gitlab_tron_core<br><a href="https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asoc/co...">https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asoc/co...</a>  | PT Application Inspector<br><a href="https://158.160.74.198/">https://158.160.74.198/</a> | Ручной         | 10/09/2024 15:11 | ● Не выполнен |                 | <a href="#">Результаты сканирования</a> |
| Gitlab_tron_front<br><a href="https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asoc/fr...">https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asoc/fr...</a> | PT Application Inspector<br><a href="https://158.160.74.198/">https://158.160.74.198/</a> | Автоматический | 10/09/2024 15:11 | ● Не выполнен |                 | <a href="#">Результаты сканирования</a> |

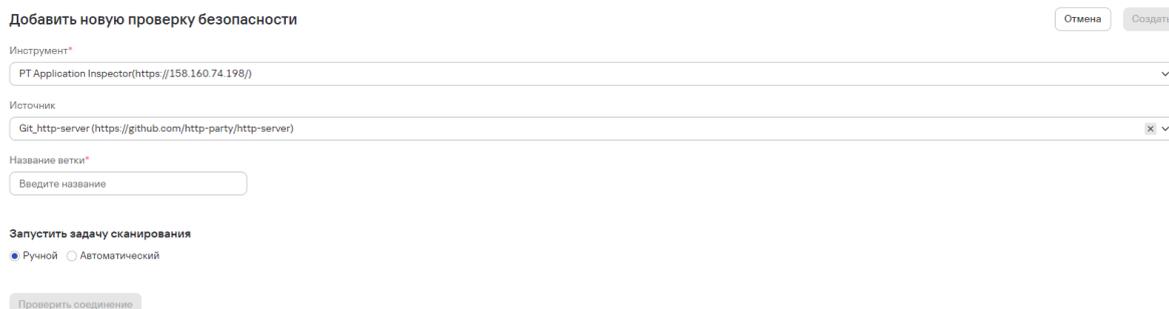
Рис. 14

## 9.4.2. Создание проверки безопасности



Рис. 15

Проекты > DEMO > Добавить новую проверку безопасности



Добавить новую проверку безопасности Отмена Создать

Инструмент\*

PT Application Inspector(<https://158.160.74.198/>)

Источник

Git\_http-server (<https://github.com/http-party/http-server>)

Название ветки\*

Введите название

Запустить задачу сканирования

Ручной  Автоматический

Проверить соединение

Рис. 16

Для настройки проверки безопасности выбор инструмента безопасности является обязательным (рис.15). Выбрать можно только инструмент, который был заранее добавлен администратором в разделе интеграции.

Если при создании интеграции с инструментом безопасности администратор не указал метод аутентификации, то при добавлении инструмента в Проверку безопасности поле выбора метода аутентификации является обязательным для заполнения. При выборе метода аутентификации на этапе создания проверки безопасности, введите данные для аутентификации в соответствующие поля (могут меняться в зависимости от метода: токен API, логин/пароль) (рис.16).

Пользователь может также добавить источник (объект) сканирования. Если при создании интеграции с источником администратор не указал метод аутентификации, то при добавлении источника в Проверку безопасности заполнение поля выбора метода аутентификации является обязательным. При выборе метода аутентификации на этапе создания проверки безопасности, введите данные для аутентификации в соответствующие поля (рис.17).

Проекты > DEMO > Добавить новую проверку безопасности

---

Добавить новую проверку безопасности Отмена Создать

Инструмент\*  
PT Application Inspector(https://158.160.74.198/) v

Источник  
GitTest (https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asoc/core) x v

Метод аутентификации\*    Логин\*    Пароль\*    Название ветки\*

Логин/Пароль            Введите название

Запустить задачу сканирования  
 Ручной     Автоматический

Рис. 17

Если заполнены все необходимые поля (инструмент безопасности, источник, методы аутентификации), можно проверить соединение с инструментами, нажав на кнопку **“Проверить соединение”** (рис.18).

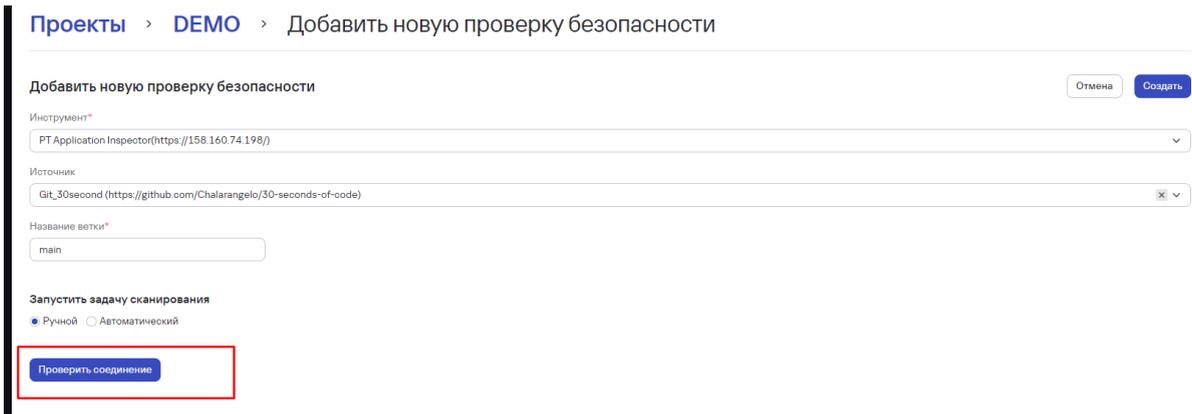


Рис. 18

Есть возможность выбрать тип запуска сканирования (ручной или автоматический), периодичность и время запуска сканирования при выборе автоматического запуска.

В проверках безопасности есть возможность не только запуска проверок, но и загрузки результатов сканирования от инструментов (рис.18). В зависимости от выбранного инструмента безопасности у чека может быть доступна опция получения результатов сканирования из внешних инструментов. Эта опция доступна не для всех инструментов безопасности.

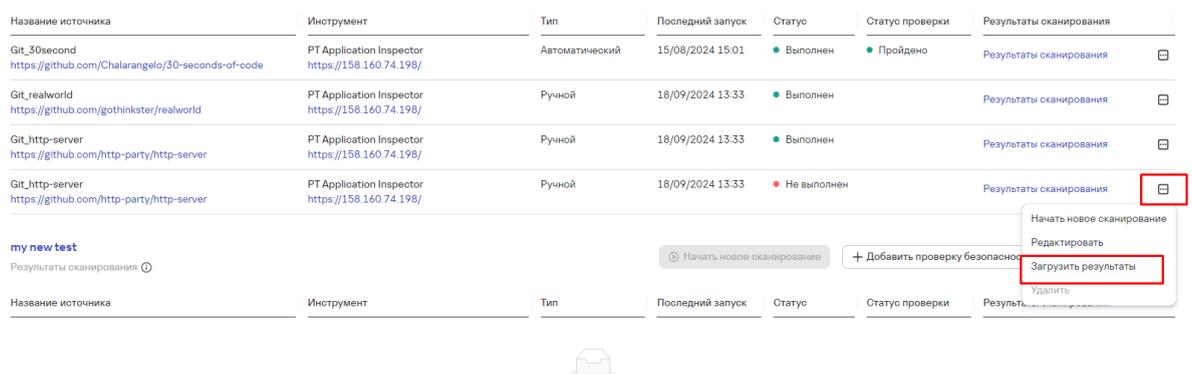


Рис. 19

### 9.4.3. Редактирование проверки безопасности

Чтобы отредактировать проверку безопасности, нажмите на Имя в списке доступных проверок безопасности. Форма редактирования аналогична форме создания новой проверки безопасности, но на форме редактирования есть блок Конечная точка API проверки безопасности (рис.20). В случае использования внешних скриптов используйте эту конечную точку API для отправки результатов сканирования инструмента.

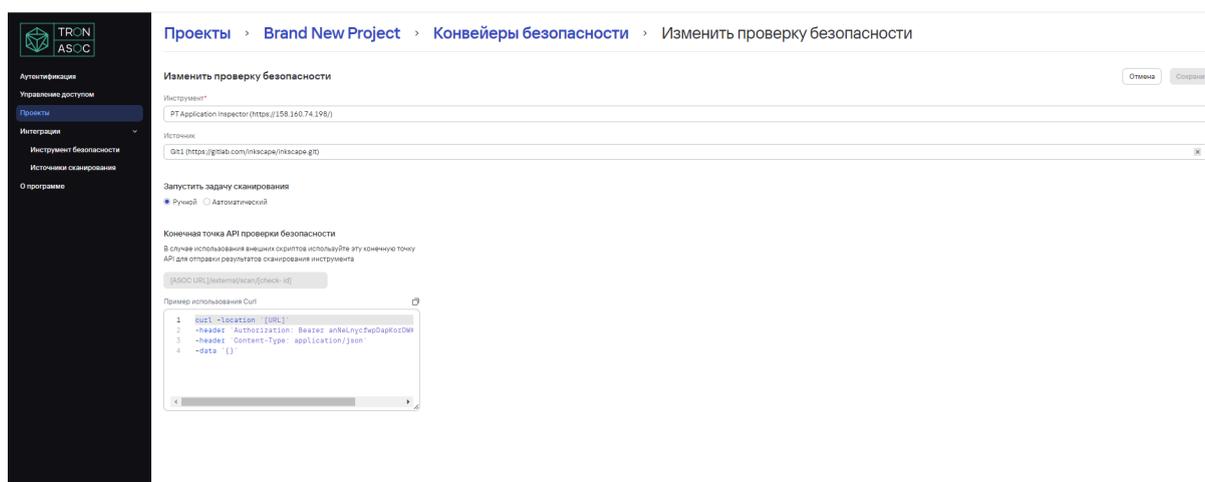


Рис. 20

### 9.4.4. Запуск конвейера безопасности

Можно провести запуск конвейера нажатием на Начать новое сканирование (рис. 21) - это приведет к запуску всех проверок безопасности в конвейере.

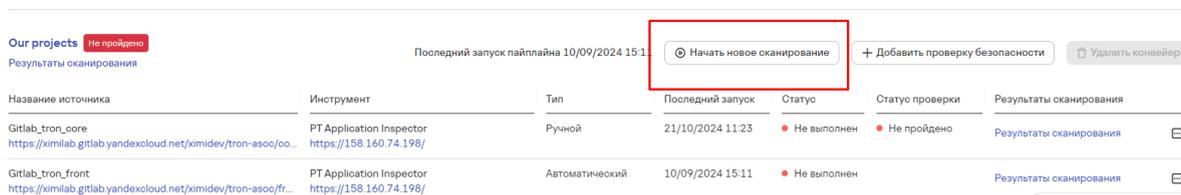


Рис. 21

#### 9.4.5. Запуск проверки безопасности

Можно произвести запуск отдельной проверки безопасности из конвейера. Запуск проверки безопасности производится вручную или автоматически. Чтобы запустить сканирование, нажмите кнопку **“Начать новое сканирование”** (рис.22) в той Проверке безопасности, которую вы хотите запустить.

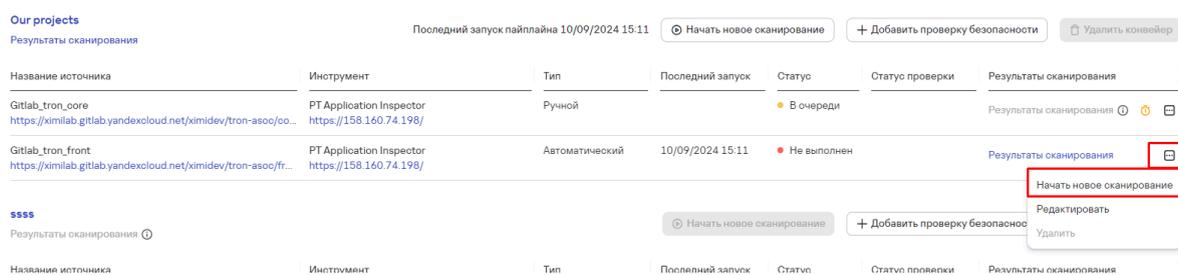


Рис. 22

Запущенная проверка получает статус **“В работе”**. После успешного завершения проверка переходит в статус **“Выполнено”**. Общее максимальное время работы цикла сканирования - по умолчанию 1 час. Если цикл достиг максимального времени работы, то проверка переходит в статус **“Не выполнено”** и процесс завершается. Статус **“Не выполнено”** также назначается, если что-то пошло не так на каком-либо из шагов сканирования.

#### 9.4.6. Остановка сканирования

Сканирование в статусе **“В процессе”** можно остановить из интерфейса в соответствующей Проверке безопасности. Чтобы остановить выполнение проверки безопасности, нажмите на кнопку **“Остановить сканирование”**.

#### 9.4.7. Загрузка отчета

Загрузка внешнего отчета может быть произведена вручную в разделе Проект - Проверки безопасности. Для этого нужно нажать на кнопку **“Загрузить результаты”** в меню справа.

| TestScanSourceForResults<br><a href="https://kimlab.gitlab.yandexcloud.net/kimdev/tron-asoc/core">https://kimlab.gitlab.yandexcloud.net/kimdev/tron-asoc/core</a> | PT Application Inspector<br><a href="https://158.160.74.198/">https://158.160.74.198/</a> | Ручной | 31/10/2024 09:52 | Выполнен    | Контроль пройден    | Результаты сканирования |
|---|---|--------|------------------|-------------|---------------------|-------------------------|
|   | PT Application Inspector<br><a href="https://158.160.74.198/">https://158.160.74.198/</a> | Ручной | 31/10/2024 10:29 | Не выполнен | Контроль не пройден | Результаты сканирования |
|   | PT Application Inspector<br><a href="https://158.160.74.198/">https://158.160.74.198/</a> | Ручной | 31/10/2024 09:52 | Не выполнен | Контроль не пройден | Результаты сканирования |
|   | PT Application Inspector<br><a href="https://10.10.102.118/">https://10.10.102.118/</a>   | Ручной | 31/10/2024 09:52 | Не выполнен | Контроль не пройден | Результаты сканирования |
|   | PT Application Inspector  | Ручной | 31/10/2024 09:52 | Не выполнен | Контроль не пройден | Результаты сканирования |

Кроме того, при использовании внешних скриптов и зависимости от выбранного инструмента сканирования (например, CLI-инструменты) у проверки безопасности может быть доступна опция получения результатов сканирования извне путём http-запроса от внешнего инструмента на эндпоинт TRON.ASOC.

Можно загрузить не более одного файла, файлы принимаются в формате JSON.

#### 9.4.8. Использование CLI-инструментов

Чтобы получить возможность отправки результатов от CLI-инструментов, их нужно предварительно добавить в доступные инструменты безопасности в разделе Интеграции.

После добавления нужно создать Проверку безопасности в конвейере безопасности нужного проекта. (для создания проверки безопасности понадобится указать кастомный источник. Добавление источника производится в разделе Интеграции- Источники сканирования. Для CLI-инструментов источником может быть любая ссылка: репозиторий, база знаний и т.д.)

## 9.5. Результаты сканирований

Результат успешного сканирования можно просмотреть как для отдельного конвейера безопасности и отдельной проверки безопасности (рис.23).

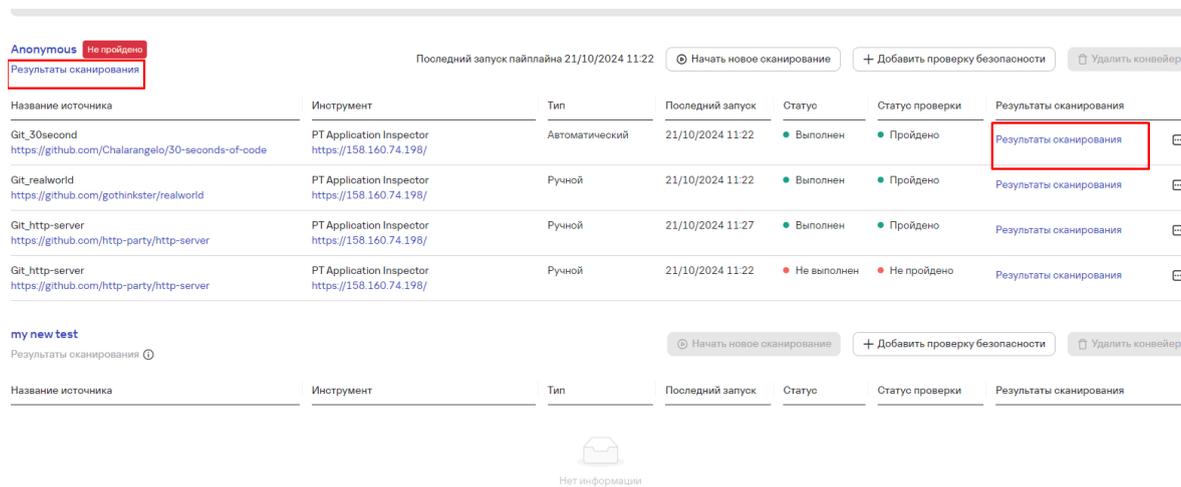


Рис. 23

Результаты сканирования (рис.24) содержат информацию о конвейере безопасности, источнике, использованном инструменте безопасности, дате начала, количестве найденных проблем безопасности, статусе сканирования.

Проекты > DEMO > Результаты сканирования

| Конвейер безопасности | Название источника | Инструмент  | Дата начала      | Всего уязвимостей | Статус      |
|-----------------------|--------------------|---|------------------|-------------------|-------------|
| Anonymous             | Git_http-server    | PT Application Inspector<br>https://158.160.74.198/ | 21/10/2024 11:27 | 154 (20)          | Выполнен    |
| Anonymous             | Git_realworld      | PT Application Inspector<br>https://158.160.74.198/ | 21/10/2024 11:22 |                   | Выполнен    |
| Anonymous             | Git_30second       | PT Application Inspector<br>https://158.160.74.198/ | 21/10/2024 11:22 | 7 (2)             | Выполнен    |
| Anonymous             | Git_http-server    | PT Application Inspector<br>https://158.160.74.198/ | 21/10/2024 11:22 |                   | Не выполнен |
| Anonymous             | Git_http-server    | PT Application Inspector<br>https://158.160.74.198/ | 21/10/2024 11:22 | 154 (20)          | Выполнен    |

Рис. 24

Когда выполнение проверки безопасности завершается, результаты проверки импортируются из инструментов AST. Результаты сканирования безопасности собираются и упорядочиваются. Каждый инструмент AST создает отчет по безопасности во время каждого запуска тестирования безопасности. Система позволяет выгружать отчеты по результатам сканирований в формате JSON, что обеспечивает удобство интеграции с другими системами и инструментами анализа данных. Отчет можно получить, нажав кнопку “Скачать”.

## 9.6. Контроли качества

Конвейеры безопасности и проверки безопасности могут содержать один или несколько Контролей качества, информацию о которых можно увидеть на вкладке Контроли качества (рис.25) внутри Проекта.

Проекты > DEMO > Контроль качества

| Конвейер безопасности  | Имя шаблона | Действие          |
|--|-------------|-------------------|
| Anonymous  |             | Добавить контроль |
| Git_realworld<br><a href="https://github.com/gothinkster/realworld">https://github.com/gothinkster/realworld</a><br>PT Application Inspector<br><a href="https://158.160.74.198/">https://158.160.74.198/</a>                    |             | Добавить контроль |
| Git_http-server<br><a href="https://github.com/http-party/http-server">https://github.com/http-party/http-server</a><br>PT Application Inspector<br><a href="https://158.160.74.198/">https://158.160.74.198/</a>                |             | Добавить контроль |
| Git_30second<br><a href="https://github.com/Chalarangelo/30-seconds-of-code">https://github.com/Chalarangelo/30-seconds-of-code</a><br>PT Application Inspector<br><a href="https://158.160.74.198/">https://158.160.74.198/</a> |             | Добавить контроль |
| Git_http-server<br><a href="https://github.com/http-party/http-server">https://github.com/http-party/http-server</a><br>PT Application Inspector<br><a href="https://158.160.74.198/">https://158.160.74.198/</a>                |             | Добавить контроль |

Рис. 25

На этой вкладке доступно управление привязкой контролей качества к пайплайну и чеку с возможностью установить правило действия выбранного контроля (информационное оповещение о провале гейта или блокирование мердж реквеста до устранения ошибок). Для добавления Контроля качества, нажмите “Добавить контроль” в столбце Имя шаблона и выберите правило действия для выбранного контроля (рис.26).

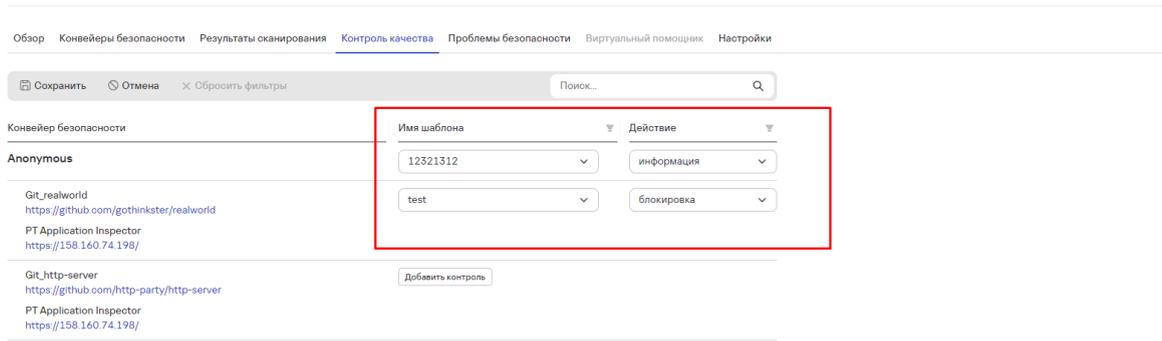


Рис. 26

Результаты прохождения Контролей качества можно отследить в проекте в конвейерах и проверках безопасности.

После добавления контроля внесенные изменения необходимо сохранить, нажав на кнопку “**Сохранить**” (рис.27). Заполнение полей с назначением контролей можно отменить, нажав на кнопку “**Отмена**”.

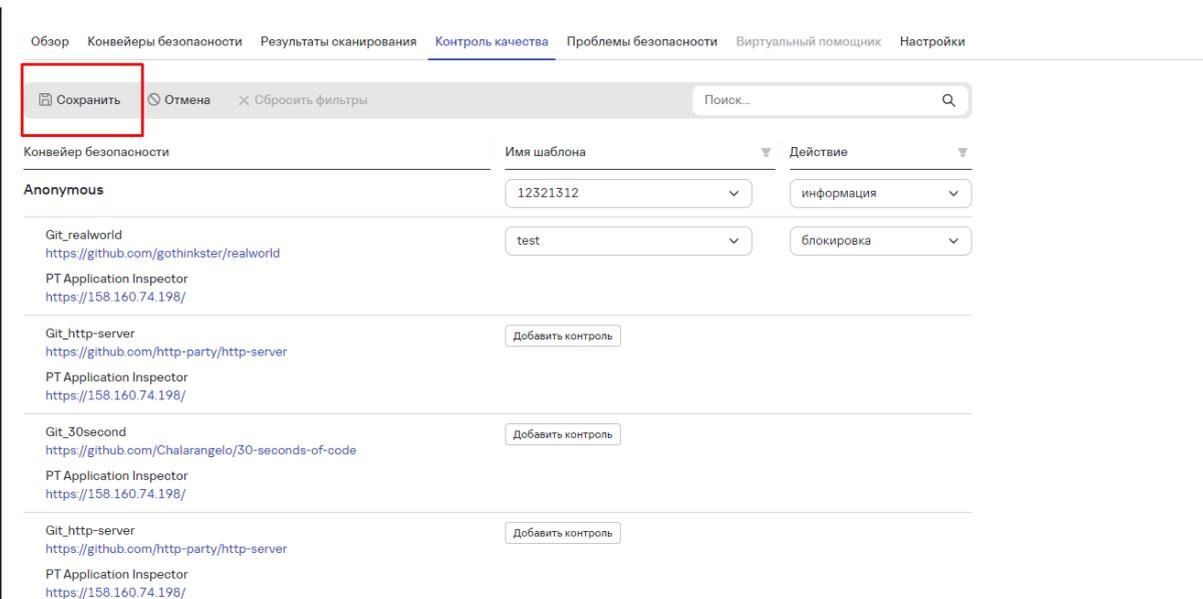
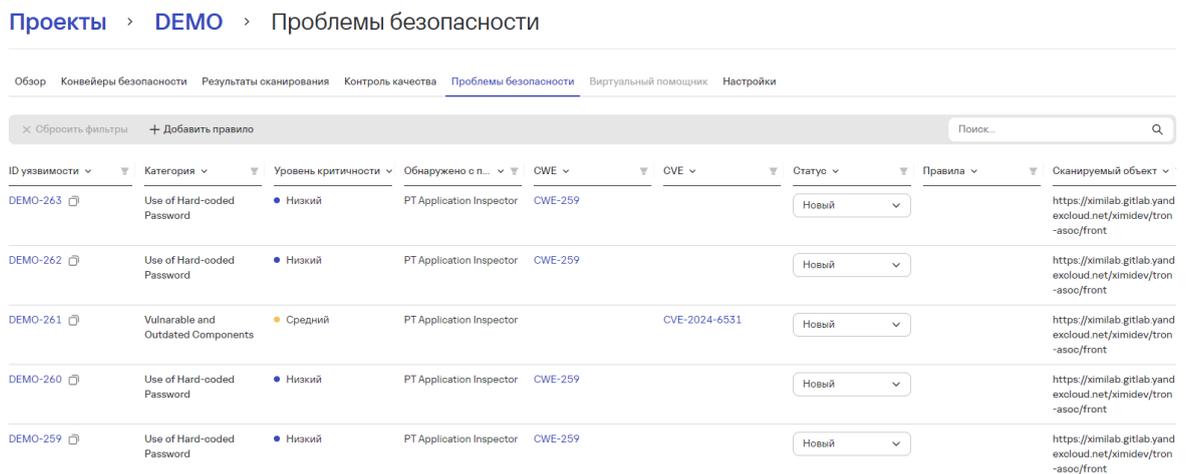


Рис. 27

## 9.7. Проблемы безопасности

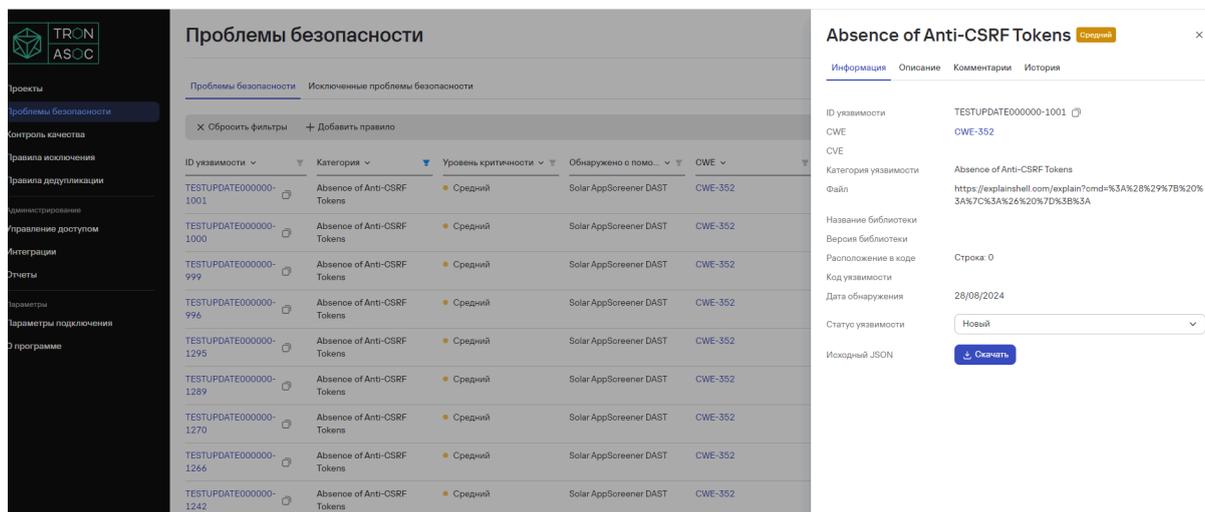
На вкладке **Проблемы безопасности** (рис.28) видны все найденные в проекте уязвимости, их уровень критичности и дополнительная информация: каким инструментом и где найдены, cwe и cve, статусы проблем безопасности и примененные правила.



| ID уязвимости | Категория                          | Уровень критичности | Обнаружено с п...        | CWE     | CVE           | Статус | Правила | Оксируемый объект  |
|---------------|------------------------------------|---------------------|--------------------------|---------|---------------|--------|---------|--|
| DEMO-263      | Use of Hard-coded Password         | Низкий              | PT Application Inspector | CWE-259 |               | Новый  |         | https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asoc/front |
| DEMO-262      | Use of Hard-coded Password         | Низкий              | PT Application Inspector | CWE-259 |               | Новый  |         | https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asoc/front |
| DEMO-261      | Vulnerable and Outdated Components | Средний             | PT Application Inspector |         | CVE-2024-6531 | Новый  |         | https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asoc/front |
| DEMO-260      | Use of Hard-coded Password         | Низкий              | PT Application Inspector | CWE-259 |               | Новый  |         | https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asoc/front |
| DEMO-259      | Use of Hard-coded Password         | Низкий              | PT Application Inspector | CWE-259 |               | Новый  |         | https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asoc/front |

Рис. 28

По каждой найденной проблеме можно получить дополнительную информацию в окне детального просмотра уязвимости (рис.29). Окно детального просмотра открывается при нажатии на ID проблемы безопасности.



| Информация           | Описание   | Комментарии | История |
|----------------------|--|-------------|---------|
| ID уязвимости        | TESTUPDATE000000-1001  |             |         |
| CWE                  | CWE-352  |             |         |
| CVE                  |  |             |         |
| Категория уязвимости | Absence of Anti-CSRF Tokens  |             |         |
| Файл                 | https://explainshell.com/explain?cmd=%3A%28%29%7B%20%3A%7C%3A%26%20%7D%3B%3A |             |         |
| Название библиотеки  |  |             |         |
| Версия библиотеки    |  |             |         |
| Расположение в коде  | Строка: 0  |             |         |
| Код уязвимости       |  |             |         |
| Дата обнаружения     | 28/08/2024   |             |         |
| Статус уязвимости    | Новый  |             |         |
| Исходный JSON        | <a href="#">Скачать</a>  |             |         |

Рис. 29

Есть возможность оставлять комментарии, просматривать комментарии других пользователей. Раздел комментариев находится во вкладке **Комментарии** в окне детального просмотре проблемы безопасности.

Статус проблем безопасности (новый, в работе, ложноположительный, подтвержденный, исправлено, исключено, вручную, дубликат) можно изменять при просмотре списка найденных проблем, а также в окне детального просмотра.

Есть фильтрация по атрибутам:

- ID уязвимости;
- статусу, степени критичности;
- инструменту обнаружения уязвимости;
- категории уязвимости, идентификатору CWE;
- объекту сканирования.

## 10. Контроли качества

Платформа позволяет создавать и настраивать точки контроля качества ПО для каждого конвейера безопасности и проверки безопасности. Раздел Контроль качества позволяет пользователям управлять шаблонами контроля качества и отслеживать метрики, которые применяются для оценки качества программного обеспечения и выявления возможных отклонений от норм. К каждому конвейеру и проверке безопасности можно добавить один или несколько контролей качества, если это необходимо в рамках проекта.

Контроль качества

| <input type="checkbox"/> Название шаблона | Количество метрик | Проекты | Автор |
|---|-------------------|---------|-------|
| <input type="checkbox"/> 2342342346       | 1                 | View    | admin |
| <input type="checkbox"/> 310nest1234      | 4                 | View    | admin |
| <input type="checkbox"/> Argent           | 0                 | View    | admin |
| <input type="checkbox"/> asdf             | 3                 | View    | admin |
| <input type="checkbox"/> DEMM1            | 0                 | View    | admin |
| <input type="checkbox"/> Demo2009         | 3                 | View    | admin |
| <input type="checkbox"/> DemoGate         | 5                 | View    | admin |
| <input type="checkbox"/> DEMOQuality      | 4                 | View    | admin |
| <input type="checkbox"/> DEMOTEST         | 0                 | View    | admin |
| <input type="checkbox"/> Gate1            | 0                 | View    | admin |

Всего 11 / Выбрано 0

1 2 3 ... 9 > 10 / страница

Рис.30

Таблица шаблонов контролей качества (рис.30) содержит список шаблонов, которые уже созданы и используются в системе. Поля таблицы:

- Название шаблона – это имя шаблона контроля качества.

- Количество метрик – показывает количество метрик, которые используются в данном шаблоне контроля качества.
- Проекты – список проектов, к которым привязан данный шаблон. Щелкнув по View, можно увидеть проекты, к которым применен этот шаблон.
- Автор – отображает имя пользователя, который создал данный шаблон.

В таблице можно сортировать шаблоны по количеству метрик, названию или автору.

Чтобы добавить новый шаблон контроля качества, нажмите кнопку "Добавить контроль качества" и укажите название шаблона. Созданный шаблон нужно отредактировать, нажав на имя шаблона в списке. Задайте необходимые метрики для отслеживания качества и сохраните шаблон (рис.31).



Рис.31

Удаление шаблонов производится по выбору пункта подменю "Удалить" в списке шаблонов.

# 11. Правила безопасности

Система предоставляет возможность создания правил исключения для работы с результатами в продукте. Страница "Правила безопасности" предназначена для управления правилами безопасности, которые применяются к уязвимостям и другим проблемам безопасности в проектах. Это позволяет временно или постоянно игнорировать определенные типы проблем, исходя из их приоритета или иных критериев. Логика работы с правилами позволяет настраивать время действия правила: на заданное время или навсегда, а также область действия (по проектам).

| Название  | Категория                  | Компонент                               | CVE            | CWE     | Отмена правила | Статус     | Кол-во примененных правил | Время действия | Область |
|---|----------------------------|---|----------------|---------|----------------|------------|---------------------------|----------------|---------|
| Suppress Rule SR68707481                                    | vulnerability              |   | CVE-2023-52426 | CWE-776 | Нет            | Активен    | 1                         |                | View    |
| Suppress Rule SR99582005                                    | vulnerability              |   | CVE-2023-52426 | CWE-776 | Нет            | Не активен | 1                         |                | View    |
| Suppress Rule for issue 17234760-0708-4513-9f4e-6448297c6b9 | Чтение произвольного файла | https.github.com/http-party/http-server |                | CWE-773 | Нет            | Не активен | 0                         | 2024-10-15     | View    |
| PTA_HttpServer_High_Salicy                                  | OS Command injection       | https.github.com/http-party/http-server |                | CWE-78  | Нет            | Активен    | 4                         |                | View    |
| Suppress Rule SR11867423                                    | vulnerability              |   | CVE-2023-52426 | CWE-776 | Нет            | Активен    | 1                         |                | View    |
| Suppress Rule SR63612362                                    | vulnerability              |   | CVE-2023-52426 | CWE-776 | Нет            | Активен    | 1                         |                | View    |
| asd   | Use of Hard-coded Password |   |                |         | Нет            | Активен    | 0                         |                | View    |
| Suppress Rule SR81418016                                    | vulnerability              |   | CVE-2023-52426 | CWE-776 | Нет            | Активен    | 1                         |                | View    |
| qwe   | HTTP usage                 |   |                |         | Нет            | Не активен | 0                         |                | View    |
| DEMO0110http  | OS Command injection       | https.github.com/http-party/http-server |                | CWE-78  | Нет            | Активен    | 0                         |                | View    |

Рис. 32

Столбцы таблицы правил безопасности (рис.32):

- Название – название или идентификатор правила безопасности.
- Категория – категория проблемы, к которой применяется правило безопасности.
- Компонент – компонент системы или путь к репозиторию
- CVE – уникальный идентификатор уязвимости в базе данных CVE.
- CWE – код CWE (Common Weakness Enumeration), который описывает тип уязвимости.
- Отмена правила – указывает на реверсивность правила
- Статус – статус активности правила.
- Количество примененных правил – количество проблем, к которым это правило было применено.
- Время действия – срок действия правила.
- Область – область проектов.

Создание правила безопасности происходит на основании указанных параметров. Набор параметров зависит от типа проблемы безопасности. При помощи правил безопасности можно также централизованно управлять статусами обнаруженных проблем безопасности, которые будут подчиняться этому правилу.

Для создания нового правила нажмите кнопку "**Добавить правило**". В открывшейся форме (рис.33) введите необходимые данные:

1. Уникальное название для создаваемого правила безопасности.
2. Тип проблемы безопасности
3. Укажите инструмент, использованный для обнаружения проблемы безопасности.
4. Выберите категорию проблемы безопасности.
5. Укажите компонент системы или путь, где была обнаружена проблема.
6. Идентификатор уязвимости из базы данных CVE
7. CWE для описания конкретного типа уязвимости.
8. Путь к файлу или директории в репозитории, где была найдена проблема.
9. Источник обнаружения
10. Укажите период, в течение которого правило безопасности будет активно. Это может быть фиксированная дата окончания действия правила, или оно может быть бессрочным.
11. Задайте статус проблемы безопасности

## 12. Укажите область применения (проекты)

### Создать правило безопасности ×

Компонент

CVE

CWE

Путь

Источник

Время действия  

Статус проблемы безопасности\*  

Область\*  

Проекты  

Рис. 33

## 12. Правила дедупликации

Правила дедупликации предназначены для работы над объединением и устранением дубликатов обнаруженных проблем безопасности в системе.

Правила дедупликации

| + Добавить правило                           |                                | Поиск...     |
|--|--------------------------------|--------------|
| Название                                     | Метод                          | Статус       |
| <input type="checkbox"/> DDRule for qa test3 | С помощью правил сопоставления | ● Не активен |
| <input type="checkbox"/> DDRule for qa test2 | По комбинированным полям       | ● Не активен |
| <input type="checkbox"/> Rule12              | С помощью правил сопоставления | ● Не активен |
| <input type="checkbox"/> Rule1Demo           | По комбинированным полям       | ● Не активен |
| <input type="checkbox"/> Rule2               | По комбинированным полям       | ● Не активен |
| <input type="checkbox"/> rule3               | С помощью правил сопоставления | ● Не активен |
| <input type="checkbox"/> RULE3               | С помощью правил сопоставления | ● Не активен |
| <input type="checkbox"/> RuleDemo2           | С помощью правил сопоставления | ● Активен    |
| <input type="checkbox"/> RulePower           | С помощью правил сопоставления | ● Не активен |
| <input type="checkbox"/> test                | По комбинированным полям       | ● Не активен |

Всего 11 / Выбрано 0 < 1 2 > 10 / страница

Рис. 34

Таблица (рис.34) содержит список существующих правил дедупликации с возможностью сортировки и просмотра подробной информации.

- Название – имя правила.
- Метод – способ дедупликации. Возможные методы:
  - С помощью правил сопоставления – дедупликация выполняется на основе предварительно заданных критериев сопоставления.
  - По комбинированным полям – дедупликация выполняется по набору полей, таких как CVE, CWE или другие параметры.
  - На основе существующей проблемы безопасности
- Статус – указывает, активно ли правило в данный момент.

Для создания нового правила нужно нажать "Добавить правило". В форме (рис.35) необходимо будет указать метод дедупликации, категорию полей для сопоставления и дополнительные параметры, зависящие от выбранного метода.

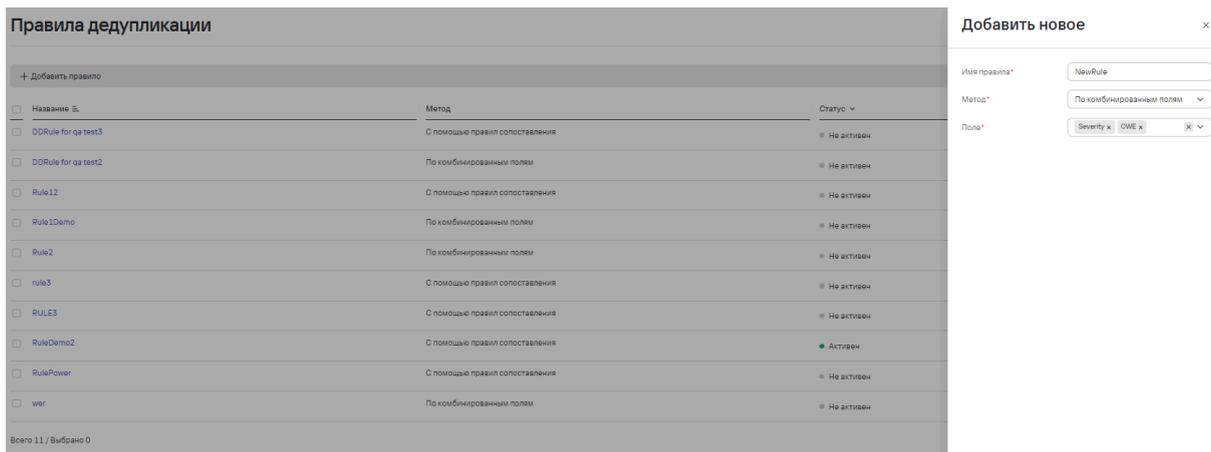


Рис. 35

### 13. Отчеты

В системе есть функционал формирования сводного отчета по доступным пользователю выбранным им проектам. Отчеты по проектам можно сформировать при просмотре списка доступных проектов, нажав на кнопку “Создать отчет” (рис.36).

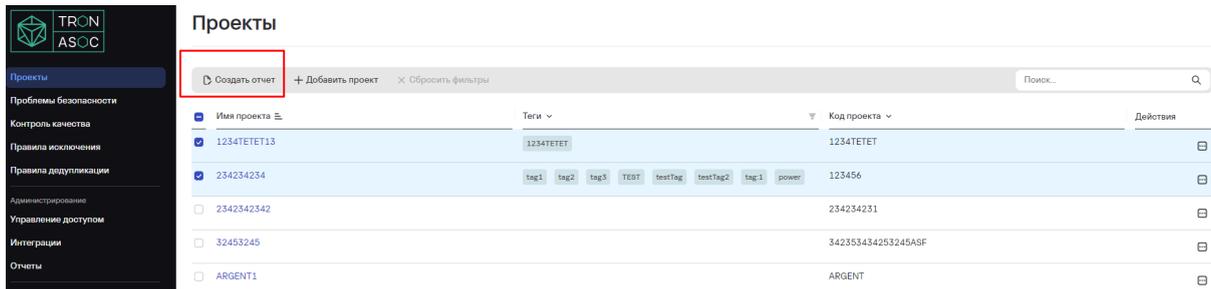


Рис. 36

Чтобы просмотреть сформированный отчет, его нужно скачать в разделе Отчеты. Пользователю предоставляется опция выбора форматов отчета: PDF, CSV, JSON. Сформированный отчет можно удалить из списка отчетов.

## 14. Требования к аппаратным и программным характеристикам рабочего места пользователя

- Процессор: Минимум 4 ядра, рекомендуемый — 8 ядер и более.
- Оперативная память: Минимум 16 ГБ, рекомендуемая — 32 ГБ и более.
- Жесткий диск: Минимум 500 ГБ свободного места, рекомендуется использование SSD для повышения производительности.
- Сетевое соединение: Высокоскоростное интернет-соединение, минимум 1 Гбит/с
- Операционная система:
  - macOS: macOS 10.14 или более поздние версии.
  - Linux: Современные дистрибутивы с поддержкой необходимых версий браузеров.
  - Windows: Windows 10 или более поздние версии.
- База данных: PostgreSQL 13 или более поздние версии, рекомендуется настроить резервное копирование и восстановление данных.
- Браузер на движке Chromium (Google Chrome, Edge, Safari и т. д.) и Firefox.