Платформа для управления уязвимостями и обеспечения безопасности в процессах разработки и DevSecOps “TRON.ASOC v.1.3”

Руководство пользователя

Апрель 2025

Содержание

Введение 4
1. Термины и определения 5
2. Общие сведения 7
3. Начало работы в системе 9
4. Описание интерфейса и функционала 12
4.1. Настройки главного меню 13
4.2. Настройки элементов рабочей области 13
4.2.1. Настройки отображения данных 13
4.3. Информационная панель 15
4.3.1. Расчеты основных метрик 18
4.3.2. Настройки виджетов 20
4.4. Проекты 21
4.4.1. Создание нового проекта 23
4.4.2. Редактирование проекта 23
4.4.3. Отчеты по проектам 25
4.4.4. Обзор проекта 27
4.5. Конвейеры безопасности и проверки безопасности 28
4.5.1. Создание конвейера безопасности 29
4.5.2. Создание проверки безопасности 30
4.5.3. Запуск конвейера безопасности 33
4.5.4. Запуск проверки безопасности 33
4.5.5. Остановка сканирования 34
4.5.6. Загрузка внешнего отчета 34
4.5.7. Использование CLI-инструментов 37
4.5.8. Интеграция в CI процесс 39
4.5.8.1. Описание переменных 39
4.5.8.2. Пример отправки результата сканирования CLI-инструмента в TRON.ASOC в рамках CI 40
4.5.9. Результаты сканирований 41
4.5.10. Контроль качества проекта 42
4.6. Проблемы безопасности 44
4.7. Библиотека зависимостей 47
4.8. Контроль качества 48
4.8.1. Добавление нового контроля качества 49
4.9. Правила безопасности 51
4.9.1. Создание правила безопасности 52
4.10. Правила дедупликации 53
4.10.1. Поиск дубликатов 53
4.10.2. Создание правил дубликатов 54

4.11. Правила реагирования 54
4.11.1. Создание правила реагирования 54
5. Отчеты 58
6. Журнал событий 59
7. Конструктор полей 60
8. Требования к аппаратным и программным характеристикам рабочего места пользователя 62

Введение

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

В роли пользователей могут быть разработчики, тестировщики, инженеры безопасности, специалисты техподдержки различных ИТ-систем, и другие участники процесса DevSecOps.

С целью более детального описания доступного функционала, данный документ был составлен для пользователя с полными правами доступа ко всем функциям системы. Видимость некоторых функций отдельного пользователя может быть ограничена в соответствии с назначенной ролью. При необходимости расширить права доступа к определенному функционалу рекомендуется обратиться к администратору системы.

1. Термины и определения

Термин/аббревиатура	Определение
ПО	Программное обеспечение
ASOC (Application Security Orchestration and Correlation)	Платформы или решения для оркестрации и корреляции безопасности приложений - платформы, предназначенные для управления и координации безопасностью приложений, позволяют 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 (Development Security Operations)	Процесс безопасной разработки - методология разработки программного обеспечения, которая интегрирует практики безопасности (Sec) в процессы разработки и поставки программного обеспечения (DevOps).
OSA (Open Source Analysis)	Анализ открытого программного обеспечения - 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.
SCA (Software Composition Analysis)	Анализ структуры программного обеспечения - позволяет определять состав программного обеспечения для выявления и управления компонентами с открытым исходным кодом и их уязвимостями.

Термин/аббревиатура	Определение
SAST (Static Application Security Testing)	Статическое тестирование безопасности приложений - 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 (Infrastructure-as-Code)	Инфраструктура как код - это подход к созданию и управлению инфраструктурой через использование кода, например, конфигурационных файлов или скриптов.
Container Security	Безопасность контейнеров - 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	Проект - это сущность, которая создается авторизованным пользователем, чтобы логически объединить весь набор связанных приложений или компонентов, которые разрабатываются и 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	Интеграция - обмен данными между системами с возможной последующей обработкой.
AD (Active Directory)	Службы каталогов – совокупности программных сервисов и баз данных (на базе Microsoft) для иерархического представления информационных ресурсов в сети и настройки доступа к ним.
LDAP (Lightweight Directory Access Protocol)	Легковесный протокол доступа к каталогам

2. Общие сведения

«TRON.ASOC» - программный продукт, платформа для обнаружения и управления уязвимостями, а также обеспечения безопасности в процессах разработки и DevSecOps.

- интегрируется с внешними сканерами безопасности, такими как статический анализатор исходного кода **PT Application Inspector** и анализатор безопасности контейнеров **Kaspersky Container Security**.
- интегрируется со статическим анализатором кода приложений **Solar AppScreener** (не только исходного, но и бинарного кода) на наличие уязвимостей и НДВ.
- взаимодействует с решениями композиционного анализа программных продуктов **CodeScoring** и **OWASP Dependency Track**.
- интегрируется с платформой **JFrog**, предназначенной для управления и развертывания программных пакетов.
- может принимать и анализировать отчеты, обрабатывать полученные результаты от следующих инструментов:
    - **Trivy** - сканер уязвимостей с открытым исходным кодом, разработанный для контейнерных сред,
    - **Grype** - эффективный сканер контейнеров, Docker-образов и файловых систем на наличие уязвимостей,
    - **KICS** (Kaspersky Industrial CyberSecurity) - решение для централизованного управления безопасностью,
    - **Semgrep** - статический сканер безопасности приложений,
    - **Aqua** - решение, обеспечивающее комплексную нативную защиту контейнеров.
- позволяет добавлять уязвимости вручную (**Manual**) для построения комплексных метрик.
- предоставляет возможность управлять проверками исходного кода и образов контейнеров на известные уязвимости, ошибки конфигурации, секреты, а также работать с результатами этих проверок в едином интерфейсе. Интеграция с инструментами позволяет настраивать сканирования, запускать проверки, консолидировать, анализировать и обрабатывать результаты, а также производить мониторинг состояния безопасности разрабатываемых продуктов.
- помогает группировать, исследовать и устранять уязвимости из различных источников, обеспечивая тем самым безопасный процесс разработки.
- упрощает работу с найденными проблемами и уязвимостями, проводя их анализ и группировку для более эффективного управления безопасностью.

- позволяет оценивать влияние уязвимостей, изменять их статусы и приоритизировать для последующих шагов, управлять исключениями. Таким образом, продукт позволяет управлять уязвимостями ПО и защитой приложений на всех этапах разработки.
- позволяет оставлять комментарии к уязвимостям и просматривать комментарии от других пользователей.
- позволяет создавать и настраивать точки контроля качества ПО для каждого ИБ-пайплайна, иметь способ организации критериев качества каждого сканирования. На основе критериев контроля качества система решает, успешно ли завершилась работа конвейера проверок безопасности и позволяет определить, может ли продукт перейти на следующий этап разработки или выпуска на основе заданных критериев качества.
- предоставляет возможность внесения исключений в результаты отработки, получаемые от сканеров, в ASOC, что позволяет не подсвечивать уже обработанные и принятые проблемы безопасности. Время действия и область применения правил исключений можно настраивать.
- является единым источником данных об уязвимостях в ПО от инструментов с разными типами проверок (SAST, Container Security, OSA/SCA, DAST) и, таким образом, может стать единым инструментом контроля качества ПО.
- предлагает использовать дашборды, отчеты и метрики внутри продукта, которые предоставляют гибкие формы отчетности и аналитические данные для оценки текущего состояния безопасности проектов, прогнозирования рисков и принятия решений. С помощью визуализации данных платформа предоставляет пользователям наглядную информацию о состоянии безопасности их проектов.
- внедряет безопасность и управление рисками в непрерывные процессы разработки, при этом не требует для работы внешних CI-конвейеров
- предлагает удобный пользовательский интерфейс, доступный в современных браузерах на движке Chromium (Google Chrome, Яндекс Браузер, Edge, Safari и т.д.) и Firefox.
- поддерживает создание гибкой ролевой модели, позволяя настроить различные уровни доступа и разрешений для пользователей, что способствует более эффективному и безопасному управлению проектами.
- поддерживает интеграцию с **LDAP** и **AD**.
- предоставляет возможности для управления сканированиями, включая настройку параметров сканирования, планирование запусков и мониторинг выполнения сканирований.
- позволяет выгружать отчеты по результатам сканирований в разных форматах, что обеспечивает удобство интеграции с другими системами и инструментами анализа данных.

3. Начало работы в системе

Для начала работы в системе TRON.ASOC необходимо запросить доступ у администратора, который после настройки учетной записи предоставит ссылку для входа и первичные данные учетной записи. По ссылке осуществляется переход на страницу авторизации в системе.

Для успешной авторизации необходимо выполнить следующие шаги:

1. Перейти на страницу авторизации (Рис. 1).

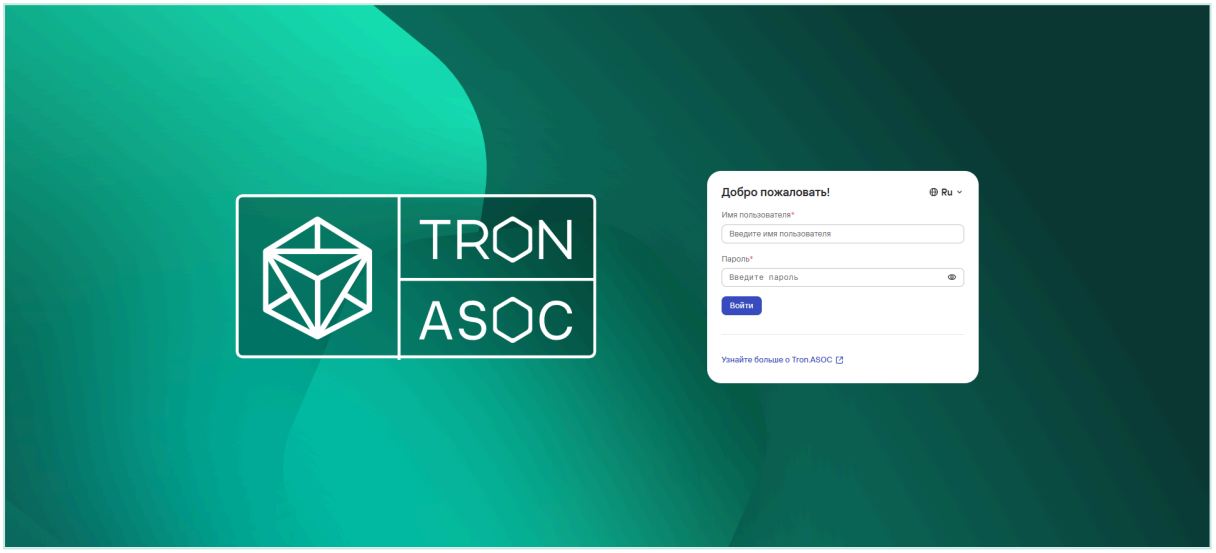

Рис. 1

2. При необходимости выбрать удобный язык веб-интерфейса с помощью кнопки 

(доступны русский и английский языки).
3. Далее ввести **Имя пользователя** и **Пароль** от учетной записи.
4. Нажать на кнопку **Войти**.

> ❕ При первом входе, а также по запросу, потребуется изменить пароль к учетной записи, следуя указанным рекомендациям к новому паролю (Рис. 2), и нажать на кнопку **Изменить**.

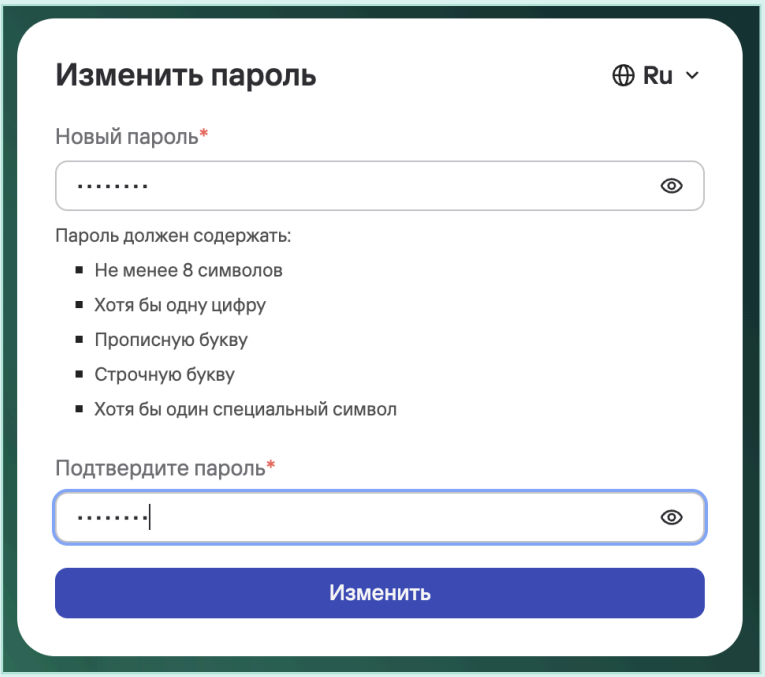

Рис. 2

При успешной авторизации откроется **Информационная панель** (Рис. 3).

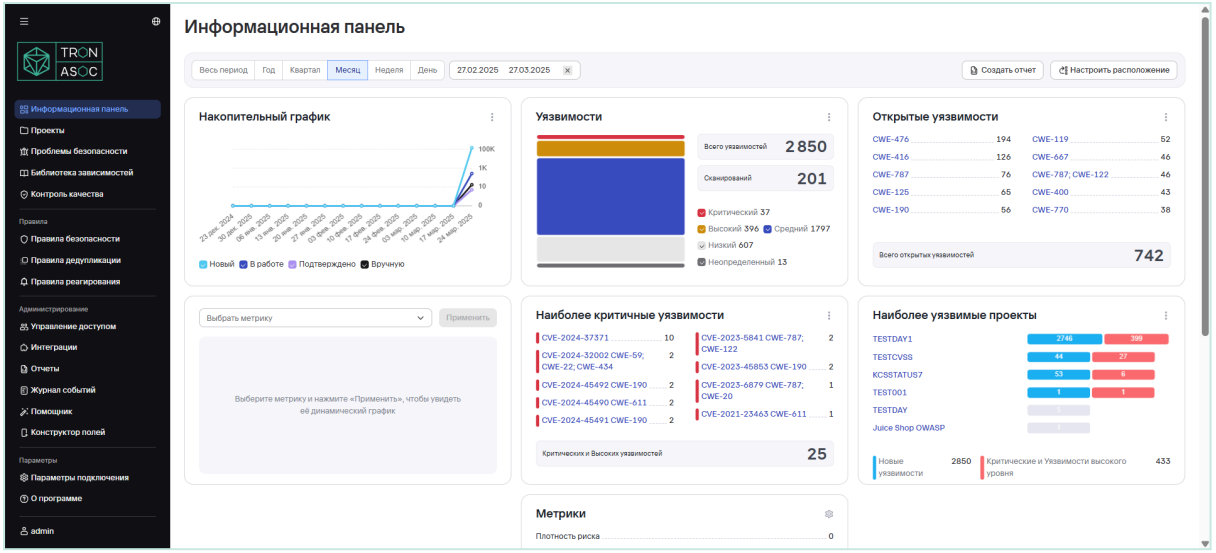

Рис. 3

❗ В случае ввода неверных учетных данных на экране отобразится сообщение “*Неверный логин и/или пароль*”. При превышении числа попыток аутентификации с неверным паролем аккаунт будет временно заблокирован. Количество попыток аутентификации и продолжительность блокировки устанавливается администратором системы (по умолчанию лимит попыток входа — 3, срок блокировки — 1 минута). При возникновении других проблем с входом в систему, необходимо обратиться к администратору.

В случае успешной настройки системы со стороны администратора (созданы необходимые учетные записи, назначены роли и доступы пользователям, внесены требуемые изменения в настройки системы, подключены инструменты безопасности, источники сканирования, инструменты уведомлений, трекеры) пользователям для начала предлагается следующий алгоритм работы с системой:

1. Необходимо создать проекты в системе, проекты должны иметь понятное название, краткое описание (см. Создание нового проекта).
2. Далее по каждому из проектов необходимо:
    1. Перейти в Обзор проекта.
    2. Добавить Конвейеры безопасности.
    3. Добавить Проверки безопасности.
    4. Добавить Контроль качества (при необходимости, возможно добавить позднее, при наличии достаточного количества проверок).
    5. Также добавить Правила безопасности, Правила дедупликации в отношении проекта (при необходимости, возможно добавить позднее, при наличии достаточного количества проверок).
    6. Далее Запустить сканирование (Конвейер безопасности).
    7. Ознакомиться с результатами сканирования. По результатам рекомендуется предпринять шаги по устранению выявленных уязвимостей, создать задачи в трекере при необходимости, и далее отслеживать исправление уязвимости, и также запускать новые сканирования для проверки.
    8. Добавить необходимые Правила реагирования.
    9. По требованию создать необходимые отчеты.
3. Дальнейшие действия зависят от индивидуальных потребностей, в рамках предложенного функционала (см. инструкцию ниже).

4. Описание интерфейса и функционала

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:
  - Информационная панель
  - Проекты
  - Проблемы безопасности
  - Библиотека зависимостей
  - Контроль качества
  - Правила безопасности
  - Правила дедупликации
  - Правила реагирования
  - Блок Администрирования
    - Управление доступом
    - Интеграции
    - Отчеты
    - Журнал событий
    - Помощник

      ❕ Раздел **Помощник** будет доступен в следующих релизах.
    - Конструктор полей
    - Параметры подключения

    ❕ Разделы блока **Администрирование** доступны администраторам системы.
    Подробнее о разделах см. Руководство администратора.
  - О программе - общая информация о системе
  - Учетная запись - данные профиля учетной записи

  ❗ Видимость разделов главного меню зависит от набора привилегий и прав роли пользователя.
  Для расширения доступа к системе необходимо согласовать изменения и обратиться к администратору для перенастройки ролей.

- Рабочая область. Информация и элементы управления в рабочей области зависят от выбранного раздела или подраздела.

4.1. Настройки главного меню

Предусмотрены следующие настройки главного меню:

- Выбор языка интерфейса (русский или английский). Для этого необходимо нажать на кнопку  и в раскрывшемся списке выбрать необходимый язык.
- Возможность свернуть/развернуть главное меню. Для этого необходимо нажать на кнопку  .

4.2. Настройки элементов рабочей области

4.2.1. Настройки отображения данных

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

- Поиск. Выполнить поиск по отображаемым данных возможно с помощью поля **Поиск…**, расположенного над таблицей (Рис. 4).

Рис. 4

- Настройка полей таблицы. Для настройки видимости полей таблицы необходимо нажать на кнопку  и в открывшейся форме скорректировать видимость полей (Рис. 5). Поля различаются в зависимости от данных таблицы и выбранного раздела.

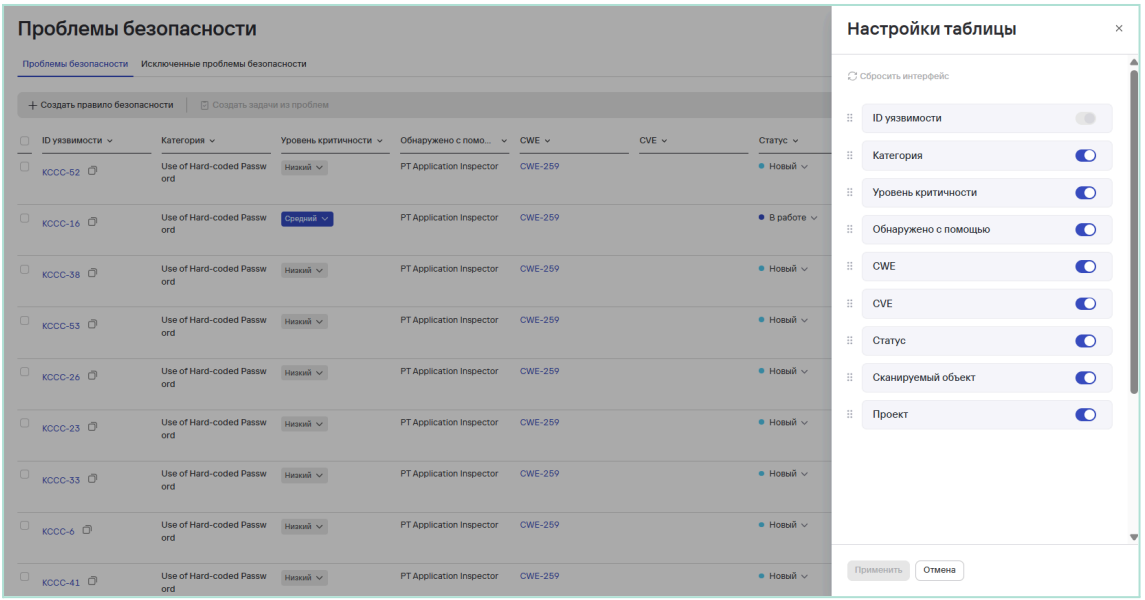

Рис. 5

- Фильтрация. Для настройки фильтрации необходимо нажать на значок фильтра  и в открывшейся форме справа указать необходимые фильтры (Рис. 6). Фильтры различаются в зависимости от данных таблицы и выбранного раздела.

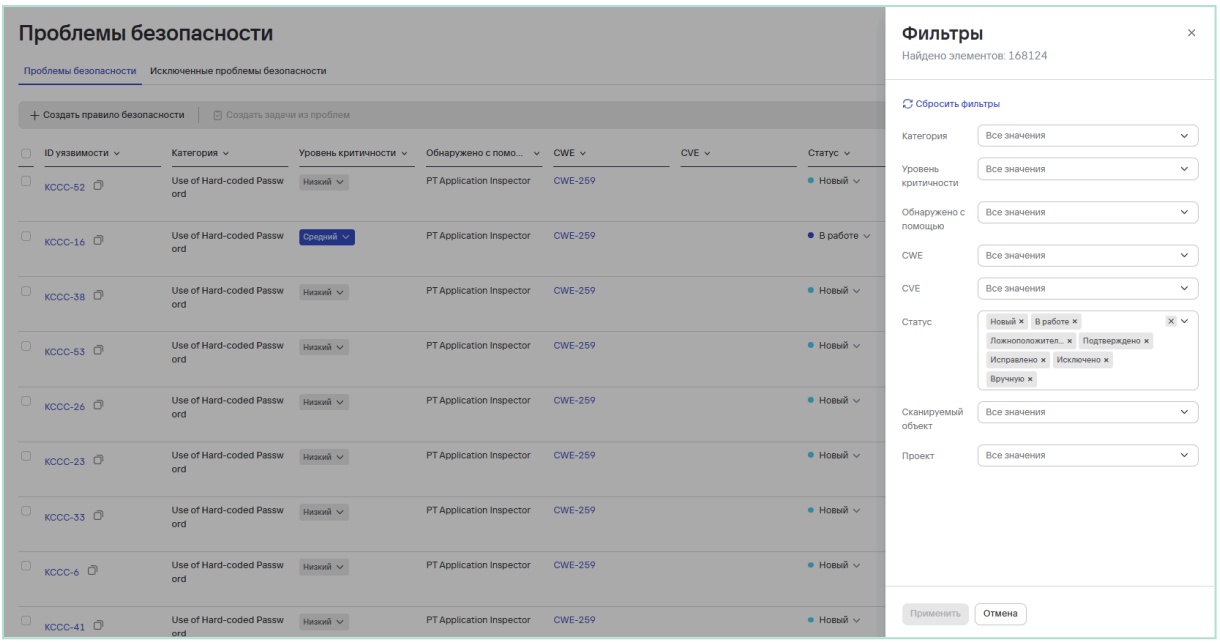

Рис. 6

- Сортировка по возрастанию или убыванию. Табличный вид позволяет сортировать список данных по выбранному столбцу с помощью раскрывающегося списка при нажатии на выбранный столбец таблицы (Рис. 7).

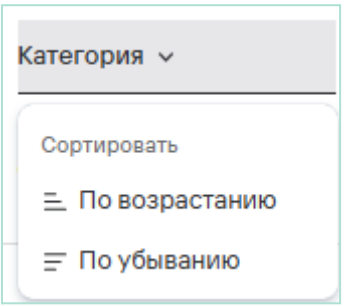

Рис. 7

4.3. Информационная панель

Информационная панель представлена в виде сводных графиков (виджетов) по уязвимостям за установленный период (Рис. 3), она предоставляет возможность отследить наиболее важные метрики по доступным пользователю проектам в разработке. Значения накопительных графиков обновляются раз в сутки.

Доступны следующие виджеты (в зависимости от прав доступа):

- Накопительный график по выявлению уязвимостей за выбранный период времени (Рис. 8)

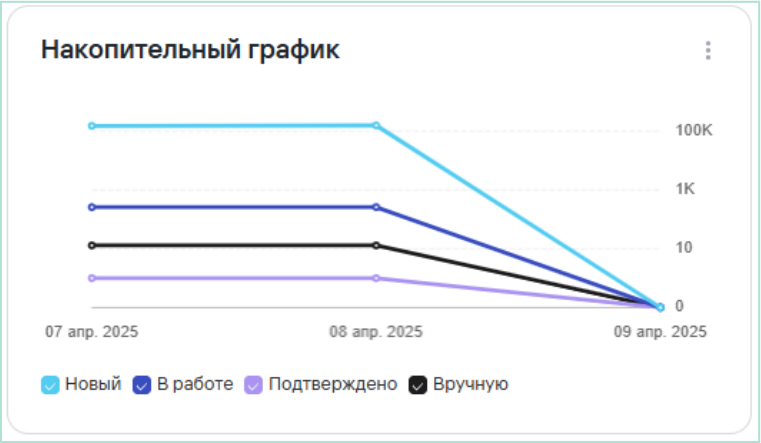

Рис. 8

- Уязвимости (Рис. 9)

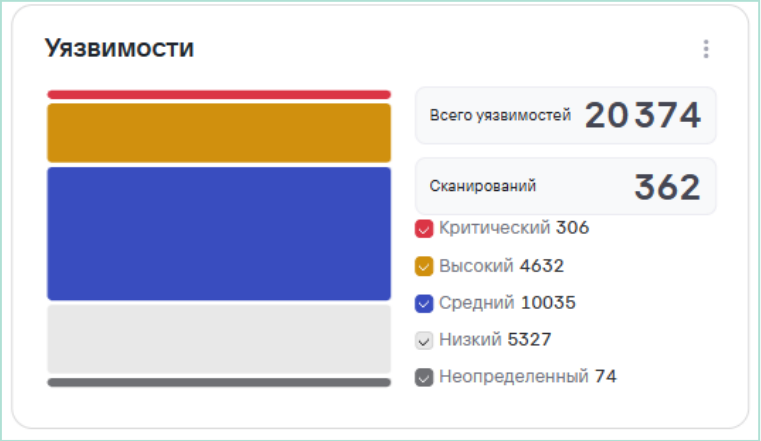

Рис. 9

- Открытые уязвимости (Рис. 10)

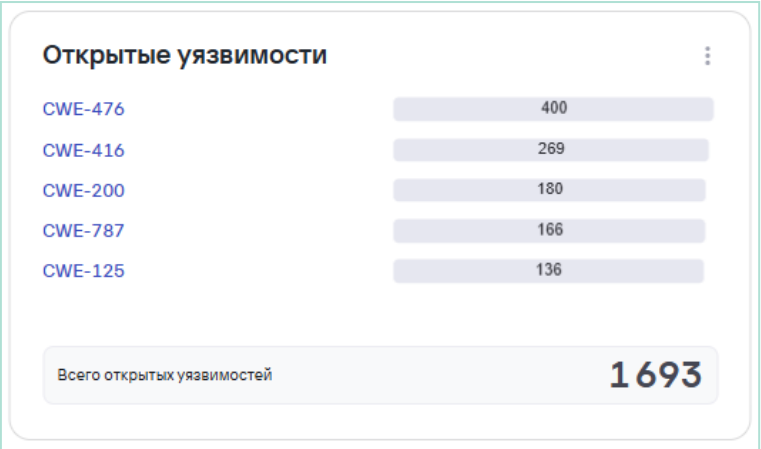

Рис. 10

- Наиболее критичные уязвимости (Рис. 11)

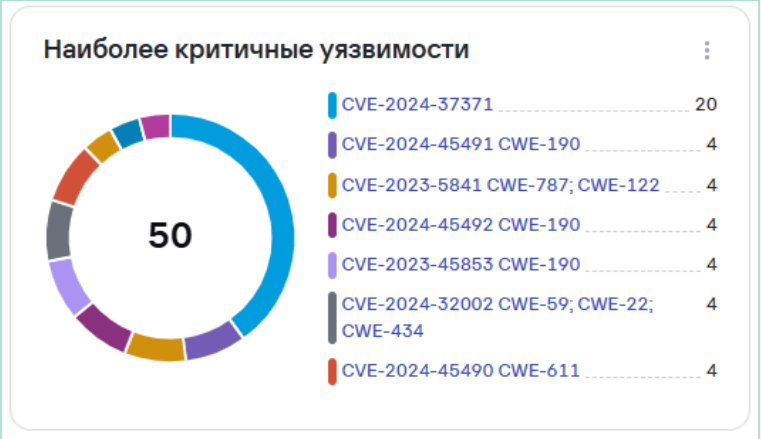

Рис. 11

- Наиболее уязвимые проекты (Рис. 12)

Рис. 12

- Среднее время выявления дефекта ИБ (Рис. 13)

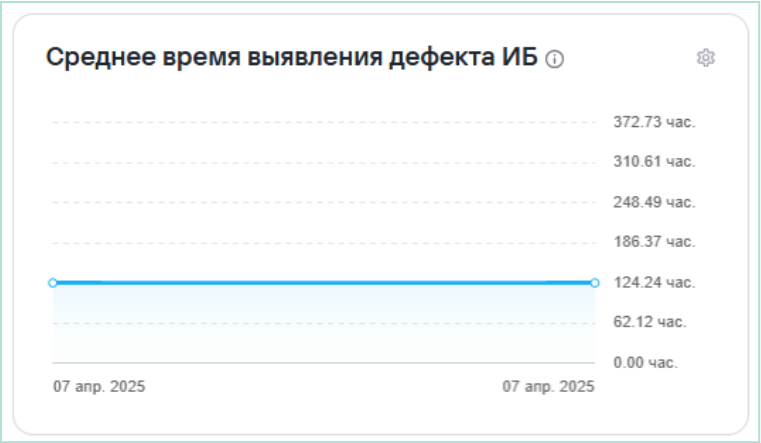

Рис. 13

- Метрики (Рис. 14)

Рис. 14

По данным метрикам предусмотрены отдельные виджеты для большей наглядности (в линейном виде):

- Коэффициент частоты сканирования
- Количество уязвимостей
- Среднее время жизни дефекта ИБ
- Процент устраненных уязвимостей
- Количество дубликатов уязвимостей

- Среднее время исправления дефекта ИБ
- Плотность риска
- Интегральный риск-индекс

4.3.1. Расчеты основных метрик

Процент покрытия имеющихся информационных систем/приложений практиками безопасной разработки рассчитывается по следующей формуле:

$$\text{Coverage\%} = \frac{\text{Количество систем с применением практик}}{\text{Общее количество систем}} \times 100$$

Среднее время жизни дефекта ИБ (Lead Time) рассчитывается, как медианное время жизни дефекта, т.е. от статуса Новый (New) до любого закрытого статуса (Suppress, Fixed и т.д.).

Среднее время идентификации дефектов ИБ (Mean-Time-To-Detect) рассчитывается, как медианное время идентификации дефектов в проекте/проектах. Под идентификацией дефекта подразумевается изменение статуса от Новый (New) до любого другого следующего статуса.

Среднее время исправления дефектов ИБ (Mean-Time-To-Resolve) рассчитывается, как медианное время от открытого статуса, отличного от Новый (New) до закрытого статуса.

Плотность риска (M) рассчитывается по следующей формуле:

$$M = \frac{C_{\text{крит}} \cdot W_{\text{крит}} + C_{\text{хай}} \cdot W_{\text{хай}} + C_{\text{медиум}} \cdot W_{\text{медиум}} + C_{\text{лоу}} \cdot W_{\text{лоу}} + C_{\text{неопредел}} \cdot W_{\text{неопредел}}}{C_{\text{все}}}$$

где:

- $C_{\text{крит}}$ — количество критичных уязвимостей в проекте.
- $C_{\text{хай}}$ — количество уязвимостей высокого уровня в проекте.
- $C_{\text{медиум}}$ — количество уязвимостей среднего уровня в проекте.
- $C_{\text{лоу}}$ — количество уязвимостей низкого уровня в проекте.
- $C_{\text{неопредел}}$ — количество уязвимостей с неопределённым уровнем критичности в проекте.
- $W_{\text{крит}}$, $W_{\text{хай}}$, $W_{\text{медиум}}$, $W_{\text{лоу}}$, $W_{\text{неопредел}}$ — весовые коэффициенты для каждого уровня критичности. Например:
  - $W_{\text{крит}} = 1.0$ (самый высокий вес).
  - $W_{\text{хай}} = 0.8$.
  - $W_{\text{медиум}} = 0.5$.
  - $W_{\text{лоу}} = 0.2$.

- $W_{\text{неопредел}} = 0.3$ (средний вес, так как неизвестный уровень критичности все же имеет некоторую значимость).

- $C_{\text{все}}$ — общее количество уязвимостей в проекте:

$$C_{\text{все}} = C_{\text{крит}} + C_{\text{хай}} + C_{\text{медиум}} + C_{\text{лоу}} + C_{\text{неопредел}}$$

Среднее время сканирования рассчитывает среднее время сканирования.

Процент устраненных уязвимостей рассчитывается, как отношение количества закрытых уязвимостей к общему числу уязвимостей в проекте.
Среднее время нахождения в определенном статусе рассчитывается, как медианное время нахождения в каждом статусе в целочисленном формате часов.

Интегральный риск-индекс в разрезе систем/сервисов/приложений рассчитывается по следующей формуле:

$$R = \sqrt[3]{H \cdot V \cdot L}$$

где:

- H - плотность риска
- V - коэффициент частоты сканирования
- L - коэффициент времени исправления и идентификации дефектов.

Коэффициент V (коэффициент частоты сканирования) рассчитывается по следующей формуле:

V = (Максимальная частота сканирования − Минимальная частота сканирования) / (Частота сканирования в проекте−Минимальная частота сканирования)

Данная формула нормирует частоту сканирования в проекте относительно минимальной и максимальной частоты сканирования по всем проектам. Это гарантирует, что Коэффициент V будет находиться в диапазоне от 0 до 1 и будет положительным.

Коэффициент времени исправления и идентификации дефектов L оценивает скорость устранения уязвимостей относительно медианного значения, рассчитывается по следующей формуле:

$$L = \frac{\mathrm{MTTR}_{\text{текущая}} + \mathrm{MTTD}_{\text{текущая}}}{\mathrm{MTTR}_{\text{медианная}} + \mathrm{MTTD}_{\text{медианная}}}$$

где:

- $\mathrm{MTTR}_{\text{текущая}}$ — среднее время исправления уязвимости (Mean-Time-To-Resolve).
- $\mathrm{MTTD}_{\text{текущая}}$ — среднее время обнаружения уязвимости (Mean-Time-To-Detect).
- $\mathrm{MTTR}_{\text{медианная}}$, $\mathrm{MTTD}_{\text{медианная}}$ — медианные значения этих времён по всем проектам.

L отражает отклонение времени обработки дефектов от медианных значений. Чем быстрее проект исправляет дефекты и идентифицирует их, тем меньше значение L.

Остальные используемые метрики рассчитываются на основе перечисленных выше метрик, подсчета количества значений по заданным параметрам, и используют простейшие операции вычисления.

4.3.2. Настройки виджетов

Виджеты можно настроить по необходимости. Для этого необходимо перейти в режим редактирования расположения (Рис. 15) с помощью кнопки вверху справа **Настроить расположение** (Рис. 3).

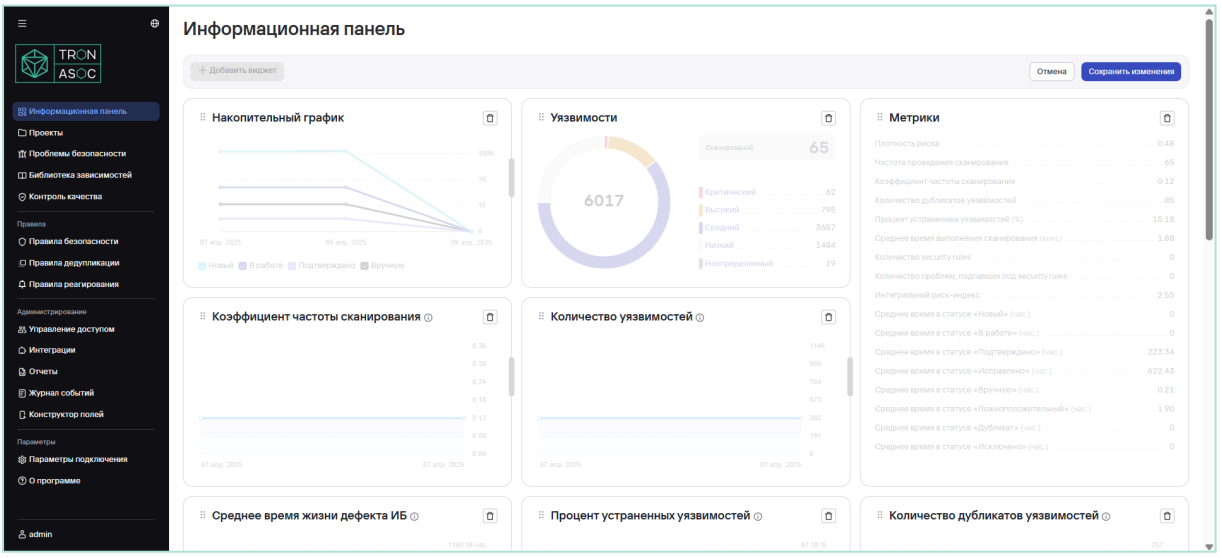

Рис. 15

В режиме редактирования расположения доступны следующие настройки виджетов:

1. Добавление новых виджетов с помощью кнопки **Добавить виджет**, в том случае, когда ранее были удалены из видимости какие-либо из представленных выше виджетов.

2. Перемещение виджетов в рамках рабочей области с помощью кнопки  на каждом из виджетов.
3. Удаление виджетов с помощью кнопки  на каждом из виджетов.
4. Увеличение длины виджета (Рис. 16).

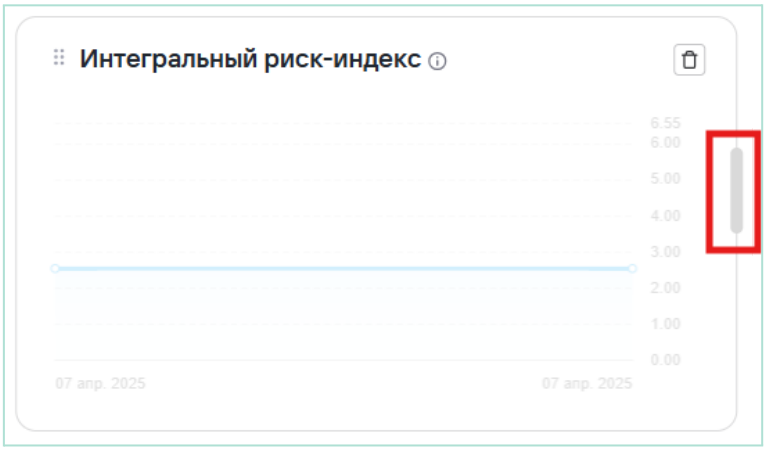

Рис. 16

После настройки расположения необходимо нажать на кнопку **Сохранить изменения**.

Также на некоторых виджетах в режиме просмотра (Рис. 3) предусмотрена возможность изменения типа виджета (Рис. 17). Предлагаются на выбор следующие типы виджетов:

- **Столбчатая диаграмма**
- **Круговая диаграмма**
- **Карточка**

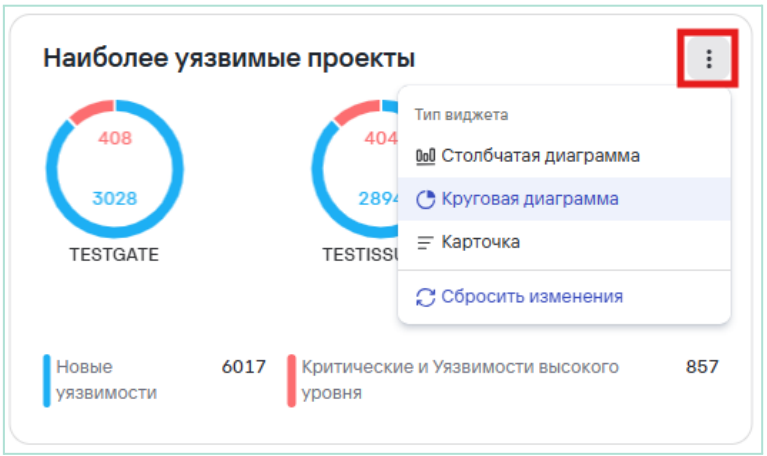

Рис. 17

4.4. Проекты

Раздел **Проекты** включает список доступных проектов, которые проверяются на соответствие политикам безопасности компании и качеству (Рис. 18). Каждый проект может иметь свои параметры безопасности и настройки. Пользователи

могут настроить как один, так и несколько проектов. Также есть возможность просматривать сводную информацию по проектам, удалять, редактировать проекты в зависимости от прав доступа.

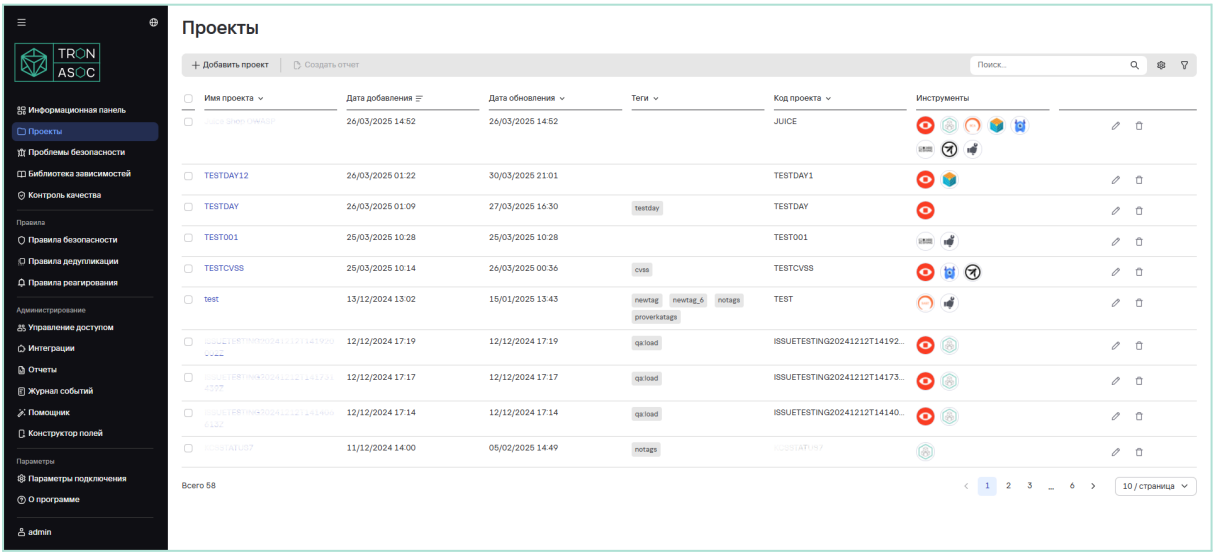

Рис. 18

Список проектов представлен в виде таблицы со следующими полями:

- **Имя проекта**
- **Дата создания**
- **Дата обновления**
- **Теги**
- **Код проекта**
- **Инструменты**

Также доступна настройка полей таблицы. Для этого необходимо нажать на кнопку  и настроить видимость полей (Рис. 19).

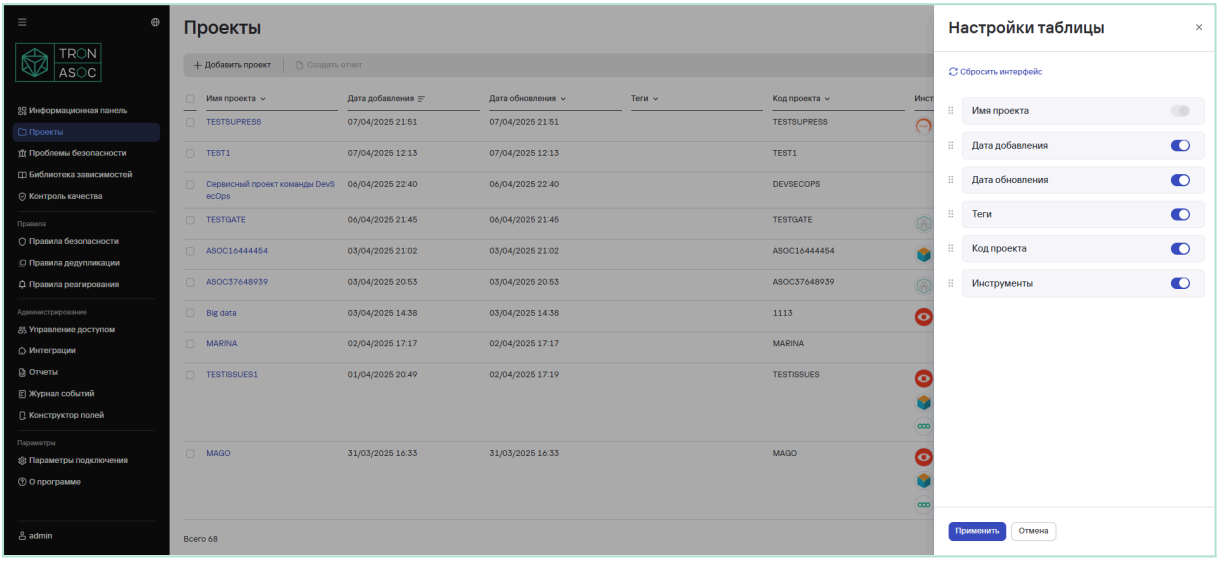

Рис. 19

В таблице проектов доступны следующие действия:

- Поиск по названию проекта.
- Фильтрация списка проектов по тегам.
- Сортировка списка по имени, тегу или коду проекта.
- Просмотр подробной информации о проекте при нажатии на имя проекта (см. раздел Обзор проекта).

4.4.1. Создание нового проекта

Чтобы создать новый проект, выполните следующие шаги:

1. Нажмите на кнопку **Добавить проект** на странице **Проекты**.
2. В открывшейся форме создания проекта (Рис. 20) заполните обязательные поля **Код проекта**, **Название проекта**, а также другие поля, при необходимости.

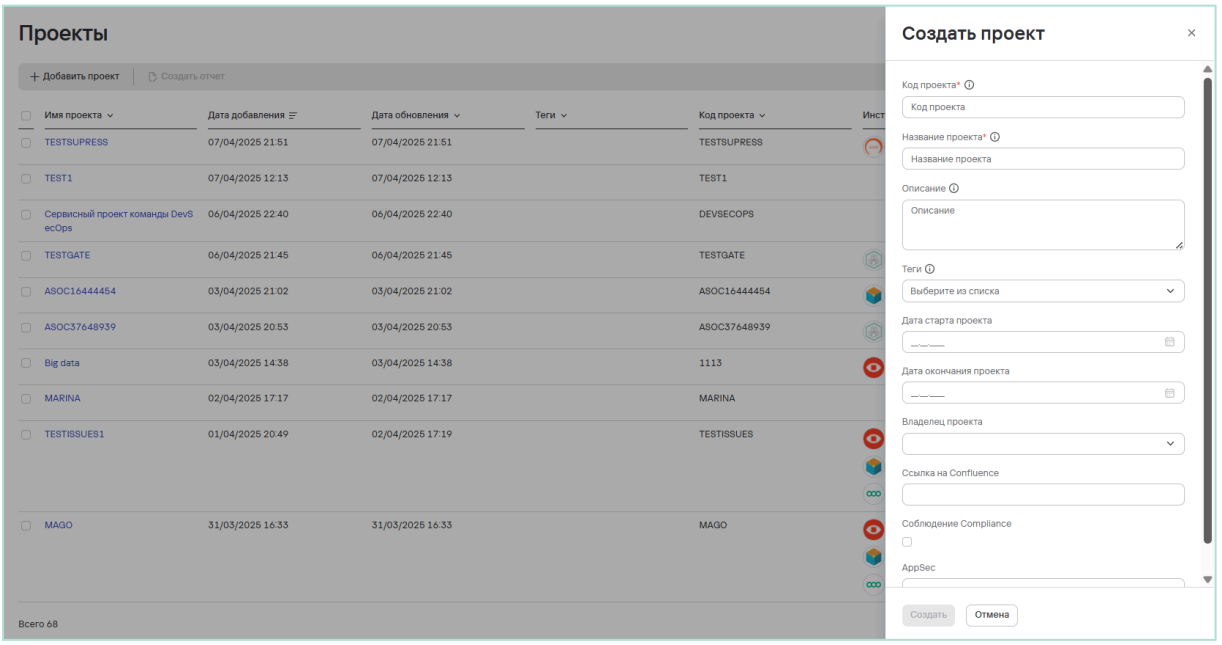

Рис. 20

> Рекомендации к заполнению некоторых полей отмечены знаком ⓘ.

3. Далее нажмите кнопку **Создать**.

4.4.2. Редактирование проекта

Для редактирования проекта необходимо нажать на кнопку ✎ напротив выбранного проекта (Рис. 18). После этого откроется форма редактирования проекта (Рис. 21).

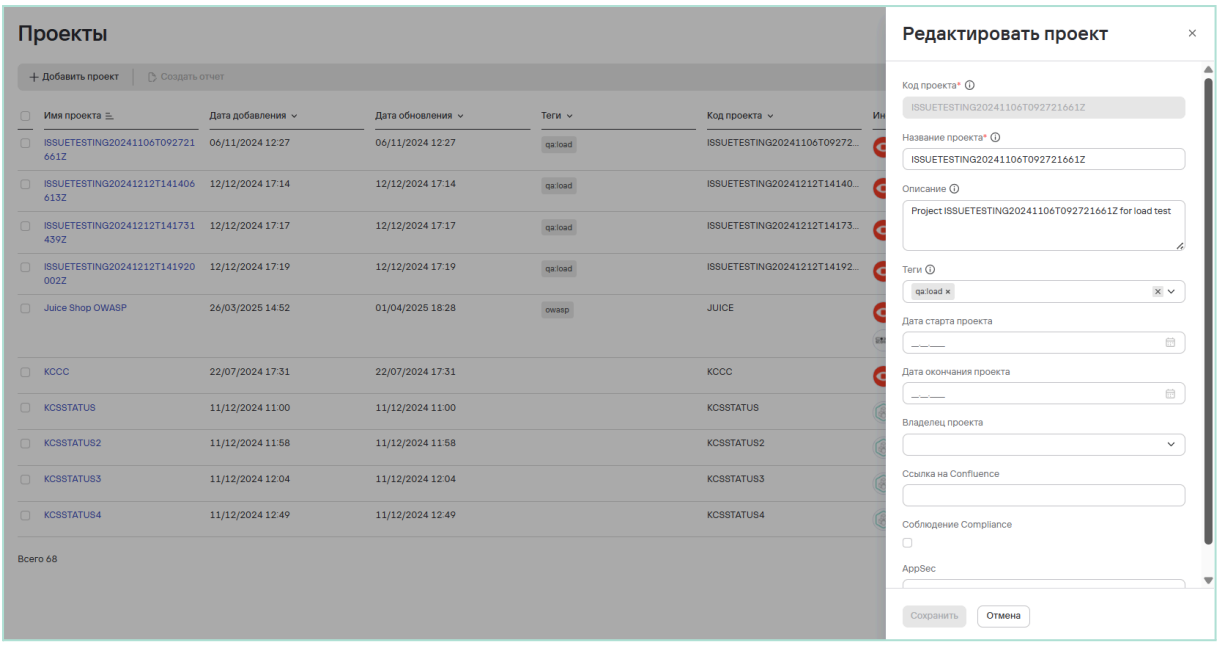

Рис. 21

После завершения редактирования, необходимо нажать на кнопку **Сохранить**.

Также, чтобы отредактировать проект, можно перейти на страницу проекта. Для этого необходимо выполнить следующие шаги:

1. На странице **Проекты** нажать на имя проекта, выделенное синим цветом (Рис. 30).
2. Перейти на вкладку **Параметры проекта** (Рис. 22).
3. Далее нажать на кнопку **Редактировать проект** (Рис. 22).

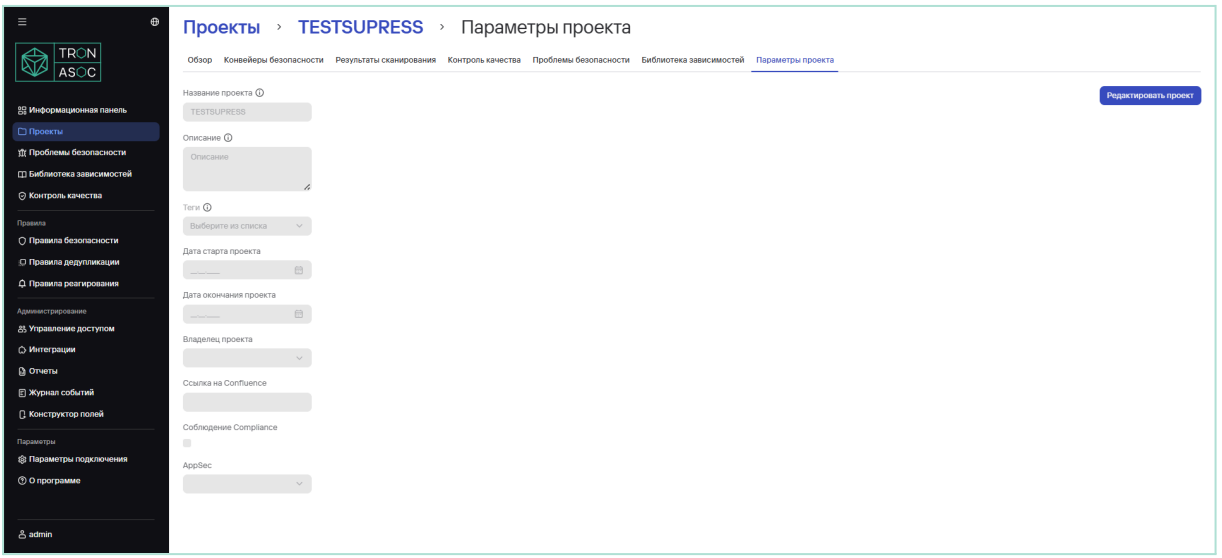

Рис. 22

4. Отредактировать параметры проекта (Рис. 21) и нажать на кнопку **Сохранить**.

4.4.3. Отчеты по проектам

В системе предусмотрены Сводный и Детализированный отчеты по проектам.

Для создания сводного отчета по проектам, необходимо выполнить следующие шаги:

1. В разделе **Проекты** выбрать проект или несколько проектов. Для этого поставить галочки в чекбоксах рядом с названиями выбранных проектов .
2. Далее нажать на кнопку **Создать отчет** (Рис. 23).

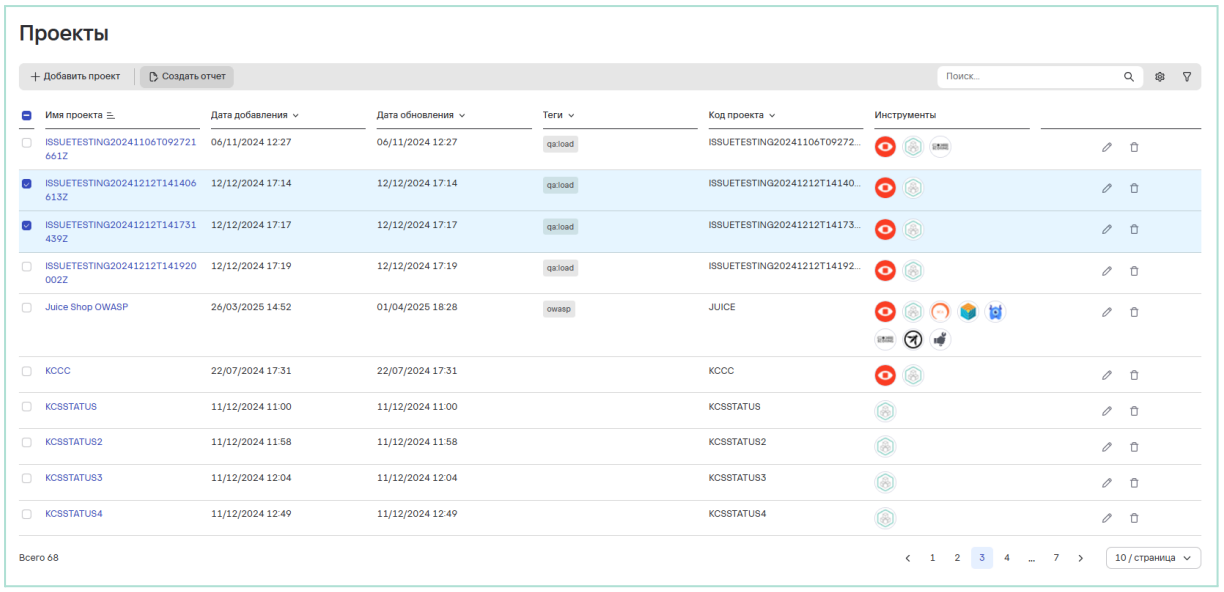

Рис. 23

3. В открывшейся форме **Создать сводный отчет** заполнить параметры и необходимые фильтры отчета, при этом рекомендуется сократить количество обнаруженных проблем до 80 (количество указано в поле **Всего проблем**), чтобы загрузка отчета не занимала много времени (Рис. 24).

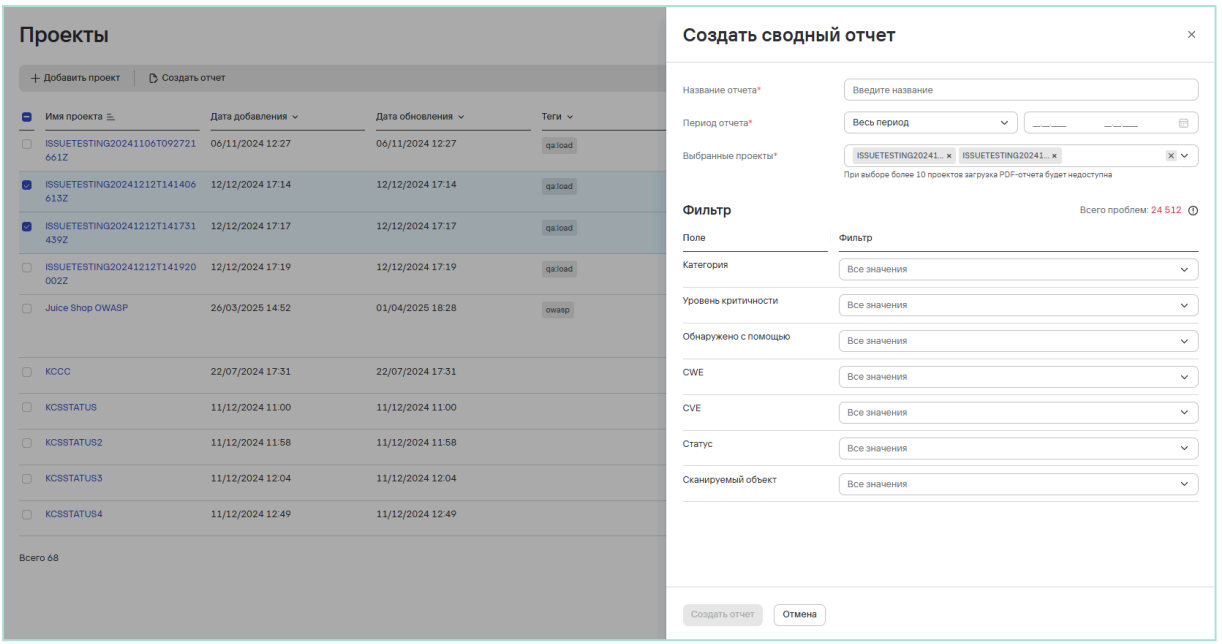

Рис. 24

4. Нажать на кнопку **Создать отчет**.
   При успешном создании пользователь увидит всплывающую нотификацию (Рис. 25). Отчет будет доступен в разделе **Отчеты** → **Сводные**.

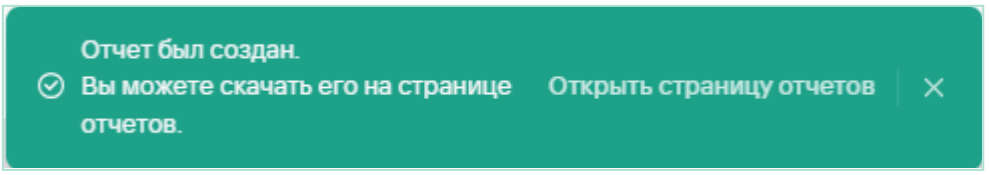

Рис. 25

Детализированный отчет доступен отдельно по проекту. Для создания данного отчета необходимо выполнить следующие шаги:

1. Перейти в Обзор проекта, нажать на кнопку **Создать отчет** и выбрать **Детализированный** (Рис. 26).

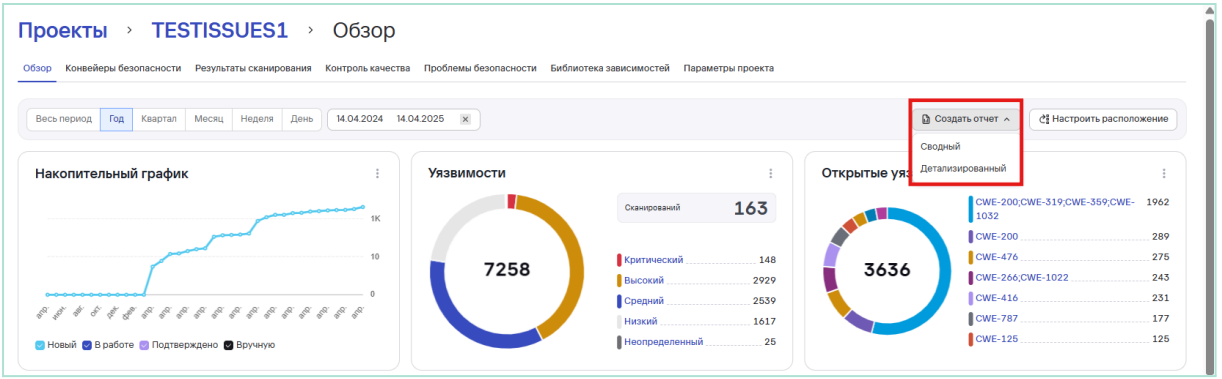

Рис. 26

2. В открывшемся окне заполнить поле **Название отчета** и добавить необходимые фильтры по полям отчета (Рис. 27), при этом рекомендуется сократить количество обнаруженных проблем до 80 (количество указано в поле **Всего проблем**), чтобы загрузка отчета не занимала много времени (Рис. 28).

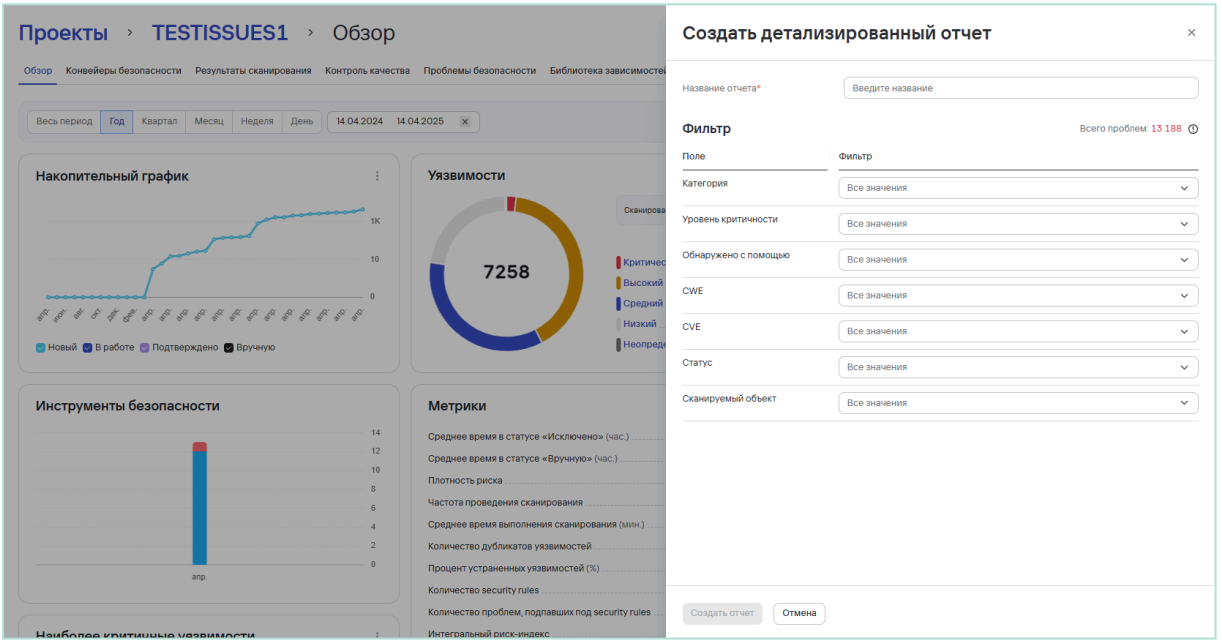

Рис. 27

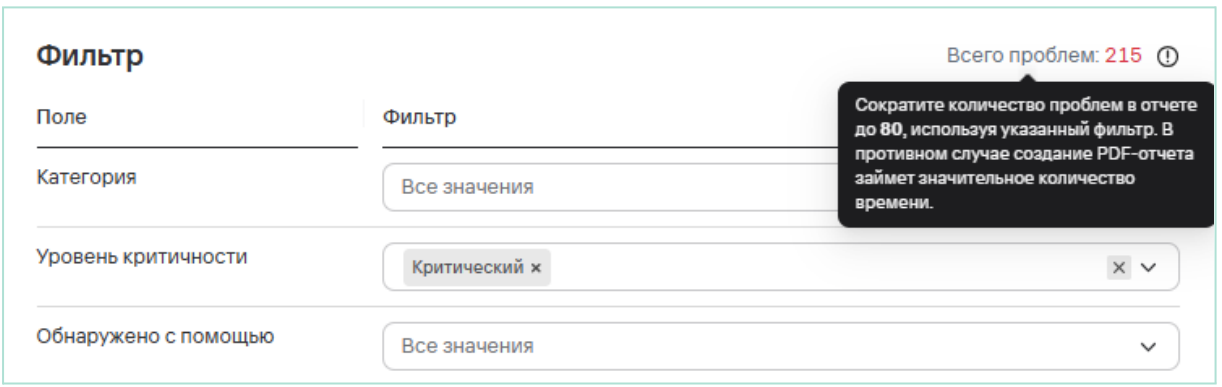

Рис. 28

3. Далее нажать на кнопку **Создать отчет**. При успешном создании пользователь увидит всплывающую нотификацию (Рис. 25). Отчет будет доступен в разделе **Отчеты** → **Детализированные**.

4.4.4. Обзор проекта

Подраздел **Обзор** (Рис. 29) предоставляет возможность просмотра Дашборда с информацией по часто встречающимся уязвимостям с параметрами критичности, источникам обнаружения и рейтингом наиболее критичных уязвимостей в рамках одного проекта. Значения накопительных графиков обновляются раз в сутки.

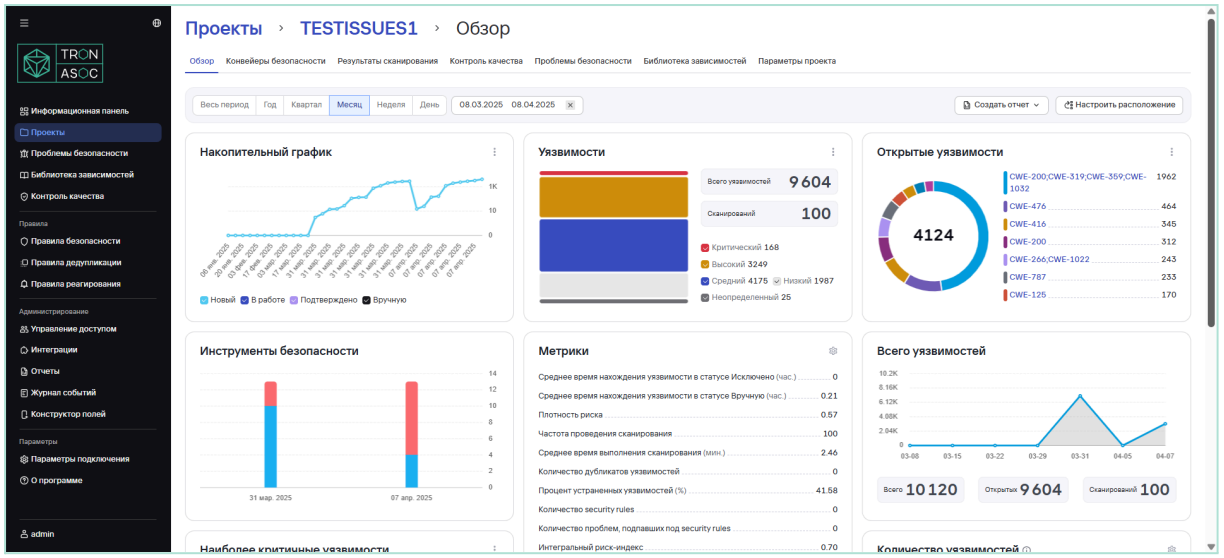

Рис. 29

Чтобы перейти к подразделу необходимо в разделе **Проекты** выбрать один из доступных проектов и нажать на имя проекта, выделенное синим цветом (Рис. 30).

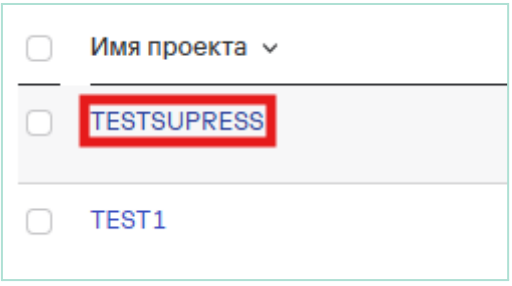

Рис. 30

Функционал настроек виджетов идентичен с настройками виджетов **Информационной панели** (подробнее см. Настройки виджетов).

4.5. Конвейеры безопасности и проверки безопасности

Конвейер безопасности (пайплайн) - это группирующая сущность для Проверок безопасности. У пользователя есть возможность создания новых и настройки доступных, в соответствии с назначенной ролью, ранее созданных Конвейеров безопасности.
В TRON.ASOC каждый Конвейер безопасности привязан к проекту.

Для того, чтобы начать работу с Конвейерами безопасности, необходимо перейти в раздел **Проекты**, найти необходимый проект, открыть его обзор, после чего перейти на вкладку **Конвейеры безопасности** (Рис. 31).

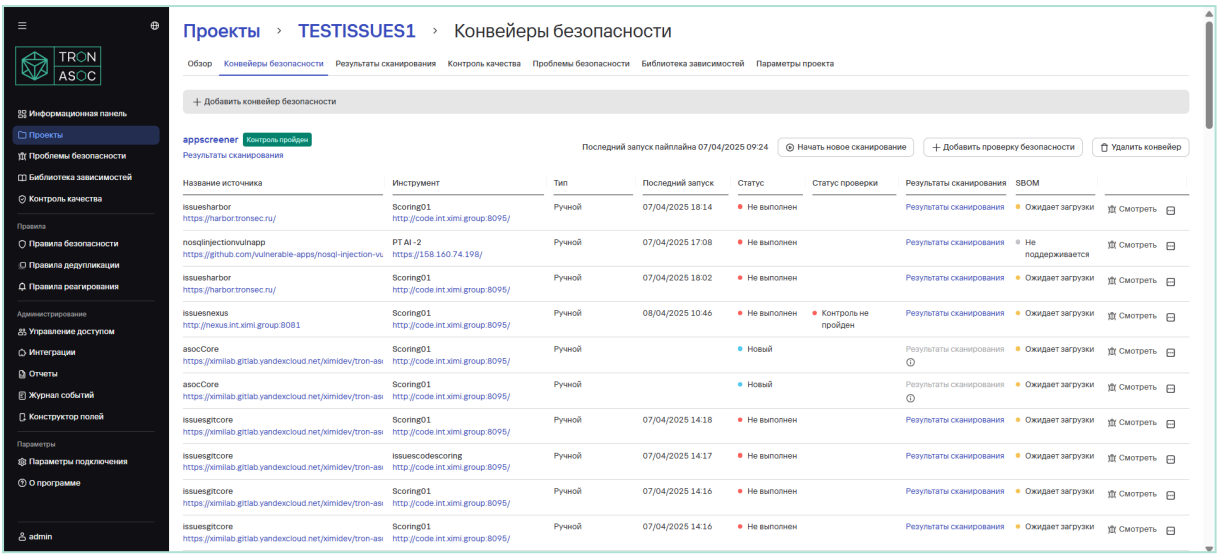

Рис. 31

Каждый **Конвейер безопасности** представлен отдельной строкой, которая содержит название и описание конвейера, ссылку на результаты сканирования, содержащиеся внутри конвейера проверки безопасности.
Также отображены данные проверки безопасности (название каждой проверки безопасности в конвейере, используемые в проверке инструменты безопасности и источники, тип проверки (ручной или автоматический), время последнего запуска, статус последнего успешного сканирования, ссылка на результаты сканирования (Рис. 31).

4.5.1. Создание конвейера безопасности

Чтобы создать новый **Конвейер безопасности**, необходимо выполнить следующие шаги:

1. В разделе **Проекты** найти необходимый проект и перейти на страницу данного проекта (Обзор проекта)
2. Перейти на вкладку **Конвейер безопасности**
3. Нажать на кнопку **Добавить конвейер безопасности** (Рис. 32).

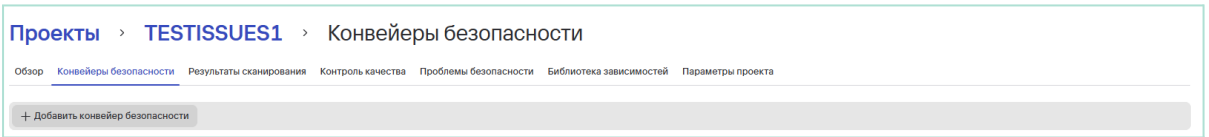

Рис. 32

4. На странице создания конвейера безопасности (Рис. 33) заполнить обязательное поле **Имя**, а также дополнительные поля **Описание** и **Шаблон** при необходимости.

❕ В роли шаблона может быть любой другой конвейер безопасности, созданный ранее. Для добавления шаблона необходимо в поле **Шаблон** ввести название конвейера безопасности, который необходимо переиспользовать. По умолчанию список шаблонов появляется при вводе символов в поле **Шаблон** (Рис. 33).

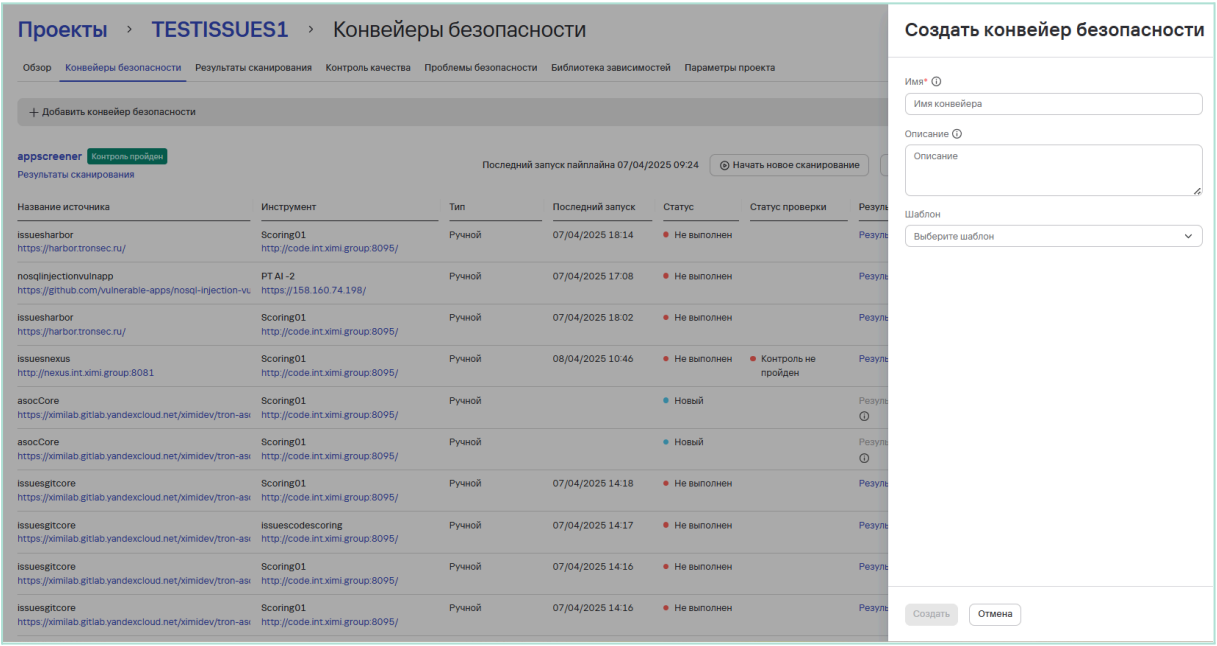

Рис. 33

5. Далее нажать на кнопку **Создать**.

После создания Конвейера безопасности необходимо добавить к нему Проверку безопасности.

4.5.2. Создание проверки 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.

Для того, чтобы добавить проверку безопасности, необходимо выполнить следующие шаги:

1. В разделе **Проекты** → *<Название проекта>* → **Конвейеры безопасности** нажать на кнопку **Добавить проверку безопасности** (Рис. 34).

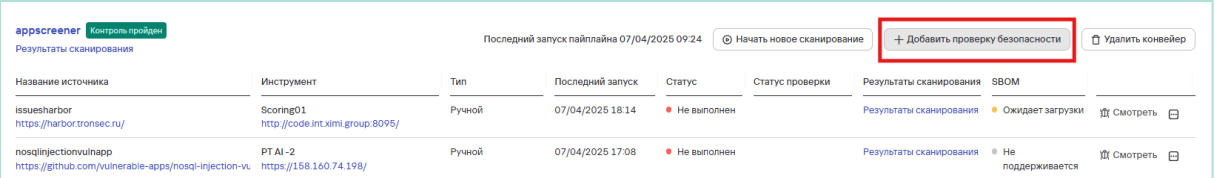

Рис. 34

2. Далее заполнить форму создания проверки безопасности (Рис. 35).

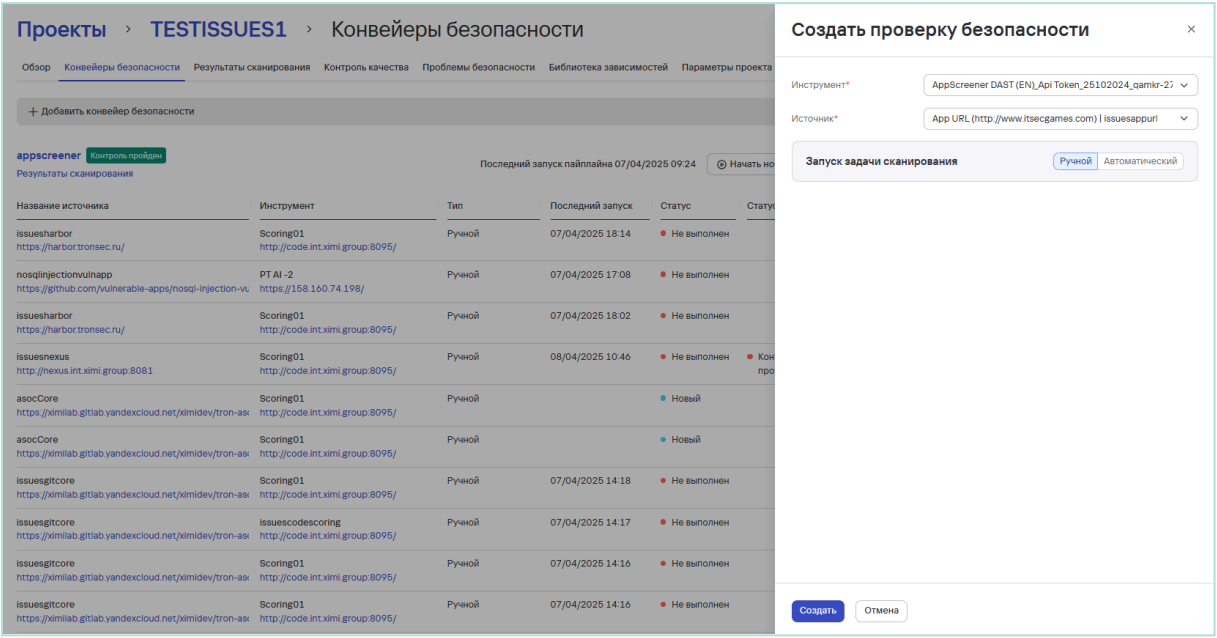

Рис. 35

Для настройки проверки безопасности выбор инструмента безопасности является обязательным (Рис. 35). Выбрать возможно только инструмент, ранее добавленный администратором в разделе Интеграции.
Поля формы зависят от выбранных полей **Источник** и **Инструмент**.

3. Нажать на кнопку **Создать**.

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, необходимо ввести данные для аутентификации в соответствующие поля (могут меняться в зависимости от метода: **Токен API**, **Логин/Пароль**).
Если при создании интеграции с источником сканирования 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, необходимо ввести данные для аутентификации в соответствующие поля (Рис. 36).

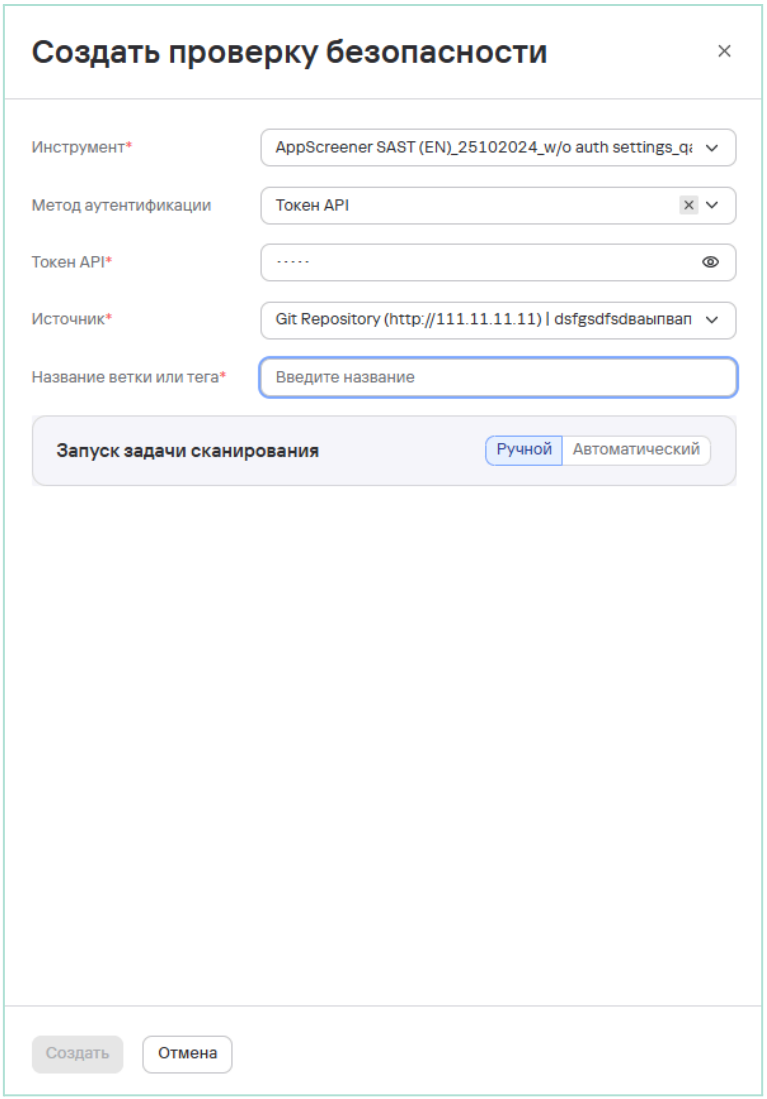

Рис. 36

Также для некоторых инструментов предусмотрена возможность выбора типа запуска сканирования (ручной или автоматический), периодичность и время запуска сканирования при выборе автоматического запуска.

После заполнения всех необходимых полей (инструмент безопасности, источник, методы аутентификации) предлагается проверить соединение с инструментами. Для этого необходимо нажать на кнопку **Проверить соединение** (в случае, если она активна).

В проверках безопасности также предусмотрена загрузка (импорт) результатов сканирования от внешних инструментов (Рис. 37) в зависимости от выбранного инструмента безопасности. Эта опция доступна не для всех инструментов безопасности.

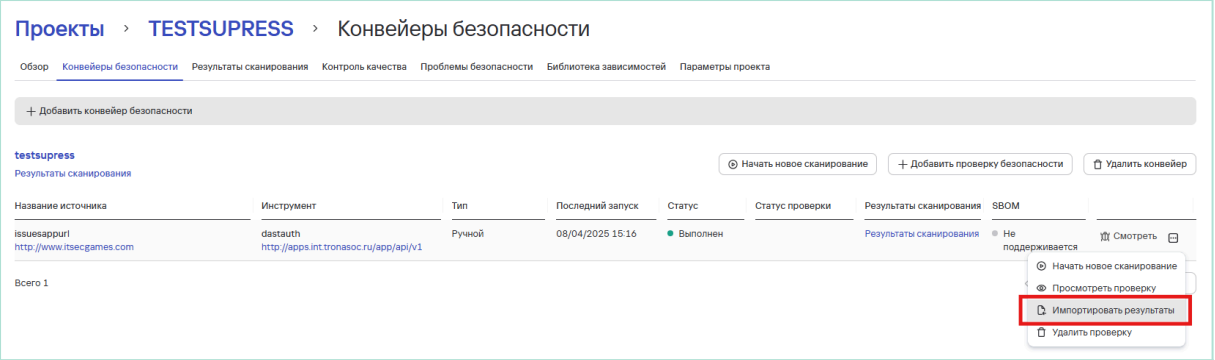

Рис. 37

4.5.3. Запуск конвейера безопасности

Для того, чтобы запустить конвейер безопасности необходимо выполнить следующее:

1. В разделе **Проекты** → <*Название проекта*> → **Конвейеры безопасности** нажать кнопку **Начать новое сканирование** (Рис. 38).

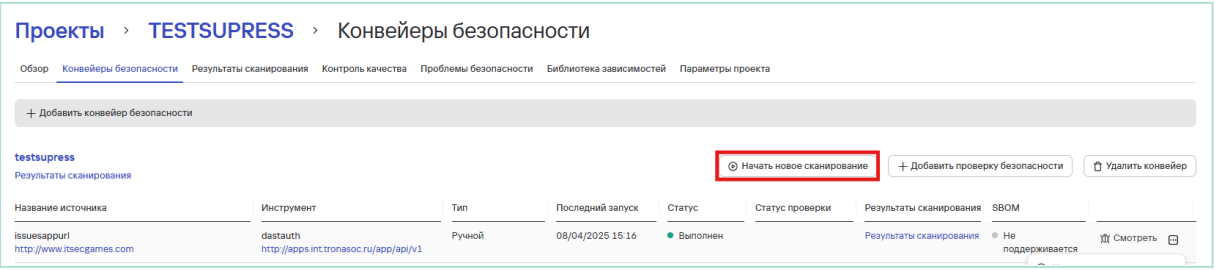

Рис. 38

Данное действие приведет к запуску всех проверок безопасности в конвейере.

❗ Ввиду архитектурных ограничений продукта **Solar AppScreener,** может возникать проблема с одновременным запуском сканирования большого (от нескольких десятков) количества проверок безопасности (конвейера безопасности с проверками). В случае возникновения указанной проблемы, рекомендуем запускать проверки безопасности по отдельности, подробнее см. 4.5.4. Запуск проверки безопасности.

4.5.4. Запуск проверки безопасности

Для того, чтобы запустить отдельную проверку безопасности необходимо выполнить следующее:

1. В разделе **Проекты** → <*Название проекта*> → **Конвейеры безопасности** найти в списке необходимую проверку безопасности и раскрыть список действий по данной проверке с помощью кнопки  .
2. В списке действий выбрать **Начать новое сканирование** (Рис. 39).

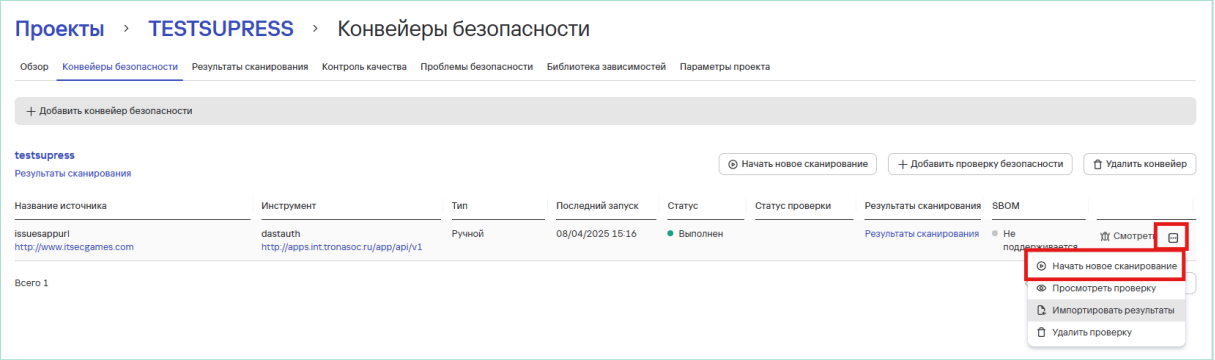

Рис. 39

При запуске проверки безопасности меняется ее статус на ***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 возникли ошибки на каком-либо из этапов сканирования.

4.5.5. Остановка сканирования

Сканирование со статусом ***В процессе*** возможно принудительно остановить. Для этого в разделе **Проекты** → *<Название проекта>* → **Конвейеры безопасности** в соответствующей Проверке безопасности необходимо нажать на кнопку **Остановить сканирование**.

4.5.6. Загрузка внешнего отчета

Загрузка внешнего отчета может быть произведена вручную. Для загрузки необходимо выполнить следующие шаги:

1. В разделе **Проекты** → *<Название проекта>* → **Конвейеры безопасности** нажать на кнопку **Импортировать результаты** в меню справа (Рис. 40).

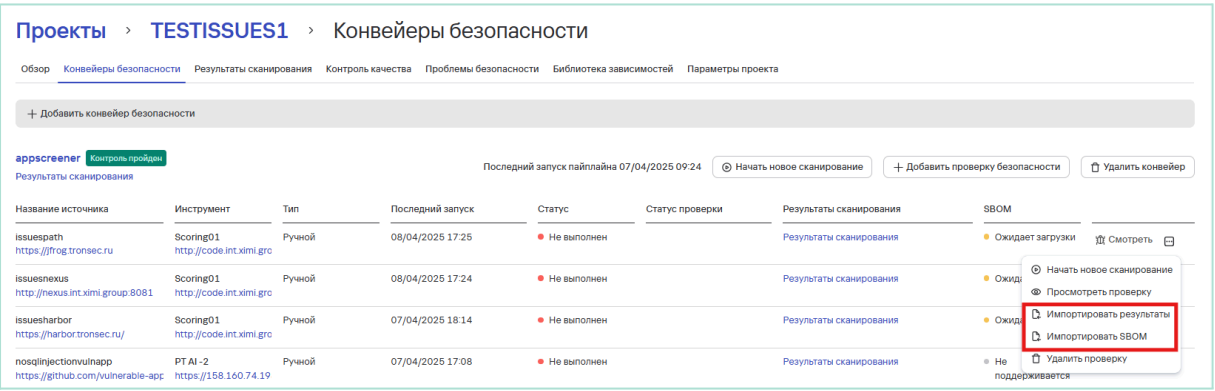

Рис. 40

2. Далее загрузить JSON-файл с результатами (Рис. 41).

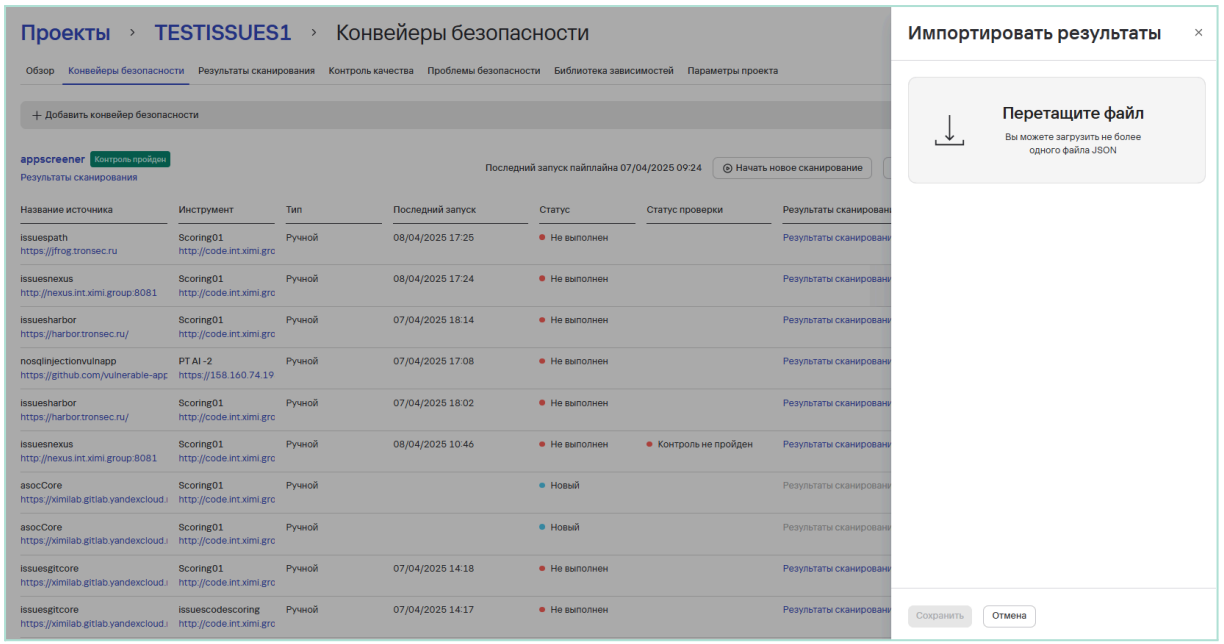

Рис. 41

3. Нажать на кнопку **Сохранить**.

Требования к JSON-файлу:

```
{
 "properties": {
   "issues": {
     "type": "array",
     "items": {
       "type": "object",
       "properties": {
         "category": { "type": "string" },
         "severity": {
           "type": "string",
           "enum": ["critical", "high", "medium", "low", "undefined"]
         },
         "id": { "type": "string" },
         "cwe": { "type": "string" },
         "cve": { "type": "string" },
         "line": { "type": "integer", "minimum": 1 },
         "code": { "type": "string" },
         "libraryName": { "type": "string" },
         "libraryVersion": { "type": "string" },
         "file": { "type": "string" },
         "links": {
           "type": "array",
           "items": { "type": "string", "format": "uri" }
         },
         "description": { "type": "string" },
         "recommendation": { "type": "string" },
         "fixedVersion": { "type": "string" },
```

```
        "ratings": {
          "type": "array",
          "items": {
            "type": "object",
            "properties": {
              "metric": { "type": "string" },
              "score": { "type": "number", "minimum": 0, "maximum":
10 }
            },
            "required": ["metric", "score"]
          }
        },
        "path": {
          "type": "array",
          "items": { "type": "string" }
        }
      },
      "required": ["category", "severity"]
    }
  }
 },
 "required": ["issues"]
}
```

Пример тела запроса:

```
[
 {
   "category": "OS dependency vulnerability",
   "severity": "high",
   "scan_object": "jfrog.tronsec.ru/tron/event-broker:1.1.2-patch",
   "cwe": "CWE-79",
   "cve": "CVE-2023-1234",
   "tool_type_name": "KCS",
   "lib_name": "example-library",
   "lib_version": "1.2.3",
   "info_links": ["https://example.com/cve-2023-1234",],
   "description": "This is a vulnerability description.",
   "recommendations": "Sanitize user input before executing
commands.",
   "fixed_version": "1.2.4",
   "ratings": "CVSS: 9.1 (Critical)",
   "path": "/src/controllers/userController.js",
   "exploit": "Proof-of-concept exploit code here."
 },
```

Кроме того, при использовании внешних скриптов и в зависимости от выбранного инструмента сканирования (например, CLI-инструмента) у проверки безопасности может быть доступна опция получения результатов сканирования извне путём http-запроса от внешнего инструмента на эндпоинт TRON.ASOC.
Предусмотрена возможность загрузки не более одного файла в формате JSON.

4.5.7. Использование CLI-инструментов

Для того, чтобы получить возможность отправки результатов от CLI-инструмента (Command Line Interface), предварительно необходимо добавить его в список доступных инструментов безопасности в разделе **Интеграции** → **Источники безопасности**, при этом необходимо заполнить поля **Название**, **Описание** и выбрать один из представленных инструментов (Рис. 42):

- **Trivy**
- **Crype**
- **OWASP Dependency Track**
- **Semgrep**
- **Aqua**
- **CodeScoring**
- **Kaspersky Container Security**
- **KICS**
- **PT Application Inspector**
- **Solar Appscreener**
- **Manual** - сторонний инструмент, из которого можно загрузить результаты сканирований в систему, которые будут учитываться при дальнейшей обработке данных. Результаты загружаются в формате JSON с теми же требованиями, что представлены в разделе выше Загрузка внешнего отчета.

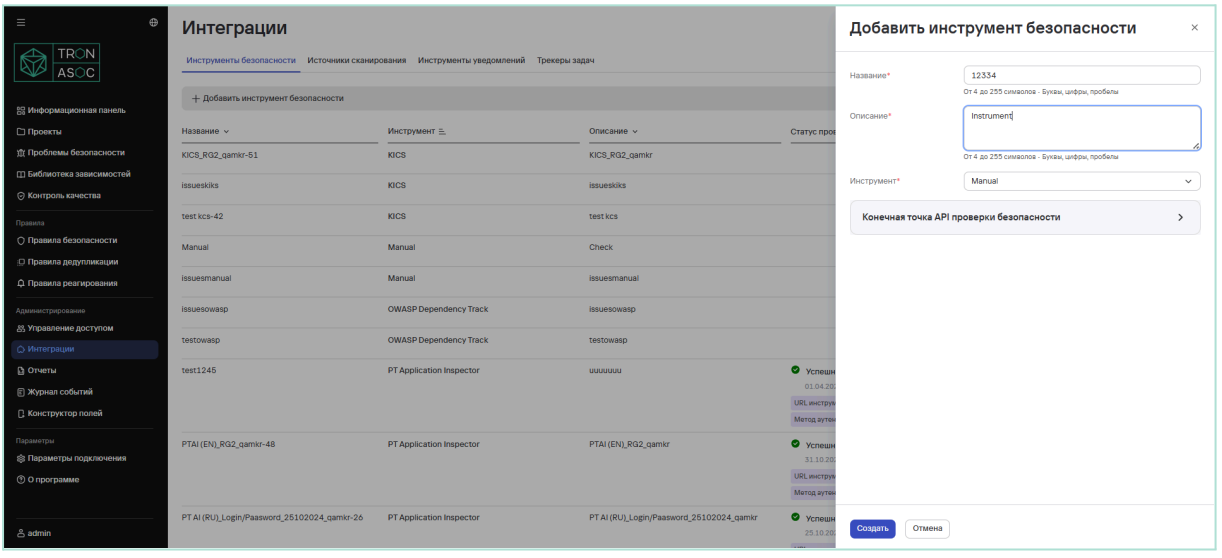

Рис. 42

После добавления инструмента необходимо добавить новый источник сканирования. Для этого необходимо выполнить следующие шаги:

1. В разделе **Интеграции** → **Источники сканирования** нажать на кнопку **Добавить источник сканирования.**
2. В открывшейся форме заполнить поля **Имя**, **Описание**, указать значение поля **Источник** = ***CLI Tool Custom Source*** (Рис. 43).
   Для CLI-инструментов источником может быть любая ссылка: репозиторий, база знаний и т.д.

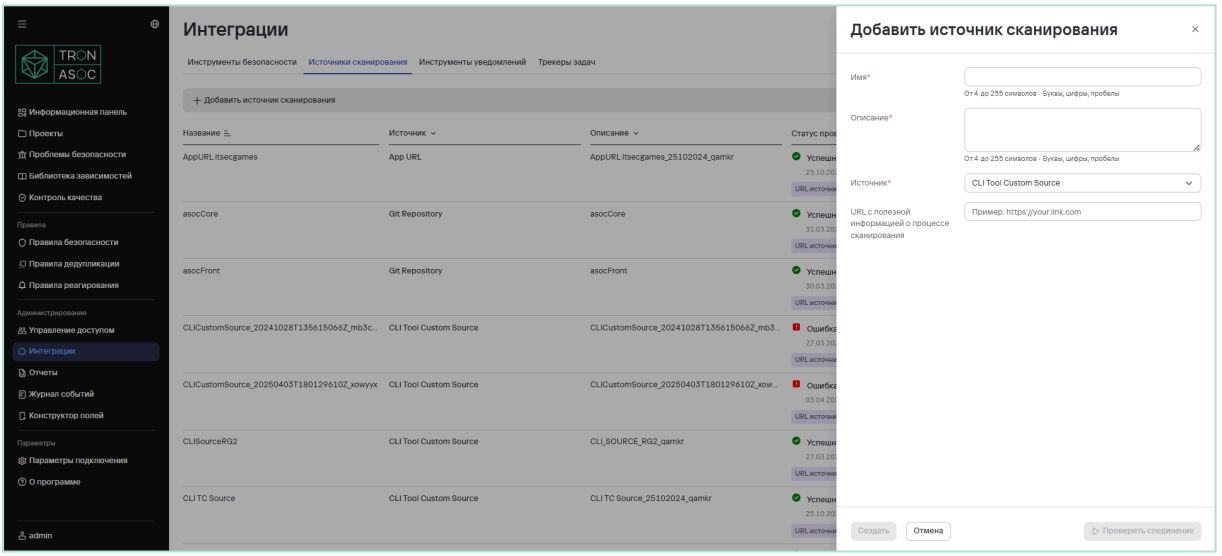

Рис. 43

3. Нажать на кнопку **Создать**.

Далее требуется создать проверку безопасности в конвейере безопасности соответствующего проекта. Для этого необходимо выполнить следующие шаги:

1. В разделе **Проекты** → <*Название проекта*> → **Конвейеры безопасности** нажать на кнопку **Добавить проверку безопасности**.
2. В открывшейся форме создания проверки указать ранее созданные инструмент сканирования и источник сканирования соответственно в полях **Инструмент** и **Источник** (Рис. 44).

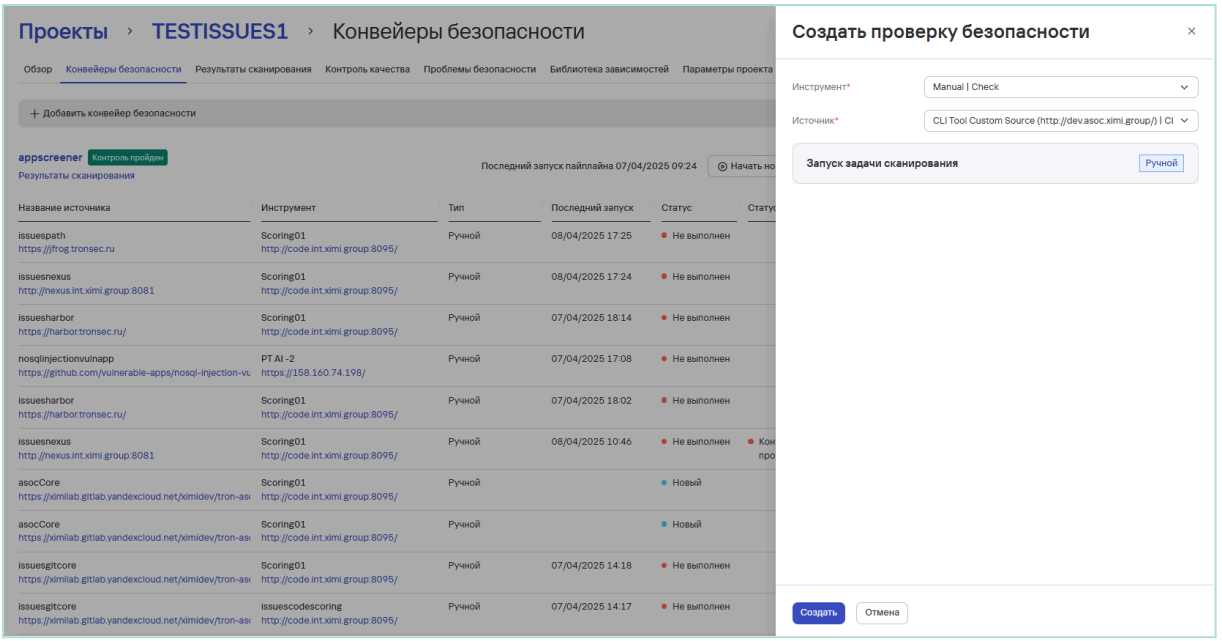

Рис. 44

3. Нажать на кнопку **Создать.**
   После успешного создания проверки будет доступен запуск сканирования данной проверки, а также всех созданных проверок выбранного проекта.

4.5.8. Интеграция в CI процесс

В системе предусмотрена возможность интегрировать сканирование уязвимостей в CI-пайплайн GitLab, используя различные инструменты для сканирования, и отправлять результаты сканирования в ASOC.

4.5.8.1. Описание переменных

Для правильной настройки скрипта необходимо использовать следующие переменные:

- `IMAGE_TO_SCAN: yourimagename/latest` - образ Docker, который будет сканироваться.
- `REPORT_FILE: trivy-report.json` - имя файла, в который будет сохранен отчет сканирования.
- `API_URL: http://your-tronasoc-url/api/v1/check/{check_id}/external` - адрес API.
- `API_TOKEN: asoc-your_api_token_here` - API токен TRON.ASOC.

Данные переменные необходимо задать в разделе `variables` в файле ***gitlab-ci.yml***.

4.5.8.2. Пример отправки результата сканирования CLI-инструмента в TRON.ASOC в рамках CI

Пример включает две стадии — scan и upload. Скрипт сначала выполняет сканирование, а затем загружает результат.

```
stages:
  - scan
  - upload

variables:
  IMAGE_TO_SCAN: anaisurlichs/cns-website:0.0.6 # Образ Docker,
который будет сканироваться.
  REPORT_FILE: trivy-report.json # Имя файла, в который будет сохранен
отчет сканирования.
  API_URL:
http://example.asoc.ximi.group/api/v1/check/{check_id}/external #
адрес API.{CheckID} становится доступным после создания Проверки
безопасности.
 API_TOKEN: asoc-exampletoken # API токен TRON.ASOC.

scan_image:
  stage: scan
  image: aquasec/trivy:latest # Docker-образ, который будет
использоваться для выполнения задачи, в зависимости от инструмента.
script:
    # Скрипт запускает trivy для сканирования указанного Docker-образа
и сохраняет результат в переменную $REPORT_FILE.
    - trivy image --format json --output $REPORT_FILE $IMAGE_TO_SCAN
    - echo "Scan completed, report saved to $REPORT_FILE"
   #  Артефакты, которые будут сохраняться в GitLab.
  artifacts:
    paths:
      - $REPORT_FILE
    when: always # Обеспечивает сохранение артефакта независимо от
успешного или неуспешного выполнения задачи.

upload_report:
  stage: upload
  image: curlimages/curl:latest # Минимальный образ на базе Alpine с
предустановленным curl.
  script:
    # Содержит команду curl для отправки POST-запроса на адрес API,
используя --data для передачи содержимого файла отчета сканирования.
    - echo "Uploading report $REPORT_FILE to $API_URL"
    - |
      curl --location $API_URL --header "x-api-token: $API_TOKEN"
--header "content-type: application/json" --data @$REPORT_FILE
```

```
  #  Задает зависимость от задачи scan_image, чтобы upload_report имел доступ к артефактам в этой задаче.
  dependencies:
    - scan_image
```

Пример использует Trivy в качестве сканера и предназначен для GitlabCI. Также предлагается использовать любой инструмент, изменив образ и команды стадии stage.

Если уже есть результат сканирования - рекомендуется использовать стадию upload для отправки результатов (артефакта). Ниже приведен пример для Grype:

```
scan_image:
  image: anchore/grype:latest
  stage: scan
  script:
    - echo "Scanning image $IMAGE_TO_SCAN"
    - grype $IMAGE_TO_SCAN -o json > $REPORT_FILE
    - echo "Scan completed, report saved to $REPORT_FILE"
  artifacts:
    paths:
      - $REPORT_FILE
    when: always
```

4.5.9. Результаты сканирований

Результат успешного сканирования можно просмотреть как для отдельного конвейера безопасности во вкладке **Проекты** → *<Название проекта>* → **Результаты сканирований**, так и для отдельной проверки безопасности (Рис. 45).

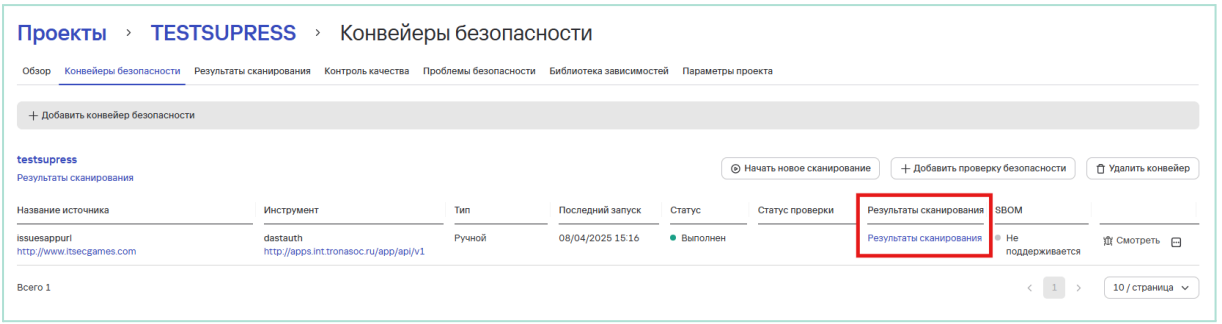

Рис. 45

Результаты сканирования (Рис. 46) содержат информацию о конвейере безопасности, источнике, использованном инструменте безопасности, дате начала, количестве найденных проблем безопасности, статусе сканирования.

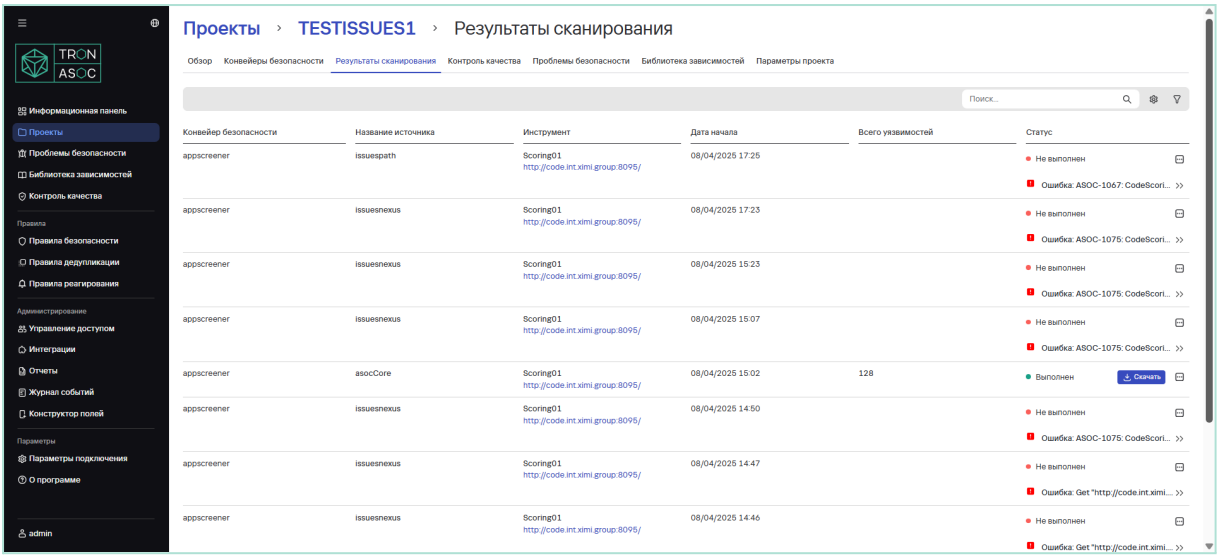

Рис. 46

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. Выполненный отчет можно скачать с помощью кнопки **Скачать** (Рис. 47).

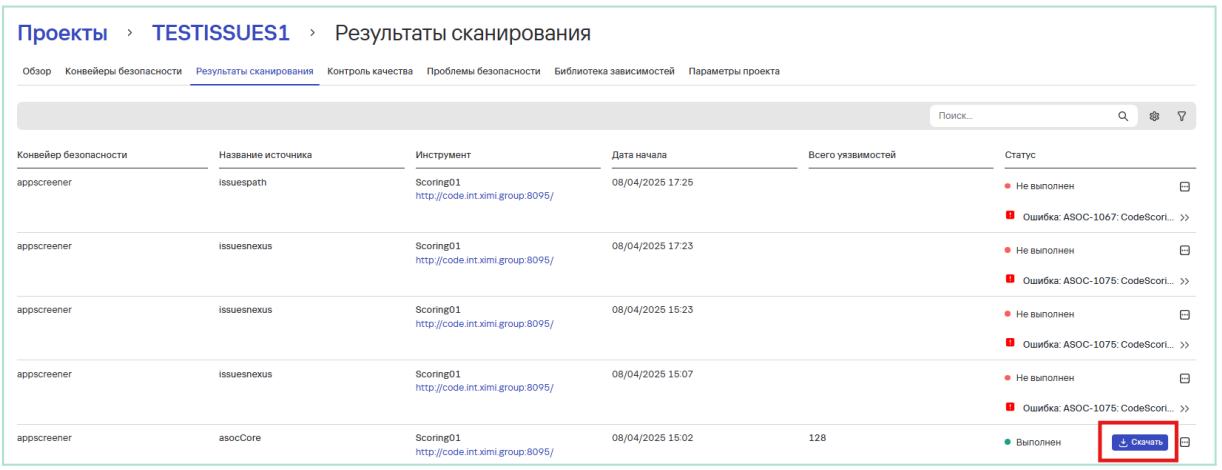

Рис. 47

4.5.10. Контроль качества проекта

Конвейеры безопасности и проверки безопасности могут содержать один или несколько Контролей качества, информация о которых представлена в разделе **Проекты** → *<Название проекта>* → **Контроль качества** (Рис. 48).

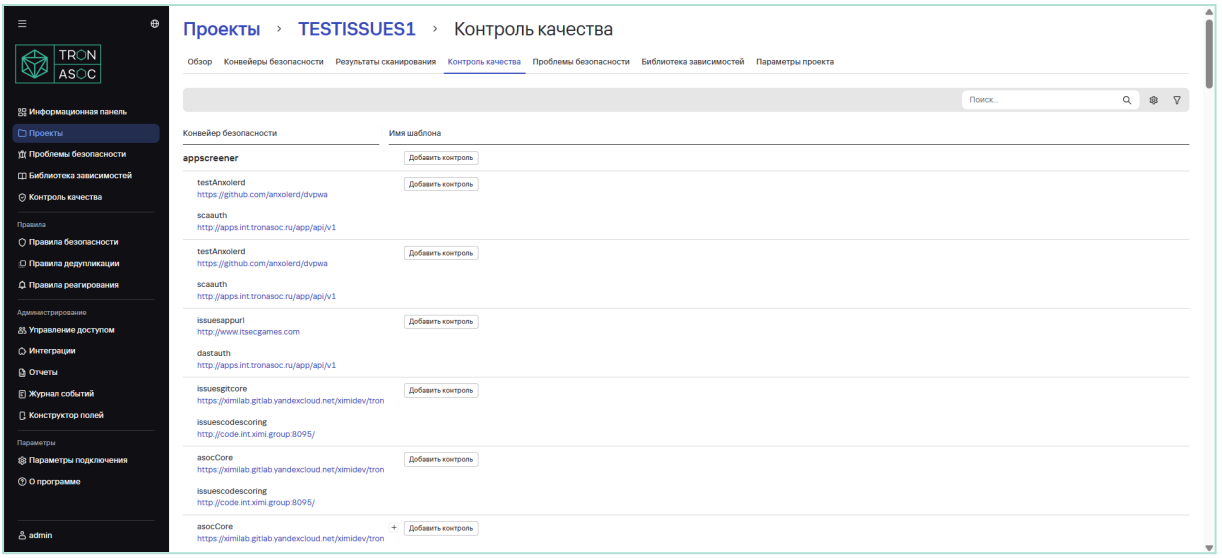

Рис. 48

На данной вкладке доступно управление привязкой контролей качества к пайплайну и чеку с возможностью установить правило действия выбранного контроля (информационное оповещение о провале гейта или блокирование merge-request'а до устранения ошибок).

Для того, чтобы добавить Контроля качества, необходимо выполнить следующие шаги:

1. В разделе **Проекты** → <*Название проекта*> → **Контроль качества** нажать на кнопку **Добавить контроль.**
2. В раскрывшемся списке (Рис. 49) выбрать требуемый контроль или нажать на кнопку **Создать новый контроль качества** (в данном случае, откроется форма создания нового контроля (Рис. 50)).

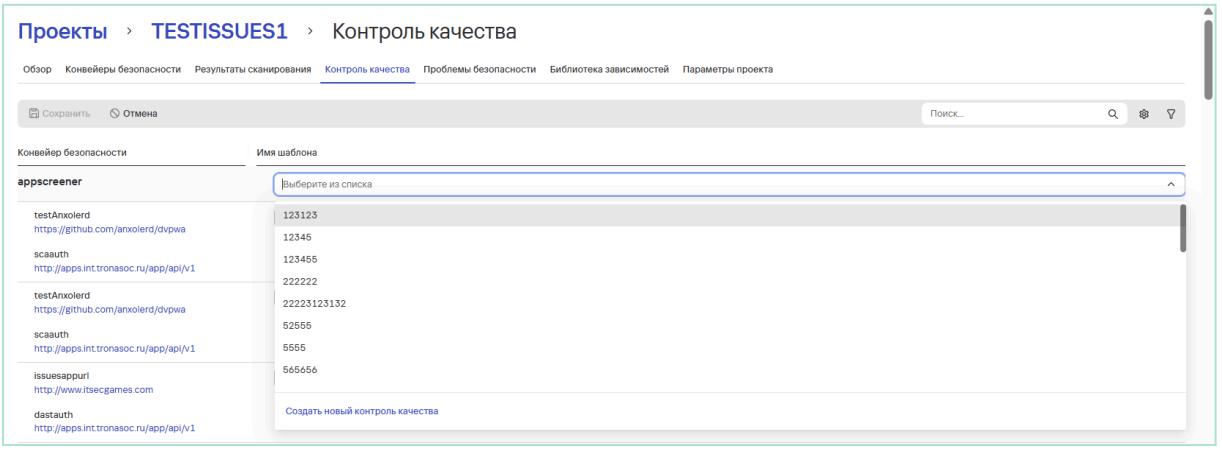

Рис. 49

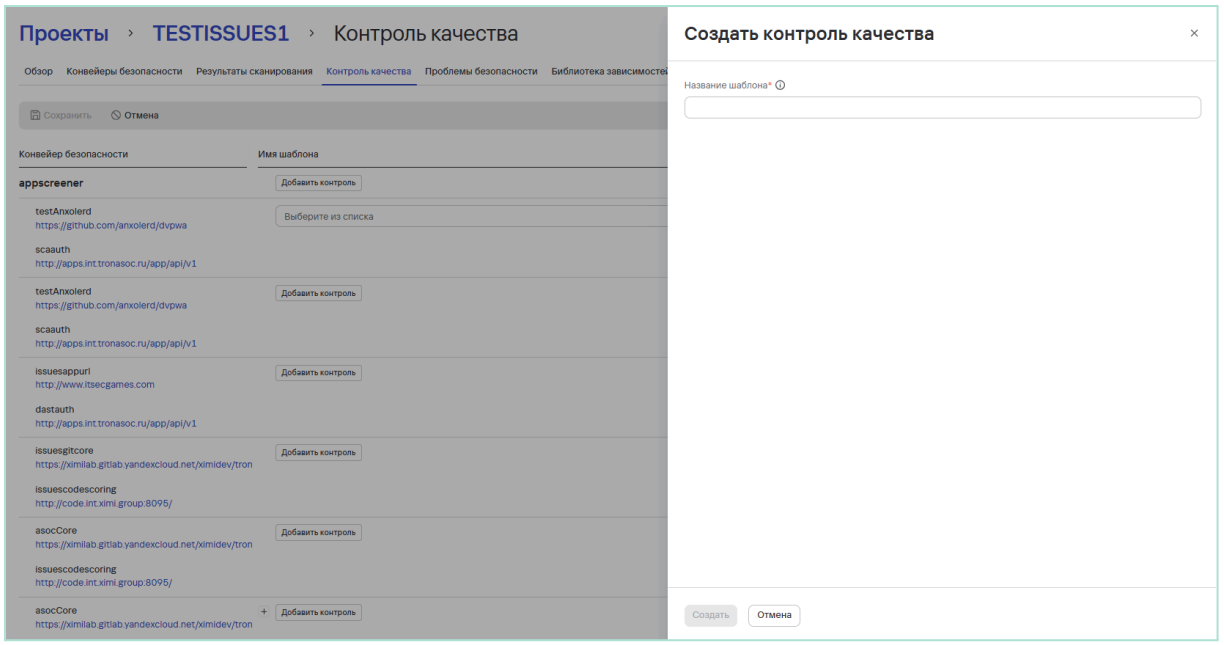

Рис. 50

3. Нажать на кнопку **Сохранить**.

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

4.6. Проблемы безопасности

В разделе **Проекты** → <*Название проекта*> → **Проблемы безопасности** (Рис. 51) (или в разделе **Проблемы безопасности** из главного меню слева) отображаются 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).

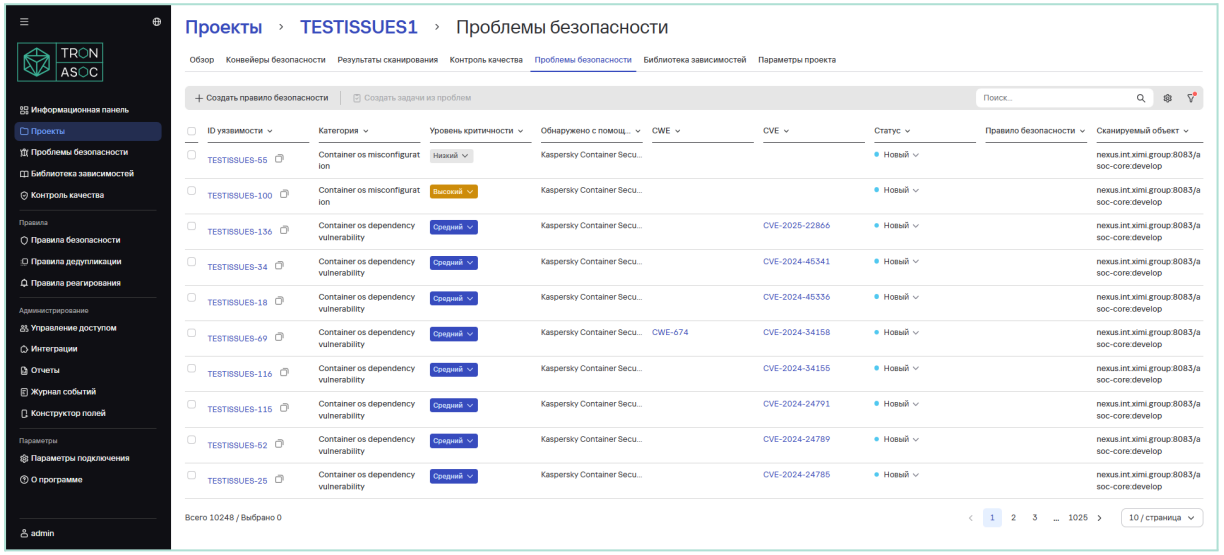

Рис. 51

По каждой найденной проблеме предусмотрена возможность получить дополнительную информацию в окне детального просмотра уязвимости (Рис. 52). Для просмотра необходимо нажать на **ID уязвимости**.

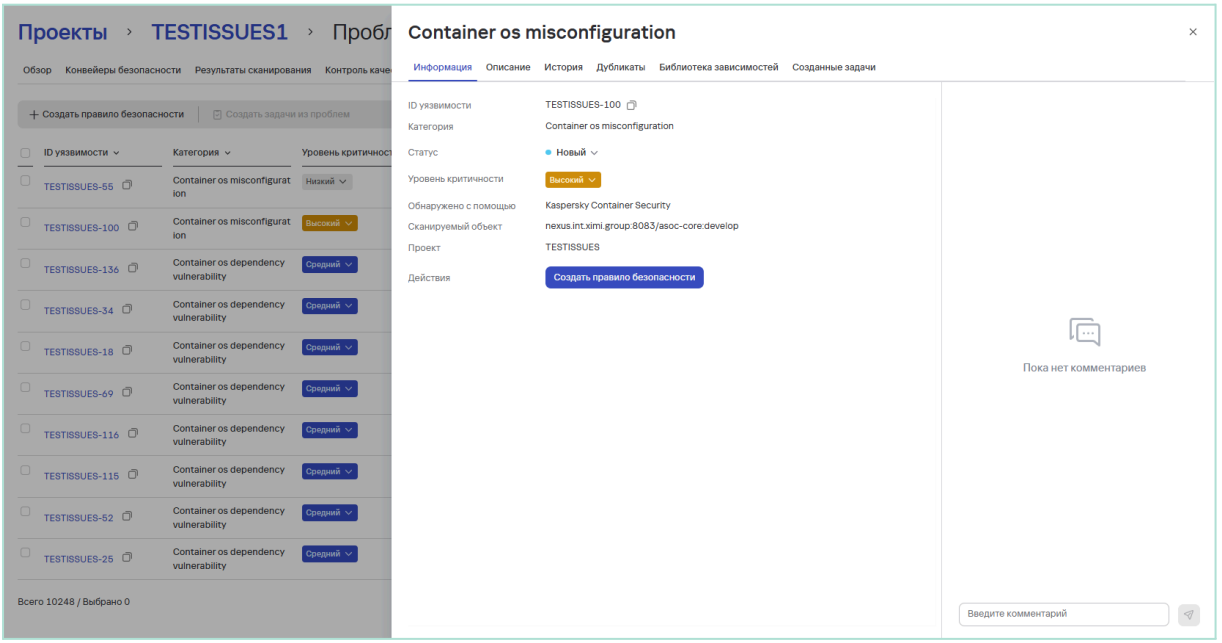

Рис. 52

Также предусмотрены следующие возможности:

- Возможность оставлять комментарии, просматривать комментарии других пользователей. Раздел комментариев находится в окне детального просмотра проблемы безопасности
- Видимость статусов проблем безопасности (Новый, В работе, Ложноположительный, Подтвержденный, Исправлено, Исключено, Вручную, Дубликат). Статусы можно изменять при просмотре списка найденных проблем, а также в окне детального просмотра.
- Фильтрация по доступным атрибутам. Для настройки необходимо нажать на кнопку  и выбрать требуемые настройки фильтрации (Рис. 53).

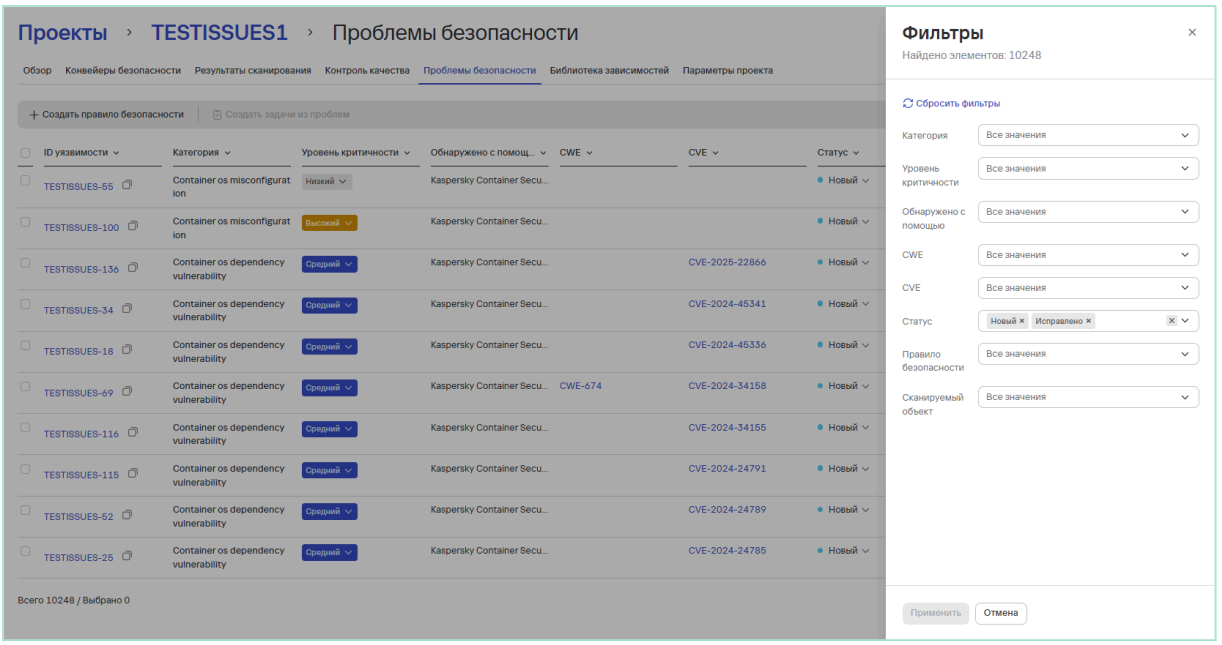

Рис. 53

- Возможность создания задач в трекере на основе выявленных проблем безопасности. Для создания задач необходимо выполнить следующие шаги:
    a. В разделе **Проекты** → *<Название проекта>* → **Проблемы безопасности** или в разделе **Проблемы безопасности** из главного меню слева выбрать уязвимости из списка с помощью чекбоксов ☐ (Рис. 54).

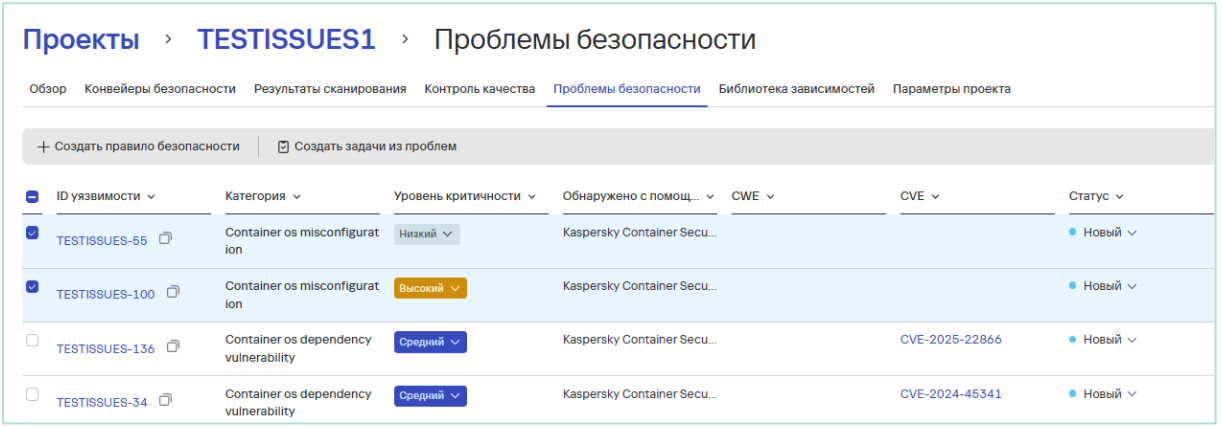

Рис. 54

    b. Далее нажать на кнопку **Создать задачи из проблем.**
    c. В открывшемся окне выбрать **Трекер задач** (*Инструкцию по созданию трекера см. Руководство администратора*) и заполнить поле **Название задачи** (Или **Префикс задач**, в зависимости от настроек трекера задач), и выбрать **Тип задачи** (Рис. 55).

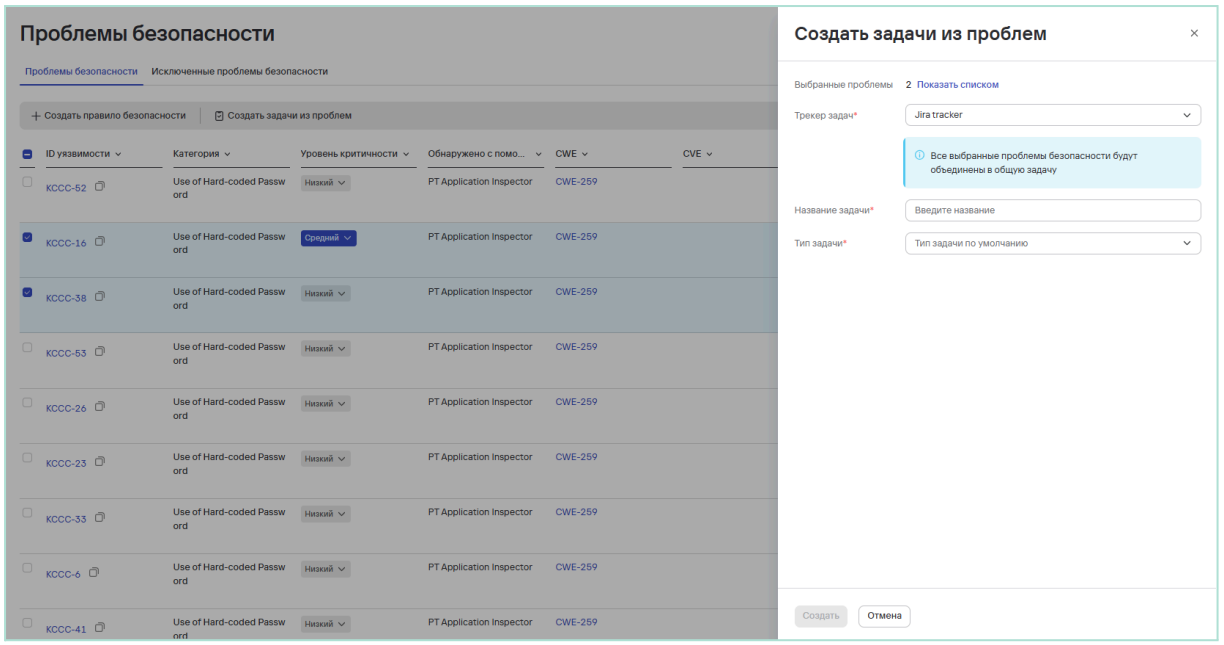

Рис. 55

d. Нажать на кнопку **Создать**.

4.7. Библиотека зависимостей

Раздел **Библиотека зависимостей** представляет информацию по зависимостям в проектах (Рис. 56).

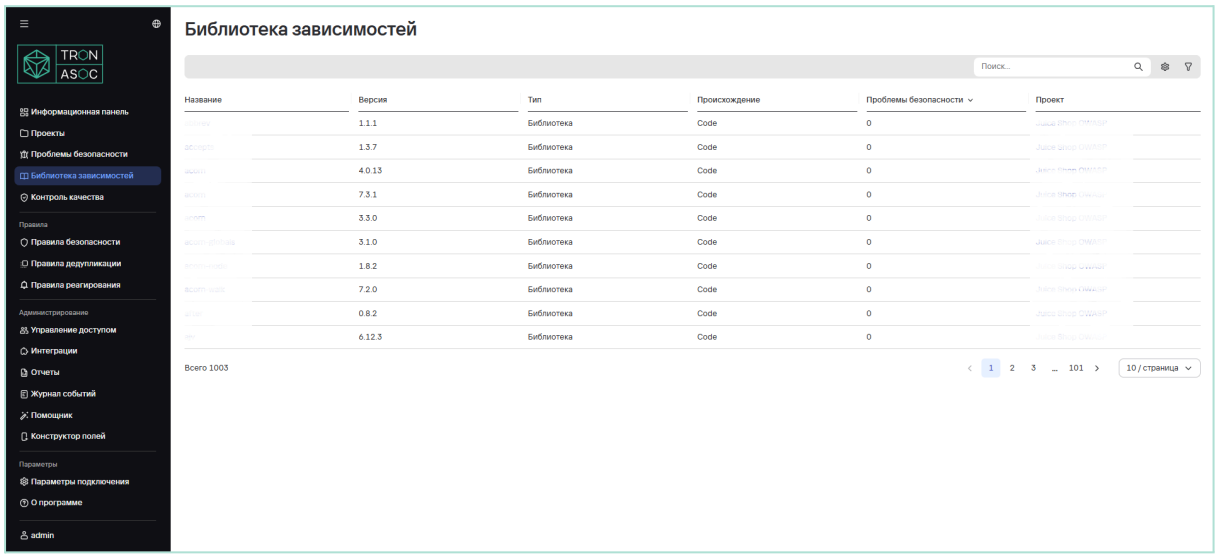

Рис. 56

Предусмотрена возможность просмотра детализированной информации по зависимостям (Рис. 57).

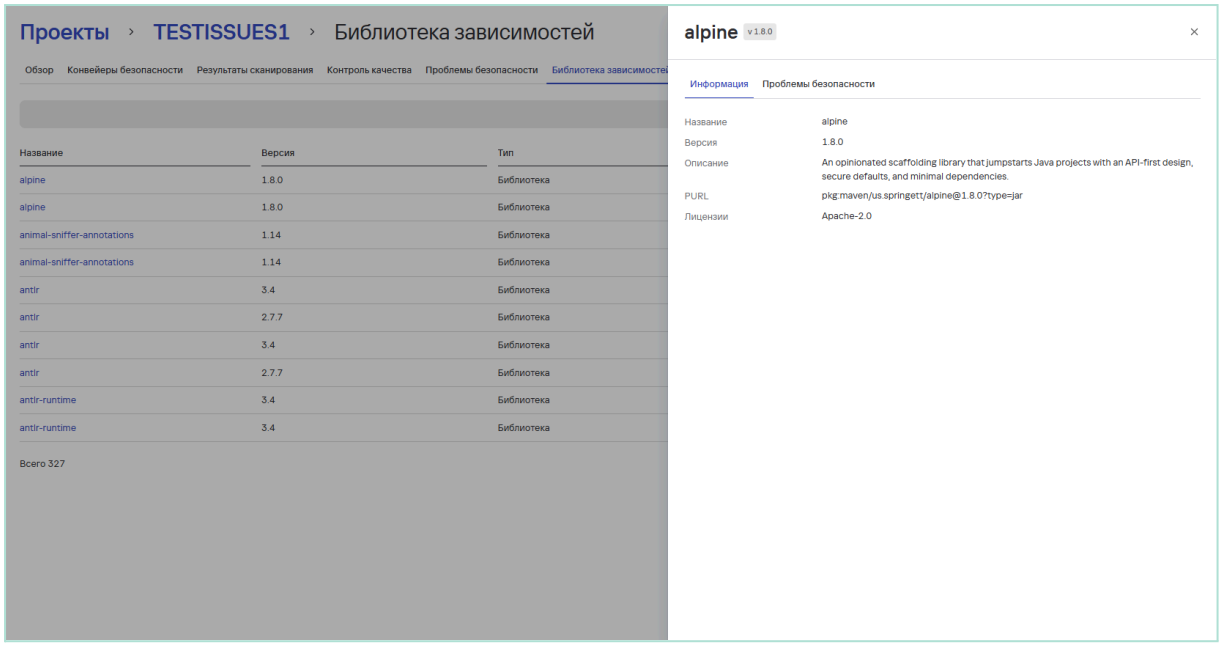

Рис. 57

4.8. Контроль 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.

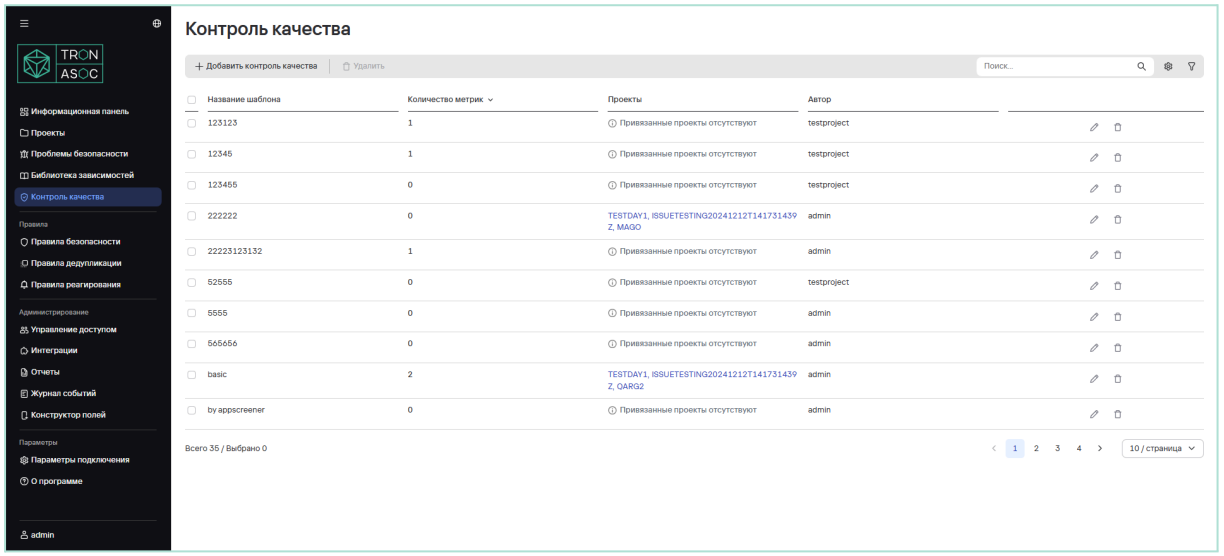

Рис. 58

Таблица шаблонов контролей качества (Рис. 58) содержит список шаблонов, которые уже созданы и используются в системе. Поля таблицы следующие:

- **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 доступна сортировка шаблонов по количеству метрик, названию или автору. Также возможно редактировать контроли качества. Для этого необходимо нажать на кнопку редактирования  и внести изменения в открывшейся форме (Рис. 59).

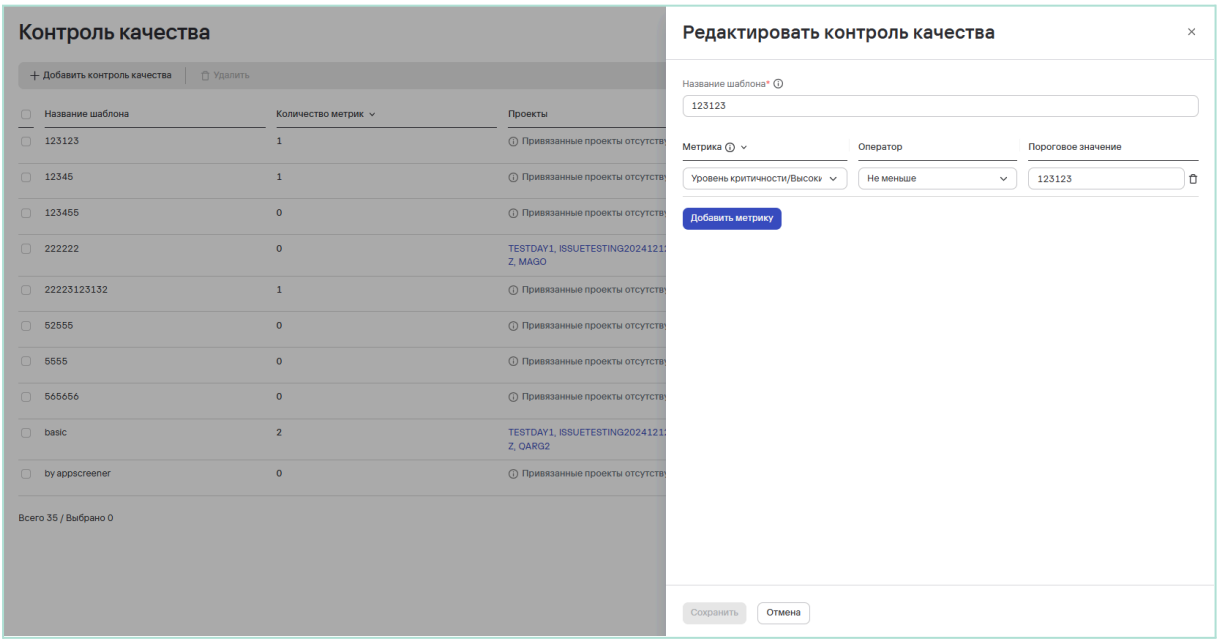

Рис. 59

4.8.1. Добавление нового контроля качества

Чтобы добавить новый шаблон контроля качества, необходимо нажать кнопку **Добавить контроль качества** и в открывшейся форме указать название шаблона (Рис. 60).

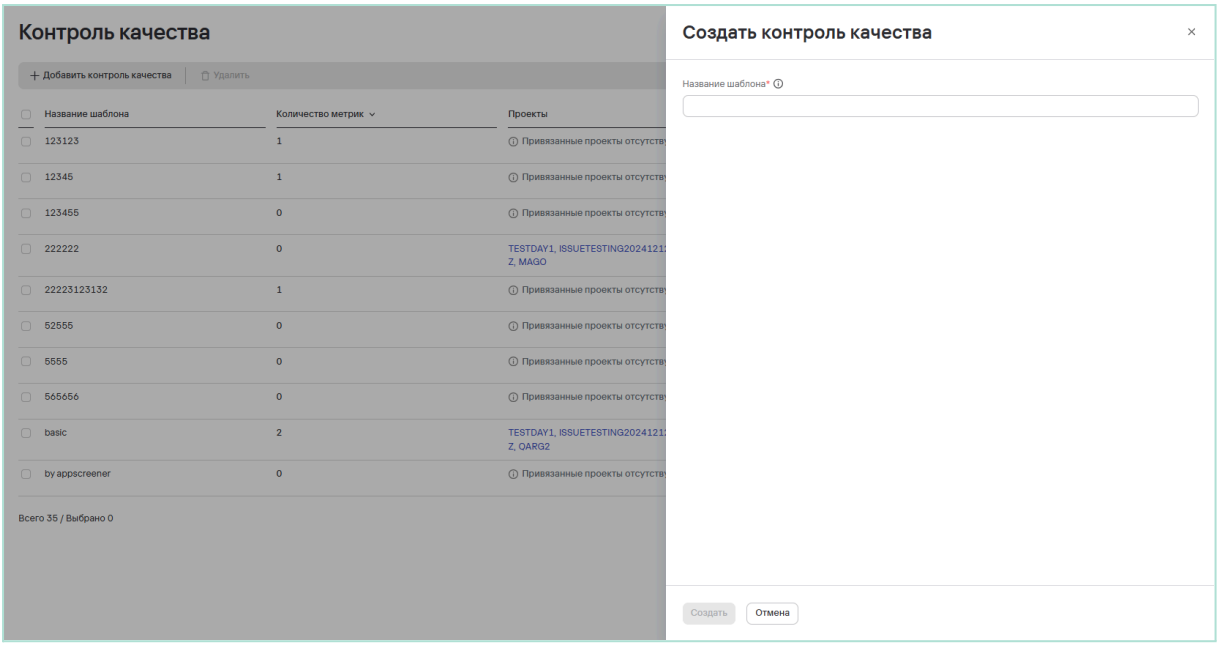

Рис. 60

Созданный шаблон необходимо отредактировать с помощью кнопки редактирования  , задать необходимые метрики для отслеживания качества и сохранить шаблон (Рис. 59).

Удаление шаблонов производится с помощью кнопки удаления  в списке шаблонов.

4.9. 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 (Рис. 61). 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).

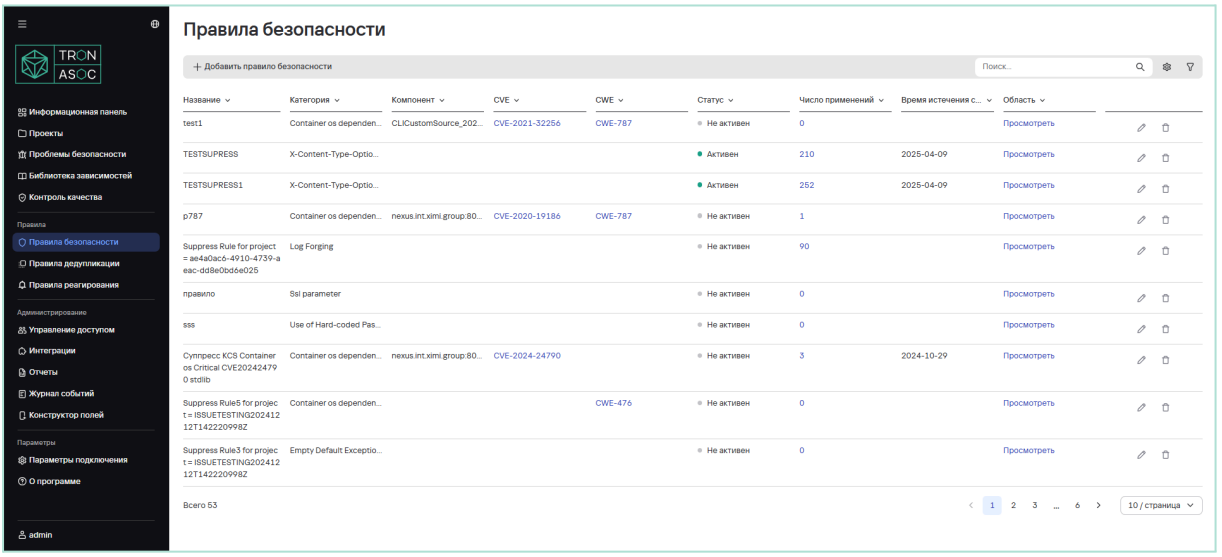

Рис. 61

Столбцы таблицы правил безопасности (Рис. 61):

- **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.
- **Статус** – статус активности правила.
- **Число применений** – количество проблем, к которым данное правило было применено.
- **Время истечения срока действия** – срок действия правила.
- **Область** – область проектов.

4.9.1. Создание правила безопасности

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 необходимо выполнить следующие шаги:

1. В разделе **Правила безопасности** нажать на кнопку **Добавить правило**.
2. В открывшейся форме (Рис. 62) ввести необходимые данные:
    a. Уникальное название для создаваемого правила безопасности.
    b. Тип проблемы безопасности
    c. Инструмент, использованный для обнаружения проблемы безопасности.
    d. Выбрать категорию проблемы безопасности.
    e. Компонент системы или путь, где была обнаружена проблема.
    f. Идентификатор уязвимости из базы данных CVE
    g. CWE для описания конкретного типа уязвимости.
    h. Путь к файлу или директории в репозитории, где была найдена проблема.
    i. Источник обнаружения
    j. Период, в течение которого правило безопасности будет активно. Это может быть фиксированная дата окончания действия правила, или оно может быть бессрочным.
    k. Статус проблемы безопасности
    l. Область применения (проекты)

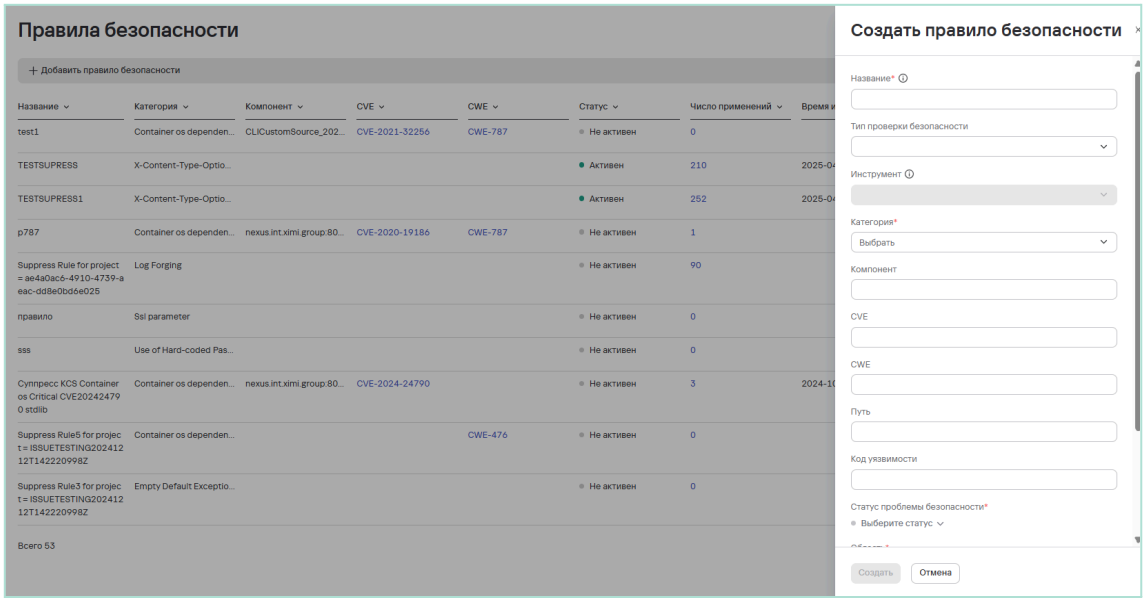

Рис. 62

3. После заполнения нажать на кнопку **Создать**.

4.10. Правила дедупликации

Правила дедупликации предназначены для работы над объединением и удалением дубликатов записей в системе путем настройки правил сравнения данных. Он позволяет автоматически находить и объединять повторяющиеся записи, снижая количество избыточной информации.

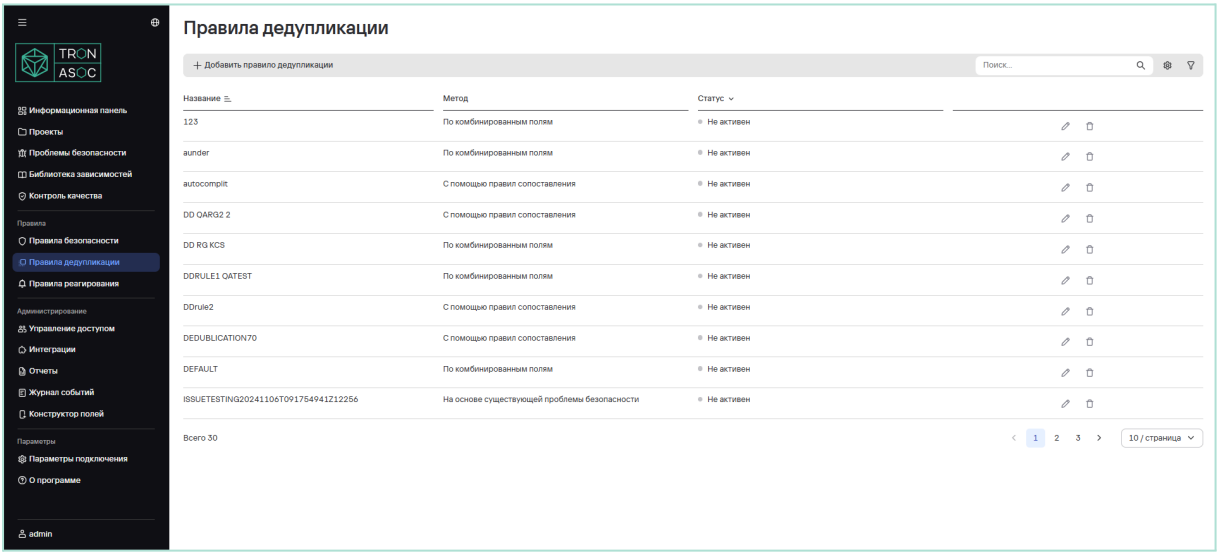

Рис. 63

Таблица (Рис. 63) содержит список существующих правил дедупликации с возможностью сортировки и просмотра подробной информации, содержит следующие параметры:

- **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.

4.10.1. Поиск дубликатов

Дубликаты возможно посмотреть в разделе **Проблемы безопасности**. Для этого необходимо выполнить следующие шаги:

1. Перейти в **Проекты** → *<Название проекта>* → **Проблемы безопасности**.
2. Найти и открыть проблему безопасности, к которой может относиться дедупликация.
3. В открывшемся окне выбрать вкладку **Дубликаты**.

В списке отобразятся записи, отмеченные как дубликаты, с их ID, названием правила и статусом.
Также возможно добавить дубликат вручную или отменить дедупликацию, используя соответствующие кнопки внизу страницы.

4.10.2. Создание правил дубликатов

Для создания нового правила необходимо выполнить следующие шаги:

1. В разделе **Правила дедупликации** нажать на кнопку **Добавить правило дедупликации**.
2. В открывшейся форме (Рис. 64) необходимо указать метод дедупликации, категорию полей для сопоставления и дополнительные параметры, зависящие от выбранного метода.

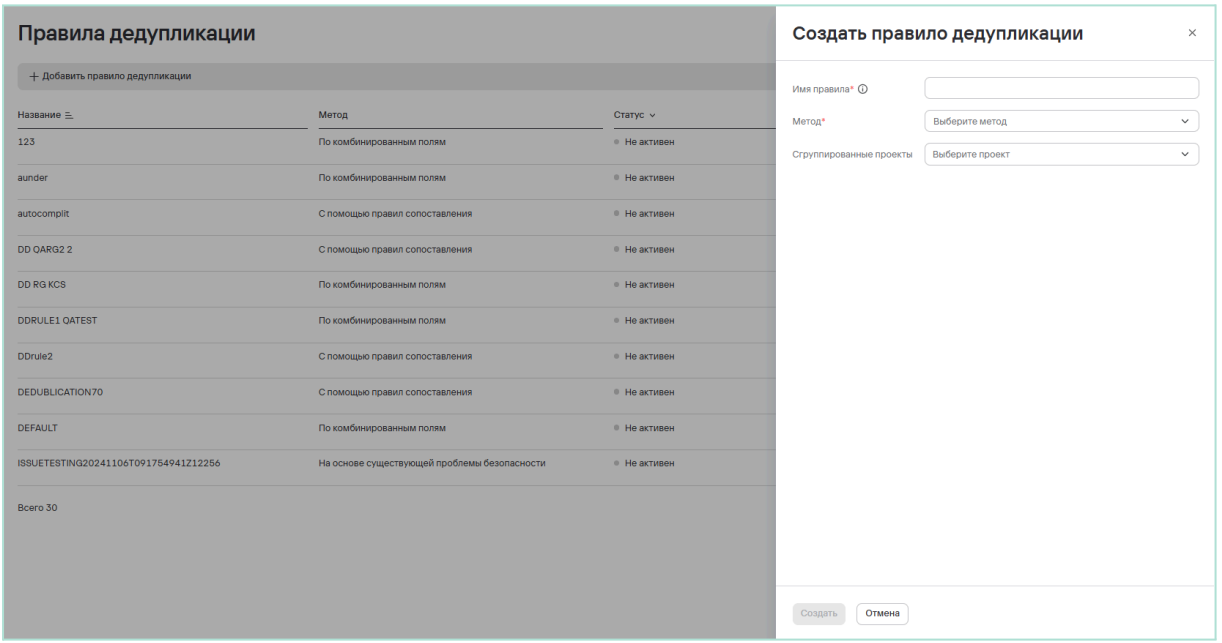

Рис. 64

3. Нажать на кнопку **Создать**.

4.11. Правила реагирования

Правила реагирования необходимы для настройки конкретных уведомлений и отправки их в соответствующие инструменты. В данном инструменте возможно автоматизировать отправку проблем безопасности в уже созданную интеграцию с трекером задач. Также возможно настроить автоматическую отправку событий на адрес электронной почты группе лиц.

4.11.1. Создание правила реагирования

Для создания правила реагирования, необходимо выполнить следующие шаги:

1. Перейти в раздел **Правила реагирования**.

2. Далее нажать на кнопку **Добавить правило реагирования** (Рис. 65).

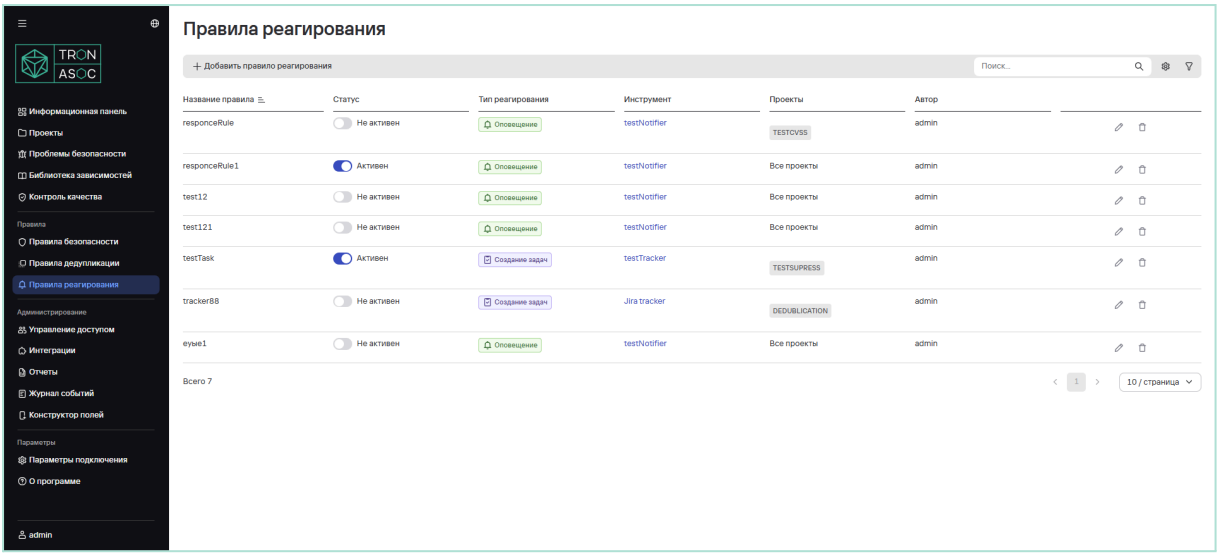

Рис. 65

3. Далее в открывшейся форме (Рис. 66) необходимо заполнить следующие поля:
    - **Имя проекта**
    - **Описание** (опционально)
    - **Проекты** – в рамках каких проектов будут собираться события или проблемы безопасности
    - **Тип реагирования** – выбор типа реагирования

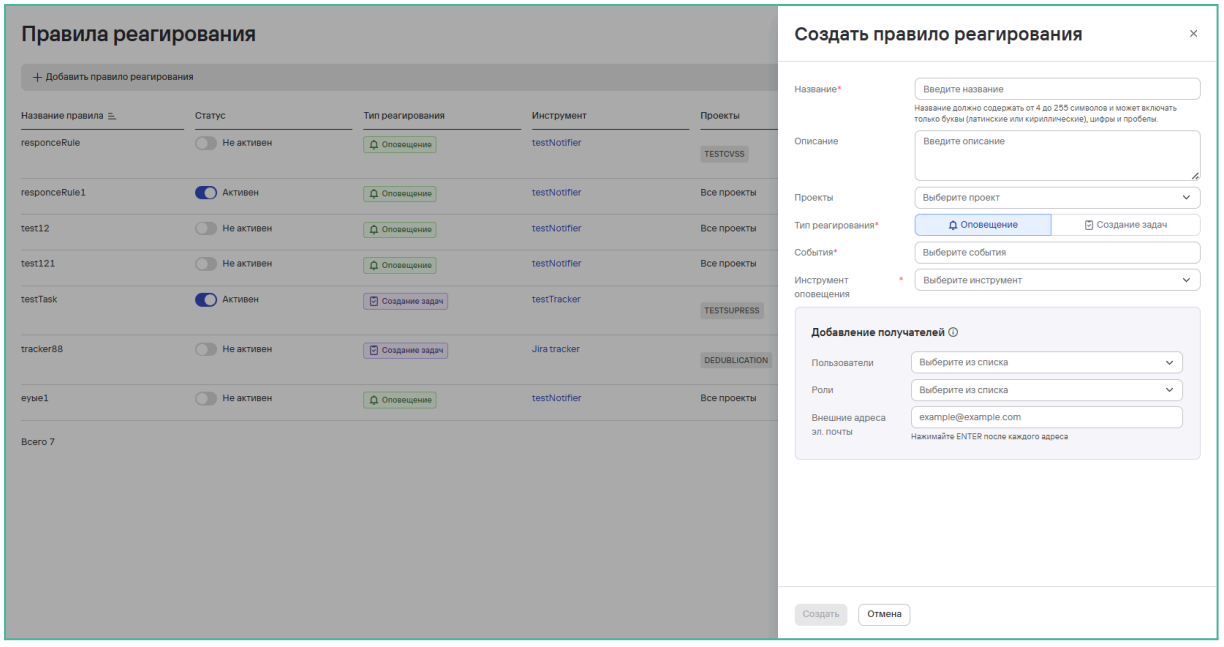

Рис. 66

- Если выбран тип **Оповещение** необходимо дополнить значениями следующих полей:

- **События** - множественный выбор из списка событий системы
- **Инструмент оповещения** - выбор из созданных интеграций Notify tool

Блок **Добавление получателей** заполняется при необходимости добавить больше получателей. Предусмотрено добавление конкретных пользователей (с помощью указанной почты в профиле), ролей (события будут отправляться пользователям с данной ролью). Также возможно добавить конкретные адреса электронной почты через в поле **Внешние адреса эл. почты** (Рис. 67).

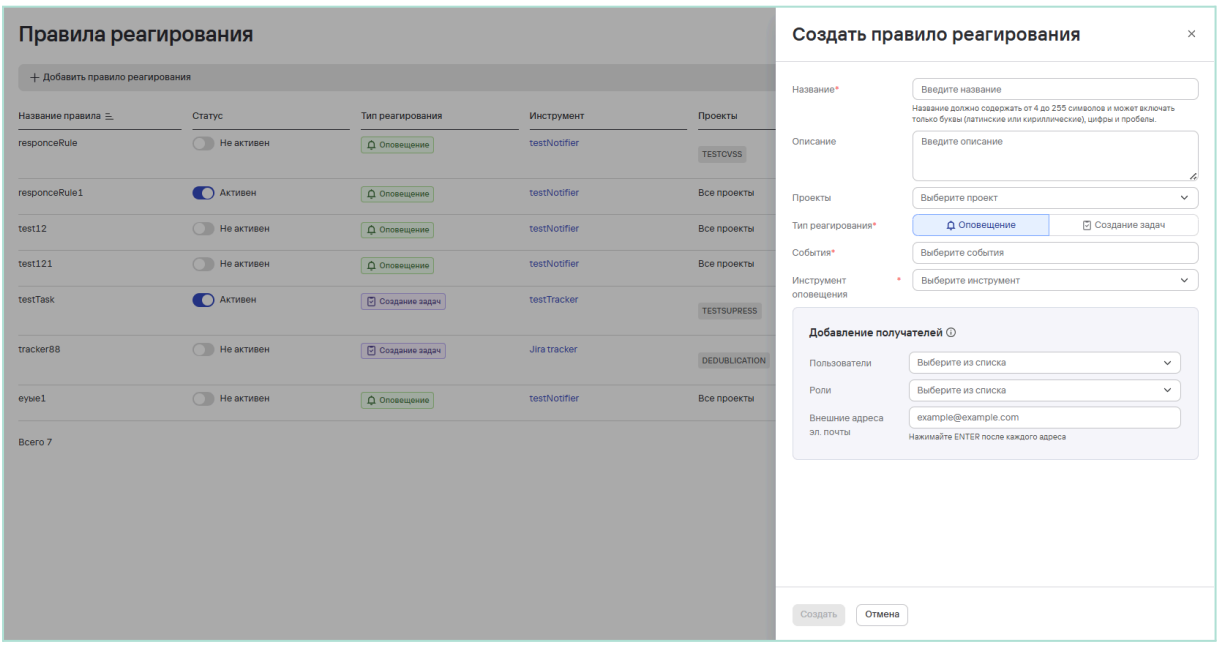

Рис. 67

- Если выбран тип **Создание задач** (Рис. 68) необходимо дополнить значениями следующих полей:
  - **Трекер задач** – выбор из созданных интеграций
  - **Фильтры** – условия фильтрации для проблем безопасности.

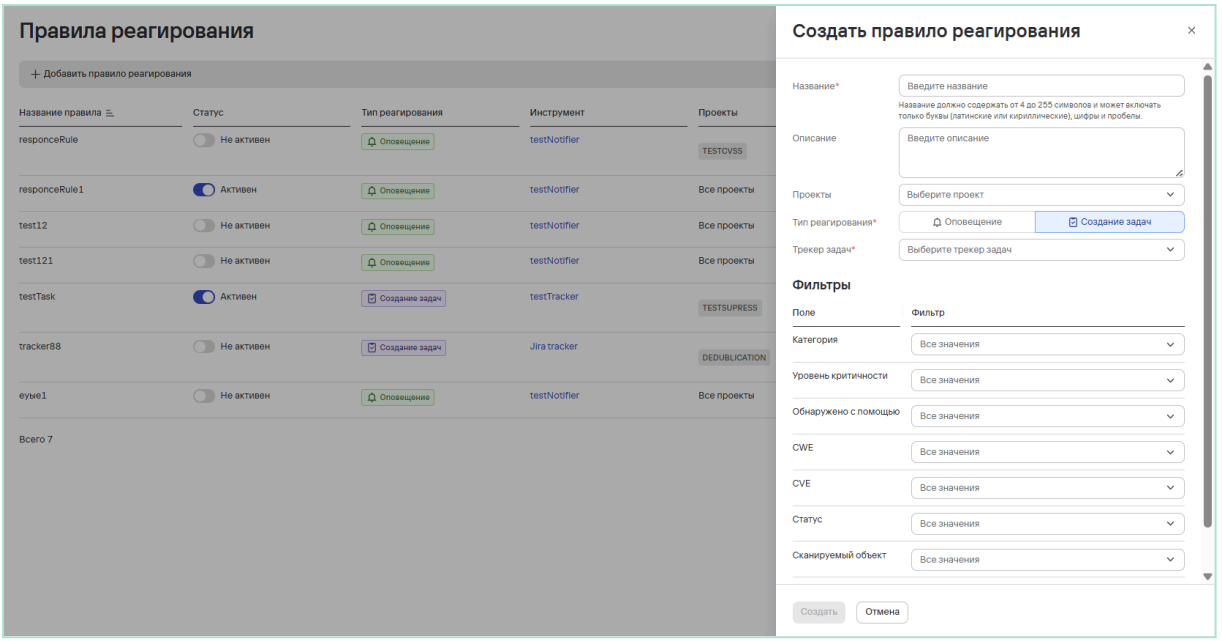

Рис. 68

Данный тип реагирования позволяет гибко настроить отправку необходимых проблем безопасности в область трекера задач.

После заполнения формы создания правил реагирования необходимо нажать на кнопку **Создать**.

5. Отчеты

Страница **Отчеты** предназначена для управления и просмотра отчетов, содержащих данные о проектах и найденных в них уязвимостях. Отчеты отображаются в таблицах **Сводные** и **Детализированные**, в которых можно увидеть основную информацию и дату создания.
Также доступна сортировка по названию, дате создания. Для этого необходимо щелкнуть на заголовок соответствующего столбца (**Название отчета** или **Создан**).
Для каждого отчета доступны три формата скачивания: **PDF** (до трех проектов в одном отчете), **JSON** и **CSV**. Для загрузки отчета необходимо нажать на соответствующую кнопку рядом с отчетом (Рис. 69).

Чтобы удалить отчет, необходимо нажать на кнопку  и в открывшемся окне нажать **Удалить**.

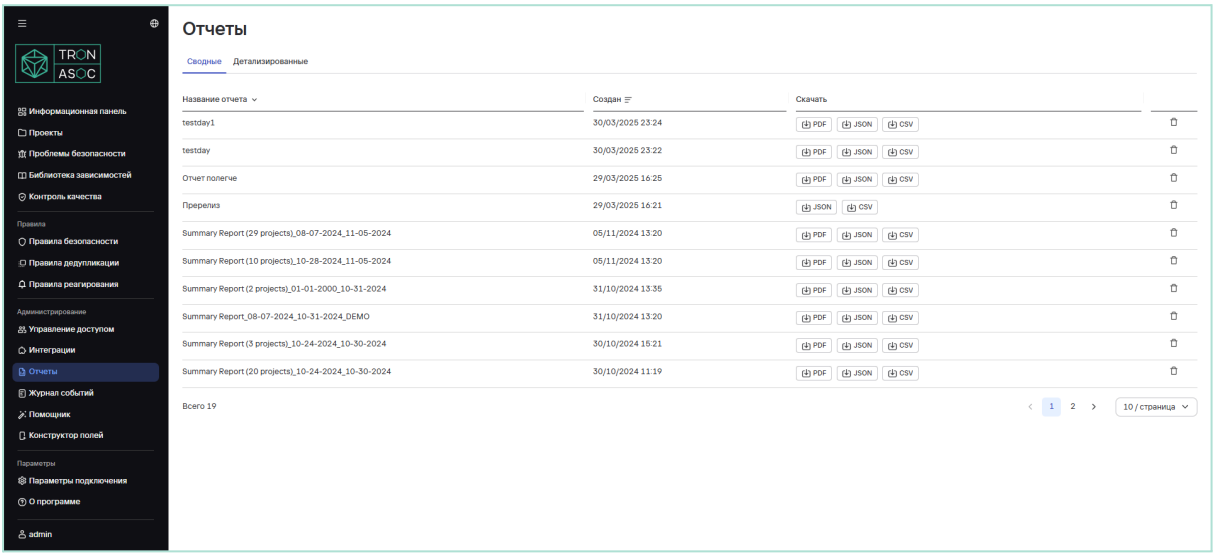

Рис. 69

6. Журнал событий

Раздел **Журнал событий** позволяет просматривать административные и функциональные события, которые совершают пользователи в системе, а также скачивать отчеты за выбранный период в формате CSV (Рис. 70). Для этого необходимо выполнить следующие шаги:

1. В разделе **Журнал событий** выбрать вкладку **Администрирование** или **Функциональные события**, в зависимости от требования.

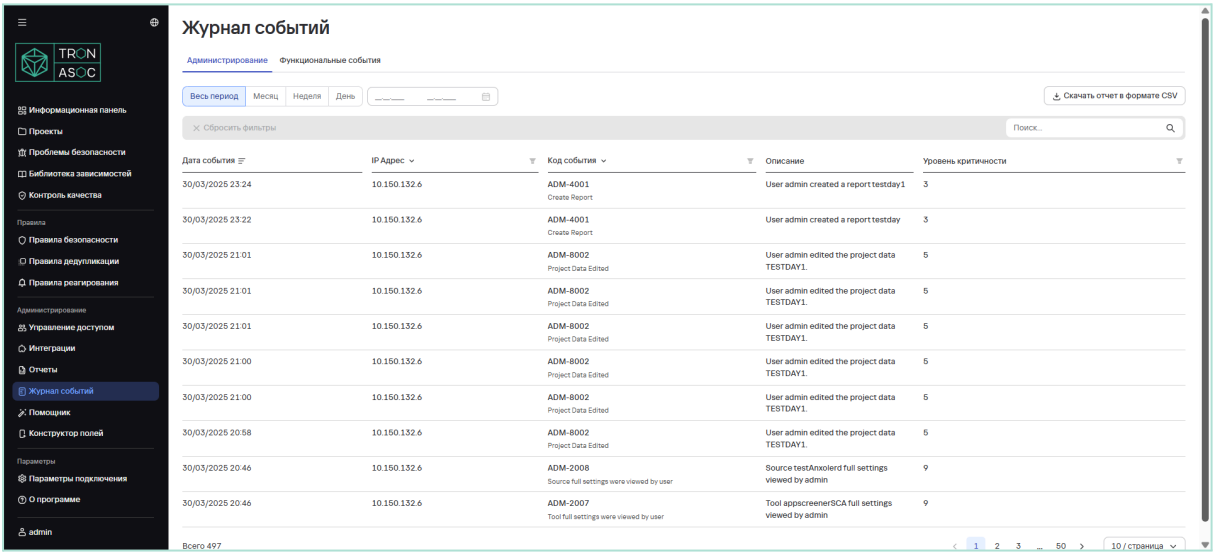

Рис. 70

2. Выберите необходимый период, за который требуется построить отчет.
3. Нажмите кнопку **Скачать отчет в формате CSV**. После этого отчет автоматически загрузится локально на ПК.

7. Конструктор полей

Раздел **Конструктор полей** позволяет настроить пользовательские поля проектов (Рис. 71).

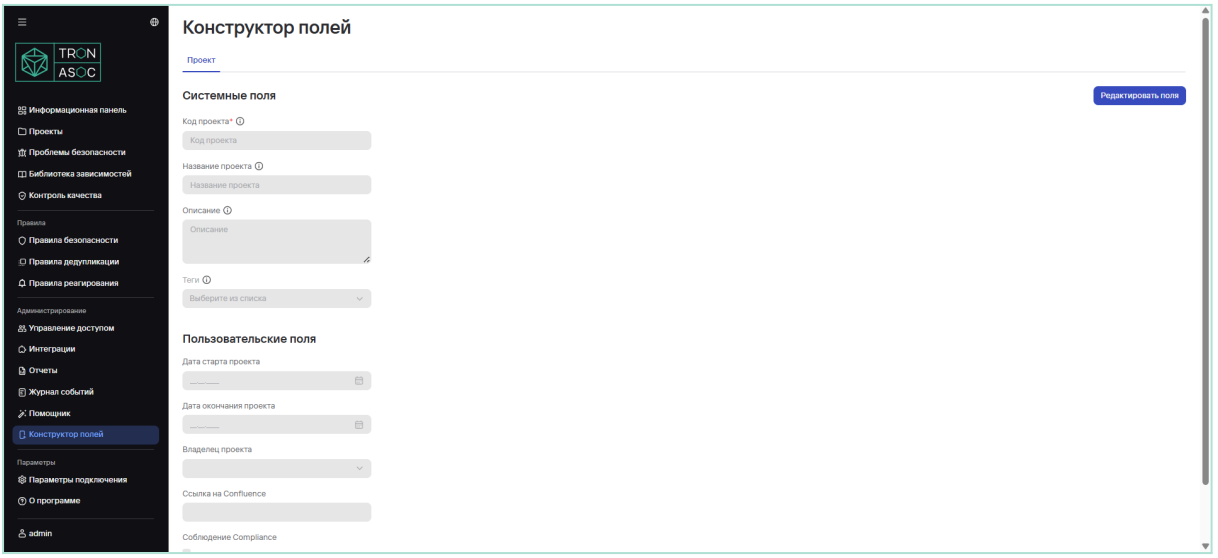

Рис. 71

Для настройки необходимо выполнить следующие шаги:

1. На странице **Конструктор полей** нажать кнопку **Редактировать поля**.
2. В открывшемся окне справа (Рис. 72) скорректировать (добавить/удалить) представленный набор полей с помощью кнопок **Добавить поле** и  .

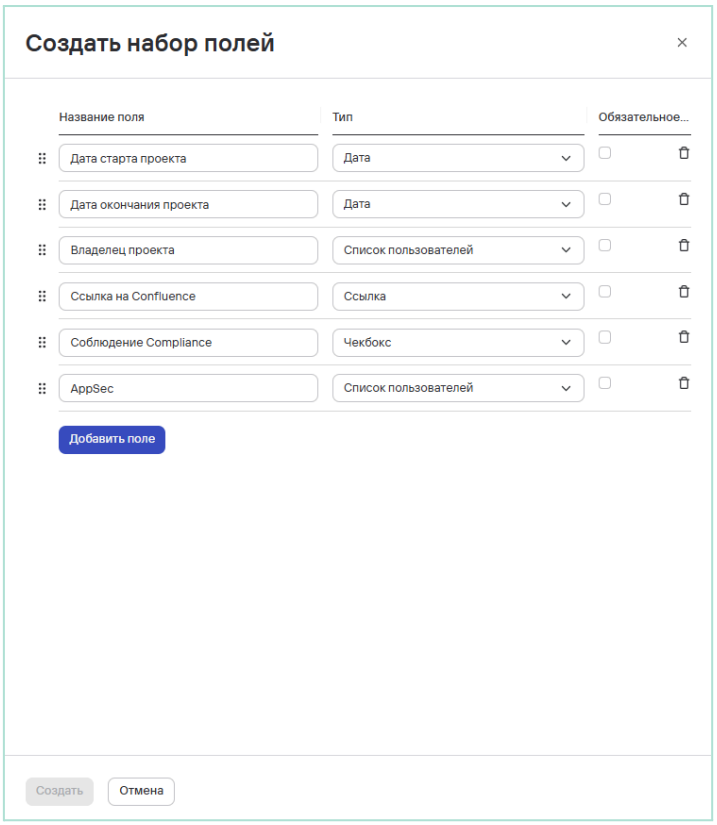

Рис. 72

3. Заполнить поля **Название поля**, **Тип** и **Обязательное поле**.
4. Далее нажать кнопку **Создать**.

8. Требования к аппаратным и программным характеристикам рабочего места пользователя

Характеристика	Минимальное значение	Рекомендуемое значение
Процессор	4 ядра	8 ядер и более
Оперативная память	16 ГБ	32 ГБ и более
Жесткий диск	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	Chromium (Google Chrome, Edge, Safari и т. д.) и Firefox.	