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

Руководство администратора

Апрель 2025

Содержание

Введение

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

В роли администраторов могут быть разработчики, администраторы, специалисты, отвечающие за развертывание и сопровождение инфраструктуры и системного программного обеспечения (операционные системы, сервера приложений, базы данных и т.п.), необходимых для непрерывной работы системы, а также отвечающих за создание и управление учетными записями, ролями и доступами пользователей, внесение изменений в настройки, контроль лицензии, подключение инструментов безопасности и источников сканирования.

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 - это 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 - это 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 - это 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 - это 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 - это 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	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	Обмен данными между системами с возможной последующей обработкой
AD (Active Directory)	Службы каталогов - это 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

Платформа «TRON.ASOC» осуществляет комплексный контроль информационной безопасности разрабатываемых проектов, обеспечивая надежную защиту на всех этапах разработки:

- 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. 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.	

4. Установка решения

4.1. Установка с помощью Docker Compose

Решение поставляется в виде образов контейнеров. Для установки необходимо выполнить следующие шаги:

1. Установить компоненты. Для этого необходимо:
    a. Скачать архив ***docker-compose-v1.2.zip.***
    b. Задать значение для переменной `ASOC_DOMAIN`, которая содержит зарезервированное доменное имя для графического интерфейса ASOC. В случае пилотного проекта, необходимо на DNS-сервере добавить A-запись для хоста, где запускается docker-compose.
    c. Далее для корректной локальной работы необходимо исправить/добавить в `/etc/hosts` следующую строку (значение из переменной `ASOC_DOMAIN`):

```
127.0.0.1 localhost asoc.testdomain.ximi
```

    d. Проверить актуальность значений переменных: `ASOC_IMG_FRONT`, `ASOC_IMG_CORE` в соответствии с нужной версией сборки.
    e. Запустить скрипт `show.sh`, который выведет значения переменных из файла ***docker-compose.yaml*** для проверки:

```
./show.sh
```

    f. Выполнить вход в реестр, позволяющий получить доступ к образам контейнеров ASOC (с помощью username от учетной записи harbor):

```
docker login harbor.tronsec.ru
```

    g. Далее выполнить следующую команду:

```
docker-compose up -d
```

    h. Проверить статус контейнеров:

```
docker ps
```

> ❕ *Корректный статус в данном случае* - Running *или* Up About a minute.

2. Проверить в любом браузере загрузку web-интерфейса решения по ip-адресу *http:///<ASOC_DOMAIN>* (например, *http://asoc.testdomain.ximi* или *http://localhost*), и выполнить вход в систему по инструкции ниже Авторизация администратора.

4.2. Установка с помощью Helm Chart

Чтобы установить решение с помощью **Helm Chart**, необходимо выполнить следующие шаги:

1. Обеспечить наличие следующих компонентов и доступов:
    - Доступ к реестру *harbor.tronsec.ru*
    - Установленные утилиты **kubectl** и **helm**
    - Доступ к **kubeconfig** для целевого кластера с правами к namespace для ASOC
2. Подготовить Helm Chart. Для этого необходимо подключить Helm-репозиторий производителя, где находится пакет Helm Chart, а именно, выполнить следующие команды:

```
export CHART_URL=xxxxxx
export CHART_USERNAME=xxxxxx
export CHART_PASSWORD=xxxxxx
export VERSION=xxxxxx
helm repo add asoc \
https://$CHART_URL/repository/public-charts/ \
--username $CHART_USERNAME \
--password $CHART_PASSWORD
helm repo update
helm pull asoc/asoc --version $VERSION
tar xvf asoc-$VERSION.tgz
```

> ❕ Значения `CHART_URL`, `CHART_USERNAME`, `CHART_PASSWORD`, `VERSION` предоставляются производителем.

3. Подготовить ***values-config.yaml***. Для этого необходимо создать и заполнить файл с параметрами установки (***asoc/values.yaml***), в которых указать следующие значения:

```
default.domain="example.com"
default.networkPolicies.ingressControllerNamespaces="ingress-nginx"
```

4. Далее выполнить установку чарта:

```
cd asoc/
helm upgrade --install asoc-release \
--namespace asoc \
--create-namespace \
--values values.yaml \
```

5. Обновление решения

При выходе новой версии решения, рекомендуется выполнить обновление. Для успешного обновления необходимо выполнить установку, используя данные новых образов и чартов (подробнее см. Установка решения).

6. Удаление решения

В случае удаления решения с помощью Docker Compose, необходимо выполнить следующие шаги:

1. Запустить папку установленного ранее архива ***docker-compose-v1.2.zip.***
2. Остановить контейнеры ASOC из манифеста ***docker-compose.yaml***:

```
docker-compose down
```

3. При необходимости удалить данные БД:

```
docker-compose down --volumes
```

Для удаления через Helm Chart необходимо выполнить следующее:

```
helm uninstall <RELEASE_NAME> -n <namespace>
```

❕ При удалении через Helm Chart сохраняется secret poll-secret и pv.

7. Авторизация администратора

Для успешной авторизации необходимо выполнить следующие шаги:

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

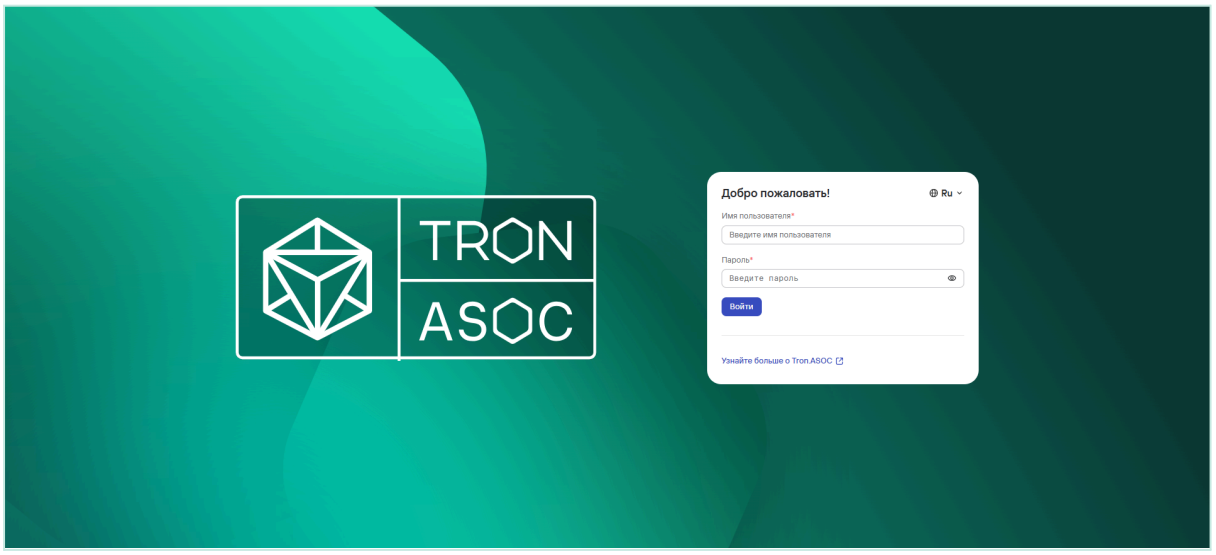

Рис. 1

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 администратора**.**

❕ При первом входе в систему необходимо использовать следующие данные учетной записи администратора:

- **Имя пользователя** - admin
- **Пароль** - admin

Также необходимо ознакомиться и принять **Согласие с EULA** (Рис. 2).

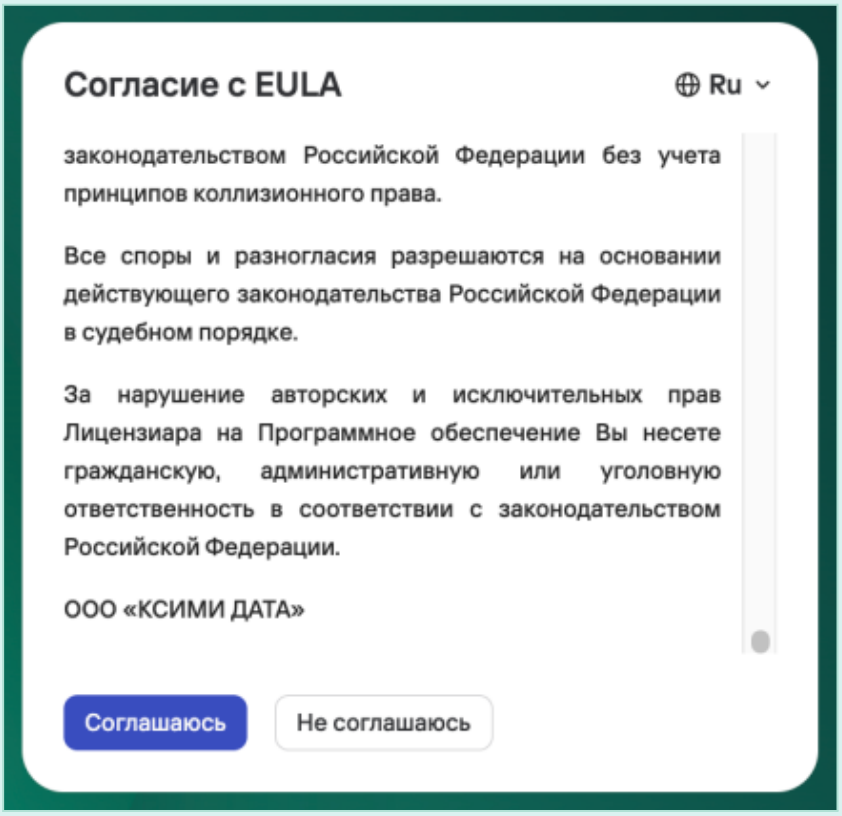

Рис. 2

Далее потребуется изменить пароль к данной учетной записи, следуя указанным требованиям к новому паролю (Рис. 3) и нажать кнопку **Изменить**.

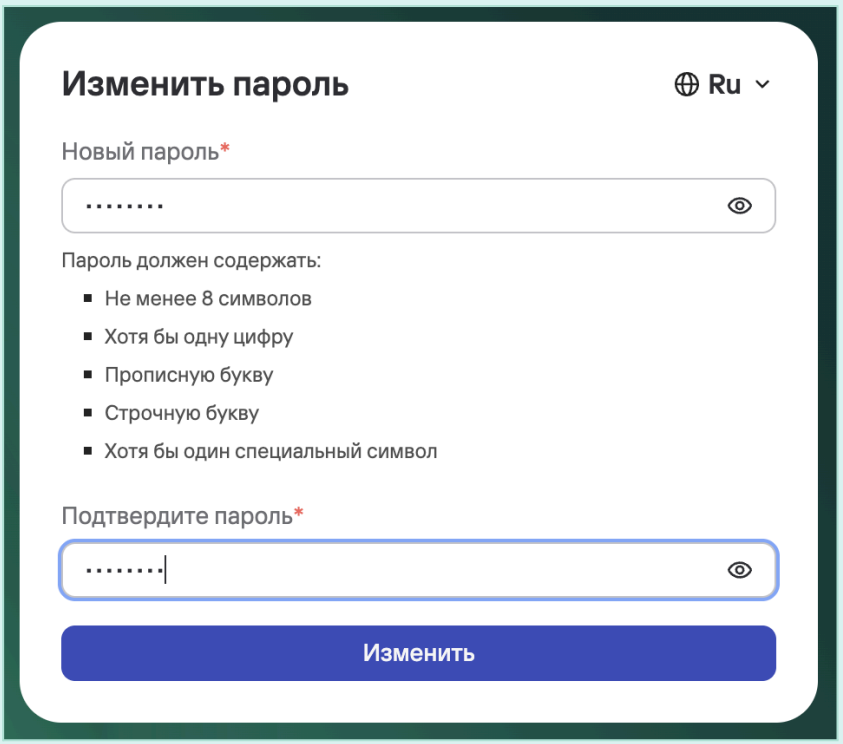

Рис. 3

4. Нажать **Войти**.

   При успешной авторизации откроется **Информационная панель** (Рис. 4).

> ❗ *При возникновении проблем с первым входом в систему, необходимо обратиться в техподдержку TRON.ASOC.*

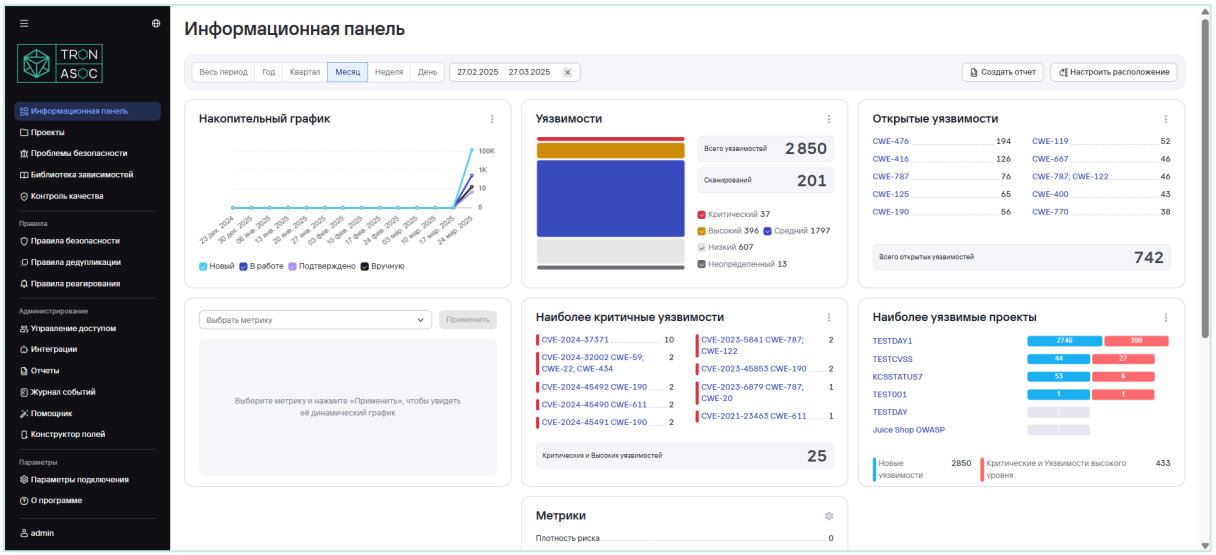

Рис. 4

8. 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
  - Управление доступом
  - Интеграции
  - Отчеты
  - Журнал событий
  - Помощник

    ❕ Раздел **Помощник** будет доступен в следующих релизах.
  - Конструктор полей
  - Параметры подключения
  - О программе - общая информация о системе
  - Учетная запись - данные профиля учетной записи
- Рабочая область. Информация и элементы управления в рабочей области зависят от выбранного раздела или подраздела.

8.1. Информационная панель

Информационная панель представлена в виде сводных графиков (виджетов) по уязвимостям за установленный период (Рис. 4). Данные виджеты можно настроить по усмотрению, с помощью кнопки **Настроить расположение**. Доступны следующие настройки виджетов:

1. Добавление новых виджетов с помощью кнопки **Добавить виджет.**
2. Перемещение виджетов в рамках рабочей области с помощью кнопки  на каждом из виджетов.
3. Удаление виджетов с помощью кнопки  на каждом из виджетов.

Подробнее о разделе, см. Руководство пользователя.

8.2. Проекты

Раздел **Проекты** включает список созданных проектов, которые проверяются на соответствие политикам безопасности компании и качеству (Рис. 5). 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.

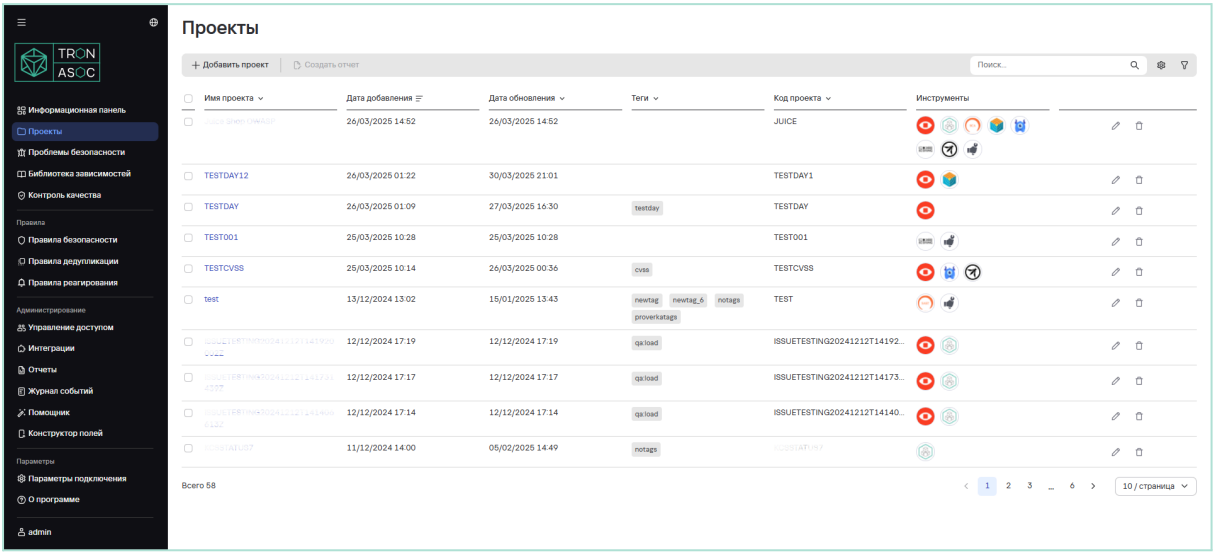

Рис. 5

Подробнее о разделе, см. Руководство пользователя.

8.3. Проблемы безопасности

Раздел **Проблемы безопасности** состоит из подразделов **Проблемы безопасности** и **Исключенные проблемы безопасности**. Данный раздел демонстрирует все найденные уязвимости и основную информацию по ним (Рис. 6).

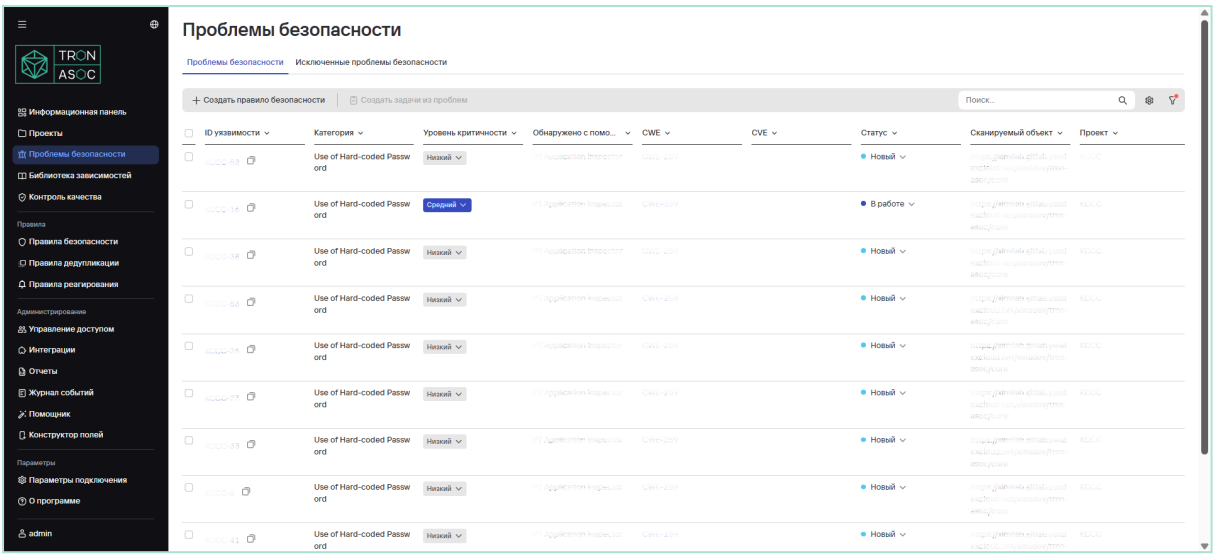

Рис. 6

Подробнее о разделе, см. Руководство пользователя.

8.4. Библиотека зависимостей

Раздел **Библиотека зависимостей** представляет информацию по зависимостям в проектах (Рис. 7).

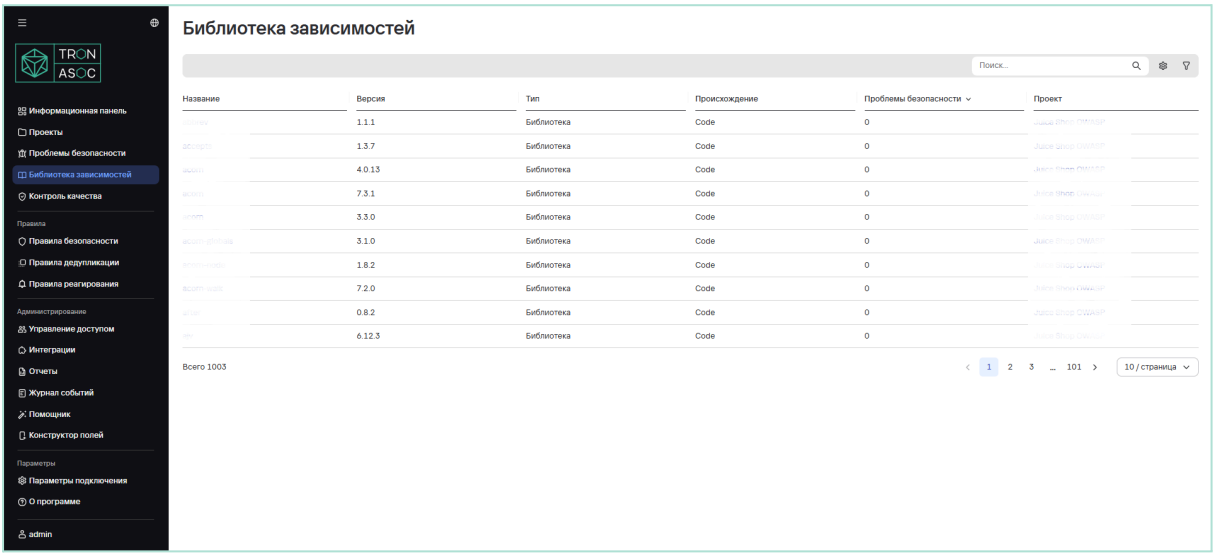

Рис. 7

Подробнее о разделе, см. Руководство пользователя.

8.5. Контроль качества

Раздел **Контроль качества** содержит список шаблонов контроля качества (Рис. 8) с возможностью добавления новых, удаления и редактирования существующих шаблонов в зависимости от потребностей безопасности.

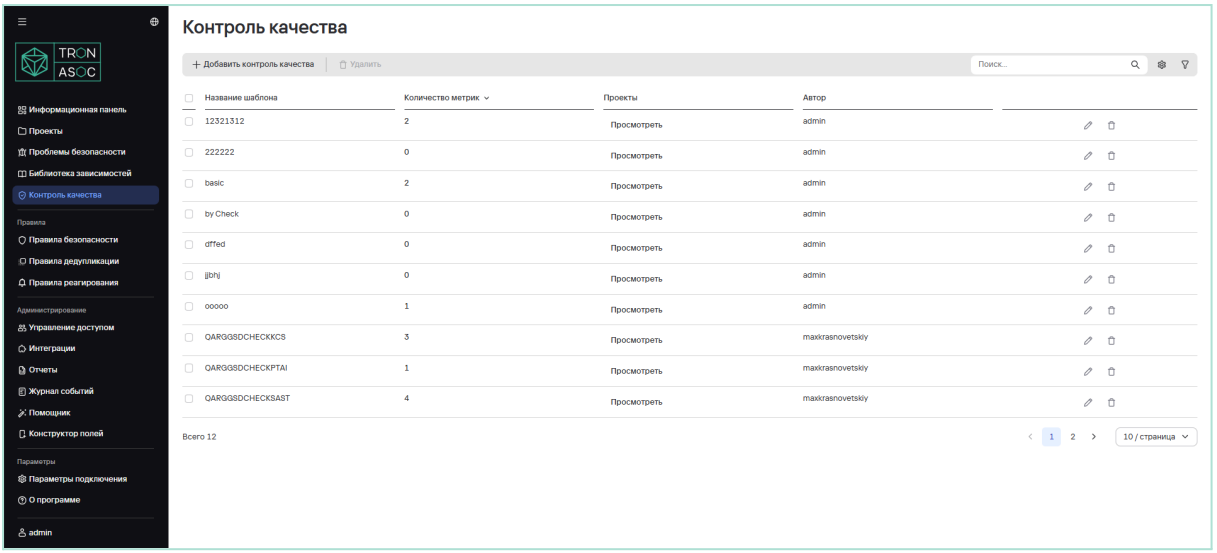

Рис. 8

Подробнее о разделе, см. Руководство пользователя.

8.6. Правила безопасности

Раздел **Правила безопасности** состоит из набора правил, с помощью которых производятся проверки безопасности (Рис. 9). Данные правила можно настраивать исходя из потребностей безопасности.

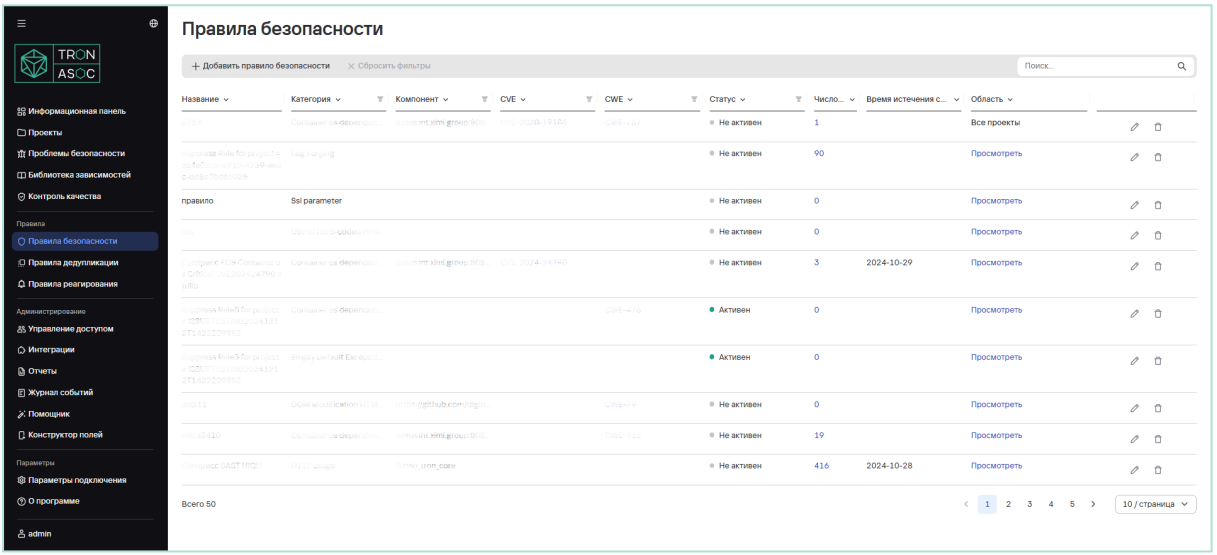

Рис. 9

Подробнее о разделе, см. Руководство пользователя.

8.7. Правила дедупликации

Раздел **Правила дедупликации** содержит информацию о правилах, методах дедупликации (Рис. 10).

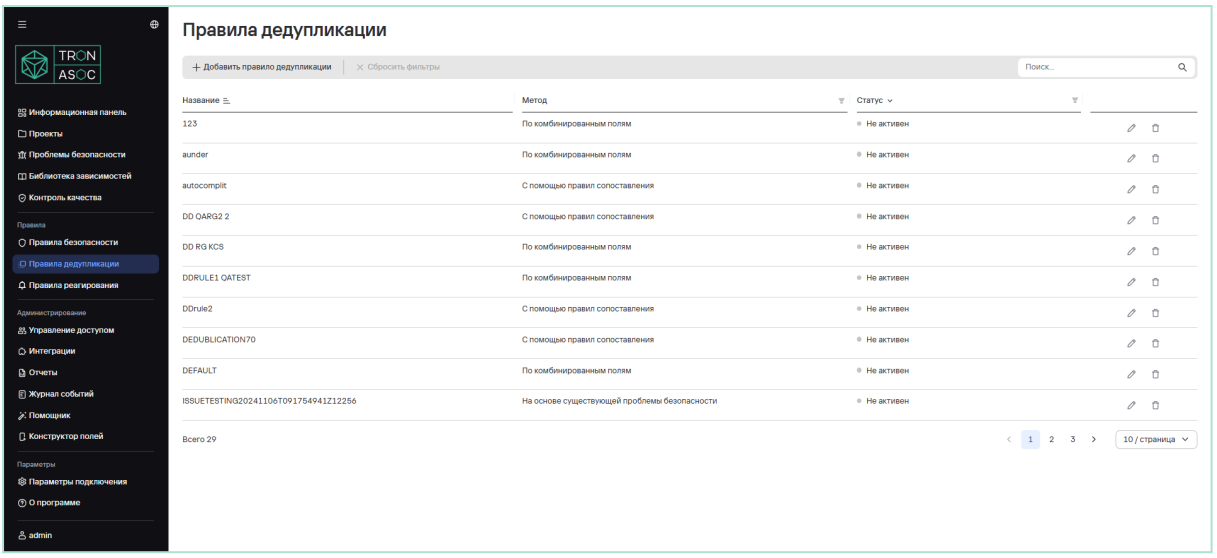

Рис. 10

Подробнее о разделе, см. Руководство пользователя.

8.8. Правила реагирования

Раздел **Правила реагирования** содержит список правил реагирования на появление уязвимостей в системах и приложениях в рамках существующих проектов (Рис. 11).

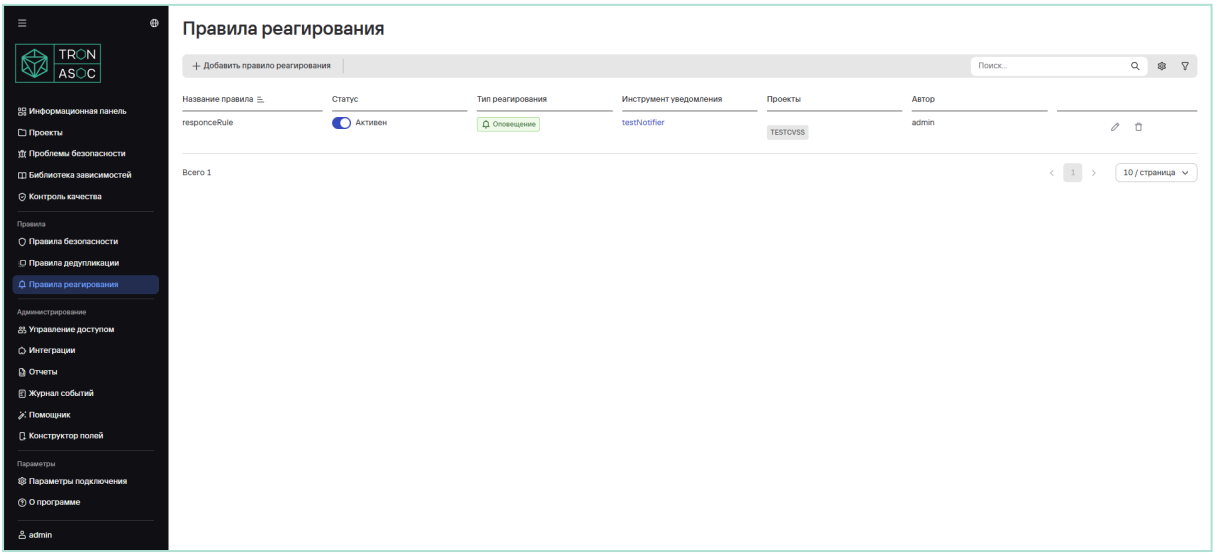

Рис. 11

Подробнее о разделе, см. Руководство пользователя.

9. Настройки системы

9.1. Настройки кастомизации

Здесь примечание для удаления статуса
При удалении статуса система сначала проверяет наличие связанных инцидентов (issues) с данным статусом. Если такие записи найдены, пользователю предлагается выбрать новый статус для переноса этих инцидентов. После переноса статусов выполняется удаление самого статуса. Обратите внимание: операция выполняется асинхронно, и время выполнения зависит от количества затрагиваемых записей. Рекомендация: Если удаляемый статус используется в большом количестве записей, рекомендуем выполнять удаление в конце рабочего дня или вне активной работы с конфигуратором. Пока все связанные issues не будут обновлены, статус останется видимым в интерфейсе. Это может привести к ошибочным действиям, например: добавлению удаляемого статуса в новые или существующие переходы,, созданию неконсистентных конфигураций., Для предотвращения таких ситуаций рекомендуем дождаться завершения операции перед внесением других изменений в конфигурацию статусов и переходов.

9.2. Настройки правил авторизации пользователей

На вкладке **Параметры подключения** (Рис.12) предусмотрены следующие возможности:

- настройка параметров требований к паролю,
- максимальная продолжительность сеанса,
- время выхода из системы после периода неактивности,
- количество попыток ввода пароля до временной блокировки,
- длительность временной блокировки.

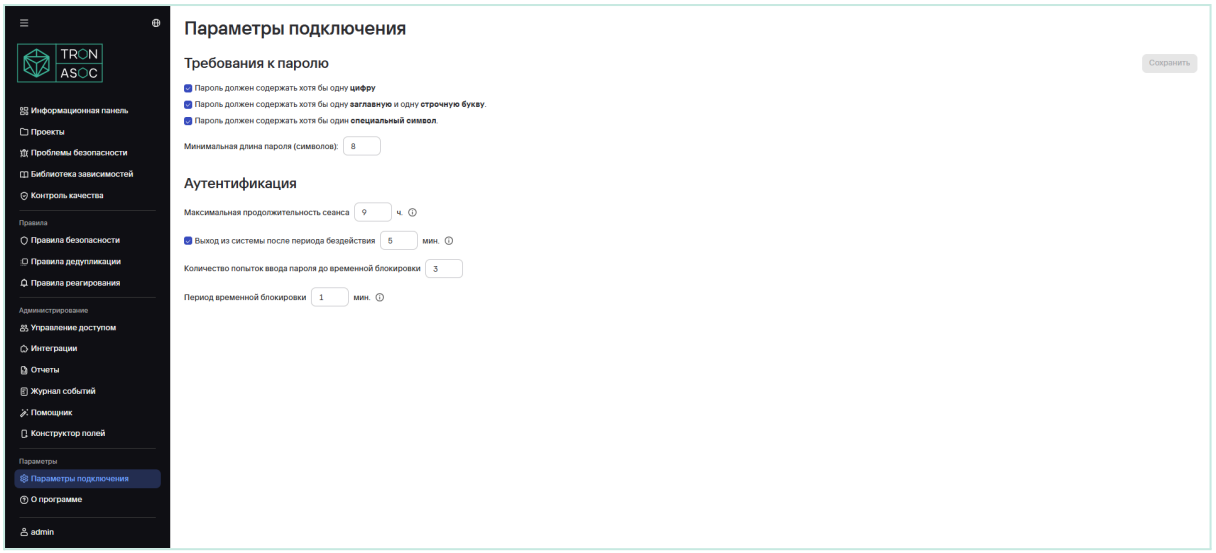

Рис. 12

Для настройки параметров подключения администратору необходимо выбрать нужные требования и нажать на кнопку **Сохранить**. После чего все пользователи принудительно должны изменить пароль при следующей авторизации в системе.

9.3. Управление пользователями и ролями

Раздел **Управление доступом** позволяет администраторам управлять пользователями и их ролями в системе (Рис. 13). Данный раздел включает четыре ключевых подраздела:

- **Пользователи**
- **Роли**
- **Группы**
- **LDAP**

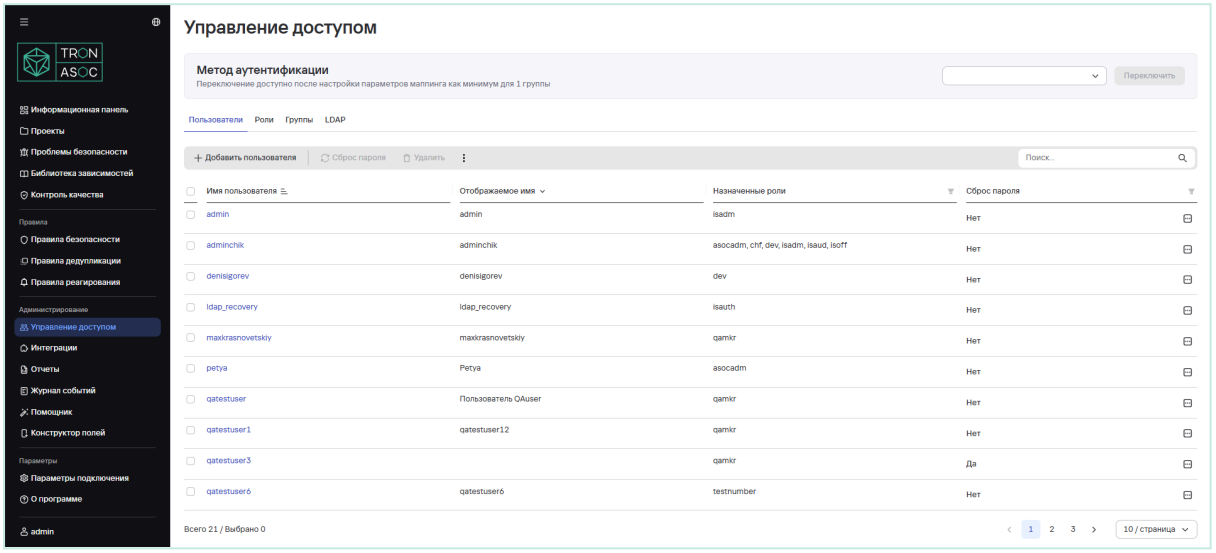

Рис. 13

Подраздел **Пользователи** предоставляет список со следующей информацией о пользователях:

- **Имя пользователя** — уникальный логин или идентификатор пользователя.
- **Отображаемое имя** — имя, которое видят другие пользователи.
- **Назначенные роли** — перечень ролей, которые присвоены пользователю. Роли определяют права доступа пользователя к различным функциям системы.
- **Сброс пароля** — индикатор того, требуется ли пользователю сброс пароля. Значение ***Да*** означает, что пользователь должен изменить свой пароль при следующем входе в систему.

9.3.1. Добавление нового пользователя

Для добавления нового пользователя, необходимо выполнить следующие шаги:

1. В разделе **Управление доступом** нажать на кнопку **Добавить пользователя.**
2. В открывшемся окне **Создать пользователя** (Рис. 14) заполнить поля **Имя пользователя**, его **Отображаемое имя** (не обязательно), **Электронная почта**.

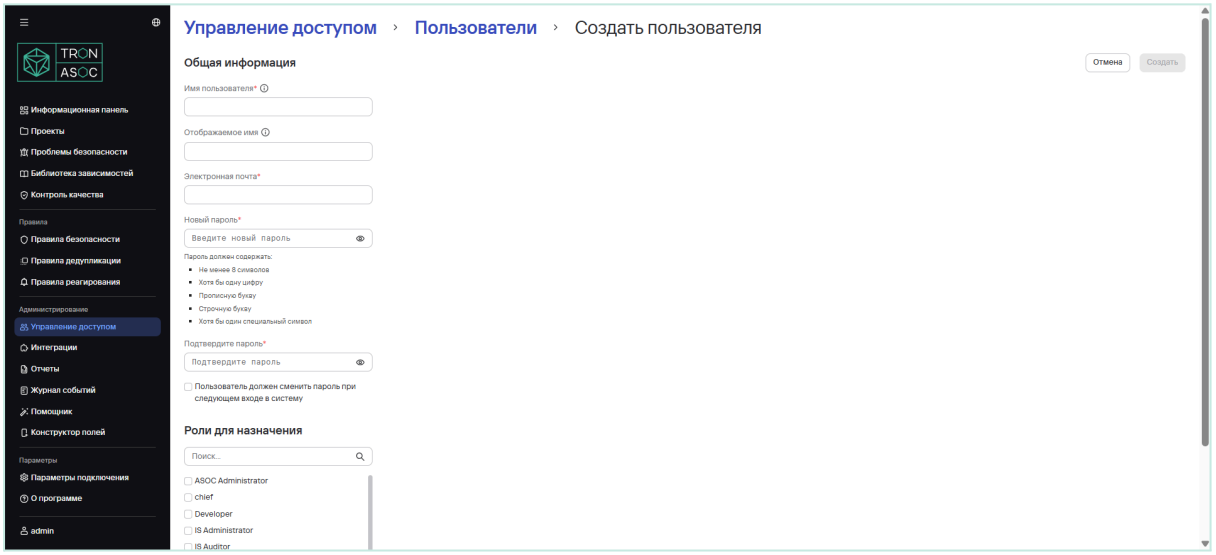

Рис. 14

3. Ввести пароль, соответствующий правилам авторизации, в поле **Новый пароль** и подтвердить его в поле **Повторите пароль**.
4. Далее при необходимости назначить пользователю одну или несколько ролей, которые определят его права доступа, с помощью поиска в блоке **Роли для назначения** (подробнее см. Настройка ролей).
5. Также при необходимости включить опцию сброса пароля.
6. Далее нажать на кнопку **Создать**.

9.3.2. Редактирование пользователя

Для того, чтобы отредактировать права доступа пользователя, необходимо выполнить следующие шаги:

1. В разделе **Управление доступом** найти пользователя в списке и нажать на его имя.
2. На открывшейся странице редактирования изменить данные пользователя (кроме имени), включая его роли и требование сброса пароля (при необходимости).
3. Нажать кнопку на **Сохранить**.

9.3.3. Удаление пользователя

Для того, чтобы удалить пользователя, необходимо выполнить следующее:

- В разделе **Управление доступом** отметить галочкой слева выбранного пользователя в списке и нажать на кнопку **Удалить**.

> ❗ Обратите внимание, что удаление пользователя может быть необратимым.

9.3.4. Сброс пароля

Для того, чтобы инициировать сброс пароля необходимо выполнить следующее:

- В разделе **Управление доступом** найти нужного пользователя и изменить значение **Сброс пароля** на ***Да***. При следующем входе пользователь должен будет принудительно изменить пароль.

> ❕ Очистить сессии пользователя и сбросить пароль можно также в пунктах подменю в списке пользователей.

9.3.5. Настройка ролей

В подразделе **Роли** (Рис.15) отображаются все роли, которые назначены пользователям системы с указанием количества пользователей, которым они принадлежат.

> ❕ В системе предусмотрены следующие базовые роли пользователей:
>
> - **Администратор (*isadm*)** - роль с полными правами, при установке продукта присваиваются все существующие права. Предназначена для пользователей, отвечающих за развертывание и сопровождение инфраструктуры и системного программного обеспечения, необходимых для работы решения (например, операционные системы, сервера приложений, базы данных), а также отвечающих за создание и управление

учетными записями, ролями и доступами пользователей, внесение изменений в настройки, контроль лицензии, подключение инструментов безопасности и источников сканирования.

- **Аудитор (*isaud*)** - роль предназначена для контроля за безопасностью данных и систем, мониторинга действий пользователей и операций системы, анализа журналов событий, контроля результатов сканирования и соответствия Контролям качества.
- **Инженер ИБ (*isoff*)** - роль предназначена для контроля и обеспечения информационной безопасности разрабатываемых проектов, настройки правил безопасности и мониторинга угроз, управление инструментами безопасности, сканированиями.
- **Разработчик (*dev*)**- минимальная базовая роль, предназначена для пользователей, осуществляющих проверку на соответствие стандартам, просмотр результатов сканирования, исключенных проблем.

Данные роли, кроме Администратора, можно удалить. Роль Администратора можно только заблокировать.

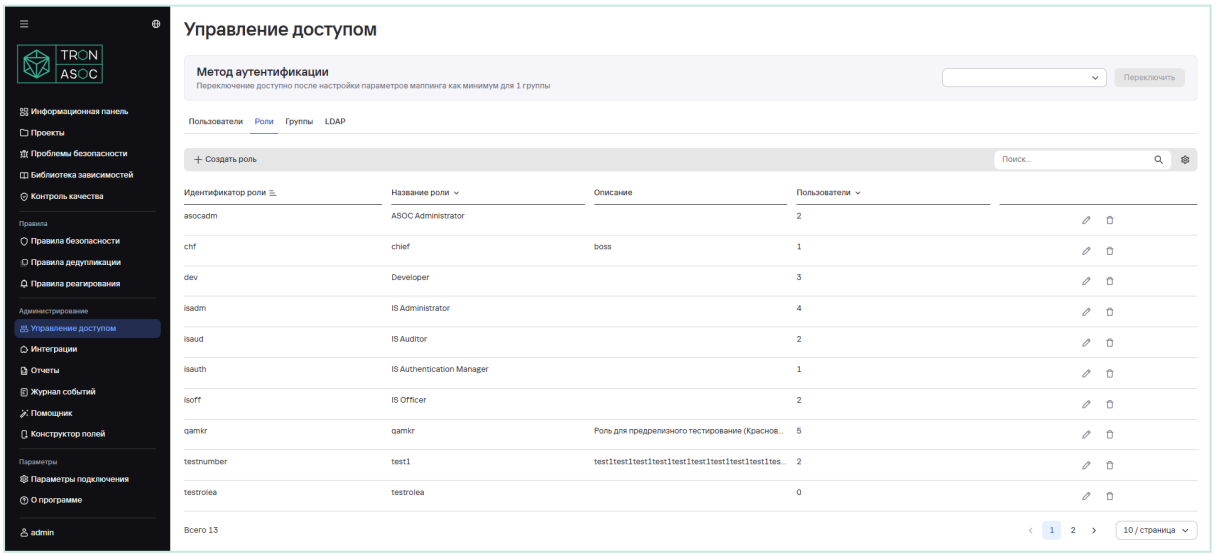

Рис. 15

Поля таблицы следующие:

- **Идентификатор роли** — уникальное имя роли в системе. Например, *activerole*, *argentgf*, *asocadm*.
- **Название роли** — название, отображаемое в интерфейсе.
- **Группы Active Directory** — если используется интеграция с AD, здесь отображены группы, с которыми связана роль.
- **Пользователи** — количество пользователей, которым назначена данная роль.

9.3.6. Добавление новой роли

❕ При добавлении новых пользователей рекомендуется назначить минимальную базовую роль (например, роль Разработчика (dev)), а настройку дополнительных узконаправленных прав добавлять с помощью новых групп, так как права по ролям и группам суммируются (подробнее см. Добавление группы пользователей).

Чтобы добавить новую роль выполните следующие шаги:

1. В подразделе **Управление доступом** → **Роли** нажмите **Создать роль**.
2. В открывшемся окне справа (Рис. 16) заполните **ID Роли**, **Название роли** и **Описание.**

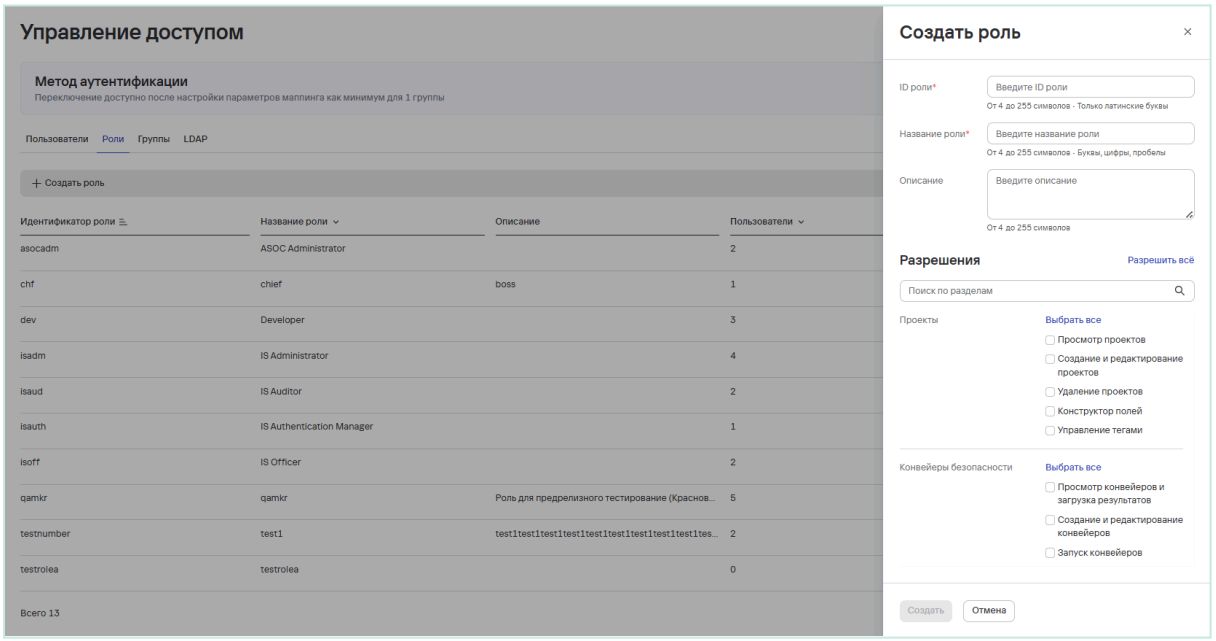

Рис.16

3. Далее настройте доступ к проектам и конвейеру безопасности в блоке **Разрешения**. Для этого поставьте галочки в нужных чекбоксах
   - **Просмотр проектов**
   - **Создание и редактирование проектов**
   - **Удаление проектов**
   - **Конструктор полей**
   - **Управление тегами**
   - **Просмотр конвейеров и загрузка результатов**
   - **Создание и редактирование конвейеров**
   - **Запуск конвейеров**
4. Нажмите кнопку **Создать**.

9.3.7. Добавление группы пользователей

Подраздел **Группы** позволяет создавать группы пользователей (Рис. 17), редактировать и удалять их, добавлять в них пользователей.

> ❕ При добавлении новых пользователей в группу указанные в группе дополнительные права суммируются с правами роли пользователя.

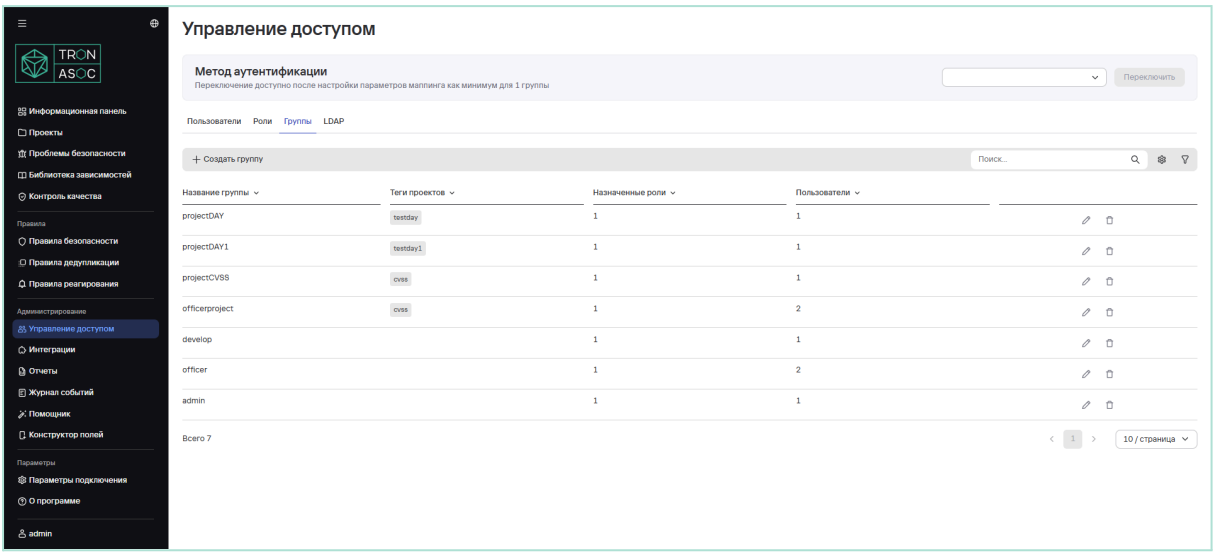

Рис. 17

Для того, чтобы добавить группу, необходимо выполнить следующее:

1. В подразделе **Управление доступом** → **Группы** нажать на кнопку **Создать группу.**
2. В открывшемся окне (Рис. 18) заполнить поля формы:
    - **Название группы**
    - **Добавить роли**
    - **Теги проектов**
    - **Добавить пользователей**

> ❕ Также предусмотрено добавление связи с группой LDAP/AD в блоке **Маппинг с LDAP**. Для того, чтобы добавить группу LDAP, необходимо добавить интеграцию с LDAP/AD (см. Аутентификация в LDAP), после чего группа LDAP/AD появится в списке групп блока **Маппинг с LDAP**.

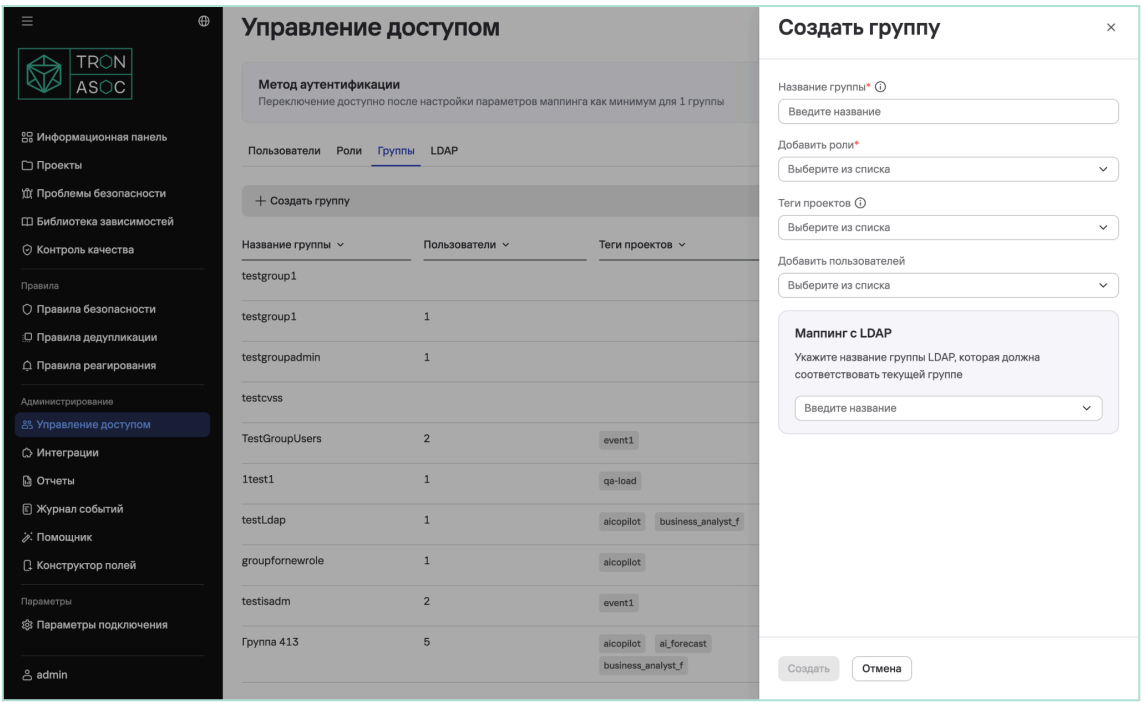

Рис. 18

3. Далее нажать на кнопку **Создать**.

9.3.8. Аутентификация в LDAP

Подраздел **LDAP** предназначен для удобного и безопасного управления пользователями и их доступом, используя интеграцию с LDAP или AD (Рис. 19).

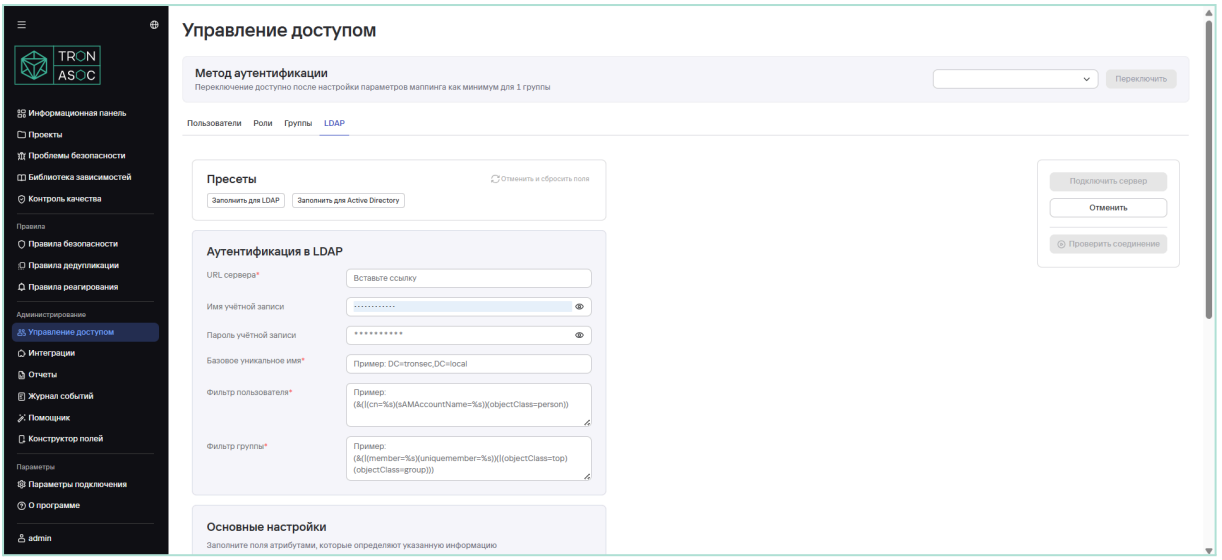

Рис. 19

Для настройки интеграции необходимо выполнить следующие шаги:

1. В подразделе **Управление доступом** → **LDAP** в блоке **Пресеты** выбрать один из предложенных вариантов предзаполнения данных:
   - **Заполнить для LDAP**

    - **Заполнить для Active Directory**
2. Далее заполнить поля соответствующими данными и атрибутами из LDAP/AD.
    - **URL сервера**
    - **Имя учетной записи** - имя учетной записи, используемой для аутентификации при подключении к LDAP-серверу
    - **Пароль учетной записи** - пароль учетной записи LDAP.
    - **Базовое уникально имя** - основной контекстный путь (Base Distinguished Name), где будут выполняться запросы LDAP.
    - **Фильтр пользователя** - фильтр поиска пользователя
    - **Фильтр группы** - фильтр поиска группы
    - **Название орг.единицы -** атрибут, который определяет организационную единицу пользователя
    - **Уникальное имя - а**трибут, который определяет дистинктивное имя (DN) пользователя или группы
    - **Имя пользователя**
    - **Фамилия пользователя**
    - **Название группы**
    - **Логин пользователя**
    - **Email пользователя**
    - **Член группы**
    - **Группы пользователя**
3. После заполнения необходимо убедиться, что все параметры LDAP настроены правильно и система сможет успешно подключиться к серверу LDAP. Для этого необходимо нажать на кнопку **Проверить соединение**.
4. В случае успешной проверки необходимо сохранить настройки с помощью кнопки **Сохранить**.

9.3.9. Метод аутентификации

После настройки интеграции с LDAP/AD рекомендуется выбрать метод аутентификации. Для этого необходимо выполнить следующее:

1. В разделе **Управление доступом** → **Группы** добавить хотя бы одну группу (или отредактировать существующую) с настроенной связью с LDAP-группой (блок **Маппинг с LDAP**).
2. Далее в блоке **Метод аутентификации** выбрать один из представленных методов аутентификации:
    - **Внутренняя модель и LDAP**
    - **Только LDAP**
    - **LDAP отключен**
3. Далее необходимо убедиться в правильности введенных данных и нажать кнопку **Переключить**.

❗ Важно! При смене метода аутентификации произойдет закрытие сессии у всех пользователей, и дальнейшая авторизация будет осуществляться в соответствии с выбранным методом (Рис. 20).

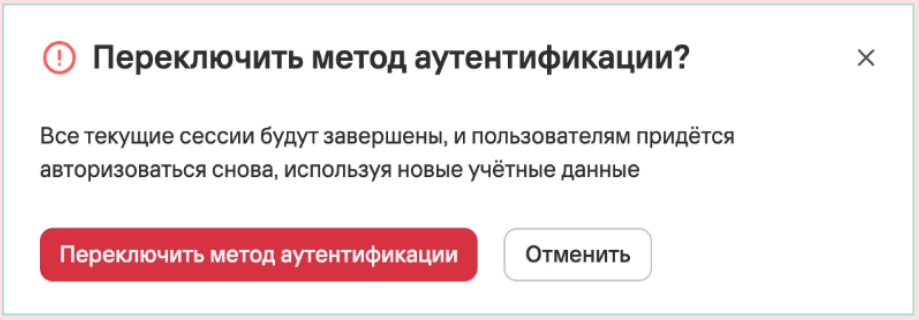

Рис. 20

10. Настройки интеграций

10.1. Инструменты безопасности

Просмотр всех подключенных инструментов безопасности доступен в разделе **Интеграции** → **Инструменты безопасности** (Рис. 21). Функционал позволяет также добавлять новые инструменты, редактировать и удалять существующие.

Поддерживаемые инструменты безопасности:

- **PT Application Inspector**
- **Kaspersky Container Security**
- **Solar AppScreener**
- **Aqua**
- **CodeScoring**
- **Grype**
- **KICS**
- **OWASP Dependency Track**
- **Trivy**
- **Semgrep**

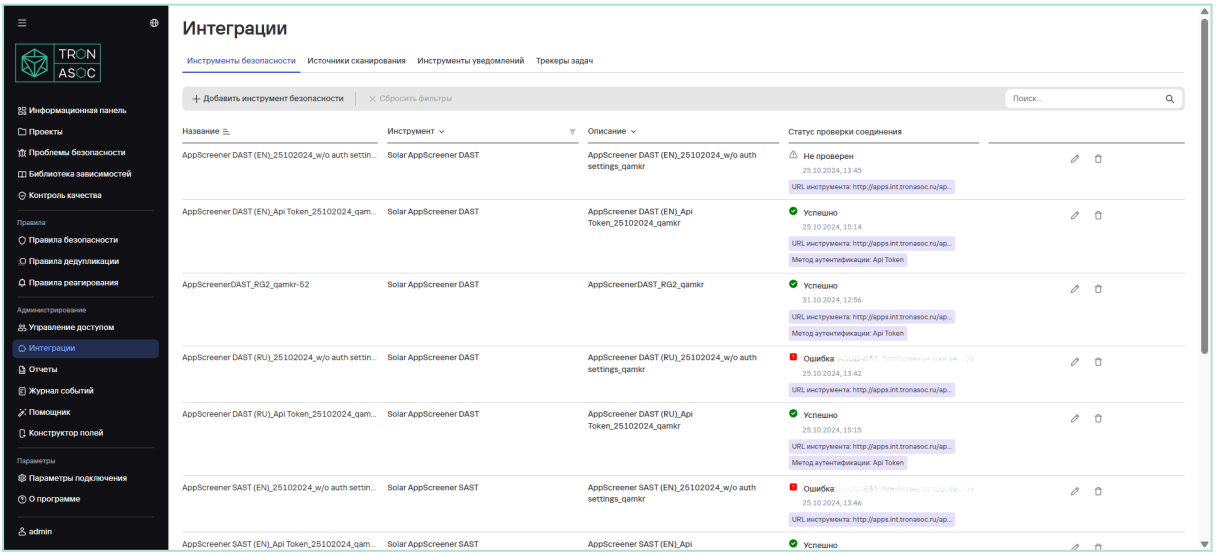

Рис. 21

10.1.1. Подключение инструментов безопасности

Чтобы добавить новый инструмент безопасности, необходимо выполнить следующее:

1. В разделе **Интеграции** → **Инструменты безопасности** нажмите кнопку **Добавить инструмент безопасности**.
2. В открывшемся окне заполнить поля **Название**, **Описание** и добавить **Инструмент**.

3. В зависимости от выбранного инструмента необходимо заполнить дополнительные поля (описание инструмента и URL, язык результатов сканирования). Выбор метода аутентификации на этом шаге не является обязательным, но без заполнения метода аутентификации нельзя проверить соединение с инструментом. Поля для заполнения далее могут отличаться в зависимости от выбора метода аутентификации. Если метод указан и выбрана аутентификация по API -токену, нужно заполнить поле **API Токен**, если выбран метод аутентификации по логину и паролю, нужно заполнить поля **Логин** и **Пароль**.
   Для инструмента **CodeScoring** могут использоваться уже существующие данные аутентификации.
   Чтобы сделать проверку соединения, нажмите **Проверить соединение**. Система отправит запрос на соединение с инструментом и в верхнем правом углу пользовательского интерфейса отобразится соответствующее уведомление.
4. Далее нажать на кнопку **Создать**.

10.1.2. Редактирование инструмента

Редактирование инструмента производится по клику на кнопку  в списке соответствующем инструменте безопасности. Форма редактирования аналогична форме добавления, но поля заполнены текущими данными (Рис. 22).

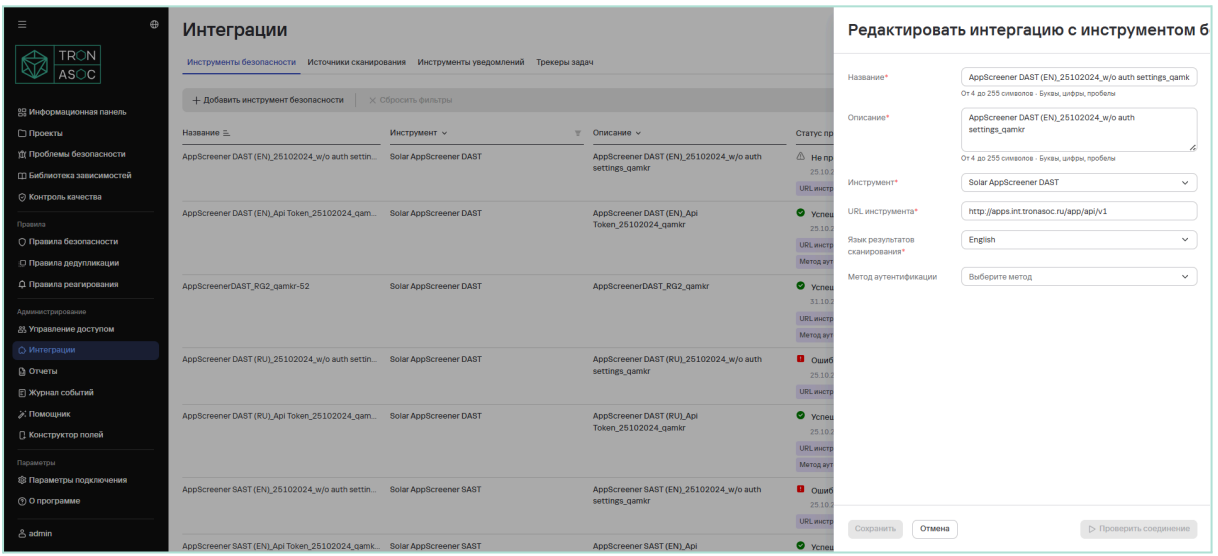

Рис. 22

10.1.3. Удаление инструмента

Удаление инструмента сканирования производится на странице **Инструменты безопасности** с помощью кнопки  в строке инструмента, который нужно

удалить (Рис. 21), после чего в открывшемся окне подтвердить удаление инструмента (Рис. 23).

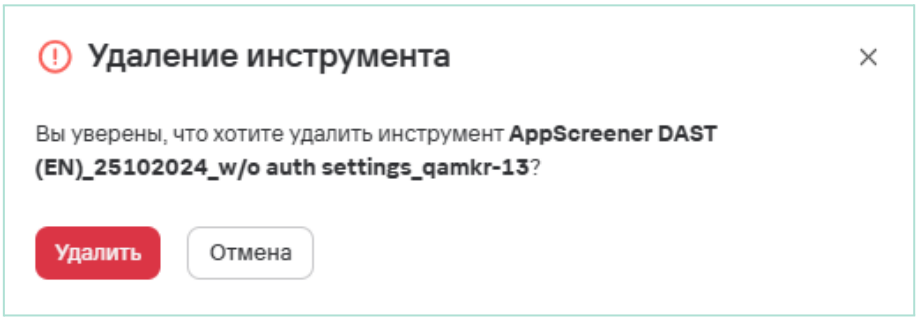

Рис. 23

10.1.4. Примеры интеграций с инструментами

10.1.4.1. Добавление в раздел Интеграции PT Application Inspector

Раздел **Интеграции** - это перечень адаптеров и параметров к ним, которые требуются для конфигурации интеграции с инструментом.

Для добавления инструмента на платформу, необходимо выполнить следующие шаги:

1. Перейти в раздел **Интеграции** и нажать на кнопку **Добавить инструмент безопасности** и в появившейся форме заполнить поля:
    - **Название интеграции** - например, *Инспектор*. Имя должно быть уникальным.
    - **Описание** - для удобства идентификации, например, *Позитивный инспектор*.
    - **Инструмент** - выбор инструмента из выпадающего списка.
2. Далее необходимо настроить параметры подключения:
    - Ввести адрес API PT Application Inspector. Например: *https://your.company.ptsecurity/api/v1*.
    - Выбрать язык результатов сканирования.
    - Выбрать метод аутентификации (*этот шаг на данном этапе не является обязательным, если метод аутентификации не указать при создании интеграции, его можно будет указать на этапе добавления новой проверки безопасности*)
        - **Login/Password** (если используется по логину и паролю).
        - **API Token** (если используется токен доступа)
            - Если выбран метод **Login/Password**, заполните соответствующие поля логина и пароля.
            - Для **API Token** вставьте токен в выделенное поле.
3. Далее нажать на кнопку **Проверить соединение**. При правильно заполненных полях статус проверки должен быть успешным. Если

соединение не установлено, нужно проверить корректность введенных данных и повторить попытку.

4. После успешной проверки соединения нажать на кнопку **Сохранить**, интеграция появится в общем списке инструментов безопасности.

10.1.4.2. Добавление в раздел Интеграции KCS

Для добавления необходимо выполнить следующие шаги:

1. В разделе **Интеграции** → **Инструменты безопасности** необходимо нажать на кнопку **Добавить инструмент безопасности**.
2. В появившейся форме необходимо заполнить следующие обязательные поля:
    a. **Название**
    b. **Описание** (добавить краткое описание для инструмента)
    c. **Инструмент** (*Kaspersky Container Security* из выпадающего списка)
3. Далее добавить дополнительные параметры инструмента:
    a. Указать **URL инструмента** Kaspersky Container Security (Например: *https://your.company.kcs/api/v1*)
    b. Выбрать язык результатов сканирования
    c. **Метод аутентификации** (в этом инструменте для авторизации используется API Token) и вставить токен в поле **Токен API**

> ❕ Выбор метода аутентификации на данном этапе не является обязательным. Если метод аутентификации не указать при создании интеграции, его можно будет указать на этапе добавления новой проверки безопасности.

10.2. Источники сканирования

Просмотр всех подключенных источников сканирования доступен в разделе **Интеграции** → **Источники сканирования** (Рис. 24). Также предусмотрена возможность отсортировать по названию, типу источника, описанию, перейти к добавлению, редактированию или удалению источников сканирования.

Поддерживаемые источники сканирования:

- **GitLab**
- **Nexus**
- **CLI Tool**
- **Jfrog**
- **Harbor**
- **AppUrl**

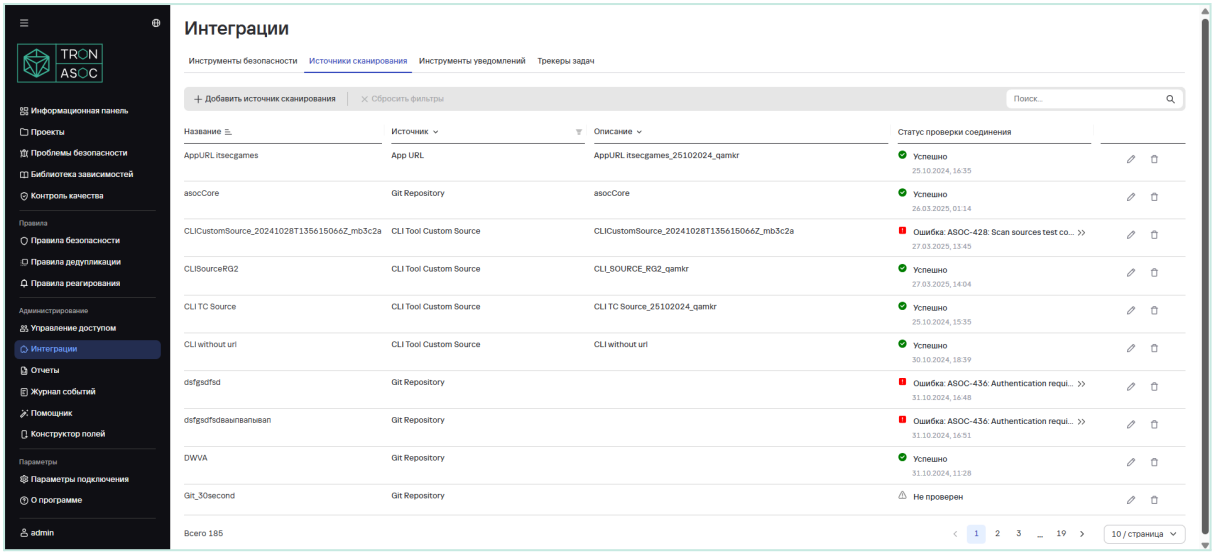

Рис.24

10.2.1. Подключение источника сканирования

Чтобы подключить источник сканирования, необходимо выполнить следующие шаги:

1. Перейти в раздел **Интеграции → Источники сканирования.**
2. Нажать кнопку **Добавить источник сканирования**.
3. В открывшейся форме добавления источника сканирования (Рис. 25) заполнить поля **Имя**, **Описание**, в раскрывающемся меню поля **Источник** выбрать источник сканирования.

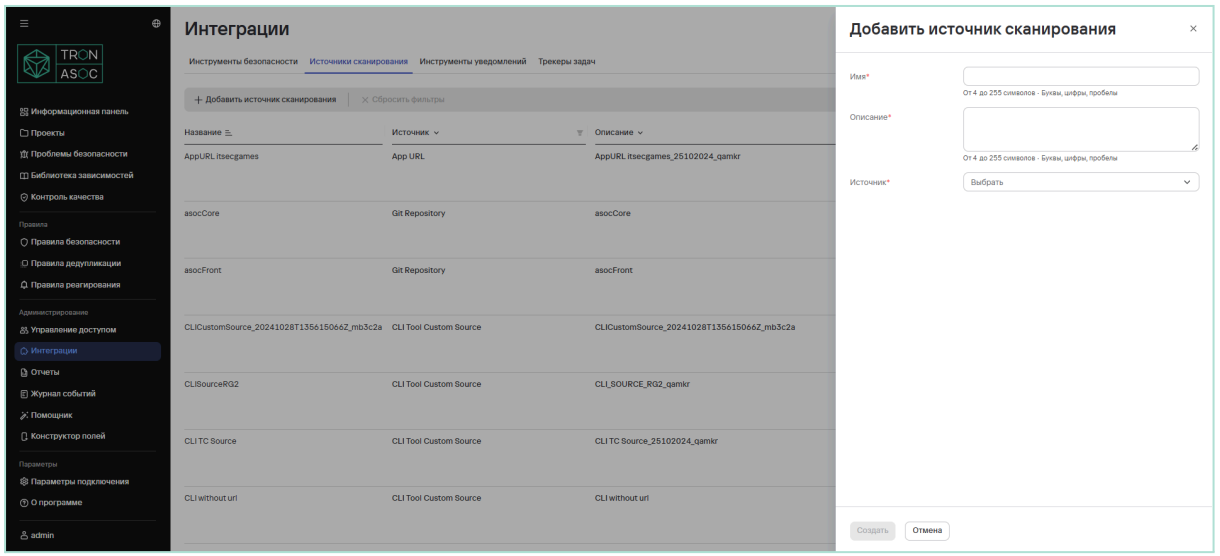

Рис. 25

4. После выбора источника инструмента необходимо заполнить дополнительные поля, специфичные выбранному на предыдущем шаге инструменту:
    a. **URL источника**.

b. **Метод аутентификации** - Заполнение поля на этом этапе не является обязательным, но без него нельзя будет осуществить проверку соединения с источником сканирования.
c. Далее поля для заполнения далее могут отличаться в зависимости от выбора метода аутентификации. Если метод указан и выбрана аутентификация по API - токену, необходимо заполнить поле **Токен API**, если выбран метод аутентификации по логину и паролю, нужно заполнить поля **Логин/Пароль**.
   Для проверки соединения, нажать кнопку **Проверить соединение**. Система отправит запрос на соединение с источником и в верхнем правом углу пользовательского интерфейса отобразится соответствующее уведомление.

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

10.2.2. Редактирование источника сканирования

Редактирование источника производится с помощью кнопки  в соответствующем источнике сканирования. Форма редактирования аналогична форме добавления, но поля заполнены текущими данными (Рис. 26).

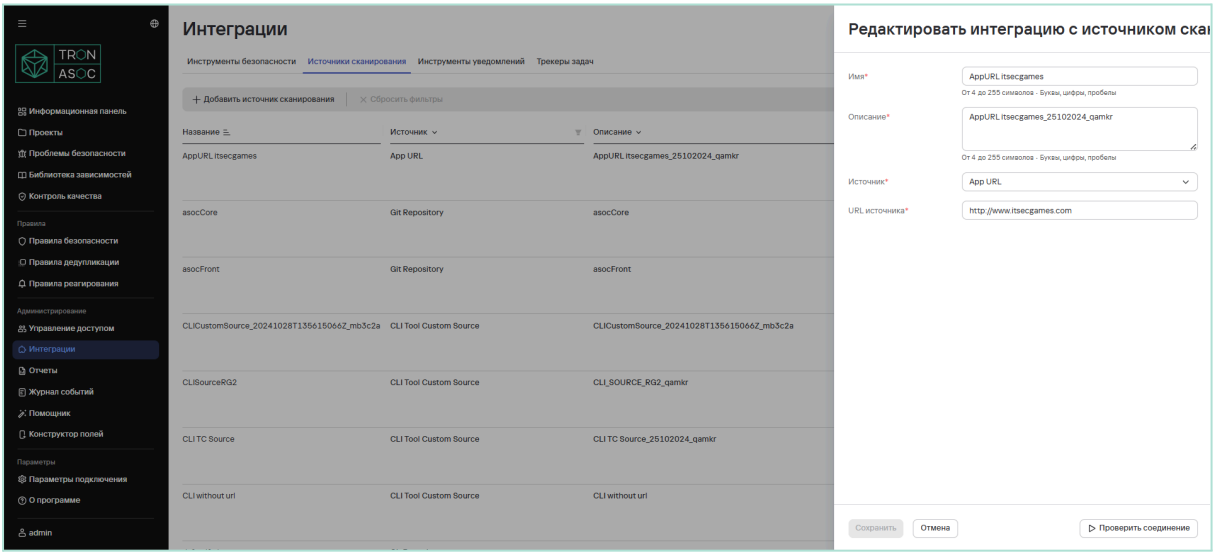

Рис. 26

10.2.3. Удаление источника сканирования

Чтобы удалить источник сканирования, перейдите в раздел **Интеграции** → **Источники сканирования,** нажмите на кнопку  в строке источника сканирования, который нужно удалить (Рис. 25), после чего в открывшемся окне подтвердить удаление источника (Рис. 27).

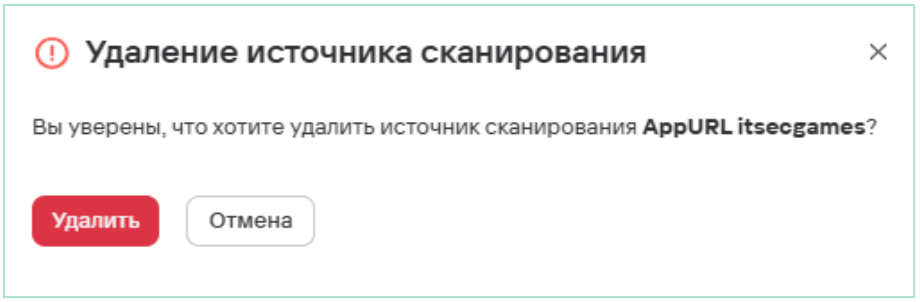

Рис. 27

10.3. Инструменты уведомлений

Подраздел **Инструменты уведомлений** позволяет настроить интеграцию уведомлений об уязвимостях, например, на электронную почту (Рис. 28).

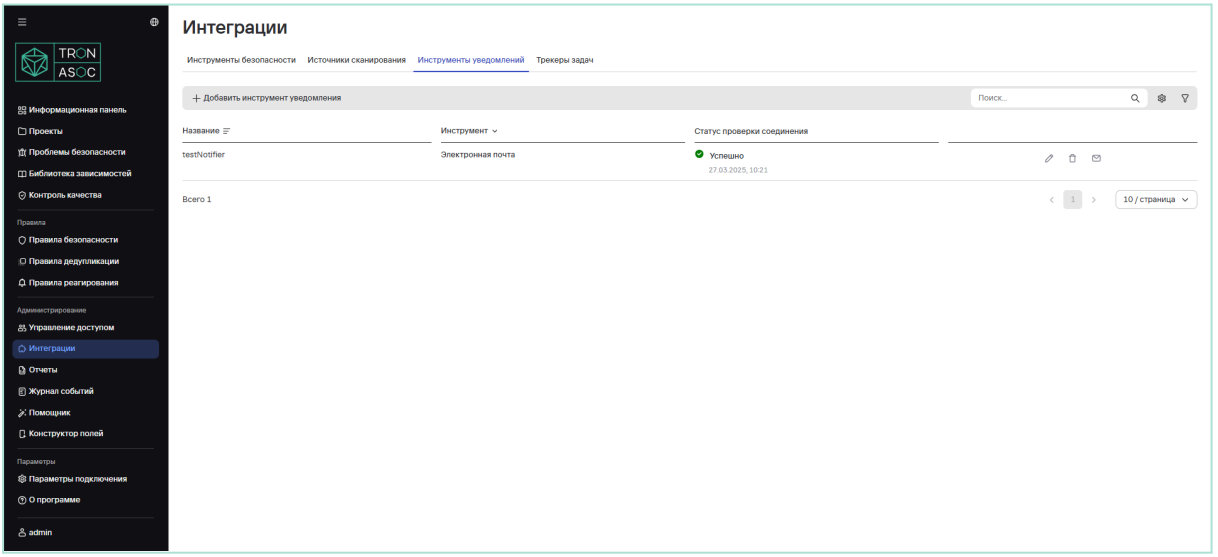

Рис. 28

Для создания инструмента уведомлений необходимо выполнить следующие шаги:

1. В разделе **Интеграции** → **Инструменты уведомлений** нажать на кнопку **Добавить инструмент уведомлений.**
2. В открывшемся окне (Рис. 29) заполнить следующие поля
    - **Название**
    - **Инструмент** - выбрать **Электронная почта**
    - **SMTP-сервер**
    - **Порт**
    - **Имя пользователя**
    - **Пароль**
    - **Отправитель**
    - При необходимости добавить адреса электронных почт конкретных получателей в поле **Получатели**

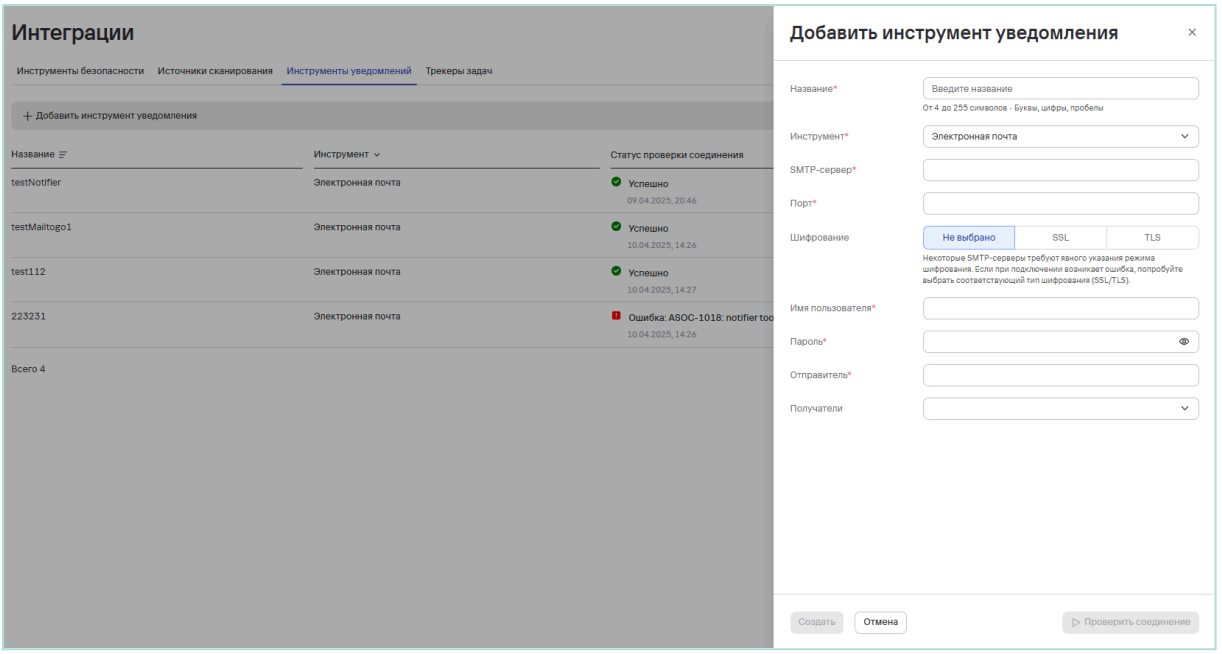

Рис. 29

3. При необходимости проверить соединение с помощью кнопки **Проверить соединение.**
   Если при подключении возникает ошибка, попробуйте выбрать соответствующий тип шифрования (SSL/TLS).
4. Нажать на кнопку **Создать**.

10.4. Трекеры задач

В подразделе **Трекеры задач** есть возможность настроить интеграции с трекерами задач (Рис. 30).

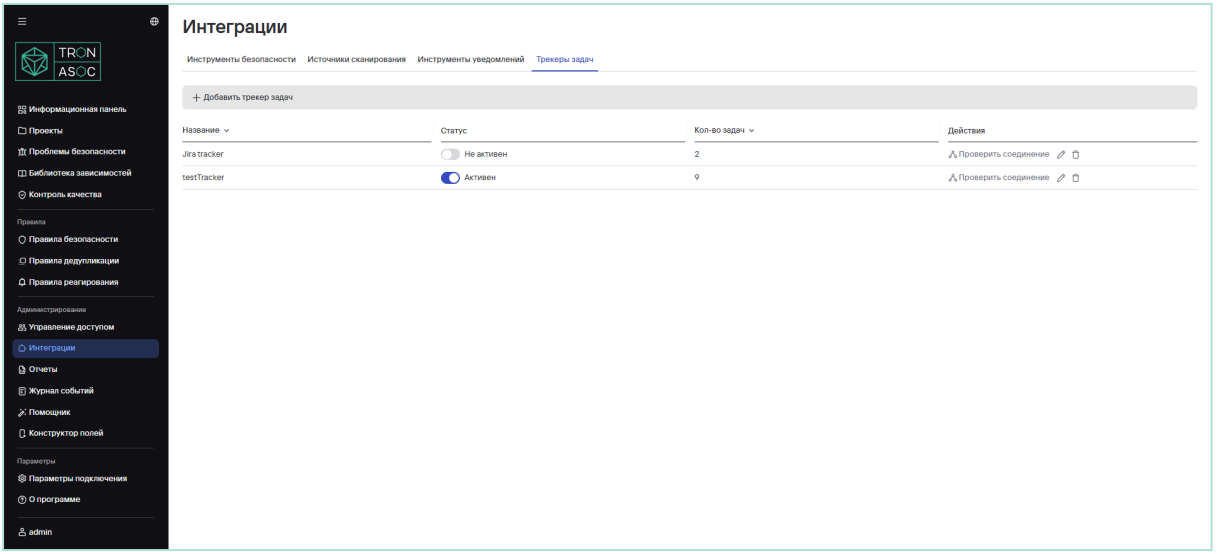

Рис. 30

❗ **Tron.Asoc версии 1.2** поддерживает интеграцию с ПО **Jira** только с использованием Jira REST API v2 (https://developer.atlassian.com/cloud/jira/platform/rest/v2/intro/#about).

10.4.1. Добавление трекера задач

Для добавления трекера задач необходимо выполнить следующие шаги:

1. В разделе **Интеграции - Трекеры задач** нажать на кнопку **Добавить трекер задач**.
2. В открывшемся окне (Рис. 31) заполнить следующие параметры подключения:
    - **Название интеграции** (например, ***Jira Tracker***)
    - **URL-адрес рабочей области**
    - **API-токен** аутентификации
    - **Логин** для аутентификации

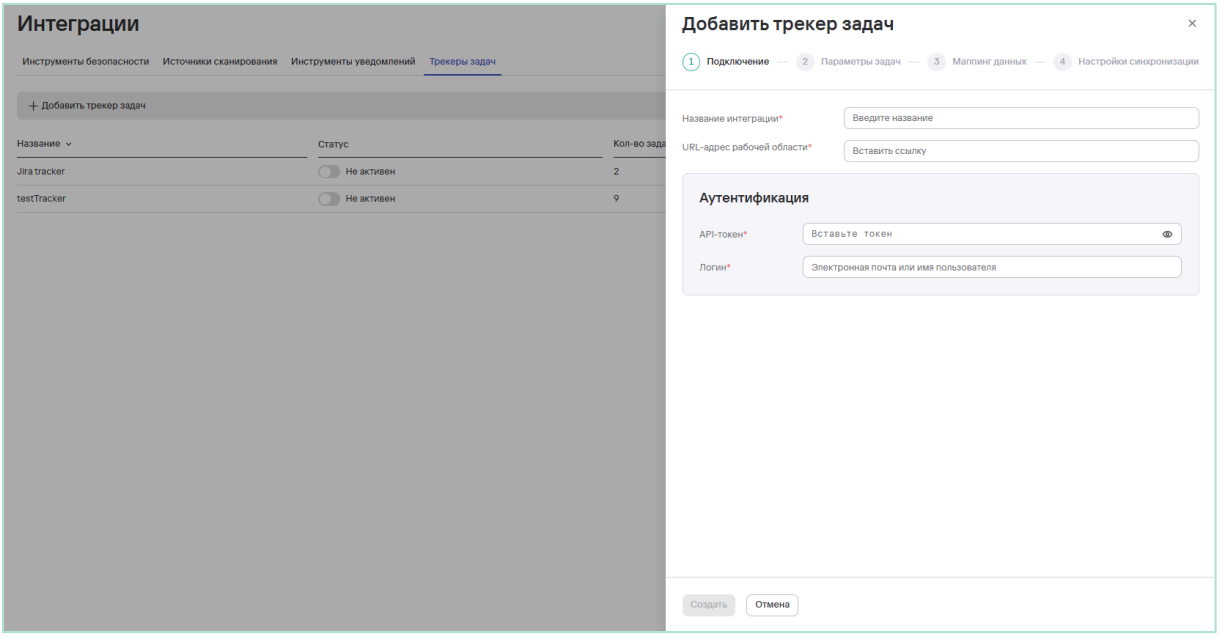

Рис. 31

3. После заполнения всех полей нажать на кнопку **Создать**.
4. Далее заполнить следующие параметры задач (Рис. 32):
    - **Проект**
    - **Тип задачи**
    - Формат отправки задач (как *Несколько отдельных задач* или *Одну общую задачу*)

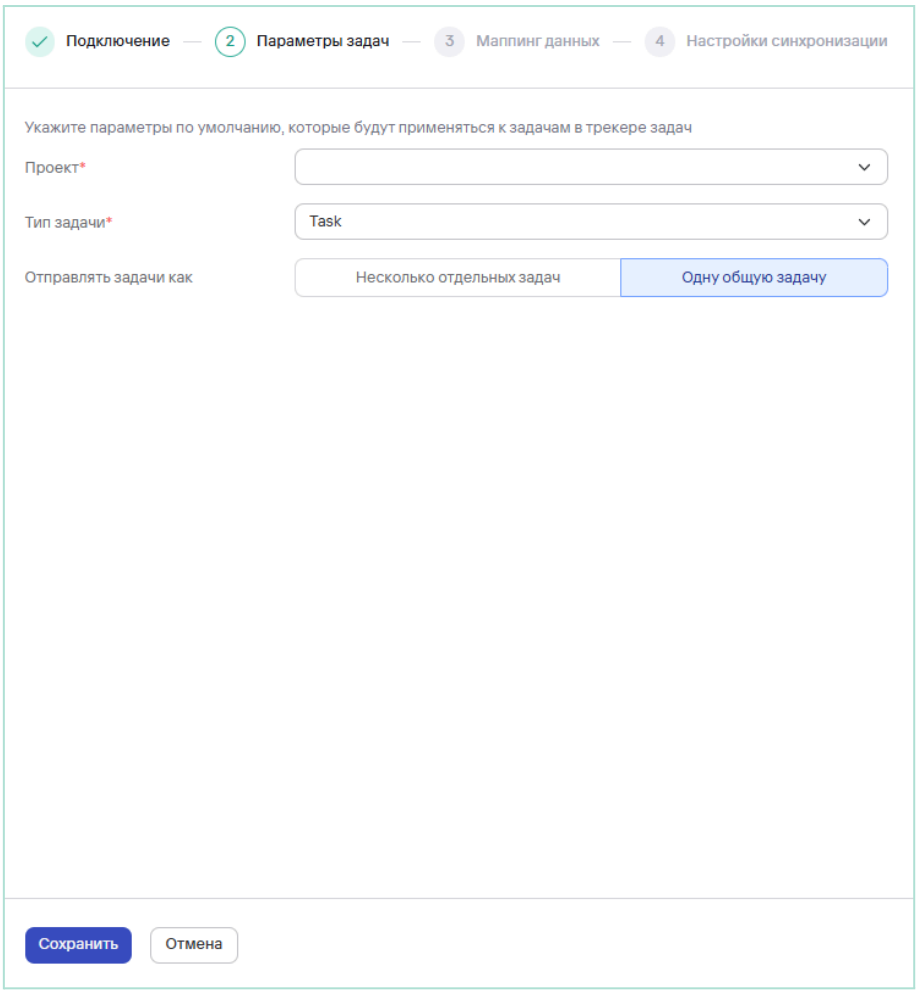

Рис. 32

5. После заполнения нажать на кнопку **Сохранить.**
6. Далее заполнить необходимые параметры маппинга задач (Рис. 33).
   Доступен выбор предзаполненных данных с помощью кнопки **Применить пресет**.
   В блоке **Поля** необходимо указать соответствие полей в ASOC с полями в трекере. Для успешного маппинга важно указать все обязательные поля из трекера. По умолчанию обязательные поля указаны в Пресетах, но они могут отличатся от настроек трекера.
   В блоке **Статусы** необходимо указать соответствие статусов ASOC со статусами трекера.

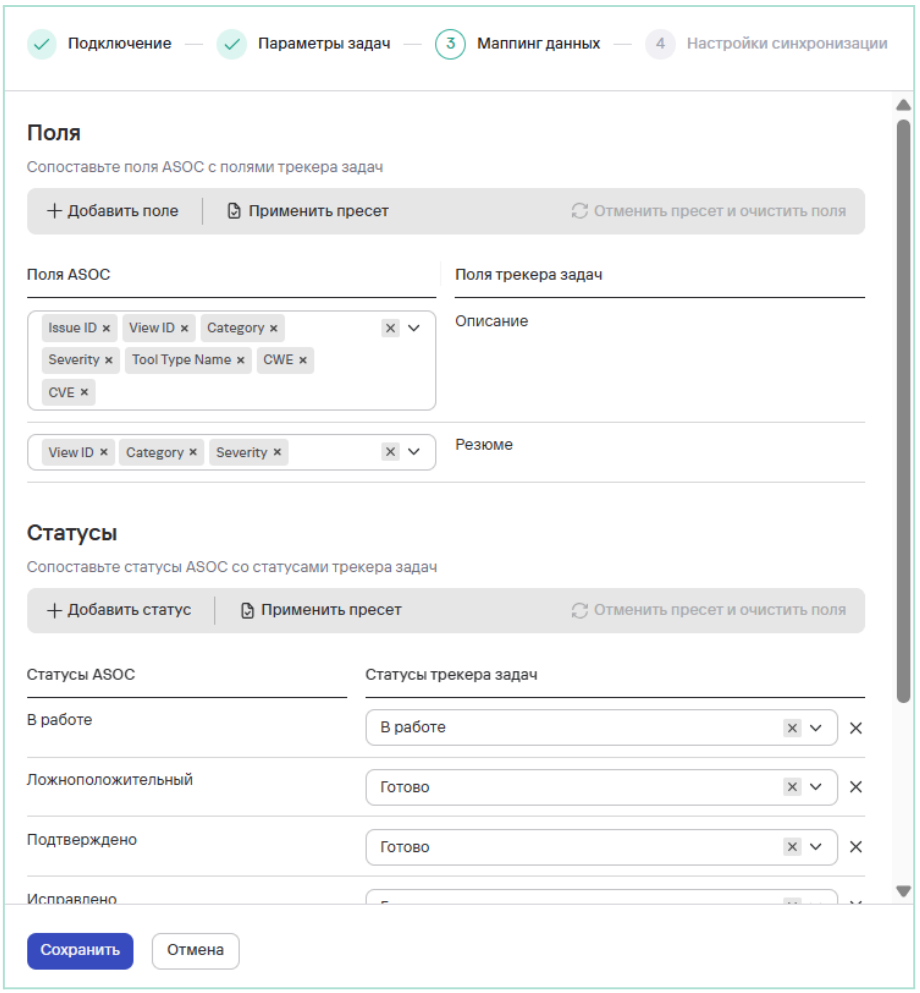

Рис. 33

7. Нажать на кнопку **Сохранить**.
8. Далее в случае необходимости обратной отправки изменений из трекера в ASOC (данное действие избавит от потребности ручного отслеживания состояния задач в трекере и обновления данных в ASOC), перевести в активное состояние **Отправку изменений, представленных в трекере задач, в ASOC** (Рис. 34) и нажать на кнопку **Сохранить**.

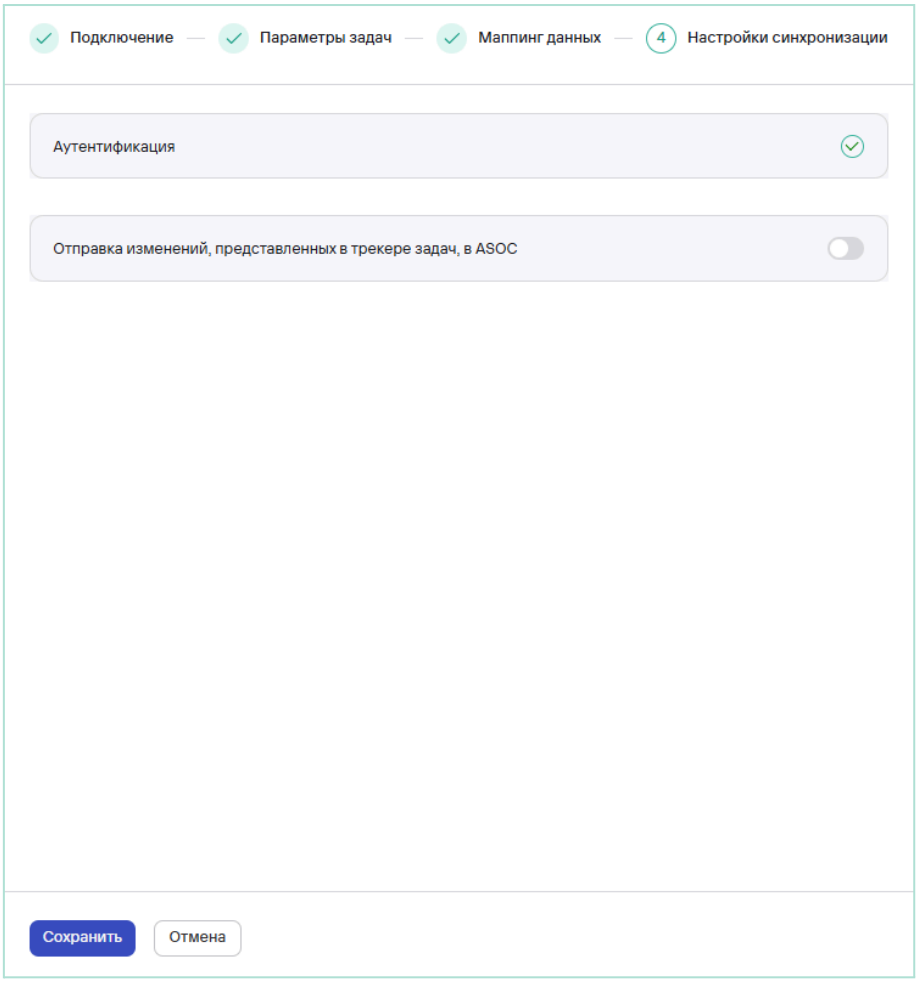

Рис. 34

После этого в случае успешного соединения трекер будет отображен в списке трекеров в статусе ***Активен***.

Также при необходимости доступна возможность проверки соединения с помощью кнопки **Проверить соединение,** и отключение трекера с помощью перевода его **Статуса** в ***Не активен*** (Рис. 35).

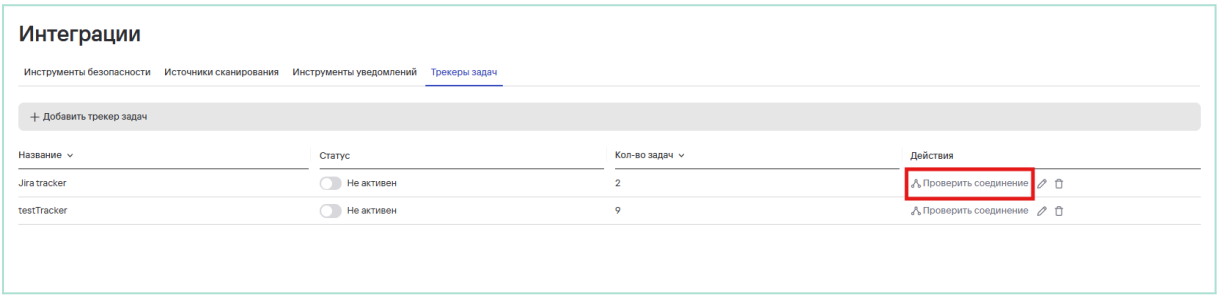

Рис. 35

Для редактирования/удаления трекера необходимо нажать на соответствующую кнопку действий (Рис. 35).

11. 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. 36).

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

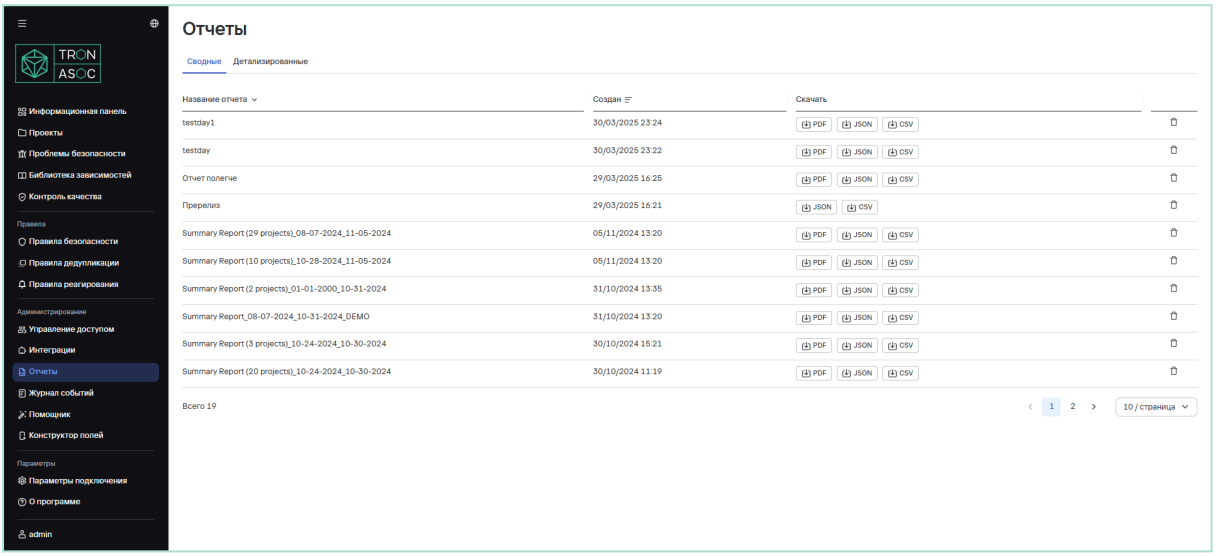

Рис. 36

12. 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. 37). Для этого необходимо выполнить следующие шаги:

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

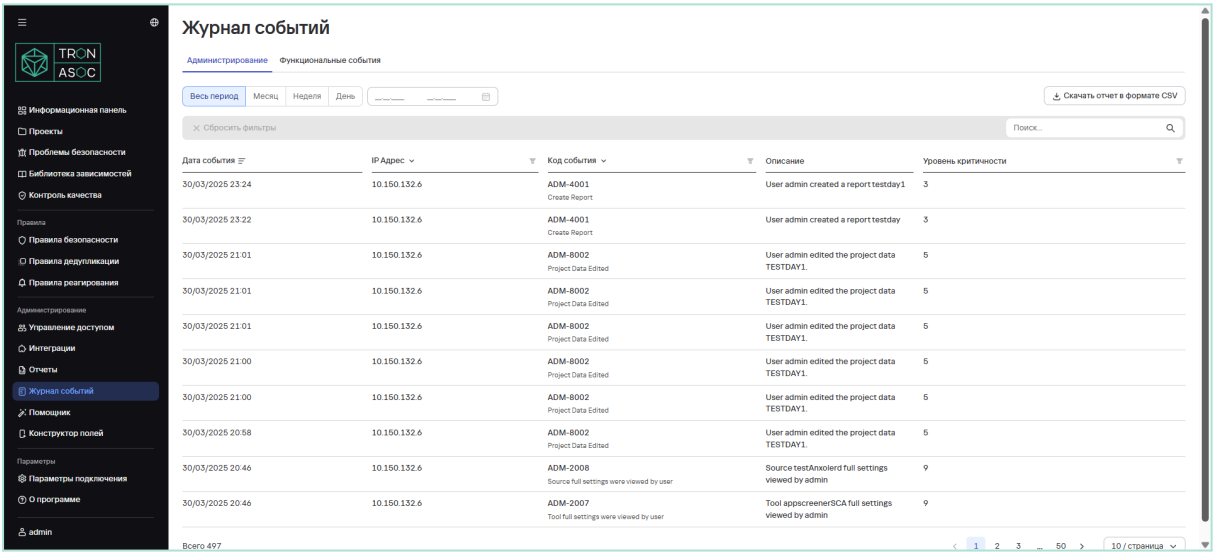

Рис. 37

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.

13. Конструктор полей

Раздел **Конструктор полей** позволяет настроить пользовательские поля проектов (Рис. 38).

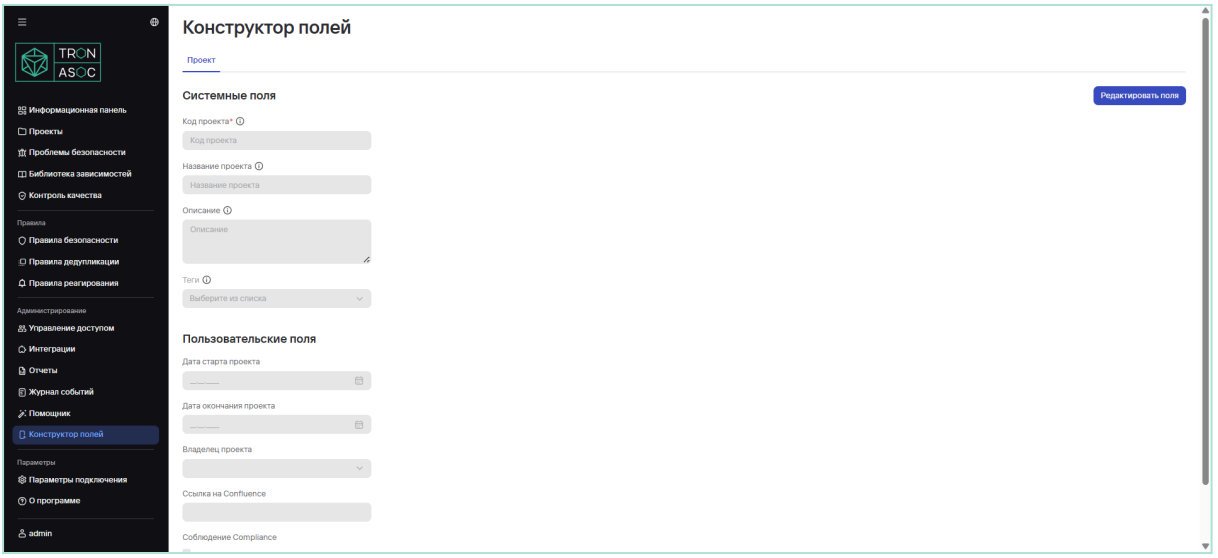

Рис. 38

Для настройки необходимо выполнить следующие шаги:

1. На странице **Конструктор полей** нажать кнопку **Редактировать поля**.
2. В открывшемся окне справа (Рис. 39) скорректировать (добавить/удалить) представленный набор полей с помощью кнопок **Добавить поле** и  .

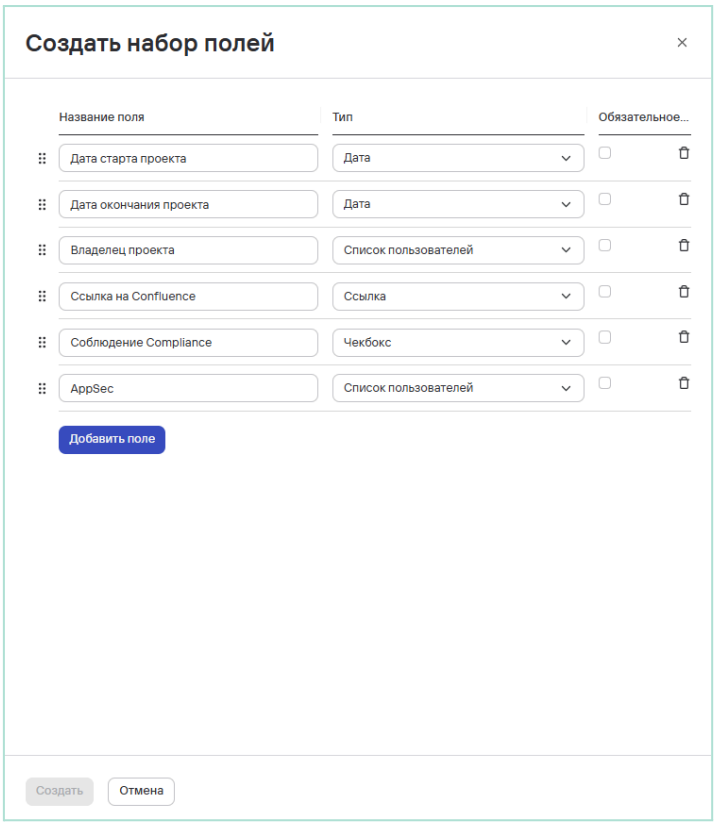

Рис. 39

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