

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

Руководство администратора

Октябрь 2024

## Содержание

Термины и определения	3
Общие сведения	4
Установка решения	8
Интерфейс	9
Страница авторизации	9
Начало работы в системе	10
Настройка правил авторизации	10
Управление пользователями и ролями	11
Роли	13
Добавление роли	14
Инструменты безопасности	15
Подключение инструментов безопасности	15
Редактирование инструмента	16
Удаление инструмента	17
Источники сканирования	18
Подключение источника сканирования	18
Редактирование источника сканирования	19
Удаление источника сканирования	19
Отчеты	20

## Термины и определения

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

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

## 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 KCS, с программным комплексом Solar AppScreener, с решениями CodeScoring и OWASP Dependency Track, а также может принимать и анализировать отчеты от инструментов Trivy, Gype, KICS для дальнейшей обработки полученных от них результатов.
  - 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.

- есть возможность 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.
- дашборды, отчеты и метрики внутри продукта 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.
- 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.

## Установка решения

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

### 1. Установка компонентов:

Скачать архив `docker-compose`

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

Задать значения переменной для `ASOC_DOMAIN`

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

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

Выполнить `docker-compose up -d`

Проверить статус контейнеров `docker ps`

### 2. Первый запуск консоли управления.

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

- Настроить интеграцию с инструментами безопасности
- Настроить интеграцию с источниками



## Интерфейс

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

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

## Страница авторизации

Вход в систему осуществляется по логину и паролю со страницы авторизации. Перед первым входом администратор должен принять условия, указанные в Соглашении с конечным пользователем.

## Начало работы в системе

На странице авторизации (рис.1) обязательные поля отмечены звездочкой. Есть возможность переключения между русским и английским языками. Для входа введите имя и пароль учетной записи и нажмите кнопку Войти.

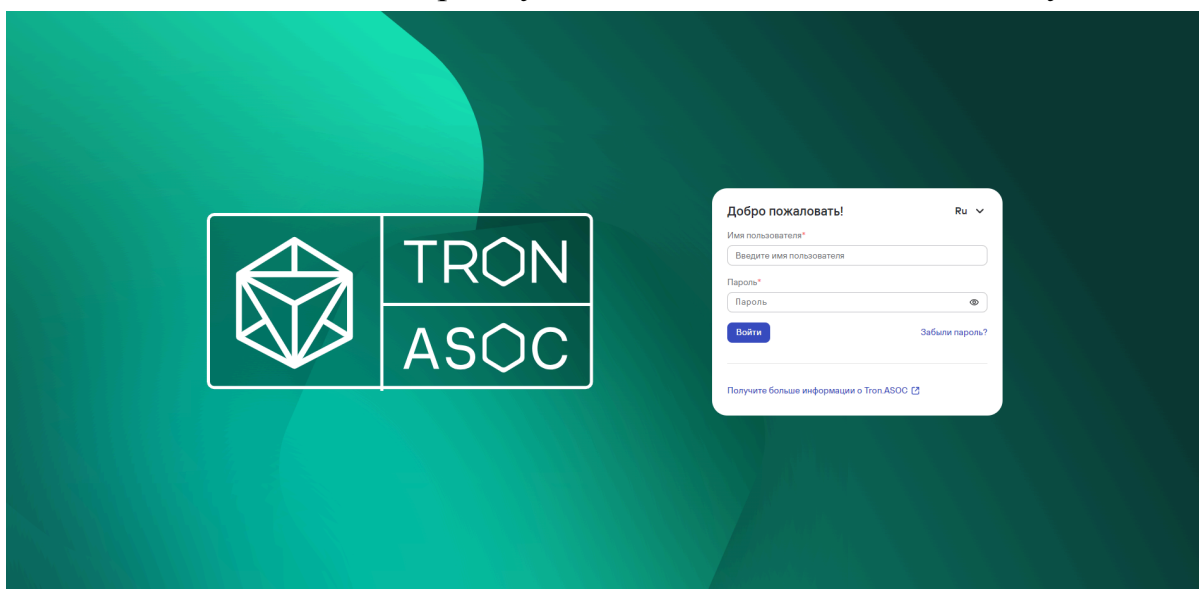


Рис.1

## Настройка правил авторизации

На вкладке Аутентификация (рис.2) можно задать параметры требований к паролю, максимальной продолжительности сеанса, время выхода из системы после периода неактивности, количество попыток ввода пароля до временной блокировки, длительность временной блокировки.

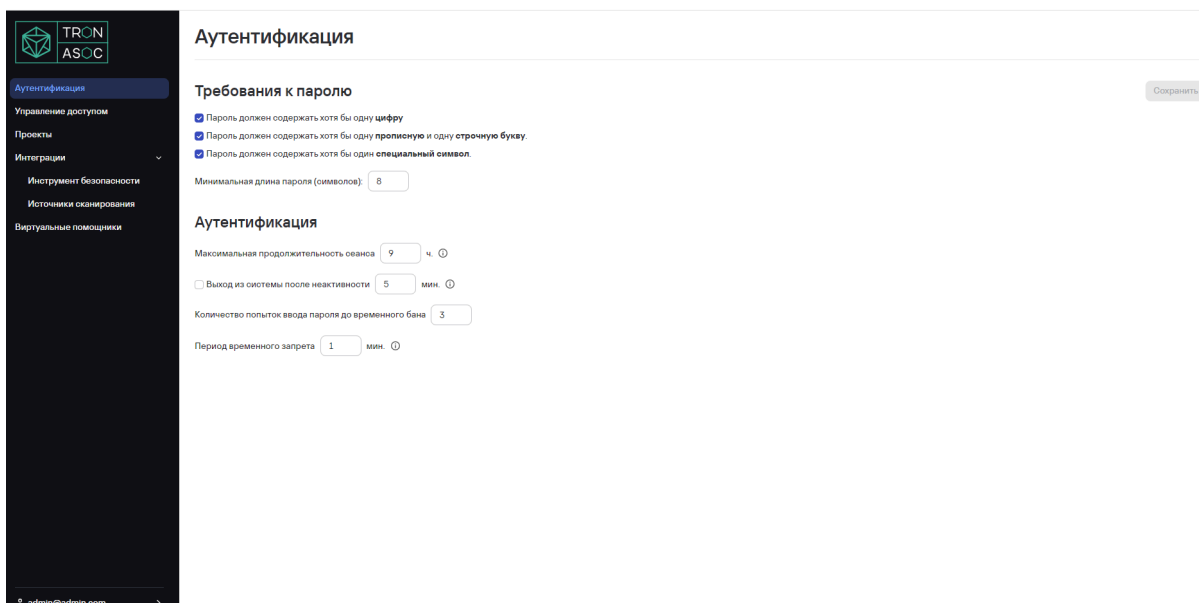


Рис.2

Администратор может задать требования к паролю, максимальное время, в течение которого пользователь может оставаться в системе, без необходимости повторной аутентификации. период неактивности, количество попыток ввода пароля.

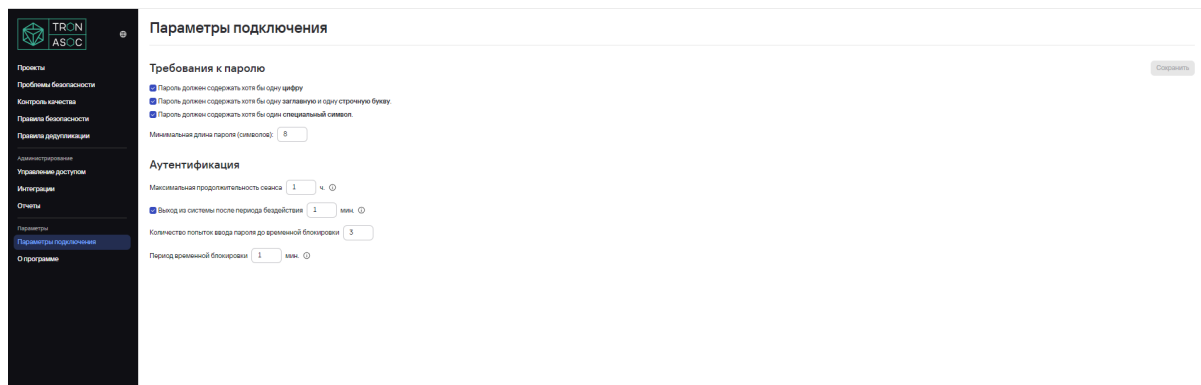


Рис.3

## Управление пользователями и ролями

Раздел "Управление доступом" позволяет администраторам управлять пользователями и их ролями в системе. Этот раздел включает два ключевых подраздела: **Пользователи** и **Роли**. Переход к разделу осуществляется из левого сайд-бар меню.

Раздел "Пользователи" предоставляет список всех пользователей системы, где отображаются их данные и назначенные роли.

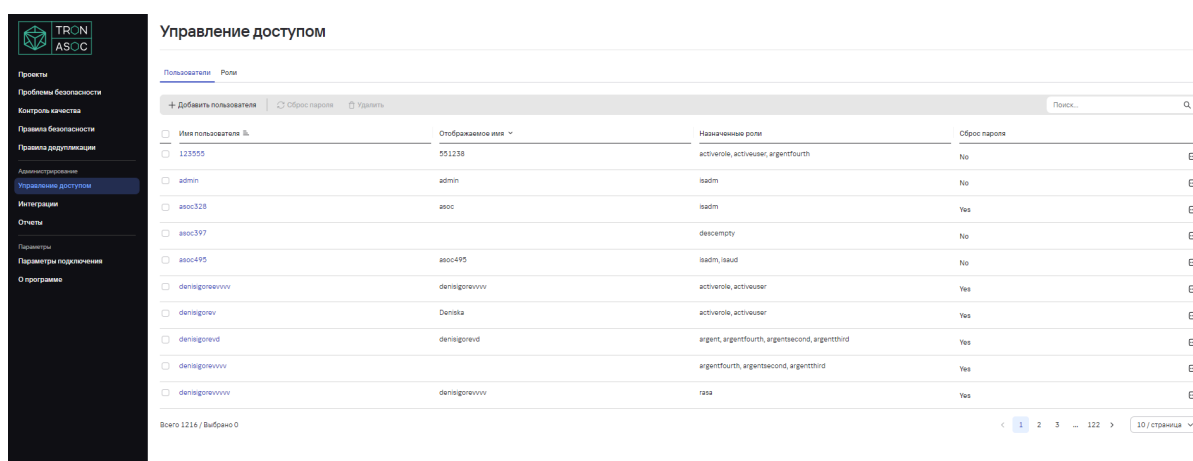


Рис.4

Основные колонки таблицы:

- 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 *Yes* означает, что пользователь должен изменить свой пароль при следующем входе в систему.

Добавление нового пользователя (рис.5):

- Нажмите кнопку "**Добавить пользователя**".
- Введите имя пользователя и его отображаемое имя, электронную почту
- Задайте и подтвердите пароль.
- Назначьте пользователю одну или несколько ролей, которые определяют его права доступа.
- При необходимости включите опцию сброса пароля.

The screenshot shows the 'Управление доступом > Пользователи > Добавить пользователя' page. On the left is a dark sidebar with navigation items: Проекты, Проблемы безопасности, Контроль качества, Правила безопасности, Правила дубликации, Администрирование, Управление доступом (highlighted), Интеграции, Отчеты, Параметры, Параметры подключения, О программе. The main content area is titled 'Общая информация' and contains the following fields and options:

- Имя пользователя\***: Input field.
- Отображаемое имя**: Input field.
- Электронная почта**: Input field.
- Новый пароль\***: A dropdown menu with 'Введите новый пароль' selected.
- Пароль должен содержать\***: A list of requirements:
  - Не менее 8 символов
  - Хоть бы одну цифру
  - Прочие символы
  - Строчные буквы
  - Хоть бы один специальный символ
- Подтвердите пароль\***: A dropdown menu with 'Подтвердите пароль' selected.
- Пользователь должен сменить пароль при следующем входе в систему
- Роли для назначения\***: A search box with 'Поиск...' and a list of roles:
  - ACTIVEROLE
  - ACTIVEUSER
  - argent
  - argentFour
  - argentStd

Buttons for 'Отмена' and 'Создать' are located in the top right corner.

Рис.5

Редактирование пользователя:

- Выберите пользователя из списка и щелкните по его имени, чтобы открыть страницу редактирования.
- Можно изменить данные пользователя (кроме имени), включая его роли и требование сброса пароля.

Удаление пользователя:

- Для удаления пользователя отметьте его в списке и нажмите **"Удалить"**. Обратите внимание, что удаление пользователя может быть необратимым.

Сброс пароля:

- Администраторы могут инициировать сброс пароля для любого пользователя, установив флаг "Сброс пароля" на "Yes". Пользователю придется задать новый пароль при следующем входе.

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

## Роли

В этом подразделе (рис.6) отображаются все роли, которые назначены пользователям системы с указанием количества пользователей, которым они принадлежат.

### Управление доступом

Идентификатор роли	Название роли	Группы Active Directory	Пользователи
activeole	ACTIVEROLE		10
activeuser	ACTIVEUSER		7
argent	argentf		4
argentfourth	argentfour		12
argentsf	argent		2
argentssecond	argentssecond		14
argentsthird	argentsthird		12
ascan	ascan		0
asocadm	ASOC Administrator		195
asocthns	ASOC-397		1

Рис.6

Поля таблицы:

- 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.

## Добавление роли

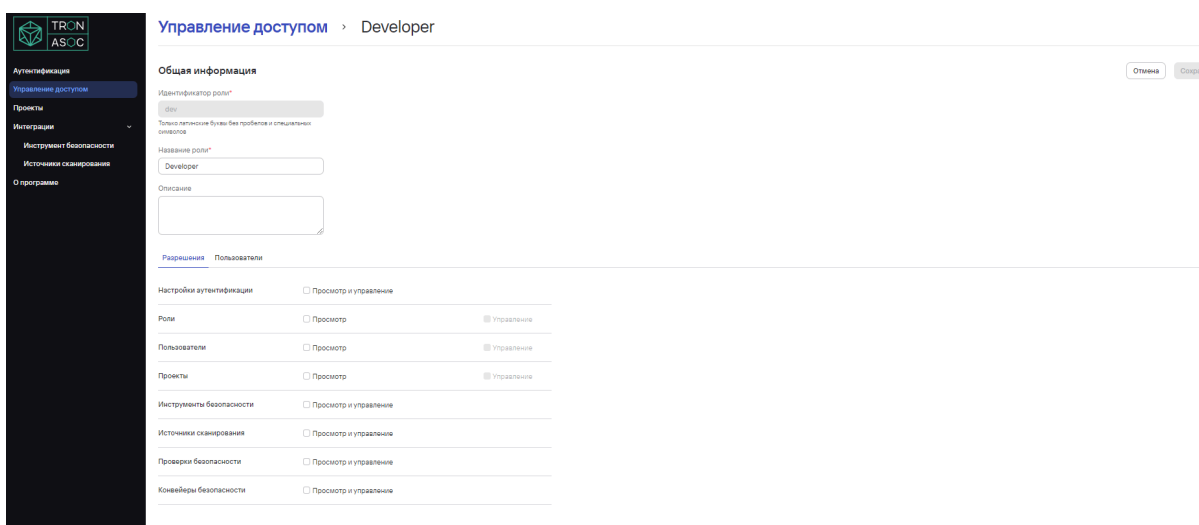


Рис.7

Чтобы добавить роль, введите уникальный идентификатор и название роли, добавьте описание. Используя список разрешений, настройте доступ к каждому разделу:

- Отметьте чекбокс **Просмотр**, если необходимо предоставить только доступ на чтение.
- Отметьте **Управление**, если нужно разрешить редактирование и управление в разделе.

После завершения настройки нажмите “Создать”, чтобы сохранить новую роль.

## Инструменты безопасности

Просмотр всех доступных подключенных инструментов безопасности производится в разделе Интеграции - Инструмент безопасности. Здесь можно увидеть название инструмента, описание (с возможностью сортировки по этим полям), а также перейти к удалению и редактированию инструмента.

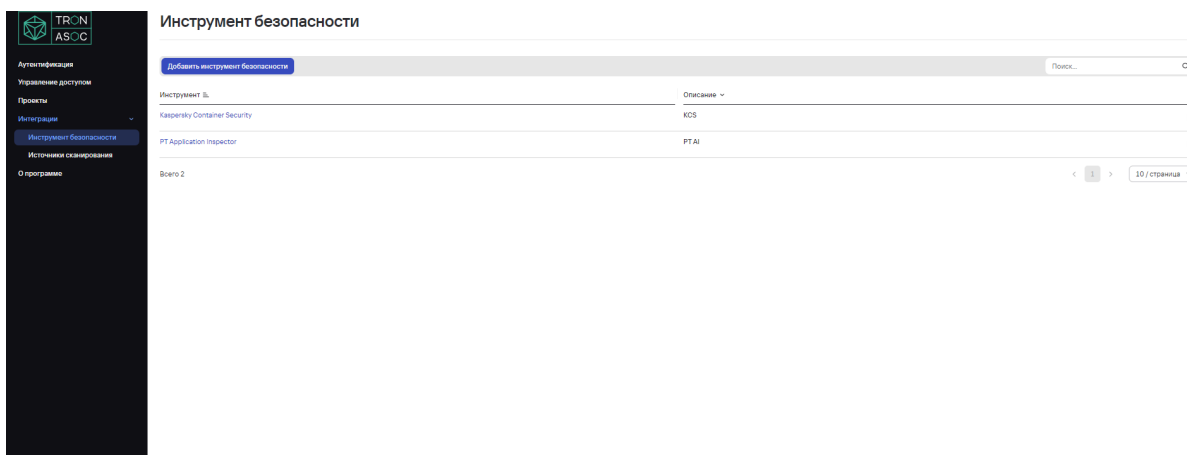


Рис. 8

## Подключение инструментов безопасности

Чтобы добавить новый Инструмент безопасности, перейдите в раздел Интеграции - Инструменты безопасности и нажмите кнопку Добавить инструмент безопасности.

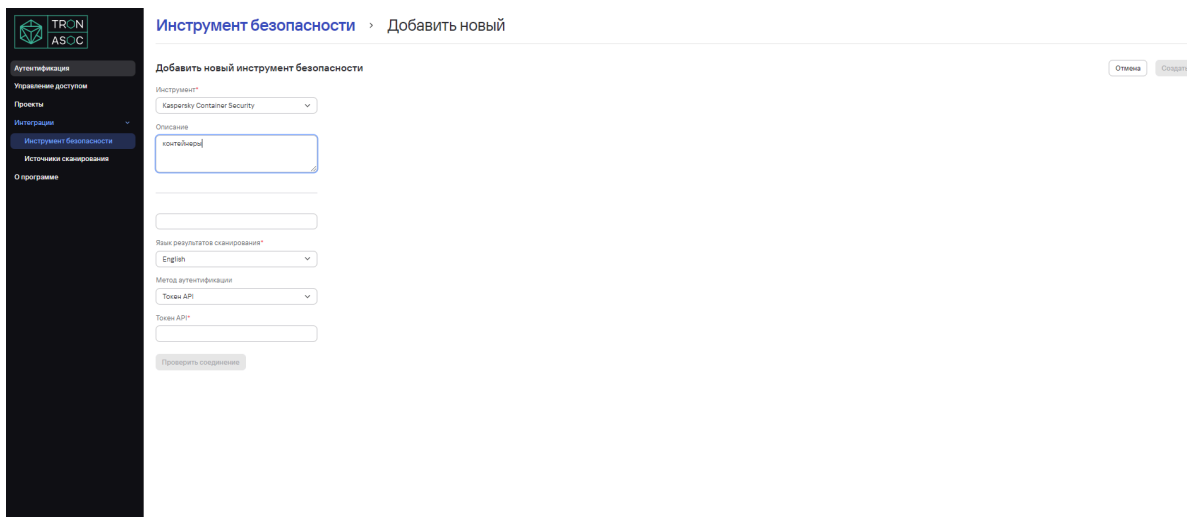


Рис.9

В форме добавления инструмента (рис.9) в раскрывающемся меню поля Инструмент безопасности выберите инструмент, добавьте описание инструмента и URL, выберите 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/Пароль”. Чтобы сделать проверку соединения, нажмите Проверить соединение. Система отправит запрос на соединение с инструментом и в верхнем правом углу пользовательского интерфейса отобразится соответствующее уведомление.

Для завершения добавления инструмента нажмите кнопку “Создать”.

## Редактирование инструмента

Редактирование инструмента производится по клику на Инструмент в списке Инструментов безопасности. Форма редактирования аналогична форме добавления, но имеет все поля предзаполненными.

The screenshot shows the 'Edit Security Instrument' form in the TRON.ASOC interface. The form is titled 'Редактирование инструмента безопасности' and is for the instrument 'Kaspersky Container Security'. The fields are pre-filled with the following information:

- Instrument: Kaspersky Container Security
- Description: KCS
- URL: https://kcs.nt.kimi.group/api/v1
- Scan Results Language: English
- Authentication Method: Токен API
- API Token: kcs\_65422ha4q27g4h5h

A 'Проверить соединение' (Check Connection) button is located at the bottom of the form. The interface also shows a sidebar with navigation options and a breadcrumb trail: 'Инструмент безопасности > Kaspersky Container Security'.

Рис.10



## Удаление инструмента

Удаление инструмента сканирования производится на странице списка Инструменты безопасности по нажатию на иконку действий в конце строки у инструмента, который нужно удалить.

## Источники сканирования

Просмотр всех доступных подключенных источников сканирования производится в разделе Интеграции - Источники сканирования. Можно отсортировать по названию, типу источника, описанию, перейти к редактированию или удалению.

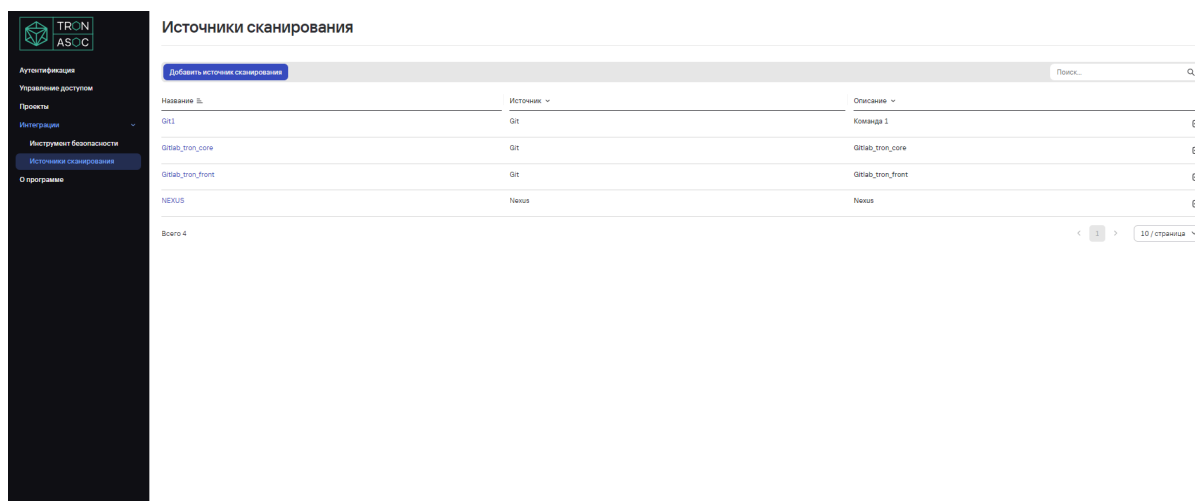


Рис. 11

## Подключение источника сканирования

Чтобы подключить источник сканирования, перейдите в раздел Интеграции- Источники сканирования и нажмите кнопку Add Scan source. В форме добавления источника сканирования (Рис. 13) задайте имя инструмента, описание, в раскрывающемся меню поля Источник выберите источник сканирования (доступные: Git-репозитории, Nexus).

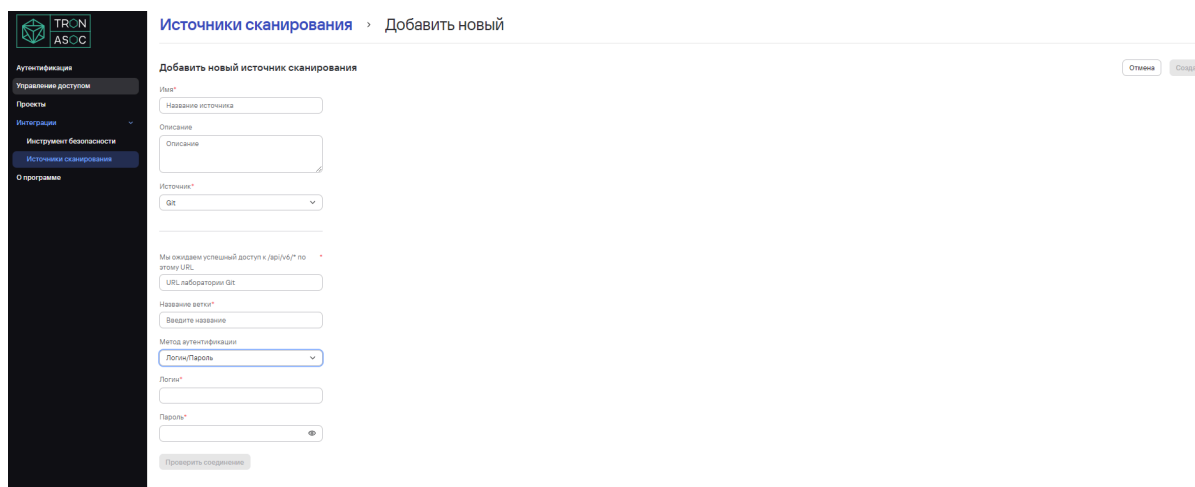
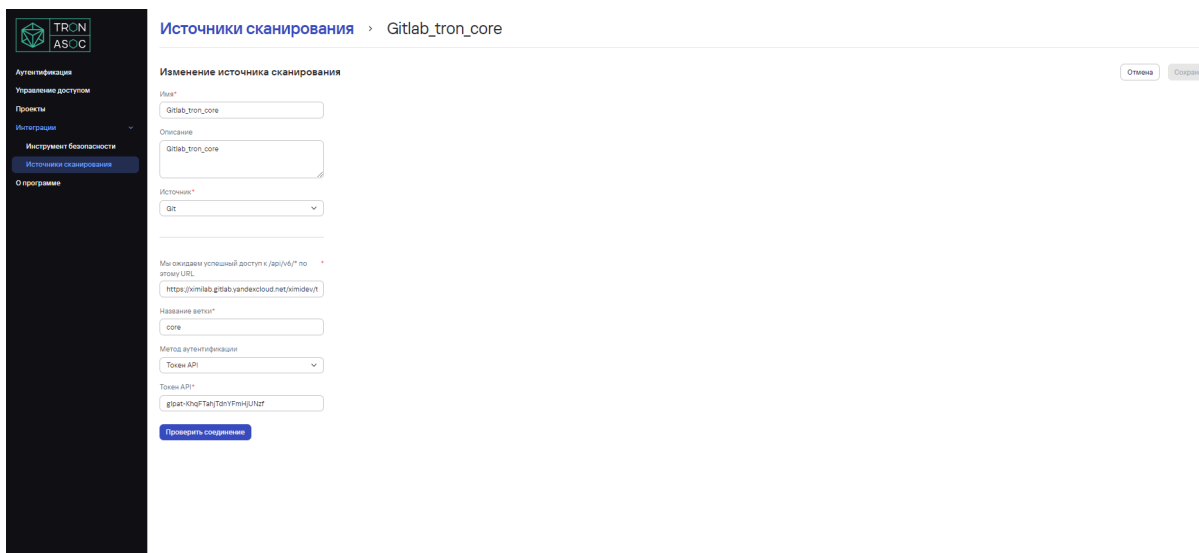


Рис. 12

После выбора типа инструмента появятся дополнительные поля, специфичные выбранному на предыдущем шаге инструменту. Заполните URL инструмента. Заполнение поля Метод аутентификации на этом этапе не является обязательным, но без него нельзя будет осуществить проверку соединения с источником сканирования. Поля для заполнения далее могут отличаться в зависимости от выбора метода аутентификации. Если метод указан и выбрана аутентификация по API - токenu, нужно заполнить поле Токен API, если выбран метод аутентификации по логину и паролю, нужно заполнить поля Логин/Пароль. Чтобы сделать проверку соединения, нажмите Проверить соединение. Система отправит запрос на соединение с источником и в верхнем правом углу пользовательского интерфейса отобразится соответствующее уведомление.

## Редактирование источника сканирования

Редактирование источника производится по клику на название источника в списке Источники сканирования. Форма редактирования аналогична форме добавления, но имеет все поля предзаполненными.



The screenshot shows the TRON.ASOC administrative interface. On the left is a dark sidebar with navigation options: Аутентификация, Управление доступом, Проекты, Интеграция, Инструмент безопасности, Источники сканирования (highlighted), and О программе. The main content area is titled 'Источники сканирования > Gitlab\_tron\_core'. Below this is a form titled 'Изменение источника сканирования'. The form contains the following fields: 'Имя\*' (filled with 'Gitlab\_tron\_core'), 'Описание' (filled with 'Gitlab\_tron\_core'), 'Источник\*' (dropdown menu with 'Git' selected), a message 'Мы ожидаем успешной доступ к URL (\*) по этому URL' followed by 'https://kmlab.gitlab.yandexcloud.net/vimidev/', 'Название ветки\*' (filled with 'core'), 'Метод аутентификации' (dropdown menu with 'Токен API' selected), and 'Токен API\*' (filled with 'g5ak-khp7TalyYFmKJzlf'). At the bottom of the form is a blue button labeled 'Проверить Соединение'. In the top right corner of the form area are two buttons: 'Отмена' and 'Сохранить'.

Рис. 13

## Удаление источника сканирования

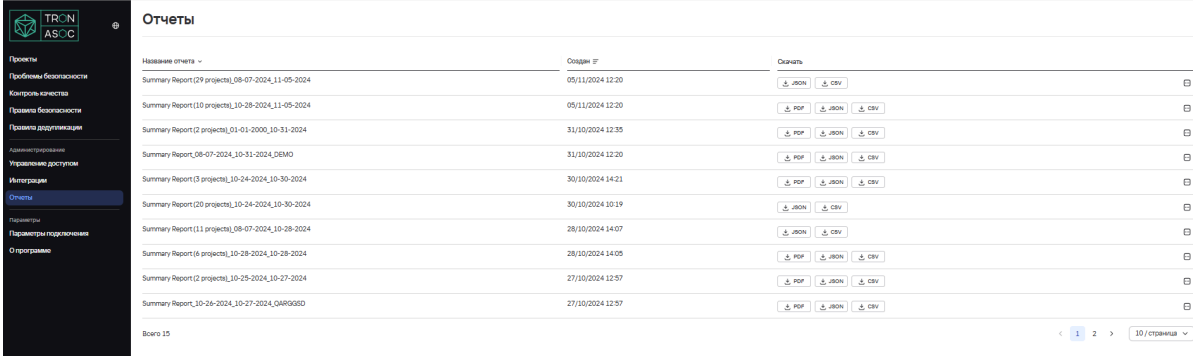
Чтобы удалить источник сканирования, перейдите в раздел Интеграции - Источники сканирования, нажмите на кнопку с тремя точками в строке нужного источника и выберите "Удалить".

# Отчеты

Страница "Отчеты" предназначена для управления и просмотра отчетов, содержащих данные о проектах и найденных в них уязвимостях. Все отчеты отображаются в таблице, где можно увидеть основную информацию и дату создания. Чтобы отсортировать отчеты по названию или дате создания, щелкните на заголовок соответствующего столбца. Для каждого отчета доступны три формата скачивания: PDF (до трех проектов в одном отчете), JSON и CSV.

Нажмите на соответствующую кнопку рядом с отчетом, чтобы загрузить его в нужном формате.

Чтобы удалить отчет, нажмите на кнопку с тремя точками в строке нужного отчета и выберите "Удалить".



Название отчета	Создан	Скачать
Summary Report (29 projects)_08-07-2024_11-05-2024	05/11/2024 12:20	<a href="#">PDF</a> <a href="#">JSON</a> <a href="#">CSV</a>
Summary Report (10 projects)_10-28-2024_11-05-2024	05/11/2024 12:20	<a href="#">PDF</a> <a href="#">JSON</a> <a href="#">CSV</a>
Summary Report (2 projects)_01-01-2000_10-31-2024	31/10/2024 12:35	<a href="#">PDF</a> <a href="#">JSON</a> <a href="#">CSV</a>
Summary Report_08-07-2024_10-31-2024_DEMO	31/10/2024 12:20	<a href="#">PDF</a> <a href="#">JSON</a> <a href="#">CSV</a>
Summary Report (3 projects)_10-24-2024_10-30-2024	30/10/2024 14:21	<a href="#">PDF</a> <a href="#">JSON</a> <a href="#">CSV</a>
Summary Report (20 projects)_10-24-2024_10-30-2024	30/10/2024 10:19	<a href="#">PDF</a> <a href="#">JSON</a> <a href="#">CSV</a>
Summary Report (11 projects)_08-07-2024_10-28-2024	28/10/2024 14:07	<a href="#">PDF</a> <a href="#">JSON</a> <a href="#">CSV</a>
Summary Report (6 projects)_10-28-2024_10-28-2024	28/10/2024 14:05	<a href="#">PDF</a> <a href="#">JSON</a> <a href="#">CSV</a>
Summary Report (2 projects)_10-25-2024_10-27-2024	27/10/2024 12:57	<a href="#">PDF</a> <a href="#">JSON</a> <a href="#">CSV</a>
Summary Report_10-28-2024_10-27-2024_OAR96SD	27/10/2024 12:57	<a href="#">PDF</a> <a href="#">JSON</a> <a href="#">CSV</a>