Платформа для управления уязвимостями и обеспечения безопасности в процессах разработки и DevSecOps “Tron ASOC v.0.5”

Руководство администратора

Июнь 2024

Содержание

Термины и определения

БДУ	Банк данных угроз безопасности информации
ПО	Программное обеспечение
Уязвимость (Vulnerability)	Уязвимость программного обеспечения — это сбой, изъян или слабое место в программном обеспечении, которое может быть использовано для нарушения функциональности или несанкционированного доступа к ресурсам приложения
ФСТЭК	Федеральная служба по техническому и экспортному контролю
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.
CI/CD	комбинация непрерывной интеграции (continuous integration) и непрерывного развертывания (continuous delivery или continuous deployment) программного обеспечения в процессе разработки. CI/CD объединяет разработку, тестирование и развертывание приложения.
CVE	Common Vulnerabilities and Exposures - база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер, описание и ряд общедоступных ссылок с описанием.
DevSecOps	методология разработки программного обеспечения, которая интегрирует практики безопасности (Sec) в процессы разработки и поставки программного обеспечения (DevOps).
NVD	National Vulnerability Database - национальная база данных уязвимостей. Американский правительственный репозиторий данных управления уязвимостями на основе стандартов, представленных с использованием протокола автоматизации содержимого безопасности.

PCI SSC	PCI Security Standards Council - открытое глобальное сообщество, задачи которого включают непрерывное развитие, совершенствование, хранение, распространение и внедрение стандартов безопасности для защиты данных платежных карт.
Pipeline	сочетание заданий для непрерывной доставки программного обеспечения, состоит из нескольких состояний или этапов, которые выполняются в последовательности один за другим.
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
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.

Общие сведения

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

«TRON.ASOC» позволяет осуществлять всесторонний контроль безопасности разрабатываемых проектов, обеспечивая надежную защиту на всех этапах разработки.

«TRON.ASOC» интегрируется с репозиторием Gitlab, реестром образов Nexus и различными инструментами анализа безопасности разрабатываемых продуктов, такими как статический анализатор исходного кода PT Application Inspector и анализатор безопасности контейнеров KCS. Программа управляет проверками исходного кода и образов контейнеров на уязвимости и помогает управлять результатами этих проверок. Интеграция с этими инструментами позволяет настроить сканирование, запускать проверки и консолидировать результаты.

«TRON.ASOC» упрощает работу с найденными при помощи инструментов AST проблемами и уязвимостями, проводя их анализ и группировку для более эффективного управления.

«TRON.ASOC» осуществляет консолидацию и визуализацию данных, предоставляя пользователям наглядную информацию о состоянии безопасности их проектов.

«TRON.ASOC» предлагает удобный пользовательский интерфейс, доступный в современных браузерах на движке Chromium (Google Chrome, Яндекс Браузер, Edge, Safari и т.д.) и Firefox.

«TRON.ASOC» предоставляет возможности для управления сканированиями, включая настройку параметров сканирования, планирование запусков и мониторинг выполнения сканирований.

«TRON.ASOC» позволяет выгружать отчеты по результатам сканирований в формате JSON, что обеспечивает удобство интеграции с другими системами и инструментами анализа данных.

.

Начало работы в системе

В браузере перейдите по адресу URL платформы ASOC. 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.

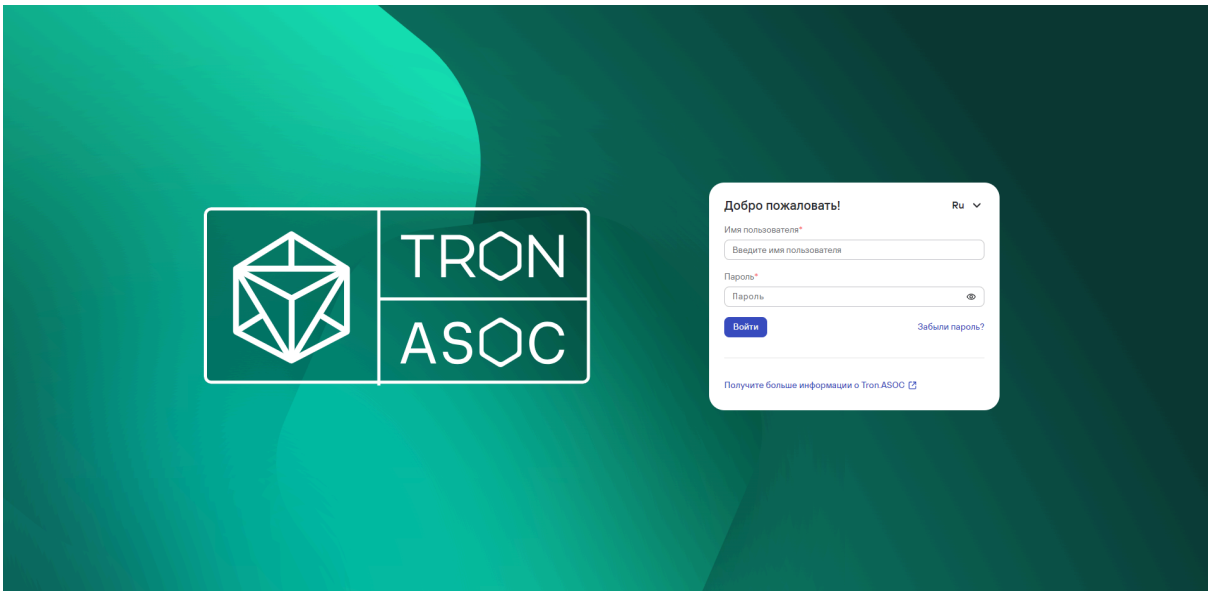

Рис.1

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.

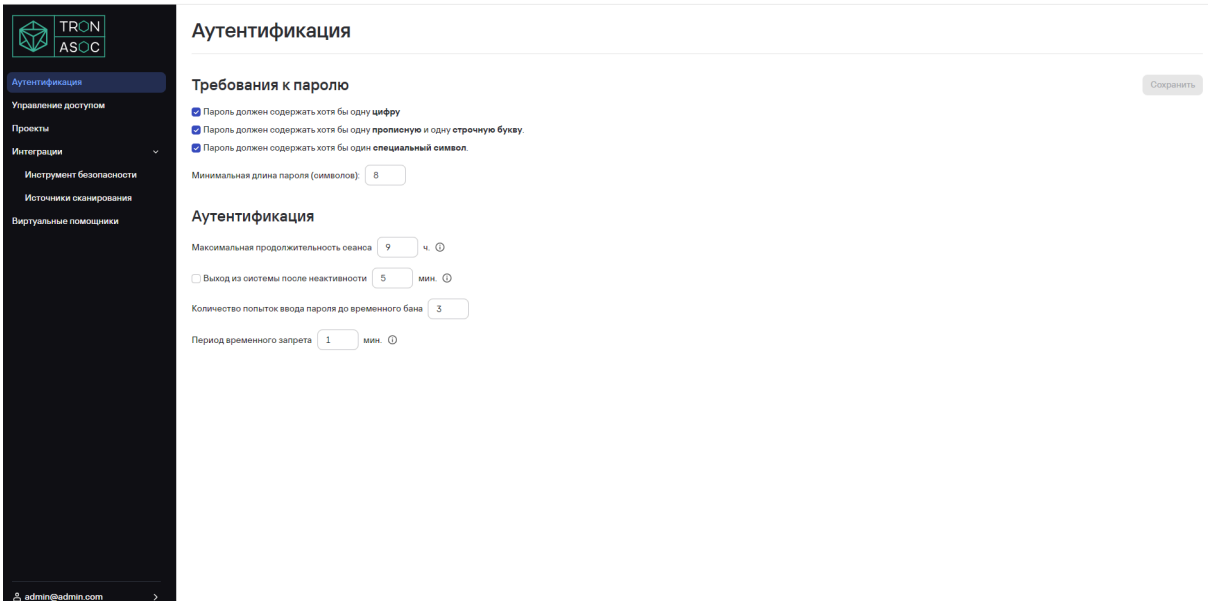

Рис.2

Управление пользователями и ролями

Управление пользователями и ролями происходит в разделе Управление доступом. Переход к разделу осуществляется из левого сайд-бар меню.

Роли

Информация о ролях в системе отображается в разделе Управление доступом на вкладке Роли (рис.3). Здесь также доступен поиск по роли, возможность просмотреть количество пользователей с определенной ролью, сортировка ролей по идентификатору, имени роли и количеству пользователей.

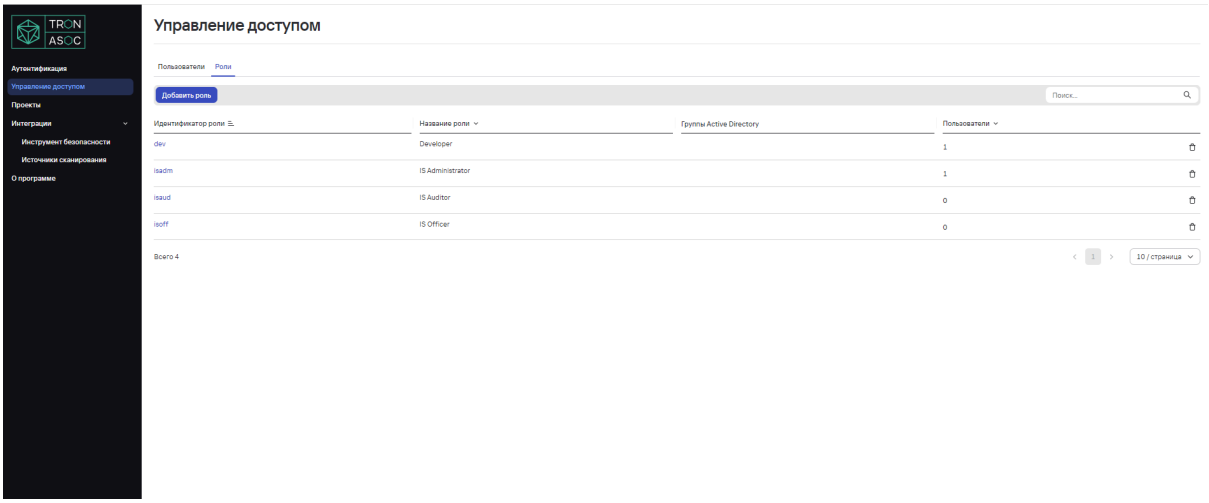

Рис.3

Добавление роли

Добавление роли (Рис.4) производится из раздела Управление доступом, вкладка Роли. Для создания новой роли нажмите кнопку Добавить роль.

На странице создания роли заполните общую информацию: идентификатор роли имя роли, описание. Обязательные для заполнения поля отмечены звездочкой.
Отметьте доступные роли разрешения на просмотр или управление разделами системы. Чекбокс Управление для назначения прав на управление разделом становится активным только после выбора чекбокса Просмотр на право просмотра соответствующего раздела.

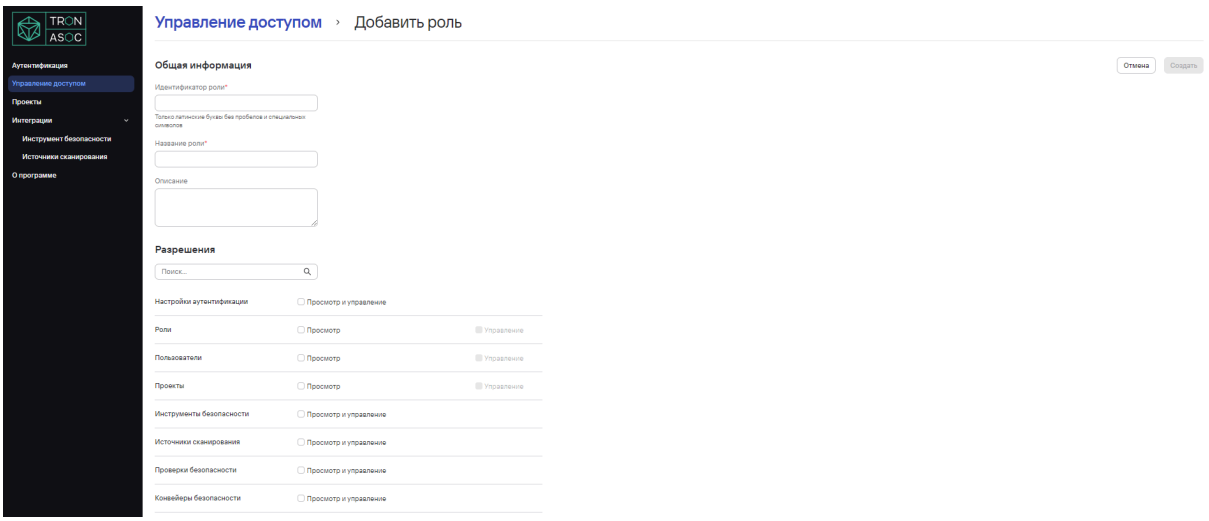

Рис.4

Изменение роли

Чтобы отредактировать роль, нажмите на идентификатор роли в списке ролей на вкладке Роли. Форма редактирования аналогична форме создания роли, за исключением поля Идентификатор роли, которое является недоступным для редактирования.

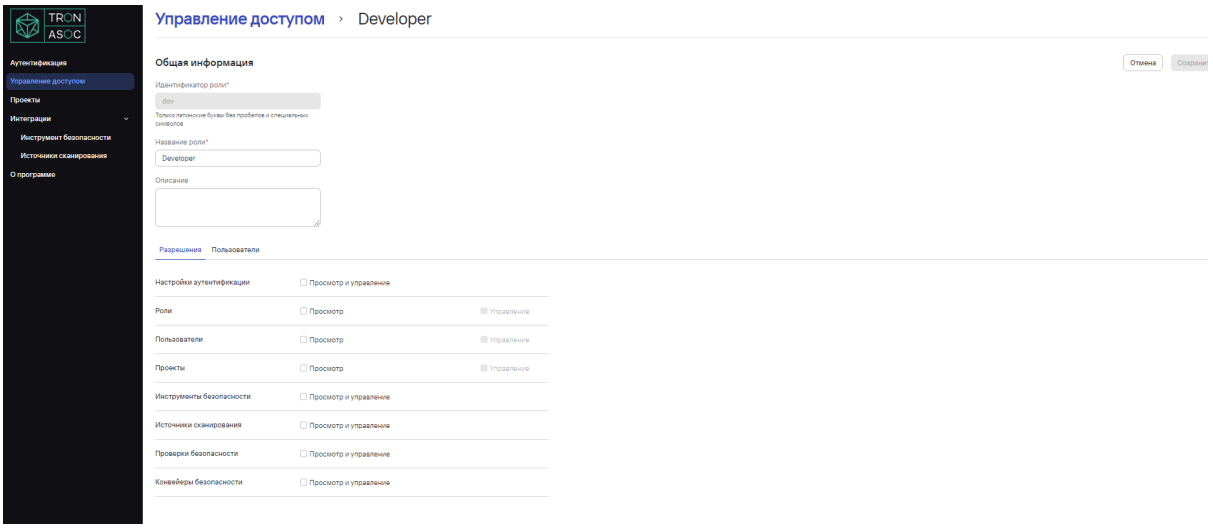

Рис.5

Пользователи

Информация о пользователях системы отображается в разделе Управление доступом на вкладке Пользователи (Рис. 5). Здесь также доступен поиск , возможность просмотреть назначенные пользователю роли, назначение принудительной смены пароля и удаление пользователя

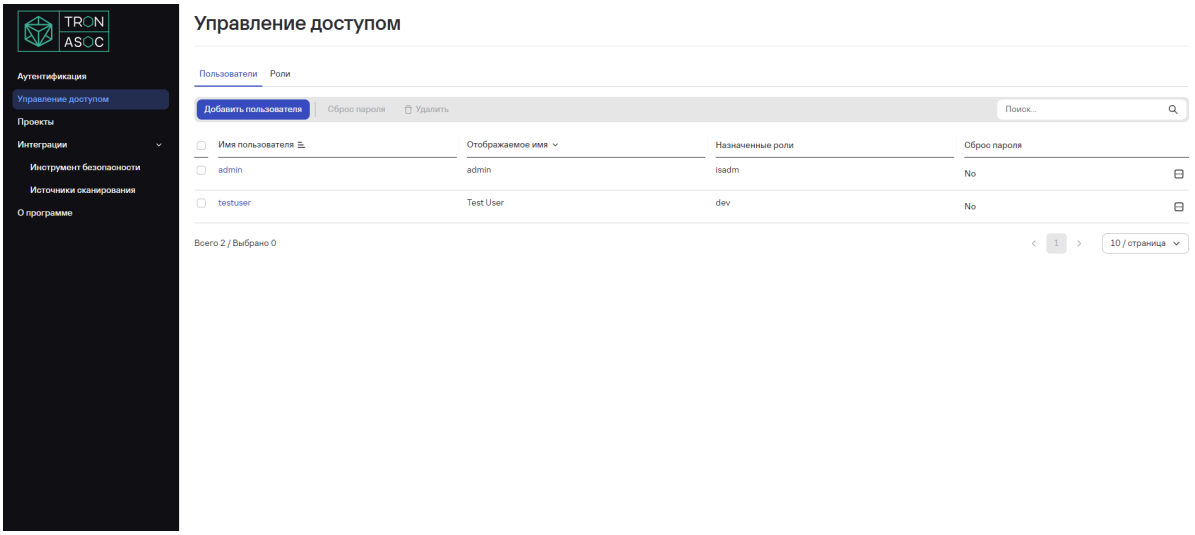

Рис.6

Добавление пользователя

Чтобы создать нового пользователя, нажмите на кнопку Добавить пользователя на вкладке Пользователи. На странице создания пользователя заполните общую информацию: имя пользователя, отображаемое имя, электронную почту, а также введите и подтвердите пароль доступа.Обязательные для заполнения поля отмечены звездочкой. Опционально можно выбрать чекбокс принудительной смены пароля, чтобы пользователь сменил пароль при следующем входе в систему. Выберите как минимум одну роль для назначения пользователю и нажмите кнопку Создать.

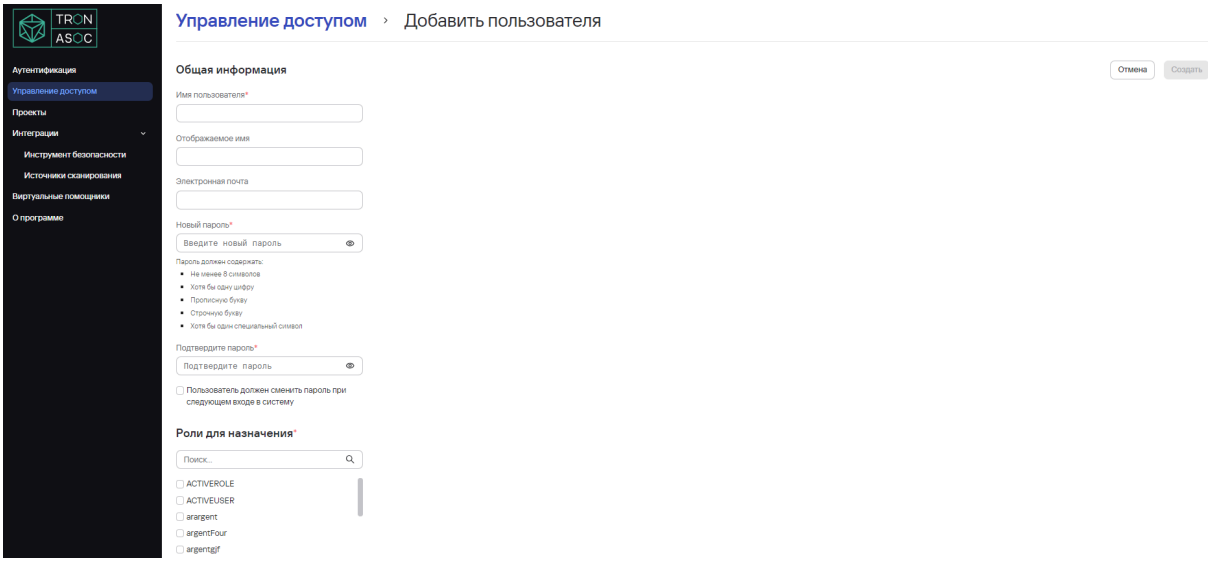

Рис.6

Редактирование профиля пользователя

Чтобы отредактировать данные пользователя, нажмите на Имя пользователя в списке пользователей на вкладке Пользователи. Форма редактирования аналогична форме создания пользователя, за исключением поля Имя пользователя, которое является недоступным для редактирования.

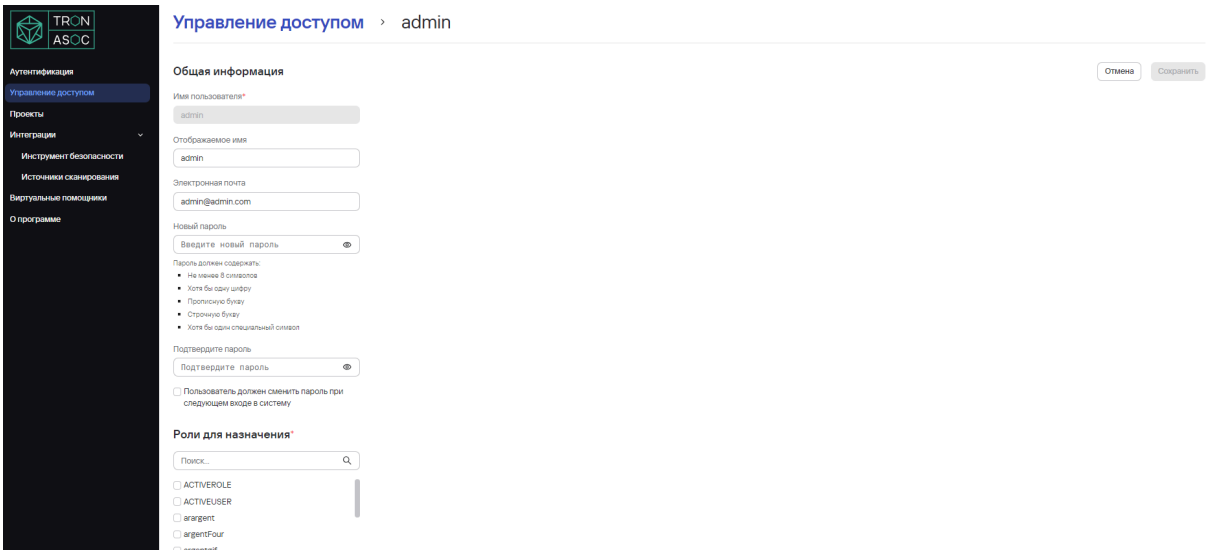

Рис.7

Изменение пароля пользователя и профиль пользователя

Администратор может отметить чекбокс принудительной смены пароля. Пользователь при своем следующем входе получает форму для смены пароля. Смена пароля может производиться пользователем в профиле.

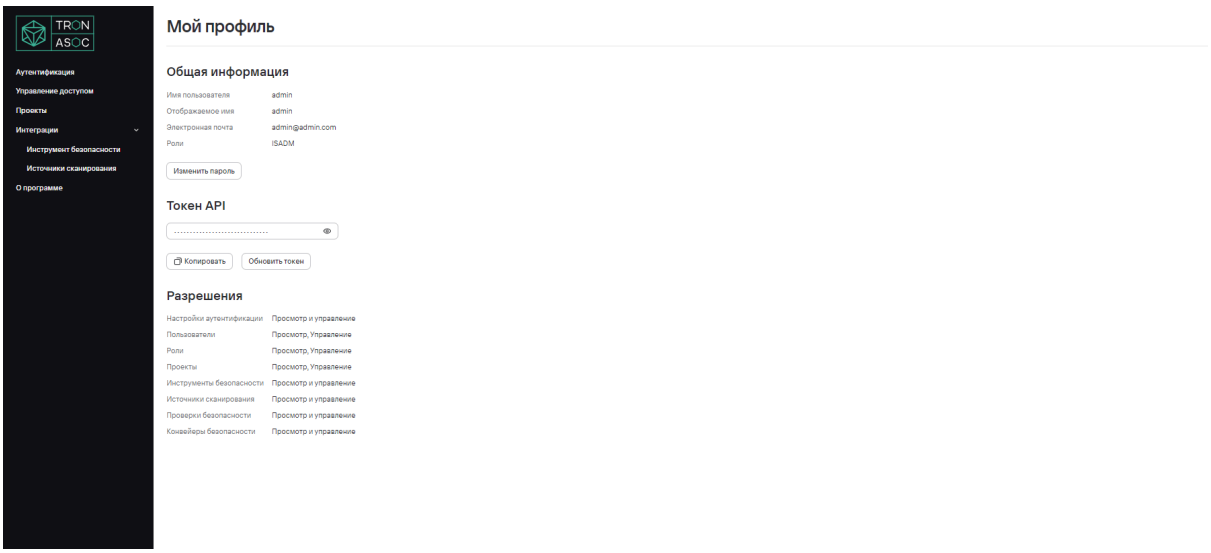

Рис.8

Настройка интеграций с инструментами

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.

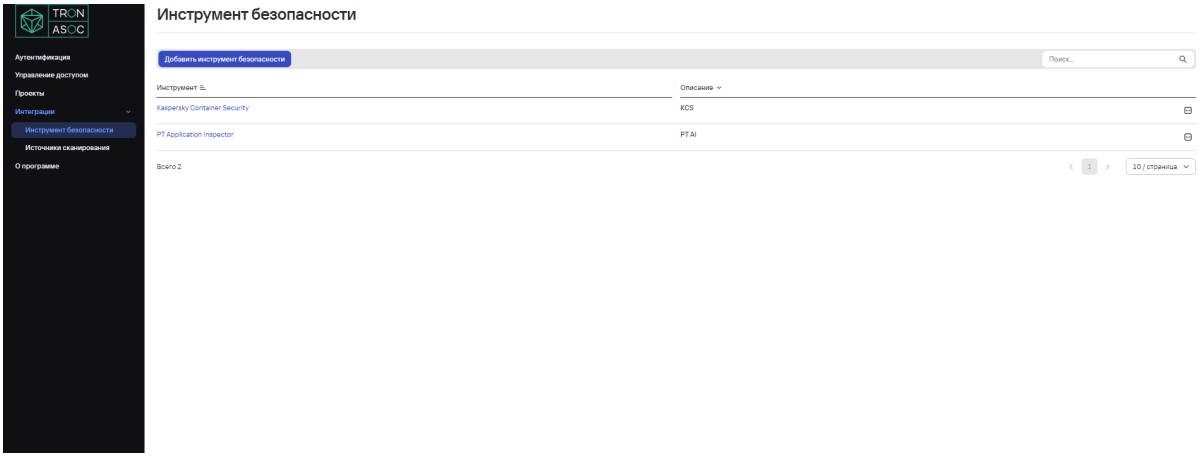

Рис. 9

Подключение инструментов безопасности

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

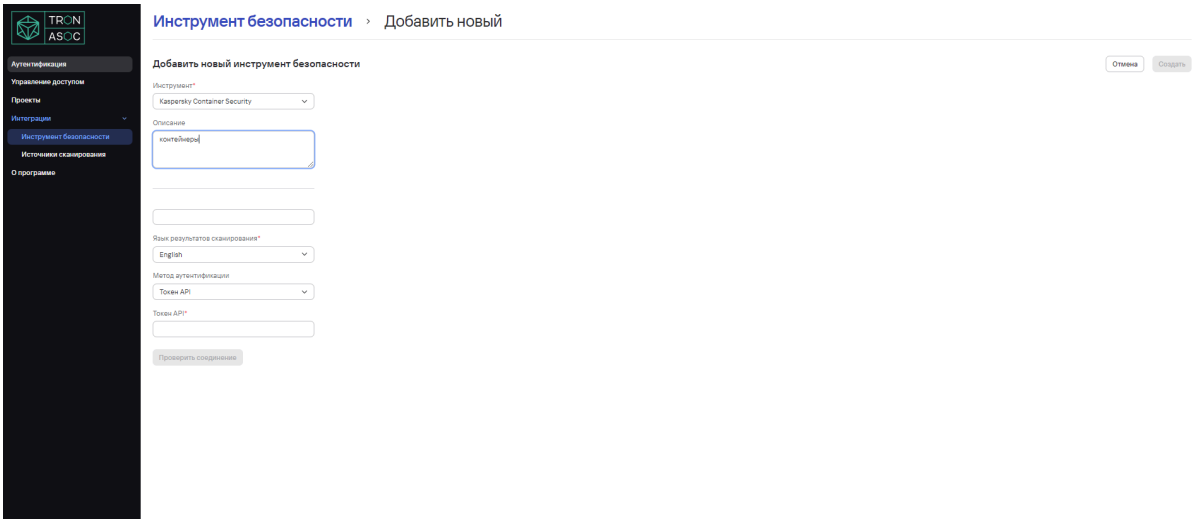

Рис.10

В форме добавления инструмента (Рис.10) в раскрывающемся меню поля Инструмент безопасности выберите инструмент (для выбора доступны: PT Application Inspector, Kaspersky Container Security), 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 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 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.

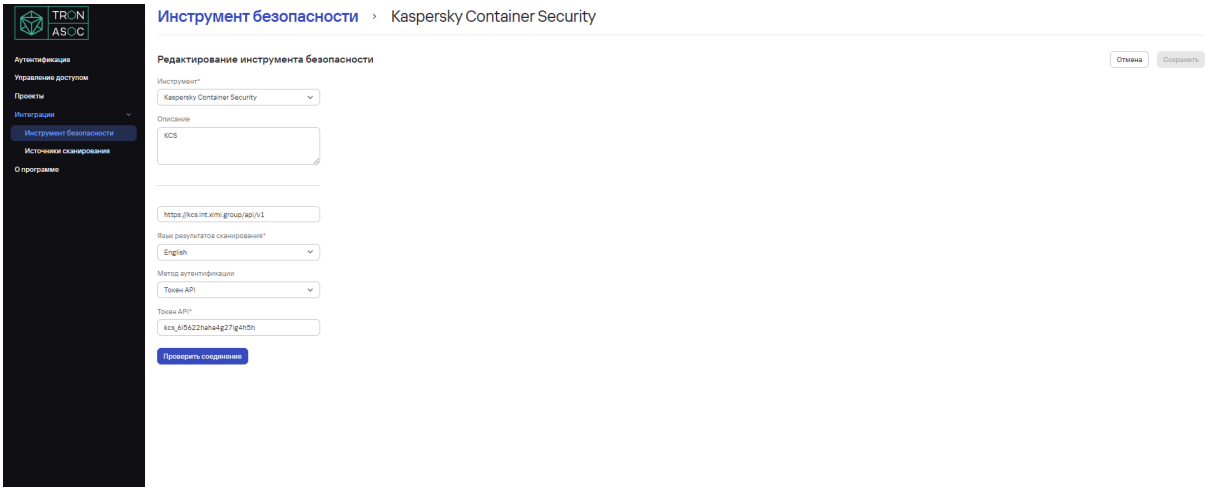

Рис.10

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.

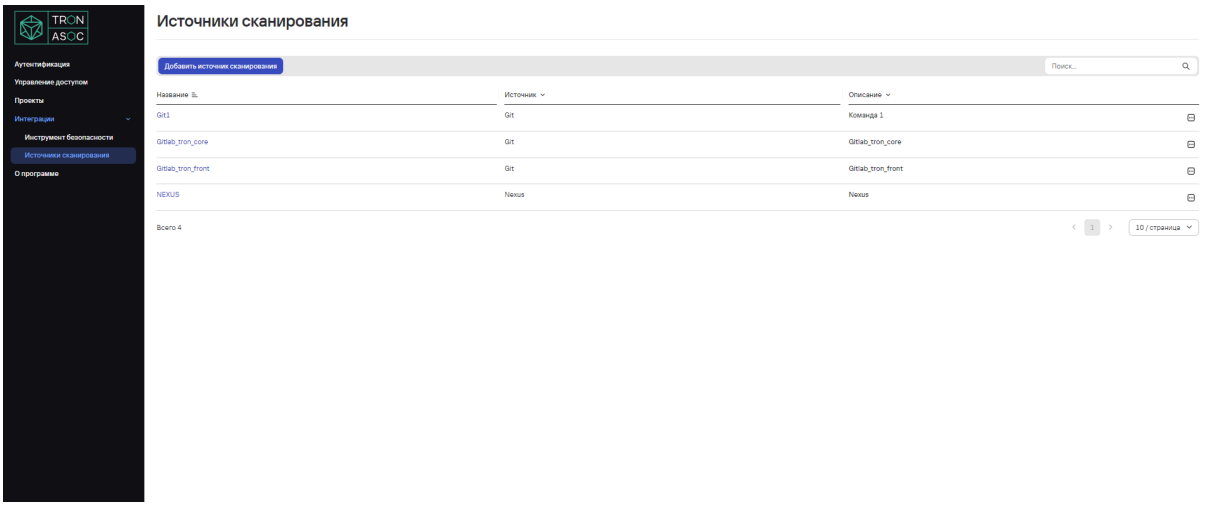

Рис.11

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.12) задайте имя инструмента, описание, в раскрывающемся меню поля Источник выберите источник сканирования (доступные: Gitlab, Nexus Repository).

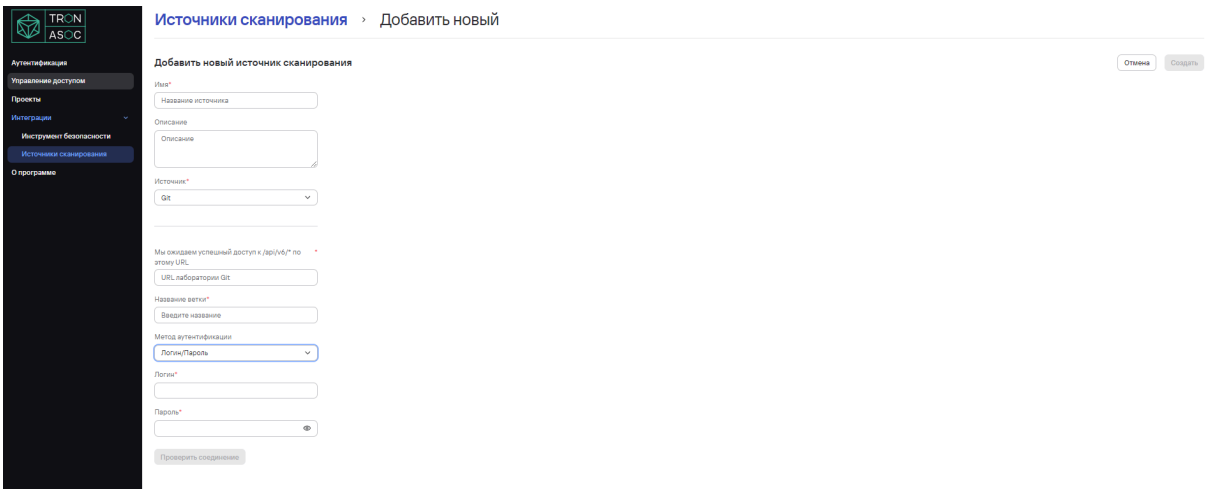

Рис.12

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 - токену, 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 Источников сканирования. Форма редактирования аналогична форме добавления, но имеет все поля предзаполненными.

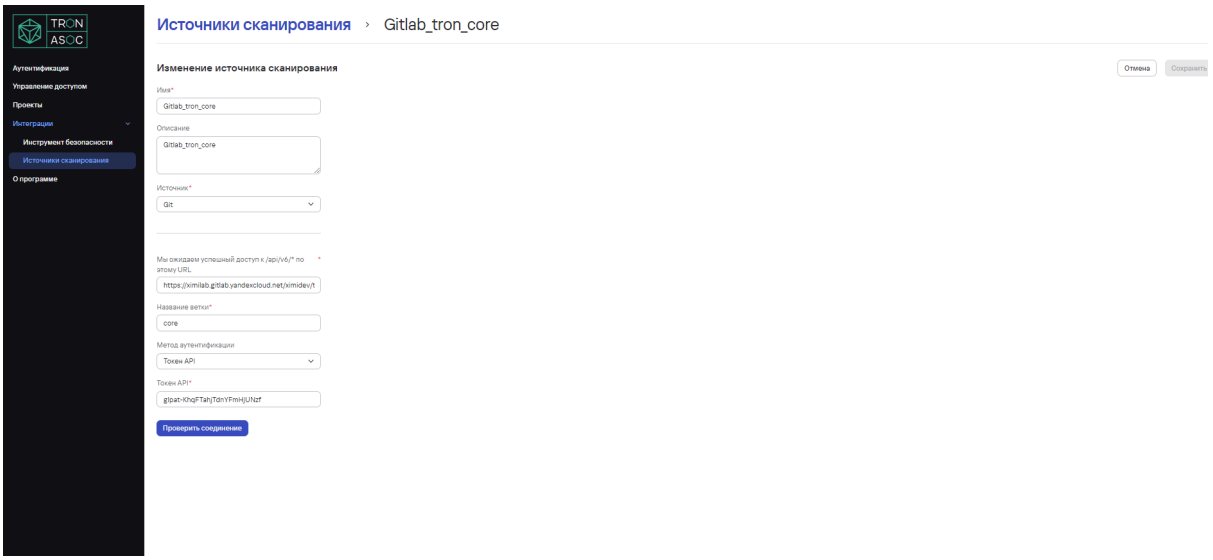

Рис. 13

Удаление источника сканирования

Чтобы удалить источник сканирования, перейдите в раздел Интеграции - Источники сканирования и нажмите на иконку удаления в конце строки источника, который нужно удалить.