

Φ-APISEC

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

SΦUAD

www.squadsec.ru

- ⊕ [Введение](#)
- ⊕ [Интерфейс пользователя](#)
 - [Начало работы](#)
 - [Панель мониторинга](#)
 - [События](#)
 - [Переход на страницу «Исключения анализаторов»](#)
 - [Отчёты](#)
 - [Язык запросов](#)
 - [Создание нового отчёта](#)
 - [Просмотр и экспорт результатов](#)
- ⊕ [Инвентаризация](#)
 - [Объединение и обновление эндпоинтов](#)
 - [Термины](#)
 - [Правила объединения](#)
 - [Механизм образования шаблона STRING](#)
 - [Мгновенная шаблонизация](#)
 - [Шаблонизация с задержкой во времени](#)
 - [Механизм образования шаблона INTEGER](#)
 - [Механизм образования шаблона FLOAT](#)
 - [Объединение эндпоинтов, у которых уже есть шаблон в URL](#)
 - [Объединение эндпоинтов, добавленных вручную](#)
 - [Правила обновления](#)
 - [Роуты](#)
 - [Список роутов](#)
 - [Метрики](#)
 - [Здоровье](#)
 - [Эндпоинты](#)
 - [Список эндпоинтов](#)
 - [Поля таблицы:](#)
 - [Метод](#)
 - [Типы авторизации](#)
 - [Тип доступа](#)
 - [Тип запроса](#)
 - [Фильтрация эндпоинтов](#)
 - [Детали эндпоинта](#)
 - [Вкладка Общее](#)
 - [Редактирование эндпоинта](#)
 - [Вкладка Параметры](#)
 - [Вкладка События](#)
 - [Вкладка Статистика](#)
 - [Добавление нового эндпоинта](#)
 - [Экспорт сваггер схемы](#)
 - [Импорт сваггер схемы](#)
 - [Черный список](#)
- ⊕ [Конфигурация \(для работы без сервиса git\)](#)
 - [Настройки:](#)
 - [Раздел «Envoy alsc»](#)
 - [Заголовки для поиска IP-адресов](#)
 - [Роуты](#)
 - [Сигнатурный анализатор](#)
 - [Сваггер анализатор](#)
 - [Статический анализатор](#)

- [Классификатор](#)
- [Раздел Request-logger](#)
 - [Маскирование данных](#)
 - [Ограничение хранения событий](#)
 - [Оповещения](#)
 - [Инвентаризация](#)
 - [База данных](#)
- ✦ [Управление файлами](#)
 - [Подраздел Конфигураций для добавления Файлов сваггер схем, для добавления и редактирования Файлов сигнатур \(Рисунок 32\)](#)
- ✦ [Пользователи и роли.](#)
 - [Раздел "Пользователи"](#)
 - [Раздел "Роли"](#)
- ✦ [Завершение работы](#)
- ✦ [Сценарии использования](#)
 - [Мониторинг безопасности API](#)
 - [Инвентаризация API и анализ отдельного эндпоинта](#)
 - [Профилирование и мониторинг конкретного API](#)
 - [Анализ событий HTTP-запросов](#)
- ✦ [Контактная информация](#)

Введение

Q-APISec – специальное решение для инвентаризации и защиты API веб-сервисов и веб-приложений.

Q-APISec обладает следующими функциональными возможностями:

- ✦ Инвентаризация используемых API.
- ✦ Выявление забытых и теневых API.
- ✦ Детектирование и блокирование атак OWASP API TOP 10.
- ✦ Детектирование и блокировка атак на основе статистических данных.
- ✦ Классификация данных обрабатываемых API с помощью машинного обучения (персональные данные, карты, финансовая информация, и пр.).
- ✦ Анализ запросов/ответов на соответствие заданной спецификации OpenAPI (Swagger).
- ✦ Построение OpenAPI (Swagger) спецификаций на основании запросов/ответов.
- ✦ Включение/отключение отдельных анализаторов и управление режимом их работы (блокировка/детектирование).
- ✦ Создание собственных правил выявления атак и чувствительных данных (на основе регулярных выражений).
- ✦ Поддержка интеграции с Nginx и Envoy (используются для проксирования запросов).
- ✦ Поддержка установки в kubernetes с istio.
- ✦ Интеграция с SIEM по протоколу syslog

Интерфейс пользователя

Начало работы

Для корректной работы приложения рекомендуется использовать браузер Google Chrome. Если указанные ниже учётные данные не подходят, обратитесь к администратору системы, так как он мог изменить учётные данные в процессе установки и настройки приложения.

Войдите в панель управления Q-APISec: <http://localhost/login> (Рисунок 1).

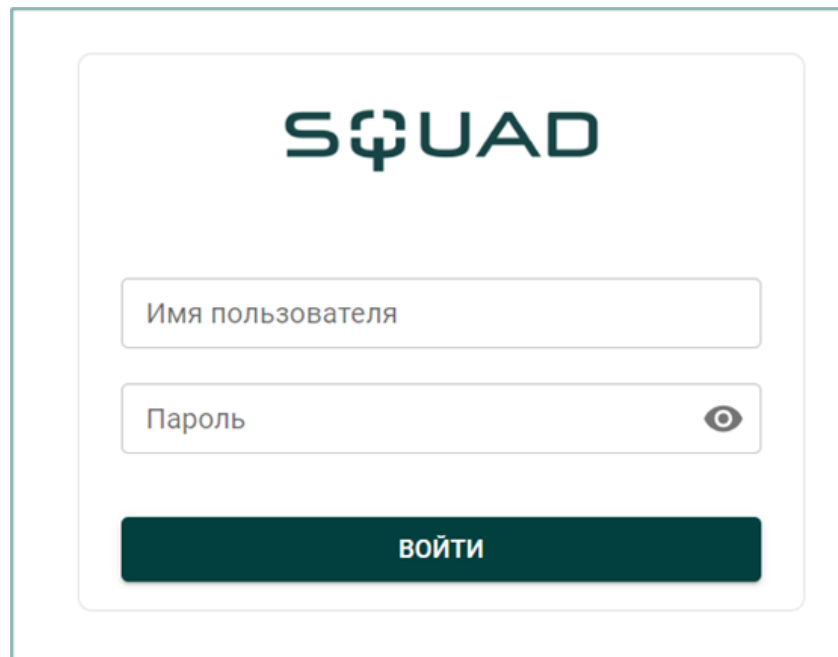


Рисунок 1 – Окно авторизации

При первом использовании программы введите учётные данные по умолчанию:

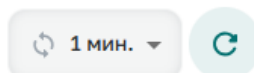
- ⊕ User: usr
- ⊕ Password: pwd

Панель мониторинга

После аутентификации открывается раздел Панель мониторинга:

<https://localhost/dashboard>. На этой странице пользователю представлена основная информация о работе Q-APISec (Рисунок 2).

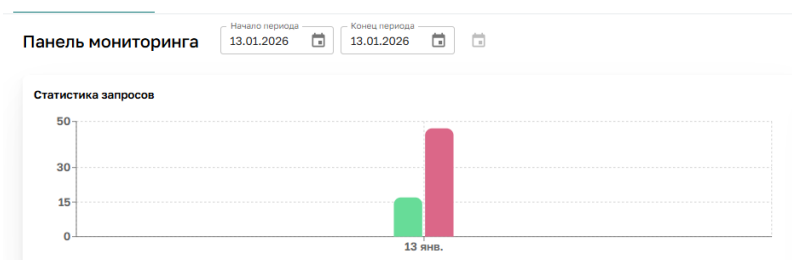
На странице доступно автообновление, кроме этого, данные можно обновить вручную.



На странице панели мониторинга пользователь может задать **начало и конец периода**

анализа данных Начало периода: 15.07.2025 Конец периода: 15.07.2025, за который отображается статистика запросов и событий безопасности.

Рядом с полями выбора периода доступна кнопка **«Сегодня»** . При нажатии на неё автоматически устанавливаются текущие дата начала и дата окончания периода анализа данных.



Выбранный диапазон применяется ко всем графикам и таблицам, включая «Статистику запросов», «Карту вредоносных запросов», «ТОП IP-адресов», «ТОП блокировок» и

«Последние вредоносные запросы» .

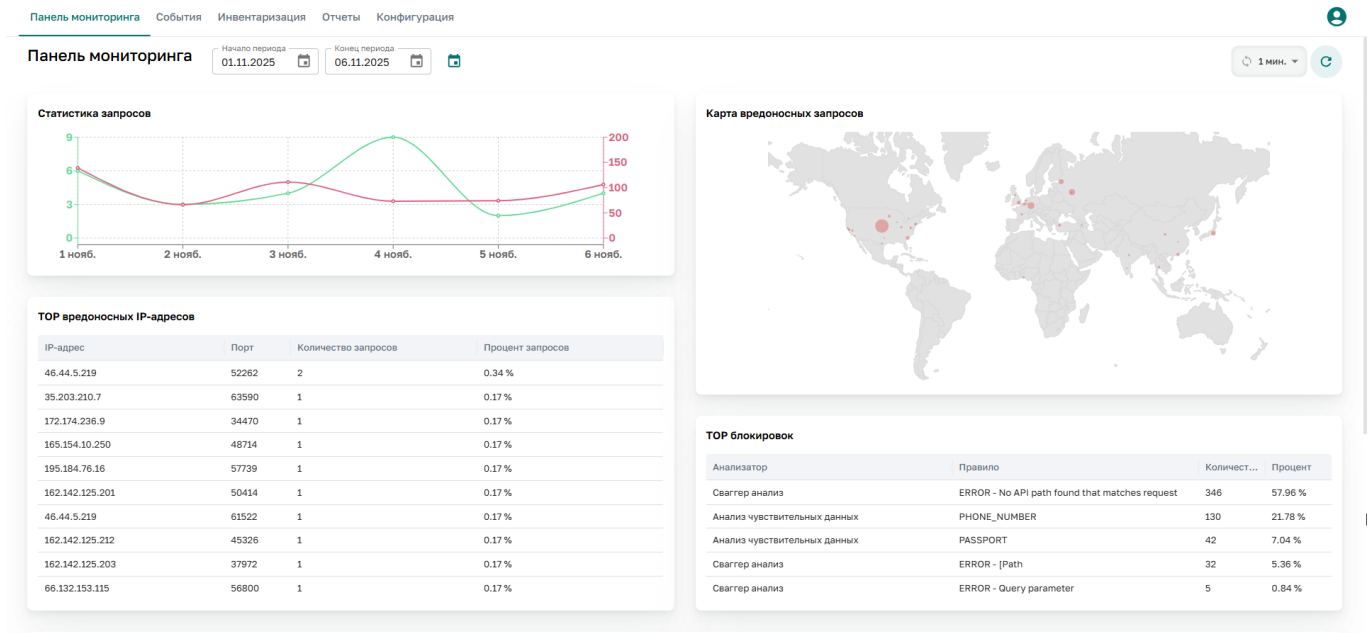


Рисунок 2 – Панель мониторинга

Графики:

- Количество запросов по дням. Зелёная кривая – количество запросов к защищаемым сервисам, для которых не сработал ни один из анализаторов (включая срабатывания на ответы). Красная кривая – количество запросов, где было срабатывание хотя бы одного из анализаторов (включая срабатывания на ответы).
- Карта вредоносных запросов. Карту можно увеличивать и перемещать, используя мышь. Размер пятна на карте качественно характеризует количество вредоносных запросов. Пользователь увидит точные координаты источника угрозы и количество вредоносных запросов, если наведёт мышь на пунсон угрозы.

Таблицы:

- ТОР 10 вредоносных IP-адресов.
- ТОР 5 блокировок.
- Последние вредоносные запросы. При нажатии на событие откроется окно деталей (см. События).

События

Перейдите в раздел События: <https://localhost/events>.

На странице отображается таблица с данными обо всех HTTP-запросах, проходящих через Q-APISec. (Рисунок. 3)

На странице доступно автообновление, кроме этого, данные можно обновить вручную



. Автообновление работает только на первой странице.

События

1 мин. ↻

Начало периода: 25.12.2025 Конец периода: 25.12.2025 🔍 Поиск по id

⬇ Скачать 🔍 Поиск...

IP отправителя	Порт	Хост получателя	Порт	Код ответа	Имя роута	URL	Метод	Дата	Проверки запросов	Проверки ответов	
85.142.100.136	52604	-	-	-	demo-service	/favicon.ico	GET	25.12.2025 17:03:50	Fail	-	>
85.142.100.136	52598	-	-	-	demo-service	/	GET	25.12.2025 17:03:49	Fail	-	>
95.214.55.71	54832	172.17.0.1	13000	200 OK	juice-shop	/	GET	25.12.2025 16:39:28	OK	Fail	>
85.142.100.134	50100	172.17.0.1	6065	200 OK	ecco	/favicon.ico	GET	25.12.2025 16:34:25	OK	OK	>
85.142.100.134	50098	172.17.0.1	6065	200 OK	ecco	/	GET	25.12.2025 16:34:25	OK	OK	>
85.142.100.107	45990	172.17.0.1	5000	404 Not Found	vamp1	/favicon.ico	GET	25.12.2025 16:15:46	Fail	Fail	>
85.142.100.107	45976	172.17.0.1	5000	200 OK	vamp1	/	GET	25.12.2025 16:15:45	OK	OK	>
162.216.149.229	63966	172.17.0.1	7442	502 Bad Gateway	wiremock	/	GET	25.12.2025 16:08:50	OK	OK	>
162.142.125.127	10862	172.17.0.1	6065	200 OK	ecco	/favicon.ico	GET	25.12.2025 16:05:28	OK	OK	>
162.142.125.127	10854	172.17.0.1	6065	200 OK	ecco	/sitemap.xml	GET	25.12.2025 16:05:28	Fail	OK	>
162.142.125.127	40980	172.17.0.1	6065	200 OK	ecco	/favicon.ico	GET	25.12.2025 16:02:17	OK	OK	>
162.142.125.127	55272	172.17.0.1	6065	200 OK	ecco	/	GET	25.12.2025 16:02:08	OK	OK	>
85.142.100.107	47892	-	-	-	demo-service	/favicon.ico	GET	25.12.2025 16:01:43	Fail	-	>
85.142.100.107	47882	-	-	-	demo-service	/	GET	25.12.2025 16:01:42	Fail	-	>
162.142.125.113	24260	172.17.0.1	6065	200 OK	ecco	/favicon.ico	GET	25.12.2025 16:01:39	OK	OK	>
162.142.125.113	49274	172.17.0.1	6065	200 OK	ecco	/well-known/security.txt	GET	25.12.2025 16:01:37	OK	OK	>
104.248.46.210	35328	172.17.0.1	5000	404 Not Found	vamp1	/favicon.ico	GET	25.12.2025 15:40:54	Fail	Fail	>
104.248.46.210	35322	172.17.0.1	5000	200 OK	vamp1	/	GET	25.12.2025 15:40:54	OK	OK	>

Рисунок 3 – Общий вид страницы События

Поиск по событиям

В верхней части страницы «События» доступно поле поиска, (Рис 3.1) позволяющее выполнять фильтрацию данных по ключевым словам. Поиск осуществляется по содержимому заголовков, тел запросов и ответов, а также по URL-адресам.

⬇ Скачать 🔍 Поиск...

Рисунок 3.1 - Поле поиска на странице "События"

Примечание:

Поиск по IP-адресам (поля Источник и Назначение) в текущей версии не поддерживается. Если необходимо найти событие по IP, используйте фильтры.

Данные на этой странице можно фильтровать.

В правой верхней части страницы есть текстовое поле поиска по событиям, которое позволяет выполнить поиск по параметрам (имя, значение) события или его части. (пр. параметров на Рисунок 4).

На странице «События» доступна возможность скачать все отображаемые события ⬇ Скачать .Файл выгрузки содержит все строки, представленные в таблице, и может быть сохранён в одном из двух форматов:

- ⊕ Microsoft Excel (.xlsx)
- ⊕ CSV (.csv)

При нажатии на любую запись в таблице отображается окно с деталями о событии (Рисунок 4). Пользователь может:

- ⊕ Скрывать и раскрывать разделы информации о событии.

- ⊕ Представлять заголовки в удобном для чтения человеком формате или как JSON.
- ⊕ Скопировать запрос в формате cURL для повторного выполнения:
 1. Нажать кнопку «Скопировать cURL» в разделе "Общее".
 2. В выпадающем списке выбрать формат команды:
 - ⊕ **Bash** - для Linux и macOS;
 - ⊕ **CMD** - для Windows (командная строка);
 - ⊕ **PowerShell** - для Windows PowerShell.

Событие # 557433

×

Общее

Анализ запроса

Анализ ответа

Имя роута	ecco	📄
URL запроса	/snits-test	Скопировать cURL bash cmd powershell
Время запроса	05.02.2026 17:07:01	
IP отправителя	5.5.5.0	
Порт отправителя	55434	
Хост получателя	172.17.0.1	
Порт получателя	6065	
Метод запроса	GET	
Код ответа	200	

Заголовки запроса

▼

JSON

Host	db-app.cloud.squadsec.ru:10001
Accept	*/*
X-Real-IP	5.5.5.0
User-Agent	PostmanRuntime/7.49.1
Content-Type	application/json
Authorization	Basic dXNyOnB3ZA==
Postman-Token	ea51d96b-a458-4e66-8bbe-07020ccc115d
Content-Length	29

Тело запроса

▼

```
{
  "document": "100000000148"
}
```

Заголовки ответа

▶

JSON

Тело ответа

▶

Показать/скрыть все

Рисунок 4 – Детали события

Вкладки **Анализ запроса** и **Анализ ответа** содержат информацию о результате проверки запроса в формате "Название анализатора: Статус анализа (OK, FAIL)" (Рисунок 5).

Событие #202066

×

ОБЩЕЕ

АНАЛИЗ ЗАПРОСА

АНАЛИЗ ОТВЕТА

Статистический анализ	OK	▶
Сигнатурный анализ	FAIL	▶
Анализ чувствительных данных	OK	▶
Сваггер анализ	FAIL	▶

Показать/скрыть все

Рисунок 5 – Вкладка Анализ запроса

При нажатии на результат проверки откроются детали проверки (Рисунок 6). В деталях отображаются результаты работы анализаторов, включая статистический, сигнатурный, анализ чувствительных данных и сваггер. В деталях события для каждого анализатора добавлена возможность **создания исключения анализатора для конкретного эндпоинта**.

При срабатывании FAIL пользователь может напрямую из Анализа запроса/ответа события добавить исключение для выбранного анализатора - исключение будет применяться только к данному эндпоинту, без влияния на остальные маршруты.

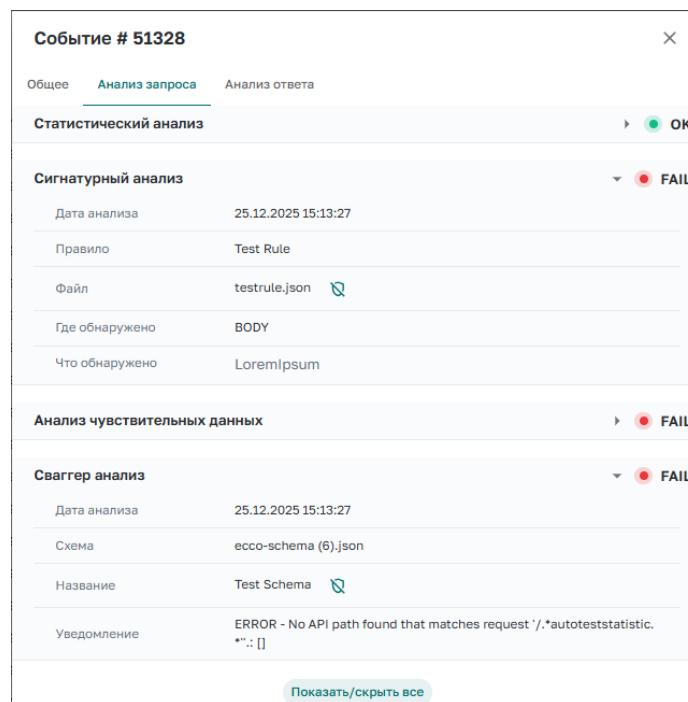


Рисунок 6 – Результаты неуспешной и успешной проверки анализатора

Страница События имеет пагинацию с возможностью показа 25, 50 и 100 событий на одной странице.

Пользователю доступна функция **фильтрации событий** по различным параметрам анализа. (Рисунок 7)

Фильтр расположен в верхней части страницы **События** и позволяет настраивать

отображение данных.  . При нажатии на кнопку «**Фильтры**» в верхней части страницы **События** справа открывается выдвигаемая панель с параметрами фильтрации.

Панель содержит поля для настройки отбора событий:

- ✚ **Включить только указанные статусы** - фильтрация событий по HTTP-коду ответа. Пользователь может указать один или несколько кодов (например, 200, 404, 500) или задать диапазон значений (например, от 400 до 499).
- ✚ **Временной диапазон** (начало и конец периода);
- ✚ **HTTP-метод;**
- ✚ **IP-адрес;**
- ✚ **Порт отправителя;**
- ✚ **Хост получателя;**
- ✚ **Порт получателя;**
- ✚ **URL запроса;**
- ✚ **Запрос заблокирован** - отображает только события, где запрос был заблокирован;
- ✚ **Проверки запросов** - выбор статуса проверки (OK, FAIL);

- ⊕ **Анализатор проверки запроса** - выбор конкретного анализатора;
- ⊕ **Чувствительные данные в запросе.**

При выборе анализатора **"ML-Классификатор"** в панели фильтров становится доступен дополнительный блок **«Чувствительные данные в запросе»**.
В этом блоке пользователь может не только выбрать типы данных (например, ФИО, СНИЛС, номер счёта и т.д), но и задать пороговое количество обнаружений для каждого типа. Если выбран другой анализатор, данное поле недоступно для выбора.

- ⊕ **Ответ заблокирован** - отображает события, где ответ был заблокирован;

Аналогично фильтрации запросов, пользователю доступен блок **"Проверки ответов"**, расположенный в нижней части панели фильтров.

При выборе в поле **«Анализатор проверки ответа»** значения **ML Классификатор** становится доступным дополнительное окно **«Чувствительные данные в ответе»**.
В этом окне можно выбрать типы данных (паспорт, ИНН, номер карты, СНИЛС, ФИО и др.) и задать **пороговое количество обнаружений** для каждого типа, аналогично фильтру запросов.

Переход на страницу «Исключения анализаторов»

На странице «События» реализована возможность быстрого перехода к управлению исключениями анализаторов.
В верхней части таблицы событий расположена кнопка «Исключения анализаторов».

События 

При переходе на страницу «Исключения анализаторов» (Рисунок 8) пользователю доступна возможность видеть все активные исключения, добавленные из деталей события в разделе «События», а также удалять ненужные правила.

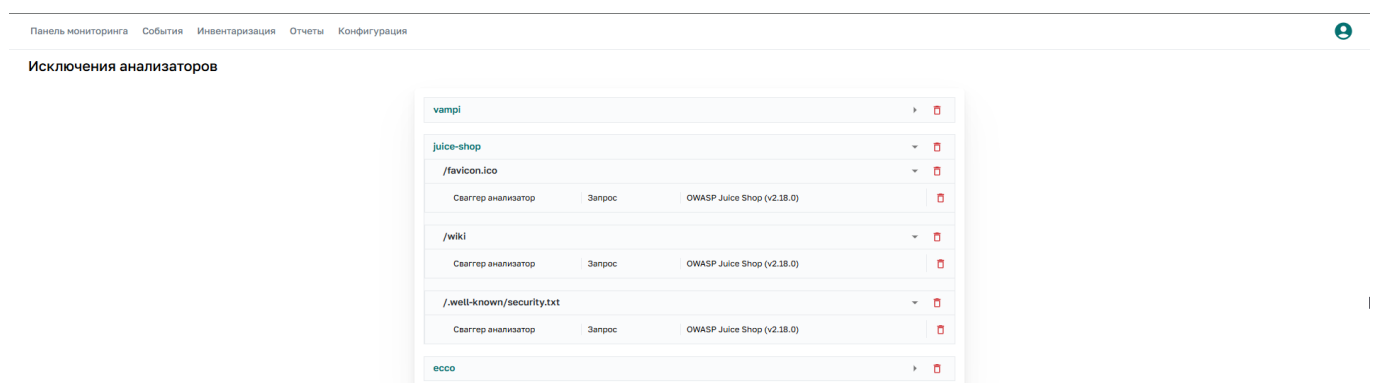


Рисунок 8 - Страница "Исключения анализаторов"

Описание интерфейса:

- ⊕ Искключения сгруппированы по **роутам**.
- ⊕ Внутри каждого роута отображаются эндпоинты, для которых создано исключение:
 - название анализатора (например, *Сигнатурный анализатор*, *Swagger анализатор*, *Классификатор*, *Статический Анализатор*);
 - тип (Запрос / Ответ);
 - файл, схема, класс данных или правило по которому задано исключение.
- ⊕ Для каждого, роута, эндпоинта и исключения доступна кнопка  - **удалить исключение**.

Как создаются исключения:

- 1) На странице «События» откройте детали события со статусом FAIL.
- 2) В Анализаторе запроса/ответа нажмите кнопку «**Добавить в исключения анализаторов**». 
- 3) Исключение автоматически появится на странице **Исключения анализаторов** в соответствующем роуте.

Как удалить исключение:

Способ №1

- 1) На странице **Исключения анализаторов** нажмите значок  рядом с нужным правилом.
- 2) Исключение будет удалено, и анализатор снова начнёт срабатывать при повторных проверках.

Способ №2

- 1) Откройте страницу «События» и выберите событие, для которого ранее было добавлено исключение.
- 2) В карточке события, в блоке «**Анализ запроса**» или «**Анализ ответа**», найдите анализатор, для которого установлено исключение.
- 3) Нажмите на значок  (**Удалить исключение**) в деталях анализатора.
- 4) После нажатия исключение будет удалено, а анализатор снова начнёт участвовать в проверках.

Отчёты

Перейдите в раздел *Отчеты*: <http://localhost/reports/draft>

На этой странице (Рисунок 9) можно создавать отчёты на основе истории запросов к защищаемым сервисам.

Панель мониторинга События Инвентаризация **Отчеты** Конструктор файлов сигнатур

Отчет: Поиск теневых API

Начало периода: 10.09.2025 Конец периода: 17.09.2025

Скачать Сохранить

WHERE response_swagger_messages::text ILIKE '%ERROR - No API path found%' AND response_status_code != 404 AND NOT (response_body LIKE '%404%' OR response_body ILIKE '%n

id_запроса_на_странице_События	route_id	method	url	response_body
34205	juice-shop	GET	/security.txt	Contact: mailto:donotreply@owasp-juice.s...
34244	ecco	GET	/SQD-1	["body":{},"hostname":"vm1.cloud.squadsec...
34250	ecco	GET	/SQD	["body":{},"hostname":"vm1.cloud.squadsec...
34276	juice-shop	GET	/favicon.ico	<!-- Copyright (c) 2014-2025 Bjoern Kimmi...
34330	juice-shop	GET	/well-known/security.txt	Contact: mailto:donotreply@owasp-juice.s...
34331	juice-shop	GET	/well-known/security.txt	Contact: mailto:donotreply@owasp-juice.s...
34332	juice-shop	GET	/well-known/security.txt	Contact: mailto:donotreply@owasp-juice.s...
34383	juice-shop	GET	/security.txt	Contact: mailto:donotreply@owasp-juice.s...
34384	juice-shop	GET	/security.txt	Contact: mailto:donotreply@owasp-juice.s...
34385	juice-shop	GET	/security.txt	Contact: mailto:donotreply@owasp-juice.s...
34408	juice-shop	GET	/login	<!-- Copyright (c) 2014-2025 Bjoern Kimmi...
34460	juice-shop	POST	/sdk	<!-- Copyright (c) 2014-2025 Bjoern Kimmi...
34462	juice-shop	GET	/nmaplowercheck1757613837	<!-- Copyright (c) 2014-2025 Bjoern Kimmi...
34464	juice-shop	GET	/evox/about	<!-- Copyright (c) 2014-2025 Bjoern Kimmi...
34465	juice-shop	GET	/HNAP1	<!-- Copyright (c) 2014-2025 Bjoern Kimmi...
34499	ecco	GET	/owa/	["body":{},"hostname":"89.169.138.66:10001...
34500	ecco	GET	/owa/	["body":{},"hostname":"89.169.138.66:10001...
34653	juice-shop	GET	/wiki	<!-- Copyright (c) 2014-2025 Bjoern Kimmi...
34657	juice-shop	GET	/favicon.ico	<!-- Copyright (c) 2014-2025 Bjoern Kimmi...
34723	ecco	GET	/CSS/Miniweb.css	["body":{},"hostname":"89.169.138.66:10001...
34724	ecco	GET	/nmaplowercheck1757804245	["body":{},"hostname":"89.169.138.66:10001...

Хранилище: access_log_swagger_view

Выбранные колонки: id_запроса_на_странице_Соб..., route_id, method, url, response_body

Доступные колонки: id, income_check_id, outcome_check_id, url, method, path, request_time, from_ip

Рисунок 9 – Общий вид страницы Отчеты

По умолчанию пользователь видит страницу для создания нового отчёта при переходе на страницу Отчеты. В выпадающем списке Отчет можно выбрать сохранённые отчёты. В комплекте поставки есть следующие отчёты по умолчанию:

- ✦ Все срабатывания – в отчёт попадают события, запрос или ответ которых получил статус FAIL хотя бы от одного анализатора.
- ✦ Срабатывания классификатора – в отчёт попадают события, в которых классификатор чувствительных данных обнаружил хотя бы одну категорию чувствительных данных хотя бы один раз. Классификатор работает только с российскими данным: фио - только на кириллице, паспорт - только внутренний российский.
- ✦ Срабатывания сваггер анализатора – в отчёт попадают события, запрос или ответ которых получил статус FAIL от сваггер анализатора.
- ✦ Срабатывания сигнатурного анализатора – в отчёт попадают события, запрос или ответ которых получил статус FAIL сигнатурного анализатора.
- ✦ Срабатывания статистического анализатора – в отчёт попадают события, запрос которых получил статус FAIL от статистического анализатора.
- ✦ Поиск теневых API – в отчёт попадают события, для которых запрос получил статус FAIL от сваггер анализатора. При этом запрос был заблокирован, потому что в сваггер-схеме нет такого эндпоинта. Также отсеиваются запросы с кодом 404.

Язык запросов

Функциональность отчётов поддерживает SQL для PostgreSQL 15. Пользователь может фильтровать запросы с помощью LIKE, BETWEEN, ILIKE и т. п. Поддерживается преобразование JSON, агрегация данных.

Создание нового отчёта

Выберите "Новый отчет" в выпадающем списке Отчет, чтобы начать конструировать новый отчёт. Введите запрос в поле "SQL запрос", который вернёт события, удовлетворяющие запросу. Строка запроса нечувствительна к регистру команд SQL, однако ошибка в регистре запрашиваемых значений может привести к неправильной выдаче. Строка запроса имеет два режима работы, которые можно изменять, нажимая в поле запроса кнопку FULL или WHERE:

- ⊕ FULL – полный SQL запрос. Нужно указать, из какой таблицы брать данные. Запрос должен начинаться с команды SELECT. В ответ возвращаются указанные колонки таблицы, нужные колонки и их псевдонимы назначаются напрямую в SQL-запросе.
 - Пример: **select * from access_log_view 'FAIL' = any(request_analyze_status) OR 'FAIL' = any(response_analyze_status)**. Фильтр вернёт все события, запрос или ответ на которые не прошли проверку хотя бы одного анализатора. В отчёте будут все колонки из таблицы access_log_view.
- ⊕ WHERE – запрос к предвыбранному хранилищу из выпадающего списка "Хранилище" (Рисунок 10). При таком режиме работы пользователь указывает в запросе только условия отбора событий, а таблица выбрана заранее. Пользователь может добавлять и удалять колонки в отчёте, давать колонкам псевдонимы.
 - Пример: **request_class_count > 0**. При выбранном хранилище access_log_analyzers_view фильтр вернёт все события, в запросе или ответе которых были обнаружены чувствительные данные хотя бы один раз.

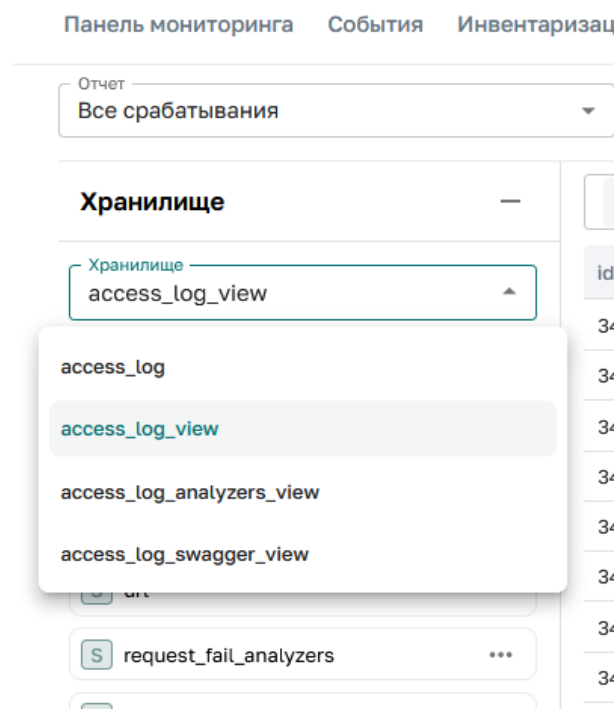


Рисунок 10 – выбор хранилища для выполнения запроса в режиме запроса WHERE

Хранилище – это таблица базы данных PostgreSQL, в которую решение записывает историю запросов. Доступны следующие хранилища:

- ⊕ access_log – таблица, где хранятся данные только о событиях. Результатов проверки анализаторами нет.
- ⊕ access_log_view – к данным таблицы access_log добавлены результаты проверки

анализаторами. Результаты проверки всеми анализаторами хранятся в одной колонке отдельно для запроса и ответа. Такая же схема используется для хранения подробностей результатов проверки FAIL.

- ✦ `access_log_analyzers_view` – данным таблицы `access_log` добавлены результаты проверки анализаторами, но для каждой сущности (статуса, пояснения, правила, обнаруженной категории чувствительных данных и т. п.), генерируемой каждым анализатором, выделена отдельная колонка.
- ✦ `access_log_swagger_view` – аналогично `access_log_analyzers_view` только с одним сваггер-анализатором.

Отчёт можно сохранить (кнопка "Сохранить") с выбранным именем (формат `.yaml`) (Рисунок 10.1) в папке дистрибутива `./rules-config/reports`. Далее внести изменения в подключенный git-репозиторий. Список отчётов в UI обновляется автоматически. При необходимости их можно редактировать вручную. (В поставке дистрибутива без сервиса git можно добавлять отчёты, редактировать и сохранять изменения непосредственно в UI)

Рисунок 10.1 – выбор имени отчета

Просмотр и экспорт результатов

После нажатия кнопки Выполнить пользователь получит результаты фильтрации. Результаты имеют пагинацию с возможностью показа 25, 50 и 100 событий на одной странице.

Режим запроса WHERE позволяет выбрать через интерфейс хранилище, к которому будет обращён запрос. Пользователь может выбрать, какие колонки будет содержать отчёт (Рисунок 11). Каждой добавленной колонке можно добавить псевдоним, который будет отображаться в шапке отчёта. Пользователь может поменять порядок колонок в отчёте перетаскиванием. Порядок колонок обновится после выполнения запроса.

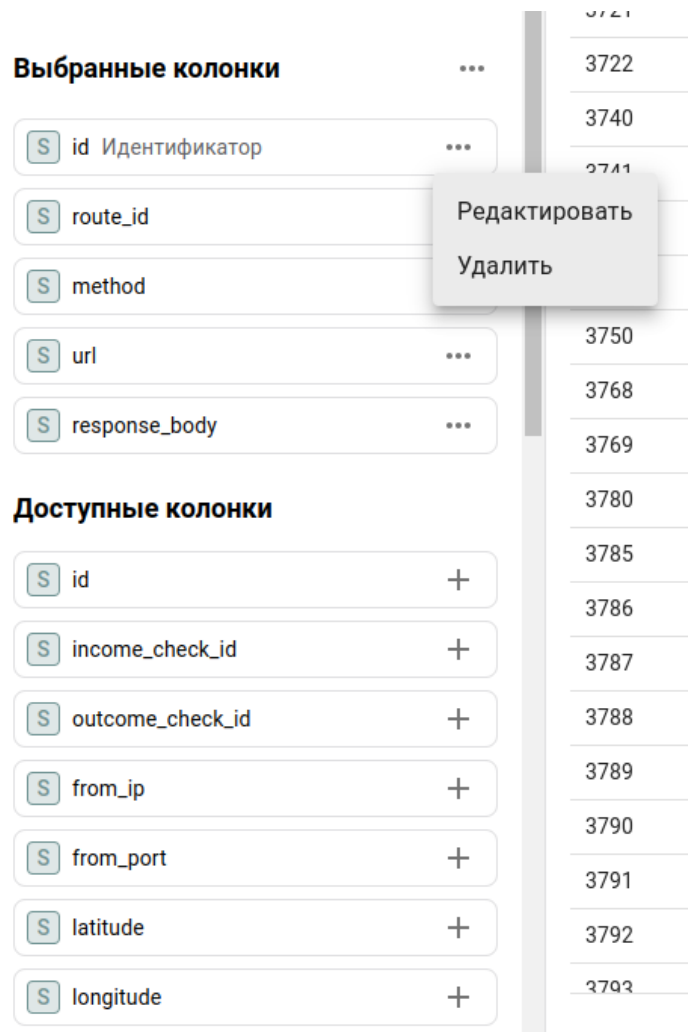


Рисунок 11 – Выбор колонок для отчета

Каждый отчёт можно применять к интересующему периоду (Рисунок 12). В отчёт попадут только те запросы, которые были получены за выбранный период. При этом даты, указанные в интерфейсе, будут проигнорированы, если в запросе указана явная фильтрация по колонке `created_day_at`.

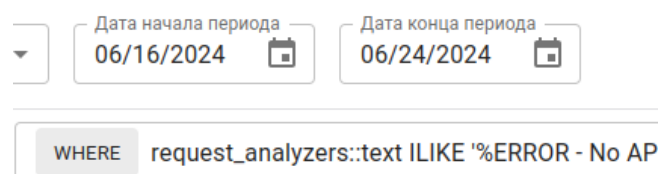


Рисунок 12 – Выбор периода для отчёта

Пользователь может Скачать отчёт в формате .csv (Рисунок 13). Предварительно требуется Выполнить запрос (кнопка "Выполнить") для скачивания актуальных результатов.

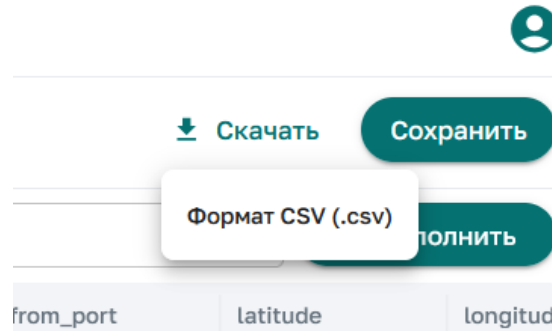


Рисунок 13 – Экспорт отчёта

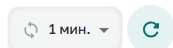
Инвентаризация

Модуль создан для обнаружения REST API эндпоинтов из анализируемого HTTP-трафика. Позволяет определять параметры запроса и ответа, определять тип запроса, тип авторизации. Пользователь может гибко управлять как списком эндпоинтов, так и параметрами каждого отдельного эндпоинта. Есть возможность экспортировать сваггер схему для последующего использования в сваггер анализаторе.

Основные возможности:

- ⊕ Определение REST API эндпоинта, параметров URL, заголовков и параметров запроса и ответа.
- ⊕ Определение типа авторизации, типа запроса, типа доступа.
- ⊕ Автоматическая шаблонизация эндпоинтов – выявление похожих значений сегментов URL.
- ⊕ Автоматическое объединение эндпоинтов в шаблонный эндпоинт.

На странице доступно автообновление, кроме этого, данные можно обновить вручную.



. Автообновление работает только на первой странице.

Объединение и обновление эндпоинтов

Термины

Шаблон – часть URL, которую модуль инвентаризации выделил как общую для группы эндпоинтов. Пример: */STRING*.

Статический URL – URL без шаблона в пути. Пример: */api/books/get/path*.

Шаблонный URL – URL с шаблоном в пути. Пример: */api/STRING/get/INTEGER*.

Параметры (эндпоинта) – список всех параметров эндпоинта: параметры в URL (query params), заголовки запроса и ответа, параметры тела запроса и тела ответа.

Узкий эндпоинт – URL с одним шаблоном в URL. Пример: */api/STRING/get*.

Широкий эндпоинт – URL с несколькими шаблонами в URL в различных его сегментах. Пример: */api/STRING/get/INTEGER*.

Правила объединения

Модуль инвентаризации может выделять общую часть для группы эндпоинтов с **единым методом**, а затем объединять эндпоинты с общей частью в единый эндпоинт. При этом статические URL удаляются, появляется шаблонный URL, у которого будут все параметры и все события статических URL до объединения. Все дальнейшие запросы к статическим URL до объединения, а также до этого неинвентаризированным статическим URL, удовлетворяющим условию шаблона, будут относиться к шаблонному URL.

Объединению не подвергаются:

- ⊕ Первый сегмент URL. Статические URL вида `/product/`, `/book/`, `/users/` всегда будут считаться отдельными эндпоинтами.
- ⊕ URL с неравным числом сегментов. Пара статических URL вида `/api/book/` и `/api/book/get/` считается различными эндпоинтами и не может быть объединена вне зависимости от используемого метода.

Пользователь может запрещать и разрешать объединение эндпоинтов.

Механизм образования шаблона STRING

Мгновенная шаблонизация

Шаблон выделяется с первого запроса к статическому URL, если в сегменте есть буквы и больше 2 цифр. Такое ограничение введено для избежания слияния по сегменту с версией API. Например, GET `/api/book/get/df2nf3f6g` будет шаблонизирован в GET `/api/book/get/STRING`.

Шаблонизация с задержкой во времени

Кроме мгновенной шаблонизации модуль с периодом 10 минут анализирует базу инвентаризированных эндпоинтов.

Эндпоинты, у которых в сегменте есть буквы и не более 2 цифр не объединяются сразу. Их объединение может произойти, если выполнено хотя бы одно из условий:

- ⊕ у нескольких (по умолчанию больше 5, см. Руководство администратора) эндпоинтов параметры совпадают на 80 % и более по имени и типу. Тогда после анализа базы эндпоинты объединятся в GET `/product/STRING`.
Пример:

- GET `/product/rhkpybtpmpa`
- GET `/product/rhkpybtpmpb`
- GET `/product/rhkpybtpmpc`
- GET `/product/rhkpybtpmd`
- GET `/product/rhkpybtpmpe`
- GET `/product/rhkpybtpmpg`

Эти эндпоинты будут объединены GET `/product/STRING`.

- ⊕ У эндпоинтов различаются параметры по имени и типу, но позже появился эндпоинт GET `/product/STRING`, шаблон которого был выделен мгновенно. После анализа базы эндпоинты GET `/product/rhkpybtpmp` и GET `/product/ipbazdqbk` объединятся в GET `/product/STRING`.

Механизм образования шаблона INTEGER

Шаблон выделяется с первого запроса к эндпоинту, если в сегменте есть только цифры:

GET `/api/book/get/15524` будет шаблонизирован в GET `/api/book/get/INTEGER`.

Механизм образования шаблона FLOAT

Шаблон выделяется с первого запроса к эндпоинту, если в сегменте есть только цифры, разделённые одной точкой: GET `/api/book/get/155.24` будет шаблонизирован в GET `/api/book/get/FLOAT`.

Объединение эндпоинтов, у которых уже есть шаблон в URL

Эндпоинты могут продолжить объединяться, если у них уже есть шаблон. Для шаблонизации широких эндпоинтов по типу STRING в ещё более широкие параметры эндпоинтов должны совпадать на 80 % и более по имени и типу. Пример:

- ⊕ GET `/product/STRING/rhkpybtpmpa`
- ⊕ GET `/product/STRING/rhkpybtpmpb`
- ⊕ GET `/product/STRING/rhkpybtpmpc`
- ⊕ GET `/product/STRING/rhkpybtpmd`
- ⊕ GET `/product/STRING/hkpybtpmpe`
- ⊕ GET `/product/STRING/rhkpybtpmpg`

Эти эндпоинты будут объединены GET `/product/STRING/STRING`. Минимальное количество эндпоинтов для объединения определяется параметром [merge-threshold](#).

Широкие эндпоинты вида GET `/product/INTEGER/INTEGER`, GET `/product/INTEGER/FLOAT` и т. п. будут образовываться с первого запроса.

Объединение эндпоинтов, добавленных вручную

Эндпоинты, добавленные вручную и потенциально подходящие по объединение с шаблоном STRING, объединяются при следующем после добавления анализе базы эндпоинтов, если выполнены условия. Эндпоинты с сегментом, потенциально шаблонизируемым в INTEGER или FLOAT, будут объединены с шаблонным URL после анализа базы.

Правила обновления

Модуль инвентаризации автоматически собирает информацию о параметрах URL запросов. Для каждого параметра определяется имя и тип значения.

Параметры, которых ранее не было у эндпоинта, но есть в текущем запросе, мгновенно добавляются к схеме эндпоинта при условии, что код ответа запроса в разрешённом диапазоне. Например, параметр `param1` запроса к эндпоинту будет добавлен в схему эндпоинта, если запрос завершился кодом 200. Однако параметр не добавится, если запрос завершился кодом 403.

Если уже инвентаризированный параметр и одноимённый параметр в запросе имеют разные типы, то будет создан ещё один параметр с тем же именем, но новым типом.

Пользователь может разрешать и запрещать обновление для выбранного эндпоинта.

Роуты

Список роутов

В списке роутов показаны все роуты, которые есть в системе (Рисунок 14). Роуты

отсортированы по дате изменения. Поля таблицы:

- ⊕ Имя роута.
- ⊕ Эндпоинты – количество эндпоинтов в роуте, включая эндпоинты в черном списке.
- ⊕ Эндпоинты с рисками – количество эндпоинтов роута, имеющих запросы с результатом анализа FAIL
- ⊕ Запросы – общее количество запросов ко всем эндпоинтам роута.
- ⊕ Запросы, не прошедшие проверку – общее количество запросов ко всем эндпоинтам роута с результатом анализа FAIL.
- ⊕ Эндпоинты в черном списке – количество эндпоинтов в черном списке для роута.
- ⊕ Здоровье – средний уровень здоровья по всем инвентаризированным эндпоинтам роута.
- ⊕ Дата изменения – дата последнего изменения параметров или добавления эндпоинта в роуте.

Панель мониторингаСобытияИнвентаризацияОтчетыКонструктор файлов сигнатур

Инвентаризация / Роуты

Поиск

Выбрать период статистики
09.07.2025 – 17.09.2025

506
Всего API

33845
Всего запросов

22924
Не прошли проверку

89 %
Здоровье

466
Эндпоинты с рисками

Blacklist

Имя роута	Эндпоинты	Эндпоинты с риска...	Запросы	Запросы, не прошедшие проверку	Эндпоинты в черном списке	Здоровье	Дата изменения
unknown	78	63	3077	1988	0	92 %	17.09.2025 12:07:22
vampi	9	7	713	364	0	52 %	17.09.2025 12:01:24
juice-shop	126	126	5664	5651	0	67 %	17.09.2025 11:24:01
ecco	279	260	8630	6753	0	97 %	16.09.2025 06:41:26
demo-service	7	7	15701	8162	0	48 %	16.09.2025 06:12:03
wiremock	7	3	60	6	0	10 %	04.09.2025 14:40:09

Рисунок 14 – Список роутов

На странице доступен поиск роута по названию.

Пользователь может посмотреть статистику за выбранный период (Рисунок 15). Роуты, у которых были срабатывания анализаторов за выбранный период, будут выделены красным. Значения колонок Эндпоинты с рисками, Запросы, Запросы, не прошедшие проверку и Здоровье определяются выбранным периодом статистики.

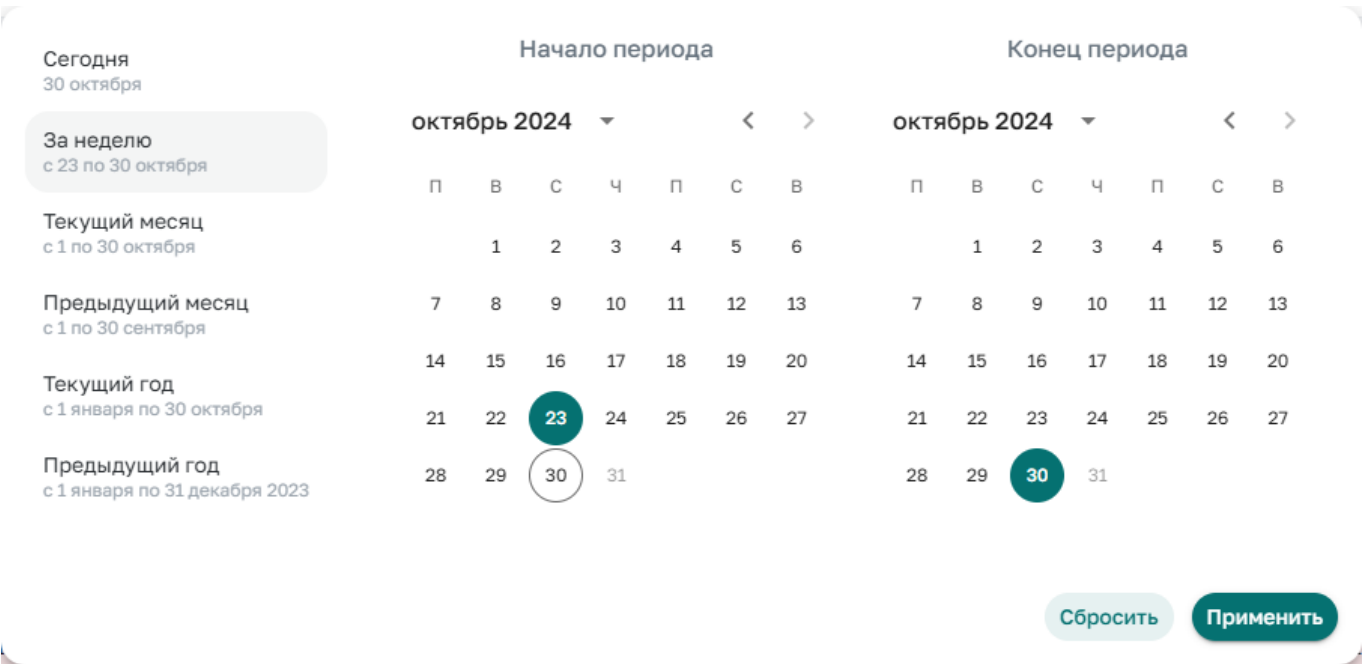


Рисунок 15 – Окно выбора статистики

Метрики

В верхней части страницы Роуты показана суммарная статистика по всем роутам. Статистика рассчитывается для выбранного периода за исключением метрики Всего API.

- Всего API – количество инвентаризированных эндпоинтов во всех роутах.
- Всего запросов – количество запросов по всем эндпоинтам всех роутов.
- Не прошли проверку – количество запросов к эндпоинтам всех роутов, которые получили FAIL хотя бы от одного анализатора.
- Здоровье – средний уровень здоровья по всем инвентаризированным эндпоинтам всех роутов.
- Эндпоинты с рисками – количество эндпоинтов, имеющих хотя бы один запрос с результатом FAIL хотя бы от одного анализатора.

Здоровье

Здоровье численно оценивает работоспособность роута или эндпоинта. Параметр рассчитывается как отношение суммы запросов с кодами 2XX и 3XX к количеству всех запросов к роуту или эндпоинту за выбранный период.

Эндпоинты

На странице доступен список эндпоинтов с возможностями его экспорта в виде сваггер схемы, импорта из сваггер схемы, просмотра детальной информации по каждому эндпоинту, редактирования эндпоинта и его параметров, а также добавления новых эндпоинтов.

Возможности:

- Φ Просмотр детализированной информации по каждому эндпоинту.
- Φ Добавление новых эндпоинтов.
- Φ Редактирование эндпоинта и его параметров.
- Φ Просмотр событий эндпоинта.
- Φ Просмотр динамики здоровья, атак и чувствительных данных эндпоинта.
- Φ Экспорт списка эндпоинтов в виде сваггер схемы.
- Φ Импорт из сваггер схемы.

Список эндпоинтов

Пользователь может открыть список эндпоинтов роута (Рисунок 16), если нажмёт на роут в списке роутов.

Панель мониторингаСобытияИнвентаризацияОтчетыКонструктор файлов сигнатур

Инвентаризация / Роуты / demo-service

ВключитьПоискВыбор периода статистики21.08.2025 – 17.09.2025ИмпортЭкспорт

☐	Метод	Эндпоинт	Типы аутентификации	Тип доступа	Тип запроса	Чувствительные...	Запросы	Запросы, не про...	Здоровье	Дата изменения
☐	POST	/response/STRING	UNAUTHENTICATED	PUBLIC	JSON	–	19	14	100 %	16.09.2025 06:12:03
☐	GET	/hi	UNAUTHENTICATED	PUBLIC	FORM	–	10	8	100 %	05.09.2025 07:09:58
☐	GET	/	UNAUTHENTICATED	PUBLIC	Не определено	–	374	374	0 %	05.09.2025 05:22:31
☐	GET	/inicio.aspx	UNAUTHENTICATED	PUBLIC	Не определено	–	1	1	0 %	04.09.2025 14:40:08
☐	GET	/xml-output	UNAUTHENTICATED	PUBLIC	JSON	–	1	1	0 %	07.08.2025 07:45:25
☐	POST	/response/name	UNAUTHENTICATED	PRIVATE	JSON	–	0	0	0 %	04.08.2025 07:50:11
☐	POST	/response/INTEGER/INTEGER/INTEGER	UNAUTHENTICATED	PRIVATE	JSON	–	0	0	0 %	09.07.2025 07:57:17

Рисунок 16 – Список эндпоинтов роута

Поля таблицы:

- ⊕ Метод – HTTP метод.
- ⊕ Эндпоинт – URL (только часть path, без параметров).
- ⊕ Тип авторизации – тип авторизации эндпоинта.
- ⊕ Тип доступа – тип подсети, из которой доступен эндпоинт.
- ⊕ Тип запроса – тип данных в теле запроса.
- ⊕ Чувствительные данные – наличие чувствительных данных в запросах к эндпоинту. При наведении мыши на информационную иконку можно увидеть обнаруженные категории чувствительных данных.
- ⊕ Запросы – количество запросов к эндпоинту.
- ⊕ Запросы, не прошедшие проверку – количество запросов с результатом анализа FAIL.
- ⊕ Здоровье – средний уровень здоровья за выбранный период статистики.
- ⊕ Дата изменения – дата последнего изменения эндпоинта (добавление эндпоинта, добавление/изменение параметра).

Значения полей Тип авторизации, Тип доступа и Тип запроса устанавливаются для эндпоинта автоматически при первом запросе к эндпоинту. Значения могут изменяться во времени. Также можно установить значения полей вручную при добавлении и редактировании эндпоинта.

Эндпоинты, у которых были срабатывания анализаторов за выбранный период, будут выделены красным.

Метод

Доступны следующие методы:

- ⊕ GET
- ⊕ POST
- ⊕ PUT
- ⊕ DELETE
- ⊕ PATCH
- ⊕ HEAD
- ⊕ CONNECT
- ⊕ OPTIONS
- ⊕ TRACE

Типы авторизации

Тип авторизации определяется по заголовку Authorization в запросе или по заголовкам, характерным для API token. Показываются все определённые типы авторизации, если их было несколько. Определяемые типы:

- ⊕ UNAUTHENTICATED – без авторизации, отсутствует заголовок Authorization.
- ⊕ JWT – в заголовке Authorization есть только JWT.
- ⊕ BASIC – в заголовке Authorization используется Basic авторизация.
- ⊕ BEARER – в заголовке Authorization используется Bearer авторизация.
- ⊕ API_TOKEN – для авторизации используется API token. Список заголовков, определяемых как API_TOKEN:
 - X-API-Token
 - Api-Key
 - X-Auth-Token
 - X-Access-Token
 - Token

- Api-Token
- Access-Token
- X-Custom-Token
- X-User-Token
- X-Security-Token
- X-App-Token
- X-Client-Token
- X-Service-Token
- X-Session-Token
- X-Application-Token
- X-Token
- ⊕ AUTHORIZATION_HEADER – используется авторизация с помощью заголовка Authorization, но её тип отличается от перечисленных выше.
- ⊕ Не определено – не удалось определить тип авторизации. Можно использовать при добавлении эндпоинта вручную в случае, когда тип авторизации ещё не известен.

Тип доступа

- ⊕ PRIVATE – запросы к эндпоинту отправляются из подсети, которая в конфигурации обозначена как приватная.
- ⊕ PUBLIC – запросы к эндпоинту отправляются из подсети, которая не указана в конфигурации.
- ⊕ Не определено – не удалось определить тип авторизации. Штатно такое значение будет у эндпоинтов, если не определены приватные сети в конфигурации. Можно использовать при добавлении эндпоинта вручную в случае, когда тип авторизации ещё не известен.

Тип запроса

Тип запроса определяется по заголовку Content-Type. Если тело у запроса есть, но нет заголовка Content-Type, то тип запроса будет определён по результатам анализа самого тела. Определяемые типы:

- ⊕ FORM – тип x-www-form-urlencoded.
- ⊕ JSON – тип JSON.
- ⊕ TEXT – тип plain text или HTML.
- ⊕ XML – тип XML.
- ⊕ Не определено – не удалось определить тип тела или у запроса отсутствует тело.

Фильтрация эндпоинтов

Доступна фильтрация эндпоинтов по следующим параметрам (Рисунок 17):

- ⊕ Тип доступа.
- ⊕ Тип запроса.
- ⊕ Статусы ответа (возможно выделить группу кодов в один клик).
- ⊕ IP отправителя.
- ⊕ Порт отправителя.
- ⊕ Персональные данные.
- ⊕ Метод.
- ⊕ Тип авторизации.

Фильтры
×

Тип доступа

▼

Тип запроса

▼

Статусы

▼

IP отправителя

Порт отправителя

Персональные данные

▼

Метод

GET

POST

PUT

DELETE

PATCH

HEAD

CONNECT

OPTIONS

TRACE

Тип авторизации

UNAUTHENTICATED

BASIC

AUTHORIZATION_HEADER

JWT

API_TOKEN

BEARER

Не определено

Сбросить

Применить

Рисунок 17 – Окно фильтров

Детали эндпоинта

Окно содержит детальную информацию об эндпоинте (Рисунок 18).

Пользователь всегда может видеть:

- ✦ Метод и URL запроса.
- ✦ [Здоровье](#) эндпоинта.
- ✦ Запросы, не прошедшие проверку.
- ✦ Чувствительные данные.

Вкладка Общее

На вкладке (Рисунок 18) доступна та же информация, что и в таблице списка эндпоинтов, а также показан режим обновления схемы, дата создания и последнего изменения эндпоинта.

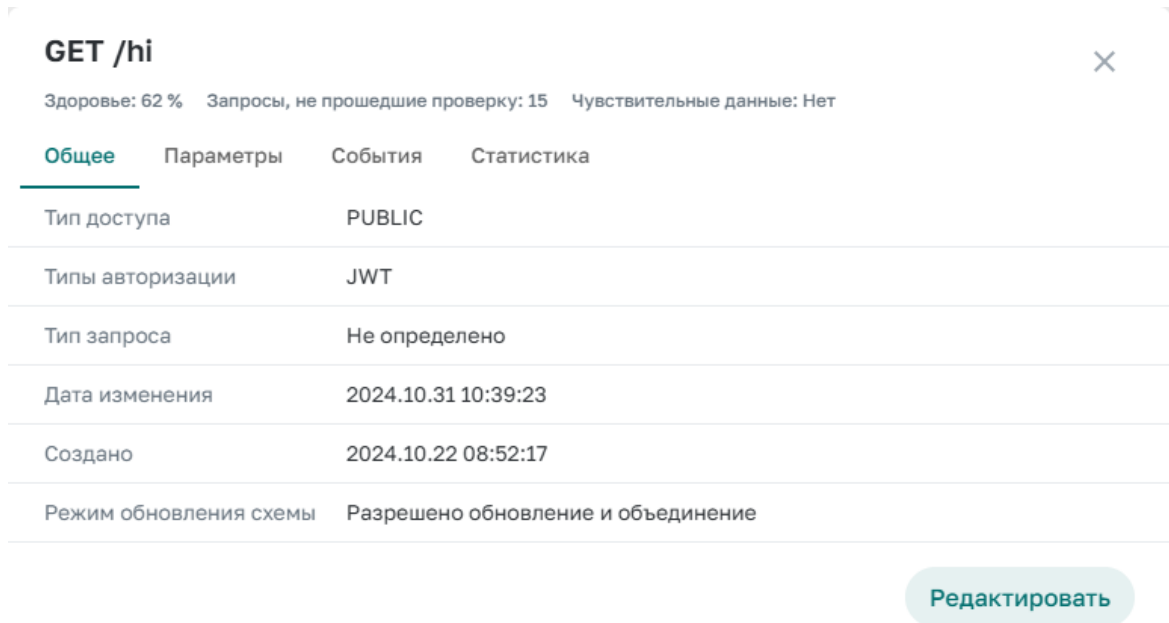


Рисунок 18 – Вкладка Общее окна деталей эндпоинта

Редактирование эндпоинта

Параметры эндпоинта можно редактировать (Рисунок 19), если нажать кнопку Редактировать на вкладке Общее.

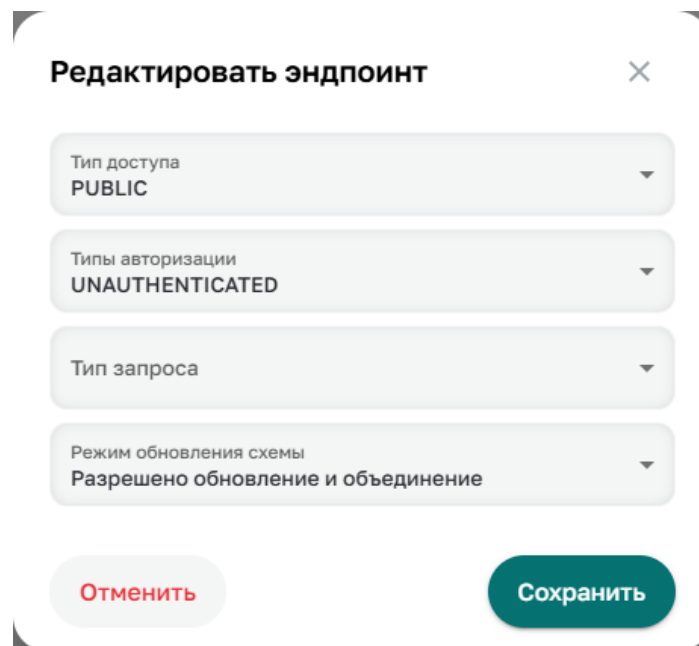


Рисунок 19 – Окно редактирования эндпоинта

Режим обновления схемы определяет:

- ⊕ Будет ли эндпоинт участвовать в объединении с другими эндпоинтами при выполнении необходимых условий.
- ⊕ Будут ли обновляться параметры эндпоинта при отправке запросов с новыми параметрами или новыми типами уже инвентаризированных параметров.

Возможные режимы обновления:

- ⊕ Разрешено обновление и объединение.

- ⊕ Запрещено обновление и объединение.
- ⊕ Запрещено обновление эндпоинта.
- ⊕ Запрещено объединение.

Вкладка Параметры

На этой вкладке приведён список параметров эндпоинта (Рисунок 20). Для каждого параметра показаны его имя в запросе и тип значения. Доступны параметры:

- ⊕ Параметры в URL запроса (query params).
- ⊕ Заголовки запроса.
- ⊕ Тело запроса.
- ⊕ Код ответа:
 - Заголовки ответа.
 - Тело ответа.

GET /hi
×

Здоровье: 62 % Запросы, не прошедшие проверку: 15 Чувствительные данные: Нет

Общее **Параметры** События Статистика

URL + ▼

Заголовки запроса + ▼

:method	string	⋮
:path	string	⋮
accept	string	⋮
accept-language	string	⋮
cookie	string	⋮
host	string	⋮
user-agent	string	⋮
x-request-id	string	⋮

Тело запроса + ▼

КОДЫ ОТВЕТА +

● **200**
▼

Заголовки ответа +

:status	integer	⋮
---------	---------	---

Рисунок 20 – Вкладка Параметры

Параметр можно добавить, удалить, изменить имя или тип параметра (Рисунок 21). Однако параметр `host` в заголовках запроса удалить и редактировать нельзя. Это необходимо для правильной работы модуля инвентаризации.

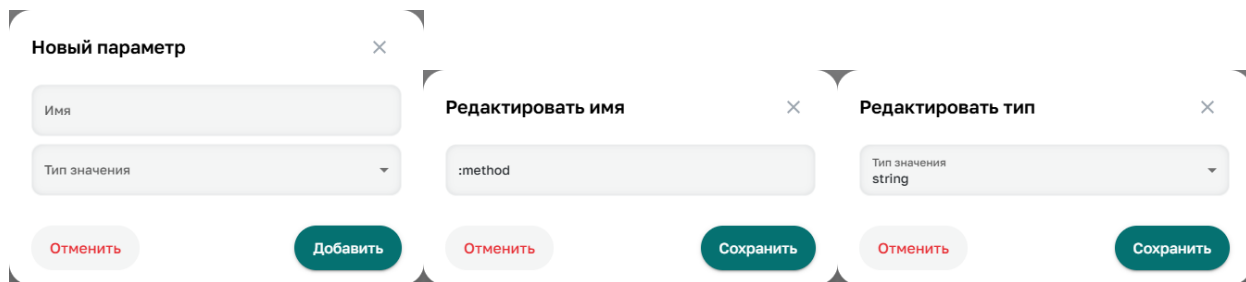


Рисунок 21 – Окна создания нового параметра, редактирования имени и типа параметра

Возможные типы параметров:

- ⊕ `string` – строка.
- ⊕ `integer` – целое число.
- ⊕ `float` – дробное число с точкой в качестве десятичного разделителя.
- ⊕ `boolean` – логическое значение `true` или `false`.
- ⊕ `array` – массив JSON. Такой тип можно выбрать только для параметра в теле. Для задания типа нужно привести пример: `[ 1, 2, "element1"]`.
- ⊕ `object` – объект JSON. Такой тип можно выбрать только для параметра в теле. Для задания типа нужно привести пример:


```
{
  "user": "Ivan",
  "age": 23
}
```

Для параметров типа `array` и `object` во вкладке Параметры в поле значения не показывается имя типа, как для прочих типов параметра. Вместо этого в качестве примера показано точное значение параметра, когда он был создан или обнаружен первый раз.

Вкладка События

На вкладке доступен список связанных с эндпоинтом событий (Рисунок 22). При нажатии на любое событие открывается окно детальной информации о событии. Функциональность вкладки аналогична странице События за исключением фильтрации. На этой вкладке фильтрация невозможна.

Событие # 126339

Общее

Анализ запроса

Анализ ответа

IP отправителя

13.73.51.185

Порт отправителя

38992

Хост получателя

-

Порт получателя

-

URL запроса

/response/autoteststatisticfailf82593e3-c319-4af1-a9a6-fa8af0a76859

Метод запроса

POST

Код ответа

Заголовки запроса

JSON

x-request-id

0230877975-1142551103-1956334027

:method

POST

Accept

/

Connection

Keep-Alive

User-Agent

Apache-HttpClient/4.5.13 (Java/21.0.4)

:path

/response/autoteststatisticfailf82593e3-c319-4af1-a9a6-fa8af0a76859

Host

vm1.squadsecfield.ru:10000

Content-Length

46

Content-Type

text/plain; charset=ISO-8859-1

Тело запроса

{

"param1": "value1".

}

POST /response/STRING

Здоровье: 14 % Запросы, не прошедшие проверку: 405 Чувствительные данные: Нет

Общее

Параметры

События

Статистика

Номер

IP и Порт отправителя

Анализ запроса

Анализ ответа

Код от...

Дата

#126339

13.73.51.185:38992

FAIL

OK

2024.11.01 10:26:19

#126338

13.73.51.185:38991

FAIL

OK

2024.11.01 10:26:19

#126337

13.73.51.185:38990

FAIL

OK

2024.11.01 10:26:18

#126336

13.73.51.185:38989

FAIL

OK

2024.11.01 10:26:18

#126335

13.73.51.185:38988

FAIL

OK

2024.11.01 10:26:18

#126334

13.73.51.185:38987

FAIL

OK

2024.11.01 10:26:17

#126333

13.73.51.185:38986

OK

OK

200

2024.11.01 10:26:11

#126332

13.73.51.185:38985

FAIL

OK

2024.11.01 10:26:11

#125860

172.214.46.2:5272

FAIL

OK

2024.11.01 09:04:22

#125859

172.214.46.2:5271

FAIL

OK

2024.11.01 09:04:22

#125858

172.214.46.2:5270

FAIL

OK

2024.11.01 09:04:22

#125857

172.214.46.2:5269

FAIL

OK

2024.11.01 09:04:22

#125856

172.214.46.2:5268

FAIL

OK

2024.11.01 09:04:21

#125855

172.214.46.2:5267

FAIL

OK

2024.11.01 09:04:21

#125854

172.214.46.2:5266

OK

OK

200

2024.11.01 09:04:15

#125853

172.214.46.2:5265

FAIL

OK

2024.11.01 09:04:15

#125069

20.55.221.65:63560

FAIL

OK

2024.10.31 13:48:41

#125068

20.55.221.65:63559

FAIL

OK

2024.10.31 13:48:41

#125067

20.55.221.65:63558

FAIL

OK

2024.10.31 13:48:40

Размер страницы

25

1-25 из 1282

Страница

1

из 52

Рисунок 22 – Детали события и список событий эндпоинта

Вкладка Статистика

На вкладке доступны графики (Рисунок 23):

- ⊕ Здоровье по дням.
- ⊕ Уровень угроз по дням – отношение количества запросов к эндпоинту, не прошедших проверку анализаторов к общему количеству запросов.
- ⊕ Количество чувствительных данных в запросах по дням. Можно увидеть график для каждой категории отдельно.

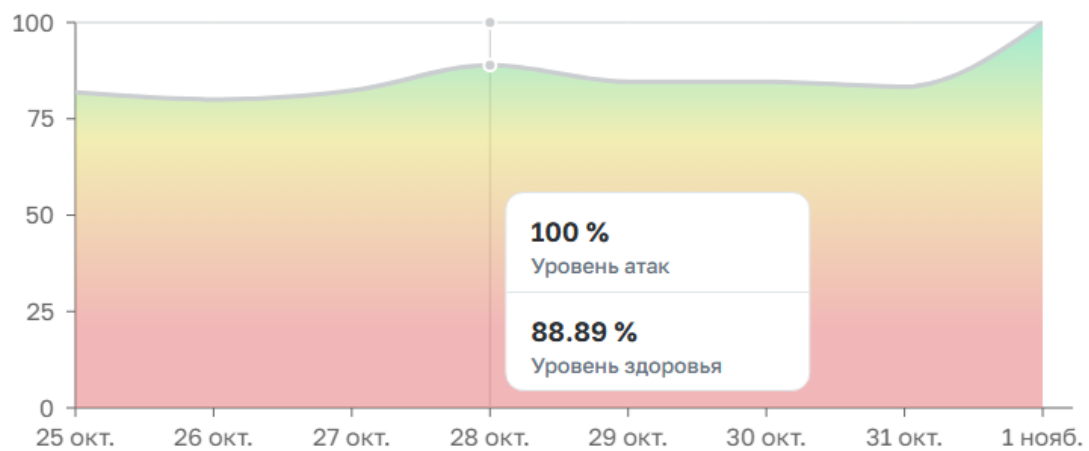
GET /



Здоровье: 85 % Запросы, не прошедшие проверку: 92 Чувствительные данные: Да

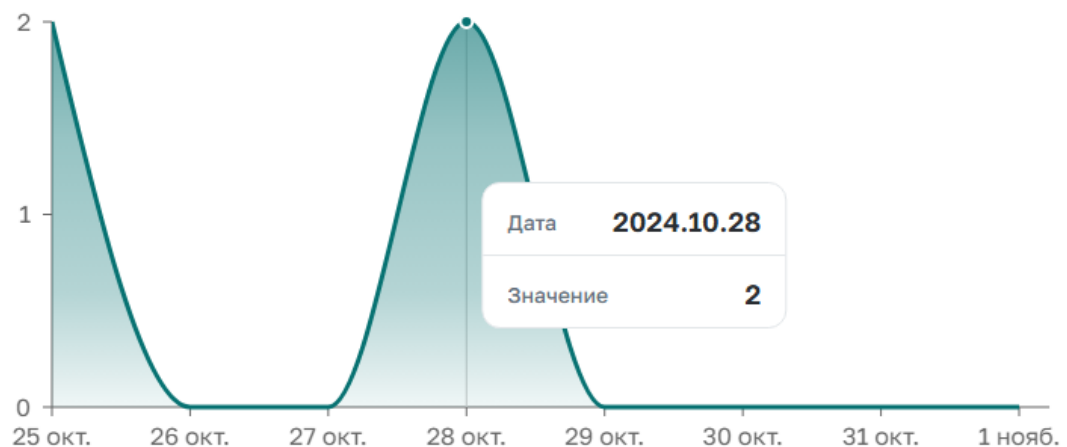
Общее Параметры События Статистика

Динамика здоровья и угроз



Класс данных

Адрес, местоположение ▾



При выборе одинаковых дат начала и окончания периода на странице "Инвентаризация" (например, 12.01.2026 – 12.01.2026) статистика отображается в виде **столбчатых графиков**.

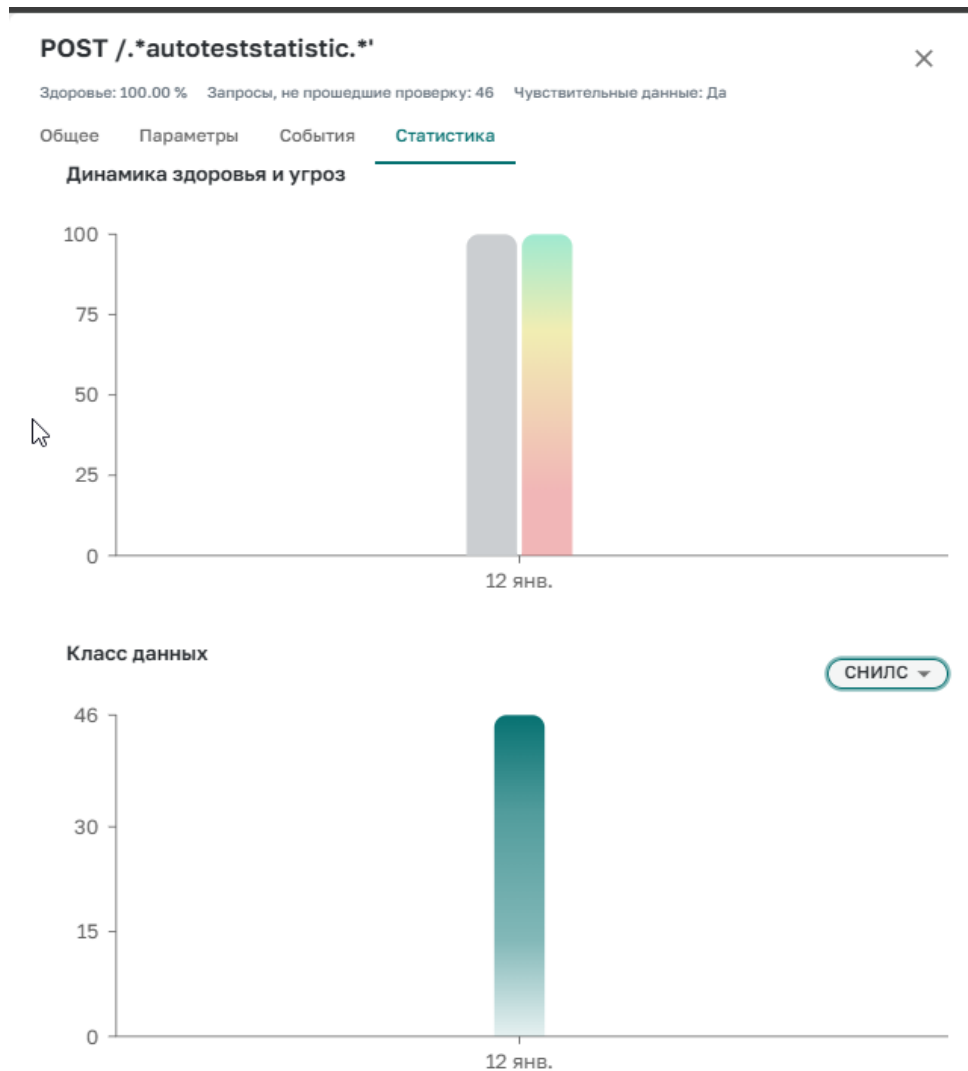


Рисунок 23 – Динамика здоровья эндпоинта, атак на него и динамика трафика чувствительных данных

Период на графиках определяется выбранным периодом статистики в списке эндпоинтов.

Добавление нового эндпоинта

Окно добавления эндпоинта появляется, если нажать кнопку добавления нового эндпоинта  в списке эндпоинтов (Рисунок 24).

Новый эндпоинт ✕

Имя эндпоинта

Опционально можно добавлять типы параметров в треугольные скобки: <INTEGER>, <STRING>, <FLOAT>

Метод

Режим обновления схемы
Разрешено обновление и объединение

Тип доступа
PUBLIC

Тип запроса
Не определено

Типы авторизации
UNAUTHENTICATED

Отменить Добавить

Рисунок 24 – Окно добавления эндпоинта

Поля формы

- ✧ Имя эндпоинта – URL без параметров эндпоинта. Должно начинаться с "/". Можно создавать эндпоинты с шаблоном, заключая шаблон в треугольные скобки: <INTEGER>, <STRING>, <FLOAT>. Пример: /books/<INTEGER>.
- ✧ Метод эндпоинта.
- ✧ Режим обновления схемы.
- ✧ Тип доступа.
- ✧ Тип запроса.
- ✧ Типы авторизации.

Экспорт сваггер схемы

Пользователь может экспортировать текущий список эндпоинтов роута в виде сваггер схемы. Для этого нужно нажать кнопку Экспорт. Файл экспортируется в формате json. Схему можно использовать для загрузки в сваггер анализатор.

Импорт сваггер схемы

Заранее подготовленную сваггер схему для роута можно импортировать, если нажать кнопку Импорт (Рисунок 25).

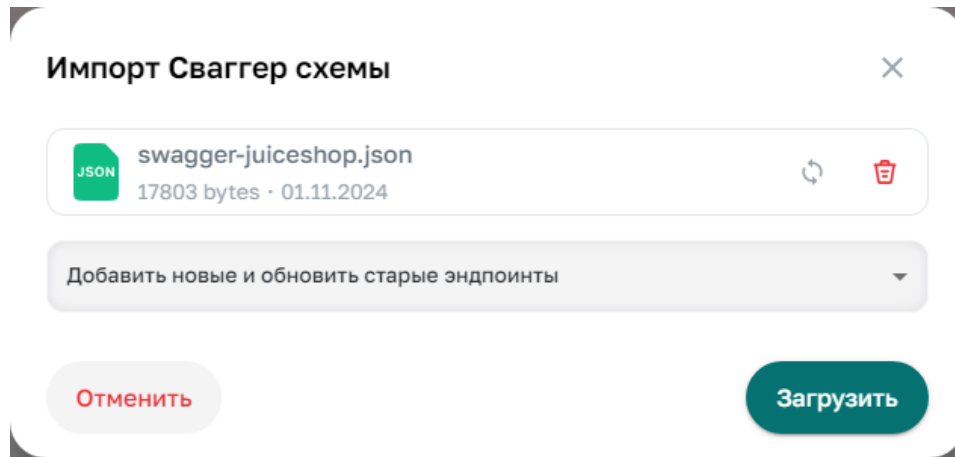


Рисунок 25 – Окно импорта сваггер схемы

- ✦ Добавить новые и обновить старые эндпоинты. Параметры из схемы добавятся к параметрам старых эндпоинтов. Текущие параметры (пара имя–тип) эндпоинтов, которых нет в импортируемой схеме, останутся в схеме эндпоинта. В список эндпоинтов будут добавлены эндпоинты с URL, которых ещё нет в списке эндпоинтов.
- ✦ Только обновить эндпоинты. Параметры существующих эндпоинтов обновятся. Эндпоинты, которые есть в схеме, но их нет в списке эндпоинтов роута, не будут добавлены.
- ✦ Добавить только новые эндпоинты. Будут добавлены эндпоинты, которые есть в схеме, но их нет в списке эндпоинтов роута. Параметры эндпоинтов, которые уже есть в списке эндпоинтов роута, не будут обновлены.

Чёрный список

Пользователь может удалить эндпоинт из списка эндпоинтов. Для этого нужно отметить чекбокс рядом с эндпоинтом и нажать кнопку . После удаления эндпоинт исчезает из списка эндпоинтов, его параметры не будут обновляться, запросы к эндпоинту не будут участвовать в статистике запросов, эндпоинт не будет экспортироваться в сваггер схему. Удалённые эндпоинты хранятся в чёрном списке (Рисунок 26). Открыть его можно, если нажать кнопку  Blacklist на странице Роуты. Пользователь может воспользоваться поиском, чтобы найти интересующий роут.

Панель мониторинга События Инвентаризация Отчеты Конструктор файлов сигнатур			
Инвентаризация / Роуты (Blacklist) Поиск			
Имя роута	Эндпоинты	Эндпоинты в черном списке	Дата изменения
juice-shop	125	1	2025.09.17 14:10:36

Рисунок 26 – Чёрный список

Эндпоинты сгруппированны по роутам. Пользователь может найти удалённый эндпоинт по URL (Рисунок 27).

☐	Метод	Эндпоинт	Типы аутентификации	Тип доступа	Тип запроса	Дата изменения
☐	GET	/config.json	UNAUTHENTICATED	PUBLIC	JSON	2025.09.17 14:10:36

Рисунок 27 – Список эндпоинтов в чёрном списке для выбранного роута

Пользователь может сразу добавить эндпоинт в чёрный список, минуя добавление эндпоинта в списке эндпоинтов, если нажмёт кнопку  (Рисунок 28). Для этого нужно указать URL и метод.

Новый эндпоинт в Blacklist

✕

Имя эндпоинта

Метод

Отменить

Добавить

Рисунок 28 – Окно добавления эндпоинта в чёрный список напрямую

Пользователь может вернуть эндпоинт в роут из чёрного списка, если отметит чекбокс эндпоинта и нажмёт кнопку . После восстановления запросы эндпоинта начнут снова участвовать в статистике, параметры эндпоинта до удаления сохранятся и начнут обновляться. Эндпоинт будет экспортироваться в swagger схему.

Конфигурация (для работы без сервиса git)

Данный раздел в интерфейсе пользователя доступен в поставке дистрибутива без сервиса git (Рисунок 29).

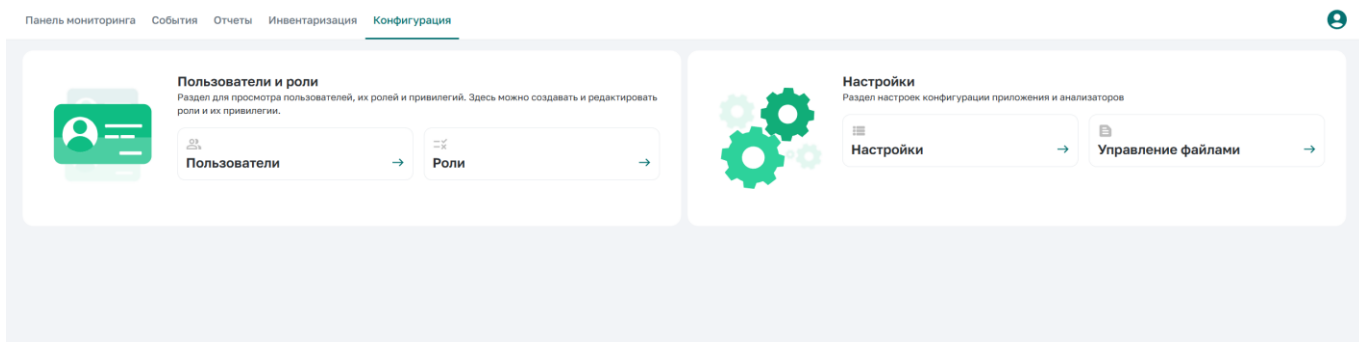


Рисунок 29 – Конфигурация

Настройки:

- Настройка - подраздел Конфигураций для настройки: правил Анализаторов, Ограничений хранения событий, Оповещений и Инвентаризации (Рисунок 30)

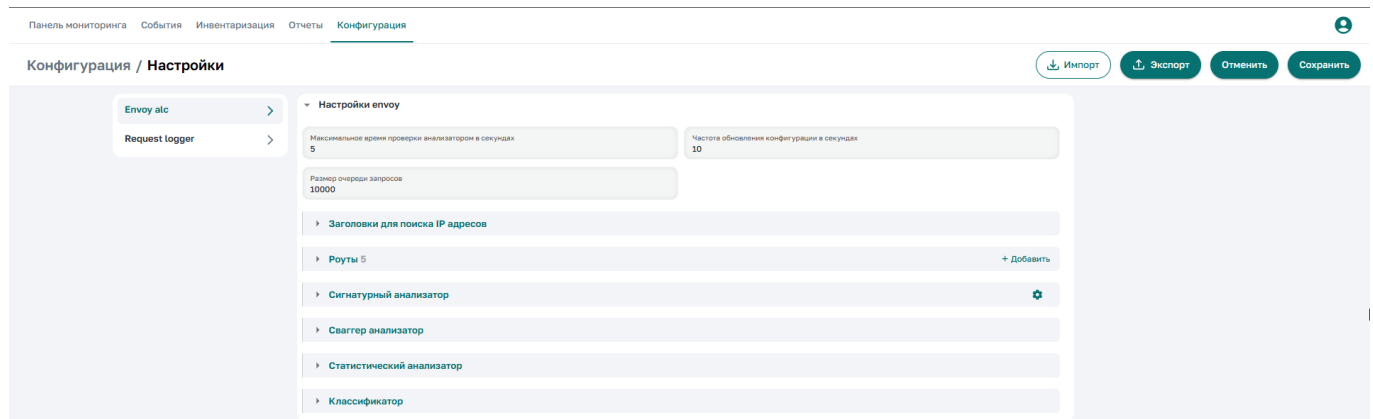


Рисунок 30 – Настройки

В верхней панели доступны кнопки:

- Импорт - загрузка конфигурации из файла
- Экспорт - сохранение текущих настроек;
- Отменить - откат несохранённых изменений
- Сохранить - применение текущих параметров

Раздел «Envoy alc»

Предназначен для настройки параметров работы прокси-сервиса и связанных с ним анализаторов.

При наведении курсора на свойства отображаются всплывающие подсказки с кратким описанием.

Настройки Envoy

В данном разделе задаются основные параметры работы сервиса (Рис 31)

- Максимальное время проверки анализатором (в секундах) - ограничивает время, в течение которого анализатор выполняет проверку запроса/ответа.
- Частота обновления конфигурации (в секундах) - определяет интервал обновления конфигурации сервиса.
- Размер очереди запросов - задаёт максимальное количество запросов/ответов, ожидающих обработки.

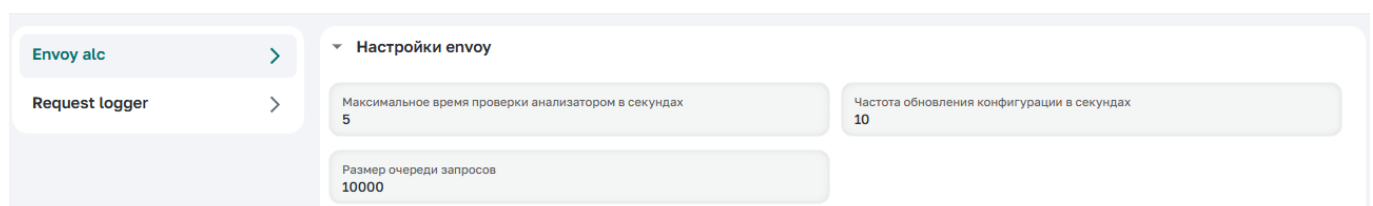


Рисунок 31 - Настройки envoy

Заголовки для поиска IP-адресов

Раздел «Заголовки для поиска IP-адресов» предназначен для указания HTTP-заголовков, из которых система будет определять реальный IP-адрес клиента. (Рис 32)

Пользователь может добавить один или несколько заголовков (например, X-Forwarded-For, X-Real-IP).

При обработке запроса envoy-als проверяет их и, если в одном из них найден корректный IP-адрес, записывает его в поле **IP отправителя** на странице "**События**".

Для добавления нового заголовка нажмите кнопку «+ **Заголовок**», введите его имя и сохраните изменения.

Пользователь может удалять ранее добавленные заголовки из списка нажав на кнопку удаления  справа от заголовка.

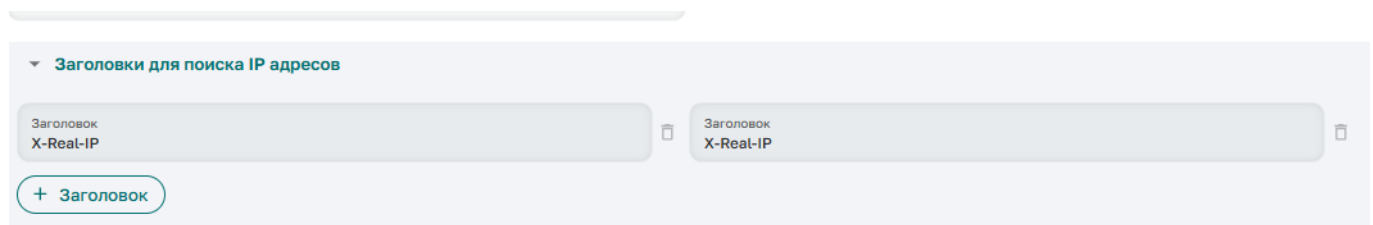


Рисунок 32 - заголовки для поиска IP адресов

Роуты

Раздел "Роуты" предназначен для настройки роутов, через которые проходят запросы в сервисе envoy-als. Каждый роут представляет собой отдельное приложение или сервис, для которого можно задать индивидуальные параметры работы и анализаторы. (Рис 33)

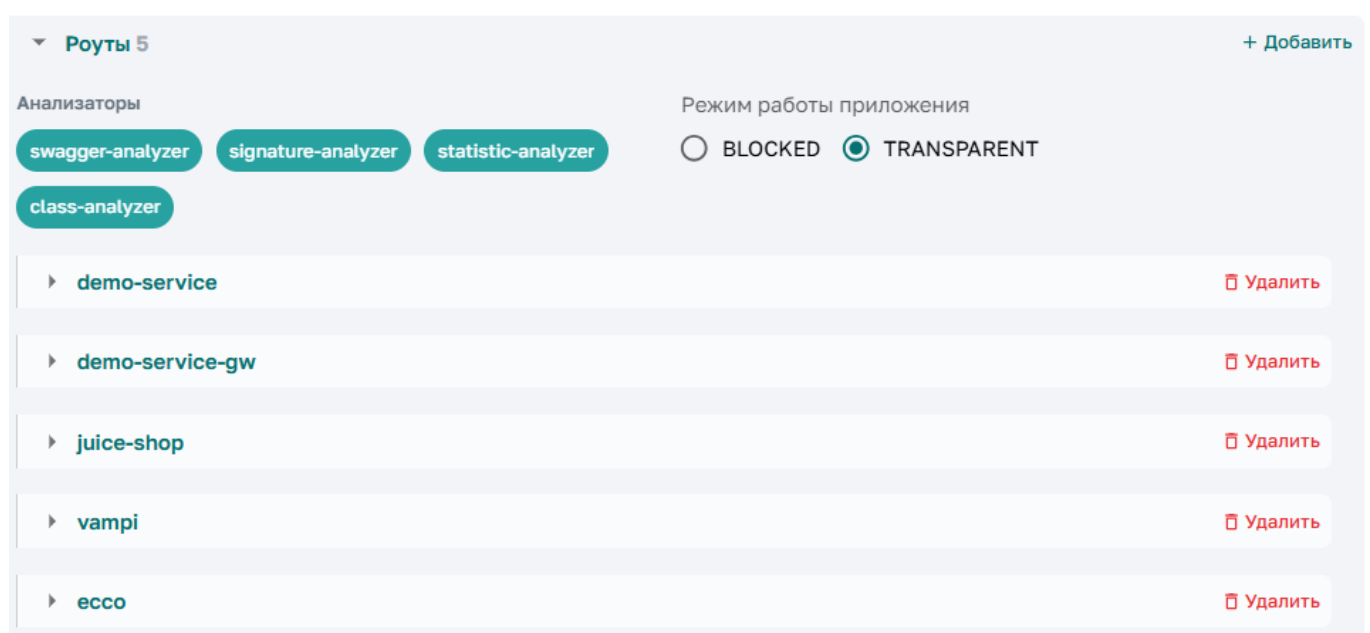


Рисунок 33 - Роуты

Основные элементы интерфейса:

- ✦ Добавить - добавление нового роута.
- ✦ Удалить - удаление выбранного роута.
- ✦ Режим работы приложения - задаёт общий режим обработки запросов:
 - BLOCKED — запросы блокируются при обнаружении нарушений.
 - TRANSPARENT - запросы проходят без блокировки, но фиксируются для анализа.

При добавлении или открытии конкретного роута отображаются настройки роутера - параметры, определяющие, как именно обрабатываются запросы для данного сервиса. (Рис 34)

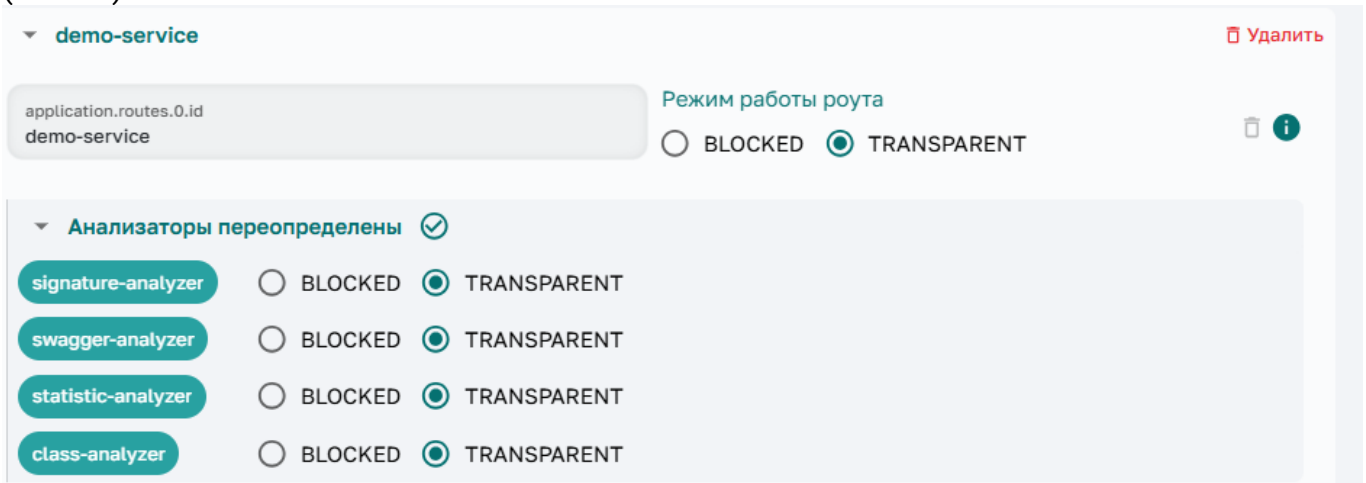


Рисунок 34 - Окно настройки параметров роута и режима анализаторов.

Пользователь может:

- ✦ Добавить новый роут, указав его идентификатор.
- ✦ Выбрать режим работы приложения и роута - BLOCKED или TRANSPARENT. Аналогично режиму приложения.
- ✦ Пользователь может удалить режим работы роута.
- ✦ Настроить активные анализаторы (signature-analyzer, swagger-analyzer, statistic-analyzer, class-analyzer).
- ✦ Сохранить изменения.

Сигнатурный анализатор

Сигнатурный анализатор — это модуль системы безопасности, предназначенный для выявления и блокировки вредоносных или нежелательных запросов на основе заранее определённых сигнатур. Он сравнивает входящие данные с базой известных шаблонов атак и уязвимостей, фиксируя совпадения и формируя отчёты о потенциальных угрозах. Основная задача анализатора - обеспечить раннее обнаружение типовых атак и повысить уровень защиты системы за счёт регулярного обновления сигнатурных правил.

В верхней части блока отображается параметр "Количество параллельных задач", который определяет, сколько потоков одновременно обрабатывают запросы.

Опция «**Несколько срабатываний за одну проверку**» позволяет управлять количеством сигнатур, фиксируемых анализатором в рамках одной проверки запроса. При активации чекбокса анализатор может фиксировать **несколько совпадений сигнатур** в рамках одной проверки запроса.

Если опция отключена, анализатор останавливает проверку после первого найденного совпадения.

Рядом расположена опция "Включить анализатор" - при активации модуль начинает анализировать входящие запросы в соответствии с заданными правилами.

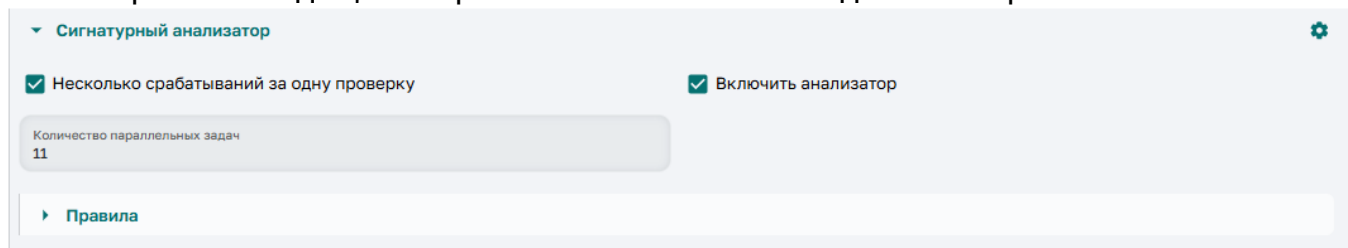


Рисунок 35 - Окно настройки параметров сигнатурного анализатора

Ниже находится подраздел "Правила", где задаётся параметр "Период обновления правил (сек.)" (Рисунок 36) - интервал, через который система автоматически обновляет сигнатурные базы.

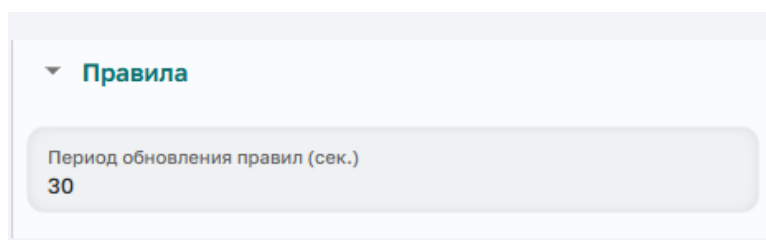


Рисунок 36 - Период обновления правил (сек.)

При нажатии на шестерёнку  в блоке открывается окно "Управление сигнатурными правилами". (Рисунок 37)

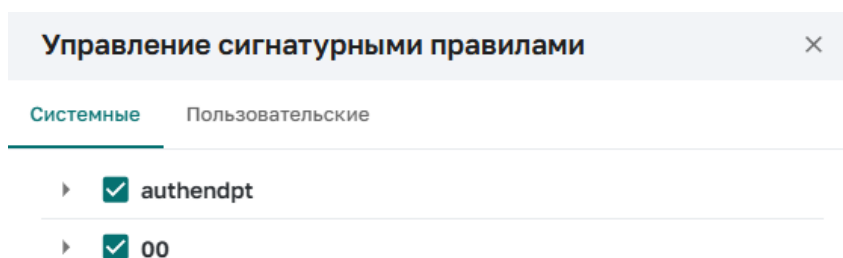


Рисунок 37 - Управление сигнатурными правилами

Окно содержит две вкладки:

- ⊕ Системные
- ⊕ Пользовательские

В каждой вкладке отображается список доступных сигнатурных правил. Пользователь может включать или отключать нужные правила, установив или сняв соответствующий чекбокс.

После внесения изменений необходимо нажать "Сохранить" (Рисунок 38), чтобы применить конфигурацию, либо "Отменить", чтобы вернуться к предыдущему состоянию, так же в нижней части окна указана дата последнего изменения конфигурации. например 04.11.2025 09:58:50.

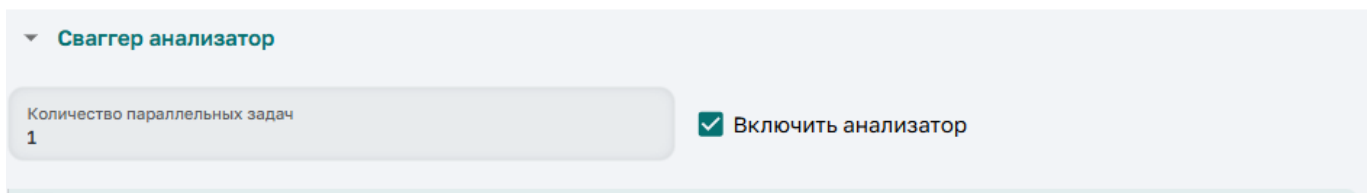
Рисунок 38 - Сохранить

Сваггер анализатор

Окно "Сваггер анализатор"(Рисунок 39) предназначено для настройки и управления анализом API-схем, используемых системой безопасности.

1) В верхней части блока находятся два основных параметра:

- ⊕ Количество параллельных задач задаёт, сколько процессов анализа могут выполняться одновременно.
- ⊕ Включить анализатор - активация этой опции запускает обработку загруженных Swagger-схем.



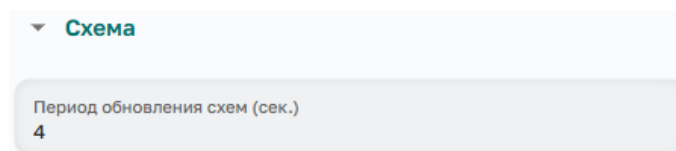
Сваггер анализатор

Количество параллельных задач
1

☒ Включить анализатор

Рисунок 39 - Сваггер анализатор

2) При открытии раздела "Схемы" пользователь может установить "Период обновления схем (сек)" (Рисунок 40)



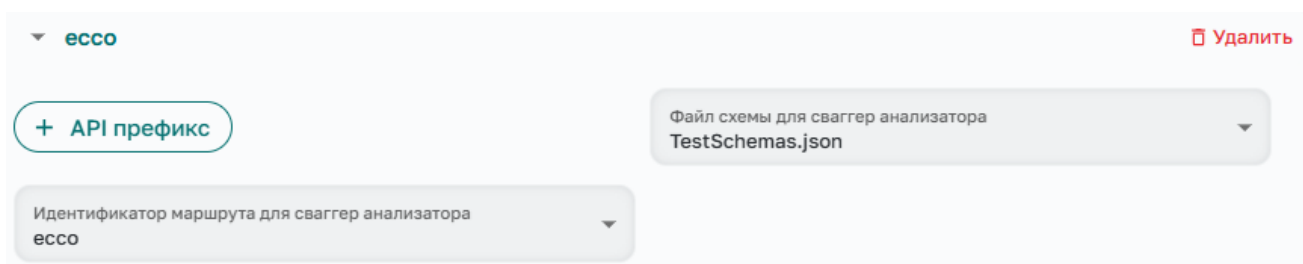
Схема

Период обновления схем (сек.)
4

Рисунок 40 - Период обновления схем (сек)

3) Параметры раздела "Роуты" (Рисунок 41)

- ⊕ Идентификатор маршрута - уникальное имя роута.
- ⊕ Файл схемы для Swagger-анализатора - JSON-файл, содержащий описание API-сервиса.
- ⊕ API-префикс - путь, по которому API-сервис использует вложенные маршруты. При необходимости API-префикс можно удалить, нажав на иконку справа.



ессо

Удалить

+ API префикс

Файл схемы для сваггер анализатора
TestSchemas.json

Идентификатор маршрута для сваггер анализатора
ессо

Рисунок 41 - Параметры раздела "Роуты"

Пользователь может:

- ⊕ Добавить новый роут с помощью кнопки "Добавить" + Добавить
- ⊕ Удалить существующий маршрут через кнопку "Удалить" справа от роута; Удалить

Статический анализатор

Окно "Статический анализатор" (Рисунок 42) предназначено для настройки правил анализа входящих запросов и определения ограничений по их количеству. В верхней части блока расположена опция "Включить анализатор", активирующая компонент, а также поле "Количество параллельных задач", задающее число одновременно выполняемых процессов анализа.

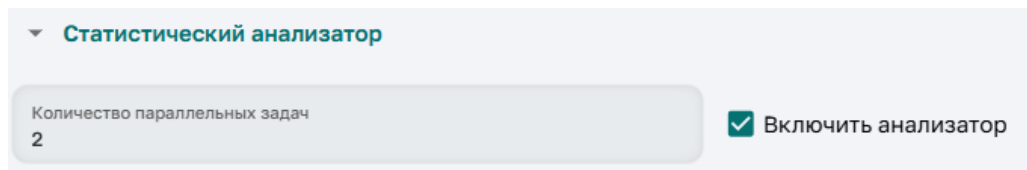


Рисунок 42 - Окно "Статический анализатор"

Статистический анализатор может работать в двух режимах:

Абсолютный и Относительный.

Абсолютный режим

В Абсолютном режиме (Рисунок 43) анализатор собирает статистику по запросам за указанный период времени, если кол-во запросов превышает указанное значение, все последующие запросы считаются как **FAIL**.

Ниже представлен раздел "Правила", где для каждого правила можно задать следующие свойства:

- ⊕ Идентификатор правила - уникальное имя правила;
- ⊕ Маршрут правила - выбирается из доступных маршрутов в выпадающем списке.
- ⊕ Режим работы
 - Абсолютный - собирает статистику по запросам за указанный период времени, если кол-во запросов превышает указанное значение, все последующие запросы считаются как FAIL.
 - Относительный - отслеживает процентное изменение нагрузки между двумя временными окнами и срабатывает при превышении порога.
- ⊕ Режим группировки - выпадающий список, в котором можно выбрать один из вариантов:
 - Все запросы (без группировок) - анализ всех запросов без группировки;
 - По IP-адресу - группировка по IP-адресу источника;
 - По пользователю - группировка по пользователю.
- ⊕ Размер временного окна в формате ISO 8601 — период, в течение которого учитываются запросы (например, PT15S, что соответствует 15 секундам).
- ⊕ Фильтр правила — выражение, определяющее, к каким запросам применяется правило. Пользователь может его удалить.

Рисунок 43 – Абсолютный режим Статистического анализатора

Пользователь может добавлять новые правила через кнопку "+Добавить" или удалять существующие с помощью кнопки "Удалить".

Относительный режим

Относительный режим (Рисунок 44) отслеживает процентное изменение нагрузки между двумя временными окнами и срабатывает при превышении порога.

Для относительного режима задаются параметры (помимо общих с абсолютным режимом):

- ⊕ **Порог изменения** - процент изменения количества запросов за период времени **duration**
- ⊕ **Минимальное количество запросов** - порог абсолютного количества запросов в текущем окне, когда срабатывает относительный порог

Отслеживается количество запросов в двух окнах, длительностью **duration** каждое: в "предыдущем" и в "текущем".

рост количества запросов (%) = (количество запросов в текущем окне - количество запросов в предыдущем окне) / (количество запросов в предыдущем окне)

В данном примере - правило сработает, если количество запросов увеличилось в два раза (Порог изменения: 100%) за последние пять минут (duration: PT5M) по сравнению с предыдущими пятью минутами, при условии, что за последние пять минут было не менее 200 (Минимальное количество запросов: 200) запросов от одного IP (group-mode: IP).

Рисунок 44 – Относительный режим Статистического анализатора

Примеры отображения относительного режима статистического анализатора:

1) Абсолютный режим, порог количества запросов не превышен (Рисунок 45).

Общее	Анализ запроса	Анализ ответа
Статистический анализ OK		
Дата анализа	23.01.2026 14:50:23	
Правило	demoAbsolute1	
Режим	Абсолютный	
Группировка	По IP-адресу	
IP-адрес	172.28.0.1	
Окно	1 мин	
Текущее значение	2 / 3	

Рисунок 45 – Абсолютный режим, порог не превышен

2) Абсолютный режим, порог количества запросов превышен (Рисунок 46).

Общее	Анализ запроса	Анализ ответа
Статистический анализ FAIL		
Дата анализа	23.01.2026 14:49:17	
Правило	demoAbsolute1	
Режим	Абсолютный	
Группировка	По IP-адресу	
IP-адрес	172.28.0.1	
Окно	1 мин	
Текущее значение	5 / 3	

Рисунок 46 – Абсолютный режим, порог превышен

3) Относительный режим, порог количества запросов не превышен (Рисунок 47).

Общее	Анализ запроса	Анализ ответа
Статистический анализ OK		
Дата анализа	23.01.2026 15:00:21	
Правило	demoRelative1	
Режим	Относительный	
Группировка	Все запросы (без группировки)	
Окно	10 сек	
Текущее значение	+50% 2 → 3, Порог: 100%, Минимум запросов: 2	

Рисунок 47 – Относительный режим, порог не превышен

4) Относительный режим, порог количества запросов превышен (Рисунок 48).

Общее	Анализ запроса	Анализ ответа
Статистический анализ		FAIL
Дата анализа	23.01.2026 15:00:25	
Правило	demoRelative1	
Режим	Относительный	
Группировка	Все запросы (без группировки)	
Окно	10 сек	
Текущее значение	+300% 2 → 8, Порог: 100%, Минимум запросов: 2	

Рисунок 48 – Относительный режим, порог превышен

Классификатор

Окно «Классификатор» (Рисунок 49) предназначено для настройки параметров анализа данных и определения типов информации, подлежащих классификации. В верхней части блока расположены поля:

- ✦ Длительность кэширования (сек.) - задаёт время хранения результатов анализа в кэше
- ✦ Частота проверки кэшированных запросов - определяет, как часто выполняется повторная проверка уже обработанных данных
- ✦ Количество параллельных задач - указывает, сколько процессов анализа могут выполняться одновременно
- ✦ Исключить заголовки из определения ключа кэширования - перечисление заголовков, которые не учитываются при формировании кэш-ключа.
- ✦ Ниже находится чекбокс «Включить анализатор», активирующий работу классификатора.

Классификатор

Длительность кэширования (сек.)
3

Частота проверки кэшированных запросов
2

Количество параллельных задач
1

Исключить заголовки из определения ключа кэширования
x-request-id, x-request-time, x-request-duration, date, x-envoy-upstr

☒ Включить анализатор

Рисунок 49 – Классификатор

В разделе «Роуты» (Рисунок 50) отображаются маршруты, для которых выполняется анализ данных.

Для каждого роута можно задать:

Маршрут анализа данных:

Пользователь может добавить новый маршрут с помощью кнопки «+ Добавить» и выбрать из выпадающего списка, а также удалить существующий через кнопку

«Удалить».

Разрешённые классы данных - выпадающий список, в котором пользователь выбирает типы данных, подлежащие анализу:

- ⊕ Адрес, местоположение
- ⊕ СНИЛС
- ⊕ Номер счёта
- ⊕ Email-адрес
- ⊕ ИНН
- ⊕ Номер телефона
- ⊕ Номер кредитной карты
- ⊕ ФИО
- ⊕ Паспорт

Выбор осуществляется с помощью чекбоксов.

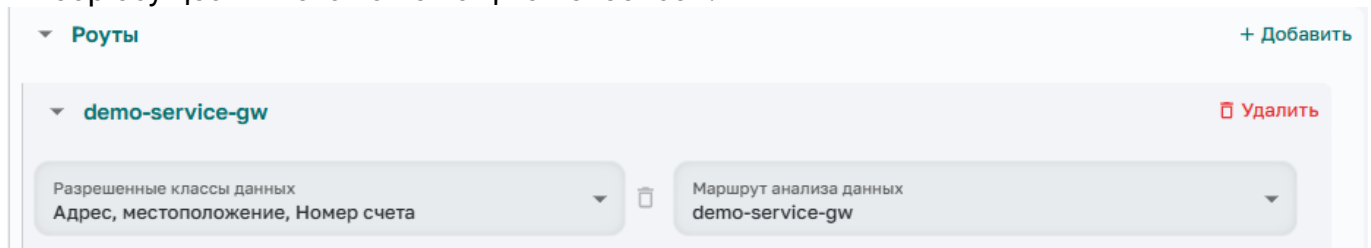


Рисунок 50 – Роуты Классификатора

Раздел: **Кастомные классы чувствительных данных:**

Раздел предназначен для создания и настройки пользовательских правил обнаружения чувствительных данных. Эти правила позволяют расширить возможности классификатора.

Описание полей:

- ⊕ **Класс данных** - устанавливается внутреннее имя класса;
- ⊕ **Наименование класса данных** - отображаемое имя, которое будет показано в интерфейсе;
- ⊕ **Регулярное выражение для поиска чувствительных данных** - шаблон (regex), по которому анализатор будет искать совпадения в тексте запроса или ответа.

Дополнительно:

Созданный кастомный класс (Рисунок 51) автоматически отображается во всех разделах системы, где выводится список классов чувствительных данных — например, в фильтрах, выпадающих списках и таблицах с результатами анализа.

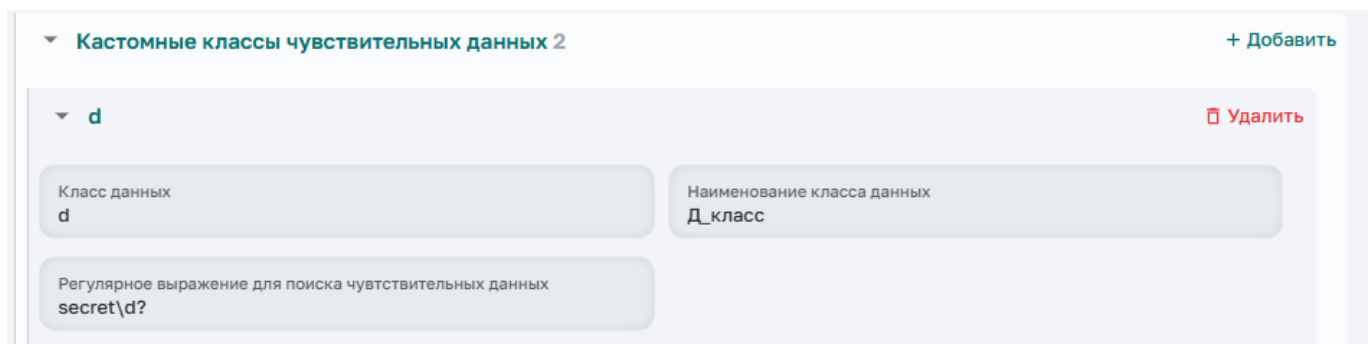


Рисунок 51 – Кастомный класс

Раздел: «**Настройки классов данных**» (Рисунок 52)

Раздел предназначен для управления параметрами анализа чувствительных данных (паспорт, ИНН, СНИЛС).

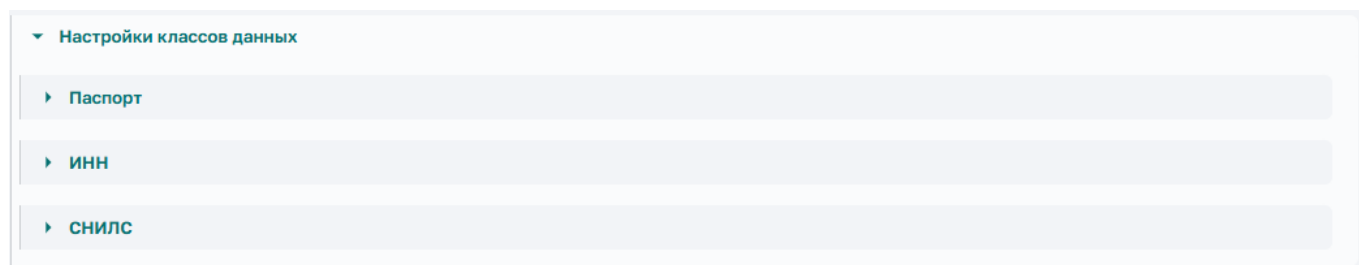


Рисунок 52 – Настройки классов данных

Для каждого класса данных можно (Рисунок 53):

- ⊕ включить или отключить использование ключевых слов;
- ⊕ задать список ключевых слов, по которым анализатор будет искать совпадения;
- ⊕ указать **максимальную дистанцию поиска ключевых слов** - количество символов, в пределах которых анализатор ищет ключевое слово относительно найденного числового значения.

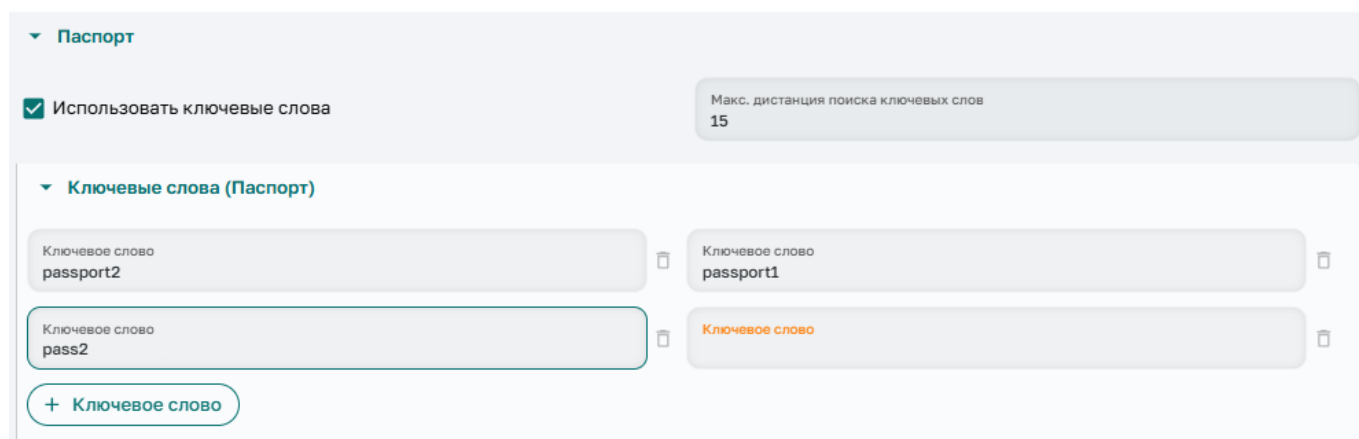


Рисунок 53 – Настройки классов «Паспорт»

Добавление и удаление ключевых слов выполняется вручную через кнопку «**+ Ключевое слово**».

Раздел Request-logger

В верхней части блока отображается поле «Диапазоны CIDR»(Рисунок 54), в котором указываются IP-диапазоны частной сети, из которой осуществляется доступ к защищаемым ресурсам.

Например:

10.3.0.0/16, 172.16.0.0/12, 192.167.0.0/16

В инвентаризации они отображаются как **PRIVATE**.

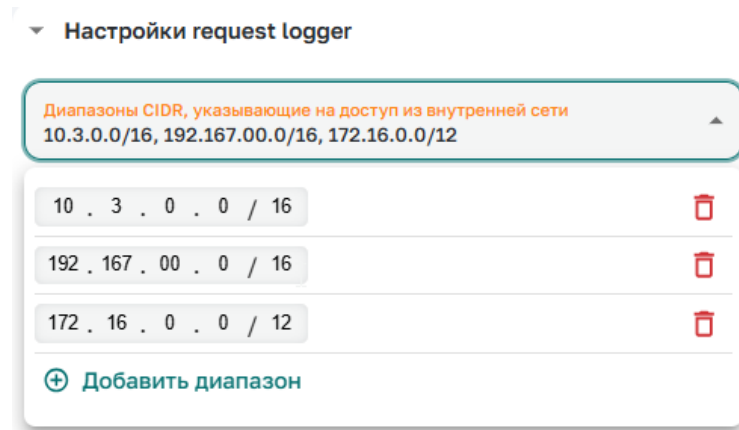


Рисунок 54 – Диапазоны CIDR

Маскирование данных

Окно «Маскирование данных» (Рисунок 55) предназначено для настройки правил скрытия конфиденциальной информации в логах запросов и ответов.

В верхней части блока расположены параметры:

- ⊕ Включить маскирование данных - активирует работу механизма маскирования
- ⊕ Маскировать чувствительную информацию - включает автоматическое скрывание данных, относящихся к определённым классам.

В выпадающем списке «Классы чувствительной информации» доступны следующие типы данных и выбор классов осуществляется с помощью чекбоксов.:

- ⊕ Адрес, местоположение
- ⊕ Номер счёта
- ⊕ Номер кредитной карты
- ⊕ Название компании
- ⊕ Email-адрес
- ⊕ ФИО
- ⊕ ИНН
- ⊕ Паспортные данные
- ⊕ Номер телефона
- ⊕ СНИЛС

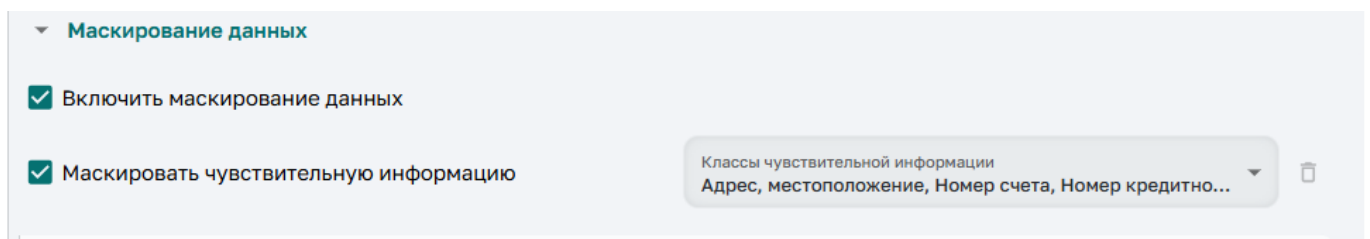


Рисунок 55 – Маскирование данных

Ниже располагается раздел «Правила» (Рисунок 56), где можно добавить и задать конкретные условия маскирования.

Пример правила:

- ⊕ Что маскировать:
 - URL;

- Заголовок запроса;
- Заголовок ответа;
- Тело запроса;
- Тело ответа.

✦ Можно маскировать заголовок: например: `X-Some-Secret-Id`;

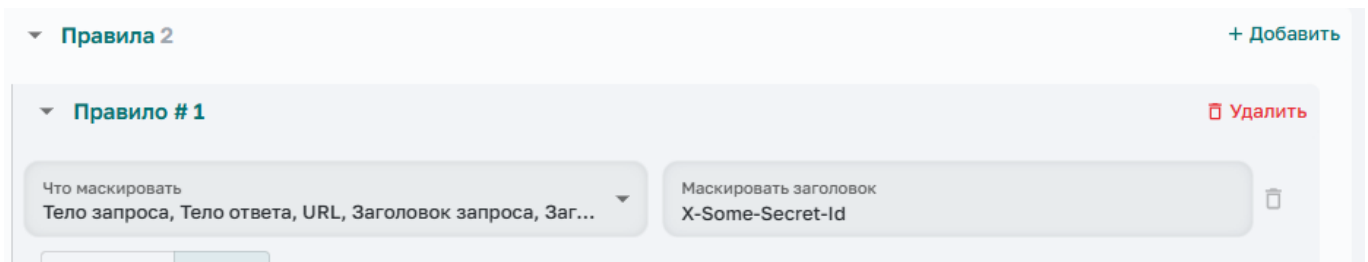


Рисунок 56 – Правила Маскирования данных

✦ Тип фильтра: `REGEX` или `JSONPATH`;

- При выборе фильтра REGEX (Рисунок 57) используется регулярное выражение. Например: регулярное выражение "some_\w+" и access_log_analyzers_view ищет все подстроки, начинающиеся с "some_" за которыми следуют буквы, цифры или подчеркивания. При тестировании (Протестировать) справа отображается совпадение - some_123, значит выражение сработало

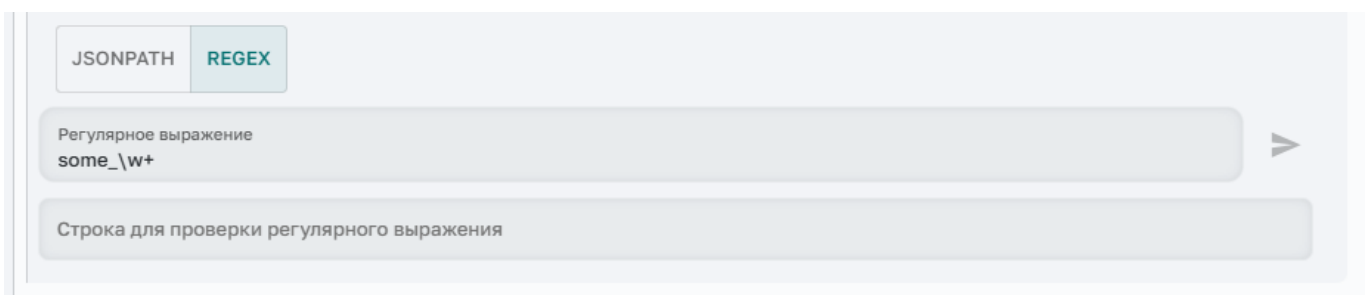


Рисунок 57 – Тип фильтра REGEX

- ✦ При выборе фильтра JSONPath (Рисунок 58) - используется механизм маскирования конкретных полей внутри JSON-структуры. В поле JSON PATH указывается путь к элементу, например: \$.user.password – маскирует значение поля password в объекте user.

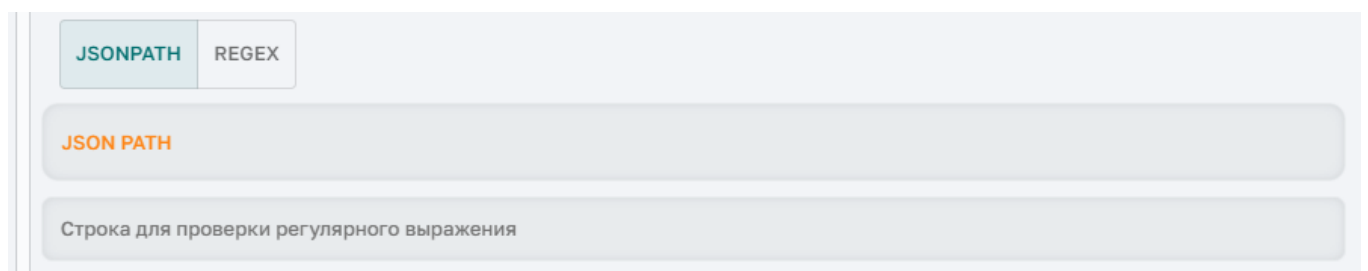


Рисунок 58 – Тип фильтра JSONPATH

Пользователь может добавлять новые правила с помощью кнопки «+ Добавить» или удалять существующие через «Удалить».

Ограничение хранения событий

При открытии раздела «Ограничение хранения событий» отображается сводная панель, включающая два основных блока:

- ⊕ **Общий фильтр** - задаёт параметры фильтрации и ограничения (Рисунок 59);
- ⊕ **Фильтр для роутов** - позволяет задать индивидуальные фильтры и лимиты для конкретных маршрутов. На панели также расположена кнопка «+ Добавить», с помощью которой можно добавить новый фильтр для отдельного роута.

Блок «**Общий фильтр**» предназначен для задания условий фильтрации и ограничений. В верхней части блока расположена опция «Включить фильтр» - при активации параметра фильтрация запросов становится активной для всех маршрутов. Ниже находится поле «Фильтр (выражение)», где задаётся условие для отбора событий. Например: `request.url =~ "^/product.*"`. Поле поддерживает синтаксис выражений **JEXL**. Это правило будет работать только для событий которое подпадает под фильтр. (можно удалить нажав на иконку справа)

Следующий параметр - «+Критерий группировки», после создания которого в выпадающем списке можно выбрать `method` и `URL` чекбоксом (можно удалить нажав на иконку справа).

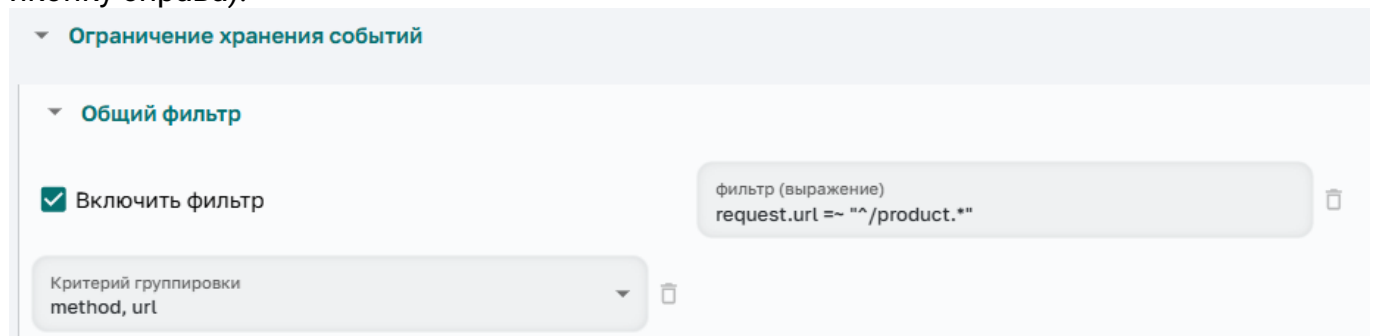


Рисунок 59 – подраздел «Общий фильтр»

Ниже расположен подраздел «Ограничения», где задаются параметры лимитов (Рисунок 60):

- ⊕ Максимальное количество запросов
- ⊕ Размер временного окна - указывается в формате ISO 8601

Блок «Фильтр для роутов»

Для каждого роута доступны следующие параметры:

- ⊕ Пользователь может добавить или удалить роут;
- ⊕ Включить фильтр - активирует применение фильтрации для выбранного роута;
- ⊕ Фильтр (выражение) - задаёт условие отбора событий. (Можно удалить)
- ⊕ Критерий группировки, в выпадающем списке которого доступны следующие значения: `method` и `url`

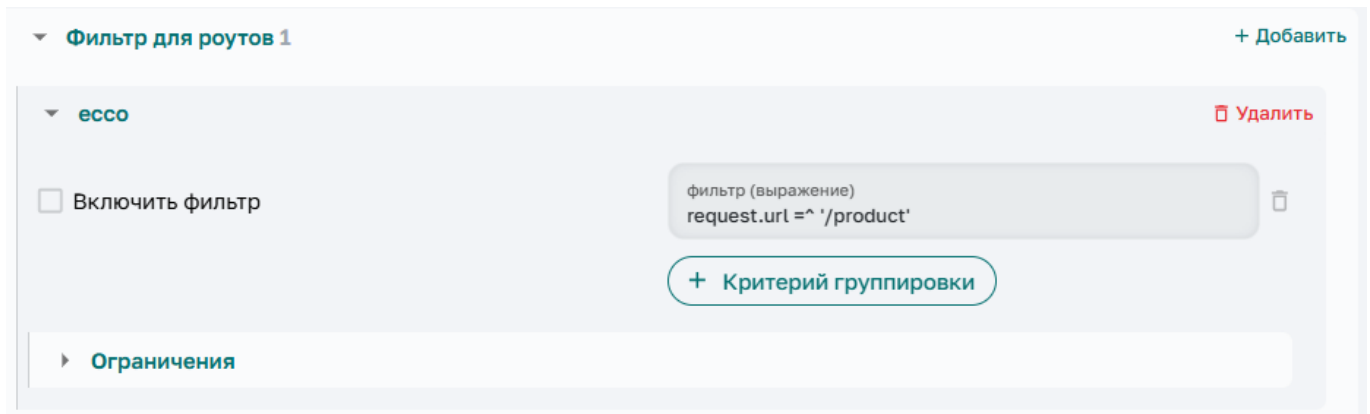


Рисунок 60 – подраздел «Ограничения»

Ниже расположен подраздел «Ограничения», где задаются лимиты:

- ⊕ Максимальное количество запросов
- ⊕ Размер временного окна в формате ISO 8601- для изменения параметра используется иконка "Настроить".

В выпадающем списке «Формат» доступны два варианта:

- ⊕ «Год, месяц, день» — позволяет задать окно в разрезе календарных единиц (годы, месяцы, дни, часы, минуты, секунды).

- «Неделя» задаёт окно в неделях, что удобно для агрегирования статистики за длительные периоды.

Поля конструктора позволяют вручную указать числовые значения для каждой единицы времени.

Например, при выборе формата «Год, месяц, день» и указании 0 лет, 0 месяцев, 0 дней, 0 часов, 5 минут, 0 секунд

система автоматически сформирует значение `PT5M`, что соответствует пяти минутам.

Полученное значение отображается в поле «Размер временного окна в формате ISO 8601».

Конструктор временного окна в формате ISO 8601

Формат Год, месяц, день		
Года 0	Месяца 0	Дни 0
Часы 0	Минуты 5	Секунды 0

Рисунок 61 – Конструктор временного окна

Оповещения

Раздел «Правила»

Раздел предназначен для создания и настройки правил оповещений, определяющих, при каких условиях система будет отправлять уведомления в SIEM.

При добавлении нового правила пользователь может выбрать **роут (route)**, к которому

это правило будет применяться. Роут определяет конкретный сервис или маршрут, для которого система отслеживает события и формирует оповещения. Например, можно выбрать один из доступных роутов: vampi, ecco, demo-service-gw, juice-shop и т.д.

После выбора роута доступны следующие параметры настройки:

- ✦ **Анализаторы** - модули, которые обрабатывают события и формируют оповещения:
 - signature-analyzer - анализирует сигнатуры запросов;
 - swagger-analyzer - проверяет соответствие запросов спецификациям API;
 - statistic-analyzer - собирает статистику обращений;
 - class-analyzer - классифицирует типы событий.

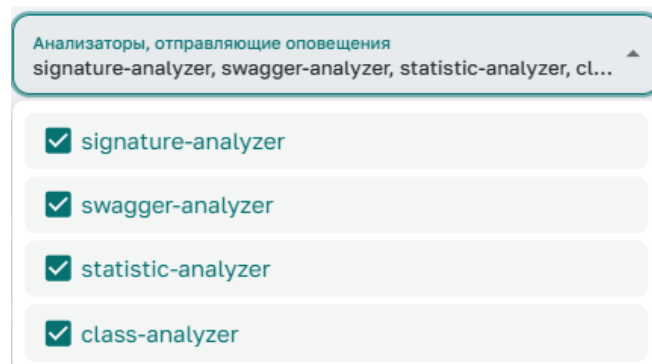


Рисунок 62 – Анализаторы

- ✦ **Статус запросов для отправки оповещений в SIEM** - задаёт, при каких результатах запросов будет срабатывать правило:
 - **OK** - при успешных запросах;
 - **FAIL** - при ошибках или сбоях.

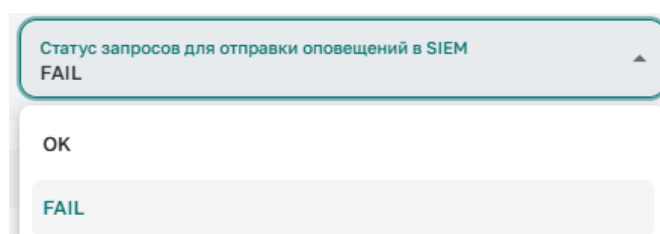


Рисунок 63 – Статус запросов для отправки оповещений в SIEM

- ✦ **Формат отправки оповещения** — определяет формат данных, в котором сообщение передаётся в SIEM (например, cef, rsyslog - отображаются по умолчанию) Пользователь может добавлять, редактировать или удалять правила.

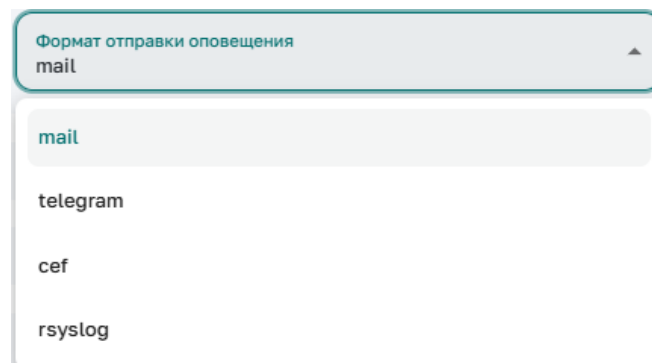


Рисунок 64 – Формат отправки оповещения

- ⊕ **Фильтр** - дополнительное условие, уточняющее, при каких событиях будет срабатывать правило.
Фильтр задаётся в виде выражения или регулярного шаблона. Например: (request.url == '/ci') - оповещение отправляется только для запросов, чей URL точно равен /ci.

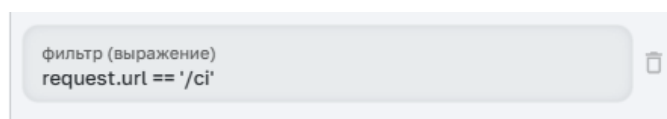


Рисунок 65 – Фильтр

Пользователь может добавлять, редактировать и удалять правила, а также комбинировать фильтры и анализаторы для гибкой настройки логики оповещений.

Раздел «Цели»

Раздел предназначен для настройки каналов доставки оповещений, которые используются правилами из предыдущего раздела.

Пользователь может **добавить новую цель** или **удалить существующую**. Каждая цель определяет, куда будут отправляться уведомления при срабатывании правил.

При создании новой цели необходимо выбрать **тип таргета** (канал отправки оповещений). Доступные варианты:

- ⊕ **rsyslog** - отправка сообщений в системный журнал;
- ⊕ **cef** - передача данных в формате Common Event Format;
- ⊕ **mail** - отправка уведомлений по электронной почте;
- ⊕ **telegram** - отправка сообщений в Telegram.

Цель "mail"

При выборе типа **mail** появляются дополнительные поля для настройки SMTP-параметров:

- ⊕ **SMTP хост** - адрес почтового сервера;
- ⊕ **Порт** - порт целевой системы оповещения;
- ⊕ **SMTP имя пользователя** и **SMTP пароль** - учётные данные для авторизации;
- ⊕ **От (email)** - адрес отправителя;
- ⊕ **Кому (email)** - адрес получателя;
- ⊕ **Тема письма** - заголовок уведомления;

⊕ **Включить TLS** - опция для защиты соединения.

mail Удалить

Smtp хост
smtp.yandex.ru

Порт для целевой системы оповещения
587

☒ Включить TLS

Smtp имя пользователя
aleksei.@squadsec.ru

Smtp пароль
nfnhpdeflaiqakkn

От (email)
aleksei.@squadsec.ru

Кому (email)
aleksei.@squadsec.ru

Тема письма
test1

Рисунок 66 – формат mail

2) Цель "CEF" и "rsyslog"

Типы целей **CEF (Common Event Format)** и **rsyslog** используются для отправки оповещений в системы SIEM. Оба типа имеют одинаковые настройки подключения и отличаются только форматом передаваемых данных.

При создании цели CEF или rsyslog необходимо указать:

- ⊕ **Имя хоста** - адрес целевой системы оповещений;
- ⊕ **Порт** - порт, на который будет отправляться трафик (по умолчанию 514);
- ⊕ **Транспорт для целевой системы** - протокол передачи данных, выбирается из выпадающего списка:
 - **UDP** - используется по умолчанию, обеспечивает быструю, но небезопасную передачу;
 - **TCP** - обеспечивает надёжную доставку сообщений с контролем соединения.

cef Удалить

Имя хоста для цели оповещения
cef_host1

Порт для целевой системы оповещения
514

Транспорт для целевой системы
udp

Рисунок 67 – формат cef

3) Цель "Telegram"

Тип цели Telegram используется для отправки оповещений напрямую в чат Telegram.

При создании цели необходимо указать два обязательных параметра:

- ⊕ **ID телеграм-чата** - уникальный идентификатор чата, куда будут поступать уведомления;

- ⊕ **Telegram API токен** - токен доступа, который выдает @BotFather при создании собственного бота.

Рисунок 68 – формат telegram

Инвентаризация

Раздел предназначен для настройки параметров, по которым система собирает и отображает данные о запросах и сервисах.

При нажатии на блок «Инвентаризация» раскрывается панель с дополнительными свойствами.

- ⊕ **«Список HTTP-статусов, участвующих в инвентаризации».**
Здесь можно выбрать, какие коды HTTP-ответов будут учитываться при сборе данных.

Рисунок 69 – Инвентаризация

- ⊕ **«Синхронизация с базой данных»**, где задаются параметры синхронизации:
 - **Порог слияния для синхронизации инвентаризации** - минимальное количество записей, при котором запускается процесс синхронизации
 - **Количество запросов для запуска синхронизации** - определяет, после какого числа запросов выполняется обновление данных
 - **Количество секунд с последнего запроса до запуска синхронизации** - задаёт интервал времени между циклами синхронизации

Рисунок 70 – Синхронизация с базой данных

База данных

Раздел предназначен для управления параметрами хранения данных, собранных сервисом Request Logger.

При нажатии на блок «База данных» раскрывается подраздел «**Партиции**», где задаётся период хранения данных.

Параметр «**Период хранения данных для раздела базы данных (в месяцах)**» определяет, сколько времени логи и события будут сохраняться в БД перед их автоматическим удалением.

Управление файлами

Подраздел Конфигураций для добавления Файлов сваггер схем, для добавления и редактирования Файлов сигнатур (Рисунок 71)

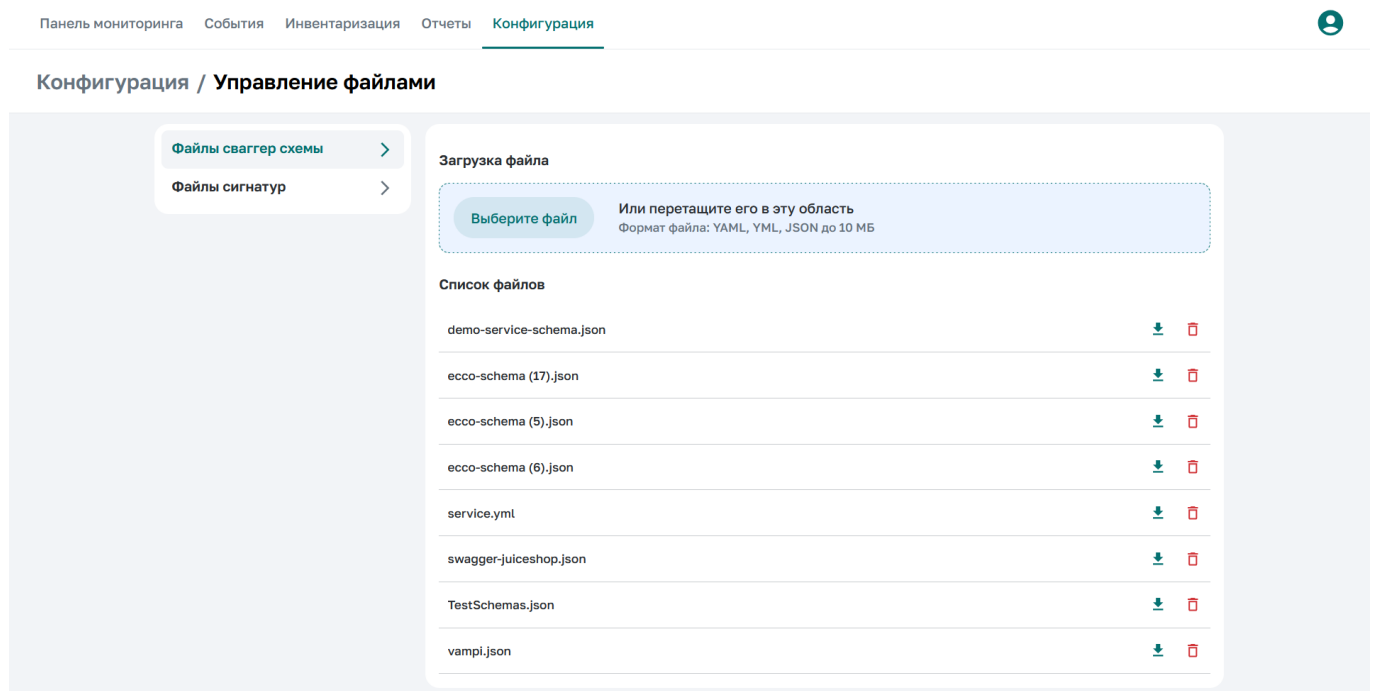


Рисунок 71 – Управление файлами

Пользователи и роли.

Раздел предназначен для управления учетными записями пользователей и их ролями в системе.

Раздел "Пользователи" (Рисунок 72)

Панель мониторинга

События

Инвентаризация

Отчеты

Конфигурация

Конфигурация / Пользователи и роли

Поиск

Пользователи	Роли
Логин ↑	Роль
ADMIN	Configurator
usr	Configurator, User
usr2	User

Размер страницы 25

1-3 из 3

Страница 1 из 1

Рисунок 72 – Пользователи

Раздел предназначен для управления учетными записями пользователей и их ролями в системе. При открытии раздела **Пользователи и роли** отображается вкладка **Пользователи**, где представлен список всех пользователей. В таблице указаны логины, назначенные роли и дата последнего входа в систему.

При нажатии на конкретного пользователя (например, ADMIN) в правой части окна открывается панель с подробной информацией о выбранном пользователе.

- ⊕ основные данные пользователя;
- ⊕ список назначенных ролей.

При нажатии на стрелку рядом с названием роли раскрывается список привилегий, входящих в данную роль.

Таким образом, пользователь может просмотреть, какие роли и привилегии назначены каждому пользователю системы.

Данные пользователя
×

ADMIN

Роли и привилегии

▼ Configurator

Привилегии: 4

Разрешается изменение настроек приложений

Разрешается получение конфигурации ролей и привилегий

Разрешается изменение конфигурации ролей и привилегий

Разрешается получение настроек приложений

► User

Привилегии: 2

► usr3

Привилегии: 6

Последний вход:

Редактировать

Рисунок 73 – Роли и привилегии

При нажатии на кнопку **Редактировать** в карточке выбранного пользователя открывается режим редактирования.

В этом режиме отображается окно **Данные пользователя**, где можно:

Данные пользователя
×

ADMIN

Назначенные роли

Configurator
×

User

×

Все роли

Поиск

+ usr3

Последний вход:

Отменить

Сохранить

Рисунок 74 – Назначенные роли

В верхней части окна отображается имя пользователя (например, ADMIN). Ниже расположен блок **Назначенные роли**, где перечислены все роли, уже закрепленные за пользователем. Каждую роль можно удалить, нажав на крестик рядом с её названием. Чтобы добавить новую роль, необходимо нажать на значок **плюс (+)** рядом с её названием. После этого выбранная роль появится в списке **Назначенные роли**.

Для сохранения изменений нажмите **Сохранить**. Чтобы отменить изменения - **Отменить**.

Раздел "Роли"

Раздел «Роли»

Во вкладке **Роли** (Рисунок 75) отображается список всех ролей, доступных в системе. Для каждой роли указаны:

- ⊕ **Название** роли;
- ⊕ **Описание** (если задано);
- ⊕ **Количество назначений** - сколько пользователей имеют данную роль;
- ⊕ **Количество привилегий**, входящих в роль.
- ⊕ **Дата создания**

Панель мониторинга События Инвентаризация Отчеты Конфигурация Конфигурация / Пользователи и роли Поиск Создать роль					
Пользователи Роли					
Название ↑	Описание	Назначена	Привилегии	Дата создания	
Configurator	-	2	4	02.07.2025 11:06:08	
User	Базовые привилегии	2	2	02.07.2025 11:06:08	
usr3	...	0	6	14.10.2025 18:47:19	

Размер страницы

25

1-3 из 3

Страница

1 из 1

Рисунок 75 – Роли

При нажатии на название роли (например, **Configurator**) в правой части экрана открывается панель **Данные роли**.

В панели отображается:

- ⊕ название роли;
- ⊕ количество пользователей, которым назначена эта роль (например, *Пользователей с ролью: 2*);
- ⊕ количество привилегий (например, *Привилегий: 4*);
- ⊕ список всех привилегий, входящих в роль.

Пример:

Для роли **Configurator** отображаются следующие привилегии:

- ⊕ Разрешается изменение настроек приложений;
- ⊕ Разрешается получение конфигурации ролей и привилегий;
- ⊕ Разрешается изменение конфигурации ролей и привилегий;
- ⊕ Разрешается получение настроек приложений.

В нижней части панели указана **дата создания** роли. Также доступны кнопки **Удалить** и **Редактировать** для управления ролью.

При нажатии на ссылку **Пользователей с ролью: 2** открывается дополнительное окно слева.

В этом окне отображается список всех пользователей, которым назначена выбранная роль. Для каждого пользователя указано:

- ⊕ имя пользователя (например, ADMIN, usr);
- ⊕ количество ролей, назначенных пользователю;
- ⊕ список этих ролей в виде меток.

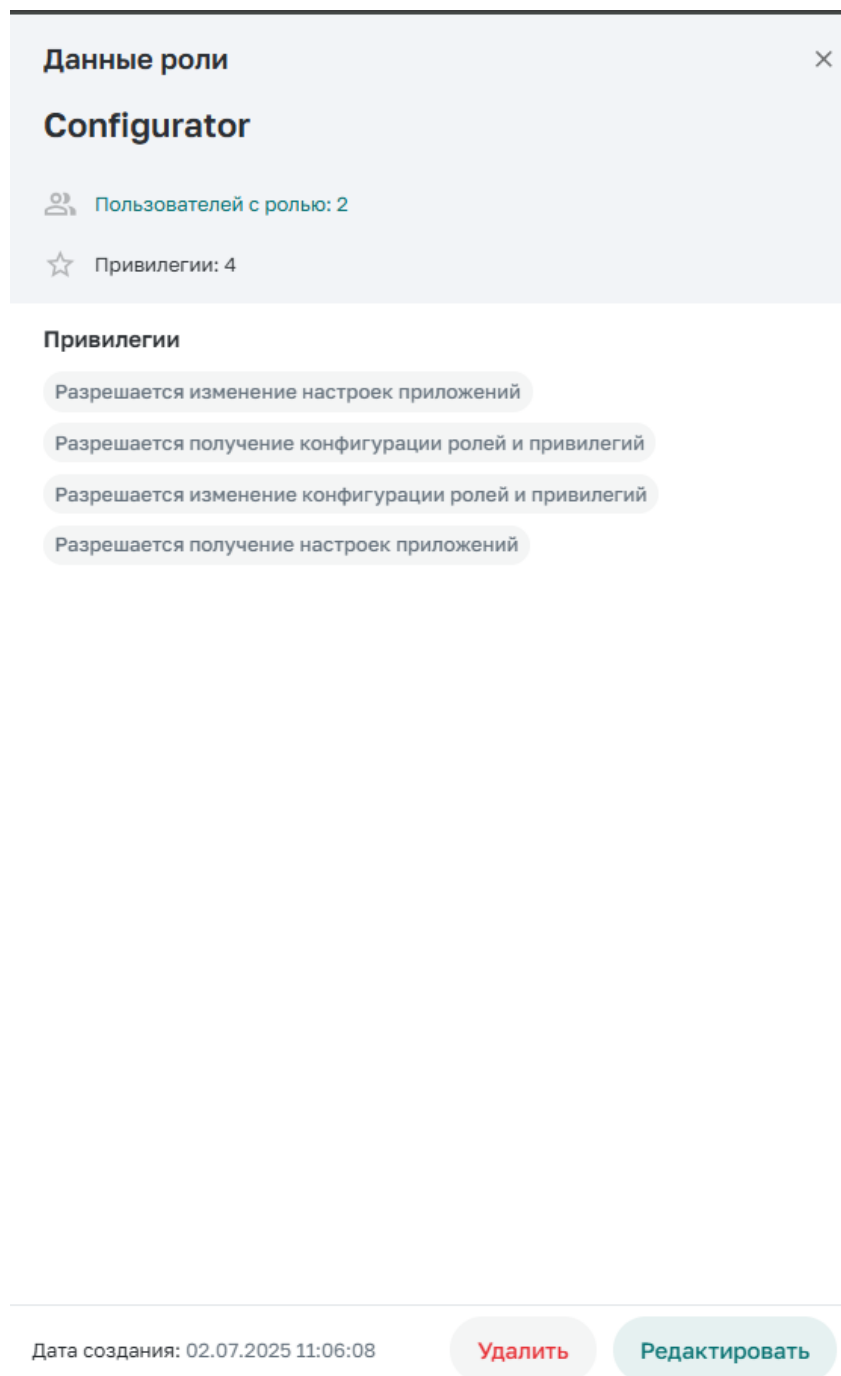


Рисунок 76 – Привилегии роли

При нажатии на ссылку **Пользователей с ролью: 2** открывается дополнительное окно слева (Рисунок 77).

В этом окне отображается список всех пользователей, которым назначена выбранная роль. Для каждого пользователя указано:

- ⊕ имя пользователя (например, ADMIN, usr);
- ⊕ количество ролей, назначенных пользователю;
- ⊕ список этих ролей в виде меток.

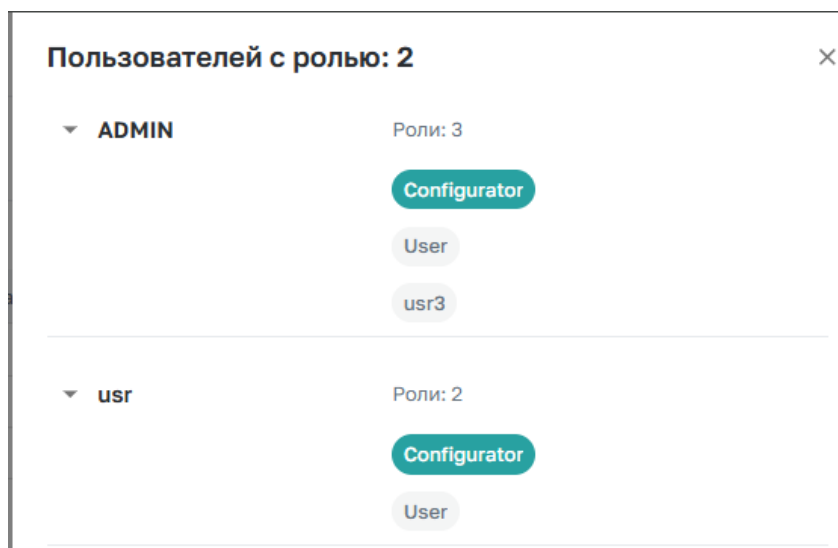


Рисунок 77 – Пользователи с ролью: 2

При нажатии на кнопку **Редактировать** в карточке выбранной роли открывается окно **Редактирование роли**.

В верхней части окна отображаются поля:

- ⊕ **Название** - текущее имя роли (например, *Configurator*);
- ⊕ **Описание** - текстовое поле для добавления или изменения описания роли.

При нажатии на кнопку **Редактировать** в карточке выбранной роли открывается окно **Редактирование роли**.

В верхней части окна отображаются поля:

- ⊕ **Название** - текущее имя роли (например, *Configurator*);
- ⊕ **Описание** - текстовое поле для добавления или изменения описания роли.

Ниже расположен блок **Назначенные привилегии**, в котором перечислены все привилегии, уже входящие в данную роль. Каждая привилегия представлена в виде метки с возможностью удаления (крестик справа).

Под ним находится раздел **Все привилегии**, содержащий полный список доступных привилегий, которые можно добавить в роль.

Для добавления новой привилегии необходимо нажать на значок **плюс (+)** рядом с её названием.

Также предусмотрено поле **Поиск**, позволяющее быстро найти нужную привилегию по названию.

Редактирование роли

×

Название

Configurator

Описание

Назначенные привилегии

Разрешается изменение настроек приложений ×

Разрешается получение конфигурации ролей и привилегий ×

Разрешается изменение конфигурации ролей и привилегий ×

Разрешается получение настроек приложений ×

Все привилегии

🔍

Поиск

+ Разрешается чтение тела запроса

+ Разрешается чтение тела ответа

Отменить

Сохранить

Рисунок 78 – Редактирование роли

Для добавления новой роли необходимо нажать кнопку **Создать роль** во вкладке **Роли**.

После нажатия открывается окно **Создание роли** (Рисунок 79) в правой части экрана.

В окне доступны следующие поля и элементы управления:

- ⊕ **Название** - текстовое поле для ввода имени новой роли.
- ⊕ **Описание** - поле, в котором можно указать назначение или краткое описание роли.

Ниже расположен блок **Назначенные привилегии**.

Пока роль не создана, этот блок пуст и содержит надпись «*Выберите привилегии для этой роли*».

Под ним находится раздел **Все привилегии**, где представлен полный список доступных

привилегий.

Каждая привилегия отображается в виде строки с кнопкой **плюс (+)** справа.

Чтобы добавить привилегию в создаваемую роль, необходимо нажать на **плюс (+)** рядом с её названием. После этого привилегия появится в списке **Назначенные привилегии**.

Для удобства предусмотрено поле **Поиск**, позволяющее быстро найти нужную привилегию по названию.

В нижней части окна расположены кнопки:

- ⊕ **Создать** - сохраняет новую роль с выбранными параметрами;
- ⊕ **Отменить** - закрывает окно без сохранения.

После успешного создания роль появляется в общем списке ролей на вкладке **Роли**.

Создание роли

Название

Описание

Назначенные привилегии

Выберите привилегии для этой роли

Все привилегии

Поиск

+ Разрешается изменение настроек приложений

+ Разрешается чтение тела запроса

+ Разрешается получение конфигурации ролей и привилегий

+ Разрешается изменение конфигурации ролей и привилегий

+ Разрешается получение настроек приложений

+ Разрешается чтение тела ответа

Отменить

Создать

Рисунок 79 – Создание роли

Завершение работы

Для выхода из приложения нажмите на иконку в правом верхнем углу веб-страницы, а затем нажмите "Выйти".

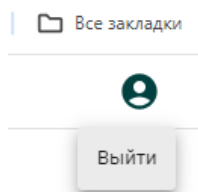


Рисунок 80 – Выход из Q-APISec

Сценарии использования

Приведём основные сценарии использования Q-APISec пользователем ПО.

Мониторинг безопасности API

В разделе "Панель мониторинга" пользователь может отслеживать основную информацию о работе Q-APISec:

- ✦ Оценивать состояние API по количеству успешных запросов.
- ✦ Оценивать количество запросов, на которые защищаемые сервисы ответили ошибкой.
- ✦ Определять регион, из которого осуществляются атаки.
- ✦ Определять IP, с которых атаки наиболее активны.
- ✦ Определять тип наиболее частых атак на защищаемый API.
- ✦ Составлять отчёты о характере запросов и инцидентах.

Инвентаризация API и анализ отдельного эндпоинта

В разделе "Инвентаризация" имеются функциональности для инвентаризации используемых веб-приложениями API. Пользователь может:

- ✦ Следить за здоровьем и уровнем угроз всего API, отдельного роута или отдельного эндпоинта.
- ✦ Классифицировать передаваемые чувствительные данные и оценивать частоту их передачи во времени.
- ✦ Узнать параметры и их тип для отдельного эндпоинта.
- ✦ Проверить журнал событий для выбранного эндпоинта.
- ✦ Экспортировать swagger схему, построенную на основе запросов к API.

Профилирование и мониторинг конкретного API

В разделе "Профиль API" имеются функциональности для профилирования используемых веб-приложениями API. Пользователь может:

- ✦ Перемещаться по дереву API-эндпоинтов и выбрать интересующий эндпоинт для мониторинга.
- ✦ Следить за динамикой здоровья и уровнем угроз всего API или отдельного

эндпоинта.

- ✦ Классифицировать передаваемые чувствительные данные и оценивать частоту их передачи во времени.
- ✦ Проверить журнал событий для выбранного эндпоинта.
- ✦ Фильтровать события по различным параметрам: статусы, даты, методы, IP-адреса и др.

Анализ событий HTTP-запросов

При выявлении атак или ошибок в работе веб-приложения пользователь может перейти в раздел **События** для просмотра данных обо всех HTTP-запросах, проходящих через Q-APISec. Пользователь может:

- ✦ Выполнить поиск событий по различным параметрам, включая результаты проверки анализаторами.
- ✦ Узнать причину, по которой запрос не прошёл проверку анализатором.

Виды анализа (тип анализатора):

- ✦ Сигнатурный анализ (srv-signature-analyzer). Определяет, является ли запрос вредоносным, по заранее составленным правилам. Анализатор показывает нарушенное правило, если запрос не прошёл проверку.
- ✦ Сваггер анализ (srv-swagger-analyzer). Анализатор проверяет соответствие запроса Swagger-схеме. Для анализатора предварительно формируется белый список запросов. Запрос не проходит проверку анализатора, если не соответствует хотя бы одному правилу для эндпоинта.
- ✦ Статистический анализ (srv-statistic-analyzer). Статистический анализатор проверяет количество отправленных запросов за временной промежуток. При превышении допустимого количества последующие запросы не проходят проверку анализатора, пока частота запросов не уменьшится до допустимой.
- ✦ Анализ чувствительных данных (srv-ml-class-analyzer). Определяет наличие чувствительных данных в запросе и ответе, при наличии запрещённых блокирует запрос или ответ. Типы чувствительных данных:
 - Адрес, местоположение.
 - СНИЛС.
 - ФИО.
 - Номер счета.
 - Адрес электронной почты.
 - Паспорт гражданина РФ.
 - ИНН.
 - Номер телефона.
 - Номер банковской карты.

Контактная информация

По вопросам использования приложения, предложений по доработке функционала, а также в случае выявления ошибок обращайтесь в службу поддержки клиентов:

Web: squadsec.ru

Email: info@squadsec.ru

Юридический адрес: 105066, город Москва, Спартаковская ул, д. 19 стр. 3а, этаж 1
помещ. 1/1, офис 3а

ООО «СКВАД»