Программное обеспечение

# «Servicepipe Cybert»

## Руководство пользователя

Москва - 2026 г.

# Оглавление

# 1 Общие сведения

## 1.1 Назначение документа

Настоящий документ является руководством пользователя программного обеспечения «Servicepipe Cybert» (далее - Servicepipe Cybert, Cybert, программное обеспечение, ПО). Руководство описывает назначение программного обеспечения, общую модель защиты веб-ресурсов и приложений, порядок работы с разделом «Защита приложений» панели управления, создание и редактирование защищаемых ресурсов, настройку политик защиты, просмотр статистики и журналов, а также типовые сценарии эксплуатации и диагностики.

Документ предназначен для работы после развертывания программного обеспечения, подключения защищаемого веб-ресурса и предоставления пользователю учетной записи с необходимыми правами. Установка серверных компонентов, первичная интеграция с сетевой инфраструктурой и выпуск служебных учетных данных выполняются в соответствии с отдельной эксплуатационной документацией.

## 1.2 Сведения о программном обеспечении

Servicepipe Cybert предназначен для защиты веб-ресурсов и приложений от вредоносного автоматизированного трафика. Программное обеспечение анализирует сетевые и прикладные признаки входящих запросов, последовательность действий пользователя в пределах сессии и дополнительные данные, получаемые при выполнении клиентских проверок. По совокупности признаков формируется оценка вероятности автоматизированной активности, после чего применяются настроенные действия: разрешение, дополнительная проверка, ограничение интенсивности либо блокирование запроса.

Основная функциональная особенность Servicepipe Cybert - автоматическое распознавание и блокирование вредоносного бот-трафика при сохранении доступа для легитимных пользователей и полезных автоматизированных клиентов. Управление пользовательскими функциями выполняется в верхнеуровневом разделе «Защита приложений».

## 1.3 Категории пользователей

Руководство рассчитано на следующие категории пользователей:

| Категория пользователя | Основные задачи |
|---|---|
| Администратор защиты приложений | Создание ресурсов, настройка доменов, сертификатов, источников, интеграций, списков доступа и геоограничений. |
| Инженер информационной безопасности | Настройка пользовательских правил, контроль действий защиты, анализ подозрительного трафика и корректировка политик. |
| Специалист SOC / аналитик | Просмотр обзора, статистики, аналитики, журналов запросов, обнаруженных аномалий и пользовательских событий. |
| Инженер эксплуатации / SRE | Контроль доступности источников, времени ответа, кодов ответа, диагностика интеграции и взаимодействия с backend-серверами. |

| Категория пользователя | Основные задачи |
|---|---|
| Владелец веб-ресурса | Просмотр показателей защищаемого ресурса, согласование настроек защиты и контроль результата изменений. |

**Примечание.** Фактический набор доступных разделов, кнопок и операций зависит от роли пользователя, состава подключенных услуг и настроек учетной записи. В интерфейсе могут отсутствовать функции, которые не включены для конкретного клиента или ресурса.

## 1.4 Термины и сокращения

| Термин | Описание |
|---|---|
| **Ресурс** | Защищаемое веб-приложение или группа доменов, для которых задаются параметры интеграции, источники трафика и политики защиты. |
| **Источник** | Backend-сервер или иной узел заказчика, к которому передаются разрешенные запросы. |
| **Схема подключения** | Способ интеграции ресурса с Servicepipe Cybert. В интерфейсе используются схемы «Прокси», «Модуль» и «Гибрид». Дополнительно программное обеспечение может поставляться в он-прем варианте. |
| **Прокси** | Схема, при которой входящий веб-трафик проходит через инфраструктуру фильтрации и затем передается на источник. |
| **Модуль** | Схема локальной интеграции с фронтенд-сервером NGINX/Angie, при которой решение по запросу применяется на стороне фронтенд-сервера. |
| **Он-прем** | Вариант поставки, при котором Servicepipe Cybert развертывается в инфраструктуре заказчика. По набору доступных функций панели управления он аналогичен схеме «Модуль». |
| **Гибрид** | Схема, объединяющая облачную защиту сетевого уровня и локальную обработку прикладного трафика средствами Cybert. |
| **Класс источника** | Результат классификации запроса: бот, вероятно бот, вероятно человек или человек. |
| **Действие** | Решение, применяемое к запросу: пропустить, заблокировать, выполнить JS-проверку, Cookie-проверку, CAPTCHA и другие доступные действия. |
| **JS score** | Оценка, полученная по результатам выполнения клиентского JavaScript и используемая правилами классификации ботов. |
| **Пользовательское правило** | Политика, заданная пользователем для ограничения запросов, применения действий защиты, сбора JS score или классификации ботов. |

| Термин | Описание |
|---|---|
| **Аномалия** | Зафиксированный системой период нетипичного или вредоносного трафика с агрегированной статистикой. |
| **RPS / RPM** | Количество запросов в секунду / минуту. |
| **ASN** | Номер автономной системы источника трафика. |
| **SNI** | Имя сервера, передаваемое клиентом при установлении TLS-соединения. |

# 2 Общая модель работы Servicepipe Cybert

## 2.1 Назначение и область применения

Servicepipe Cybert может размещаться в контуре обработки веб-трафика перед защищаемым приложением, взаимодействовать с фронтенд-сервером приложения в модульной схеме либо поставляться в он-прем варианте с развертыванием в инфраструктуре заказчика. Для он-прем поставки набор функций панели управления аналогичен схеме «Модуль». Для каждого запроса система собирает доступные признаки соединения и HTTP-запроса, сопоставляет их с профилем защиты и пользовательскими правилами, определяет класс источника и возвращает решение о дальнейшей обработке запроса.

Программное обеспечение применяется для решения следующих задач:

- выявление и блокирование вредоносных ботов, сканеров и автоматизированных средств злоупотребления веб-функциями;
- сохранение доступа для легитимных пользователей и полезных поисковых роботов;
- защита веб-форм, личных кабинетов, страниц авторизации, публичных API и других чувствительных точек приложения;
- ограничение интенсивности запросов по URI и пользовательским условиям;
- дополнительная проверка подозрительных клиентов при помощи JavaScript, Cookie и CAPTCHA;
- анализ действий защиты, источников трафика, кодов ответа и времени обработки;
- поиск отдельных запросов в журнале и экспорт данных для расследования;
- фиксация аномалий и формирование пользовательских событий по заданным порогам метрик.

## 2.2 Признаки, используемые при анализе

Решение по запросу формируется на основании совокупности доступных признаков. Конкретный состав признаков зависит от схемы интеграции, протокола и настроек ресурса.

| Группа признаков | Примеры |
|---|---|
| Сетевые признаки | IP-адрес и подсеть, ASN, географическое положение, принадлежность к хостинговой или анонимизирующей инфраструктуре. |
| TLS и транспорт | Версия протокола, наборы шифров и расширений, характеристики соединения и согласованность отпечатков. |
| HTTP-запрос | Метод, Host, путь, Query string, Referer, User-Agent, заголовки, Cookie, Content-Type, версия HTTP. |
| Поведение | Последовательность запросов, частота и временные интервалы, переходы между страницами, признаки новой сессии. |
| Клиентские проверки | Результаты JavaScript-проверок, JS score, Cookie-проверок и CAPTCHA. |
| Контекст защиты | Наличие DDoS-атаки, состояние ресурса, совпадение с белыми/черными списками и пользовательскими правилами. |

## 2.3 Последовательность обработки запроса

1. Клиент отправляет запрос к домену защищаемого ресурса.
2. Запрос поступает в контур Servicepipe Cybert согласно выбранной схеме подключения или архитектуре он-прем поставки.
3. Система получает сетевые, транспортные, HTTP- и сессионные признаки запроса.
4. Проверяется принадлежность источника к белому или черному списку, а также действующие геоограничения.
5. Запрос сопоставляется с пользовательскими правилами в установленном порядке.
6. Вычисляется или уточняется класс источника и, при наличии, значение JS score.
7. Применяется итоговое действие: пропуск, блокирование, ограничение, JS-проверка, Cookie-проверка, CAPTCHA или другое предусмотренное правило.
8. Разрешенный запрос передается источнику; сведения о запросе и результате обработки используются в статистике и журналах.

**Важно.** Порядок правил имеет значение. Для правил защиты используется первое подходящее правило, поэтому более узкие и приоритетные условия следует располагать выше общих.

## 2.4 Схемы подключения и он-прем вариант поставки

| Схема / вариант поставки | Модель работы | Когда применяется |
|---|---|---|
| Прокси | Трафик проходит через инфраструктуру фильтрации Servicepipe, после чего разрешенные запросы проксируются на источник. | Для централизованной облачной защиты веб-приложений и минимизации изменений на стороне заказчика. |
| Модуль | Компонент интегрируется с NGINX/Angie. Фронтенд-сервер принимает соединение, передает метаданные для принятия решения и локально применяет вердикт. | Когда трафик должен оставаться в контуре заказчика либо требуется локальная интеграция с фронтенд-сервером. |
| Он-прем | Компоненты Servicepipe Cybert развертываются в инфраструктуре заказчика. Набор доступных функций панели управления аналогичен схеме «Модуль». | Когда обработка трафика и компоненты защиты должны размещаться в контуре заказчика. |
| Гибрид | Облачная фильтрация сетевого уровня сочетается с локальным анализом и применением решений на прикладном уровне. | Для совмещения защиты от сетевых атак и детального контроля L7-трафика. |

**Примечание. После выбора схемы «Модуль» или «Гибрид» интерфейс предлагает обратиться в техническую поддержку для завершения интеграции. Для он-прем поставки набор функций панели управления аналогичен схеме «Модуль», а особенности развертывания и первичной интеграции определяются проектом внедрения. Набор самостоятельно доступных настроек может отличаться от схемы «Прокси».**

# 3 Работа с панелью управления

## 3.1 Вход и требования к доступу

Для работы с Servicepipe Cybert пользователь открывает панель управления Servicepipe и проходит аутентификацию под учетной записью, которой предоставлен доступ к сервису «Защита приложений». Порядок выдачи учетных данных, настройки двухфакторной аутентификации и восстановления доступа определяется политикой организации и конфигурацией учетной записи.

После входа в панель пользователь выбирает сервис «Защита приложений» в общем переключателе сервисов. При отсутствии раздела необходимо проверить наличие подключенной услуги и права пользователя.

## 3.2 Верхнеуровневая навигация

| Раздел | Назначение |
|---|---|
| Ресурсы | Список защищаемых ресурсов, переход к обзору, статистике, аналитике, журналам, пользовательским правилам и настройкам выбранного ресурса. |
| Обнаруженные аномалии | Список зафиксированных аномалий и подробные данные о трафике в период аномалии. Раздел отображается при наличии соответствующей функции. |
| Пользовательские события | Создание пороговых условий по метрикам и просмотр сработавших событий. Раздел отображается при наличии соответствующей функции. |

## 3.3 Навигация внутри ресурса

После выбора ресурса в интерфейсе доступны следующие подразделы:

| Подраздел | Назначение |
|---|---|
| Обзор | Ключевые показатели и графики по ресурсу за выбранный период. |
| Статистика по трафику | Подробные временные ряды по действиям защиты, полосе, классам источников, кодам и времени ответа. |
| Аналитика | Топы и распределения трафика по IP-адресам, подсетям, запросам, User-Agent, странам и другим измерениям. |
| Логи запросов | Поиск отдельных запросов, просмотр подробных атрибутов, экспорт и отправка выгрузки. |
| Пользовательские правила | Настройка лимитов запросов, правил защиты, сбора JS score и классификации ботов. |
| Настройки | Основные параметры ресурса, домены и SSL, источники, списки доступа и геоограничения. |

## 3.4 Общие приемы работы со списками

- Кнопка «Добавить» или «+ Добавить» открывает форму создания объекта.
- Строка поиска и фильтры ограничивают список по идентификатору, имени ресурса, домену, сервисному IP или другим доступным признакам.
- Меню действий строки используется для просмотра, редактирования, очистки кэша или удаления объекта.
- Пагинация и выбор количества строк позволяют перемещаться по большим спискам.
- После успешной операции интерфейс отображает уведомление; при ошибке необходимо прочитать текст сообщения и исправить указанные поля.
- Удаление и другие необратимые операции требуют подтверждения.

## 3.5 Общие правила заполнения форм

| Тип элемента | Правило работы |
|---|---|
| **Обязательное поле** | Отмечается в интерфейсе. Сохранение невозможно, пока поле не заполнено корректно. |
| **Переключатель** | Включает или отключает функцию; зависимые поля могут становиться доступными только после включения родительской настройки. |
| **Выпадающий список** | Позволяет выбрать одно значение из поддерживаемого набора. |
| **Множественный выбор** | Позволяет выбрать несколько значений, например страны или HTTP-методы. |
| **Список условий** | Каждое условие состоит из параметра, оператора и значения. Условия могут объединяться логикой, показанной в интерфейсе. |
| **Дата и время** | Задаются в локальном формате интерфейса; для срока действия выбирается будущий момент времени. |
| **Файл / PEM** | Загружается или вставляется содержимое сертификата и ключа в поддерживаемом формате. |
| **Поле с ограничением длины** | Интерфейс показывает допустимую длину или ошибку при превышении ограничения. |

**Рекомендация.** Перед сохранением сложного правила проверьте название ресурса, область действия, порядок правила, условия, лимиты и итоговое действие. Изменения политик могут немедленно повлиять на обработку рабочего трафика.

# 4 Управление защищаемыми ресурсами

## 4.1 Список ресурсов

Раздел «Ресурсы» содержит все веб-ресурсы, доступные пользователю. Для поиска используются фильтры по идентификатору, имени ресурса или домену и сервисному IP. Выбор строки открывает контекст выбранного ресурса.

| Элемент | Назначение |
|---|---|
| ID | Уникальный идентификатор ресурса. Используется при обращении в поддержку, интеграциях и поиске. |
| Имя ресурса или домен | Человекочитаемое имя и связанные защищаемые домены. |
| Сервисный IP | Адрес, используемый для интеграции или направления трафика в зависимости от схемы подключения или варианта поставки. |
| Меню действий | Переход к разделам ресурса, настройкам, очистке кэша и удалению. |

## 4.2 Создание ресурса

Чтобы создать ресурс, выполните следующие действия:

1. Перейдите в «Защита приложений -> Ресурсы».
2. Нажмите «Добавить ресурс».
3. Выберите схему подключения: «Прокси», «Модуль» или «Гибрид». Для ресурса в он-прем поставке используется набор функций панели управления, аналогичный схеме «Модуль».
4. Введите имя ресурса.
5. Нажмите кнопку создания и дождитесь уведомления об успешной операции.
6. Для схемы «Прокси» перейдите к настройке доменов, сертификата и источников. Для схем «Модуль» и «Гибрид», а также для он-прем поставки выполните инструкции, согласованные с технической поддержкой.

| Поле | Обязательность | Назначение и правила заполнения |
|---|---|---|
| Схема подключения | Да | Выбор способа интеграции. Доступные в интерфейсе значения: «Прокси», «Модуль», «Гибрид». Выбор влияет на дальнейший набор настроек и порядок подключения. Для он-прем поставки используется набор функций панели управления, аналогичный схеме «Модуль»; конкретный порядок подключения определяется проектом внедрения. |

| Поле | Обязательность | Назначение и правила заполнения |
|---|---|---|
| Имя ресурса | Да | Уникальное в пределах учетной записи понятное имя защищаемого приложения. Минимальная длина - 3 символа. Рекомендуется включать название приложения и окружение. |

**Пример имени.** Для производственного сайта можно использовать имя «portal-production», для тестового окружения - «portal-stage». Не включайте в имя секреты, ключи или персональные данные.

## 4.3 Действия с существующим ресурсом

| Действие | Результат и особенности |
|---|---|
| Открыть обзор | Переход к сводным показателям выбранного ресурса. |
| Открыть статистику / аналитику / логи | Переход к соответствующему разделу с автоматически выбранным ресурсом. |
| Открыть пользовательские правила | Переход к политикам, действующим для ресурса. |
| Открыть настройки | Изменение имени, описания, общих переключателей, доменов, SSL, источников и других параметров. |
| Очистить кэш | Запуск операции очистки кэша для ресурса. Перед выполнением оцените влияние на нагрузку на источники. |
| Удалить | Удаление ресурса после подтверждения. Операция прекращает управление защитой этого ресурса в панели и может повлиять на обработку трафика. |

**Важно.** Не удаляйте ресурс, пока DNS, маршрутизация и интеграция приложения продолжают направлять трафик через его сервисные адреса. Сначала согласуйте вывод ресурса из эксплуатации.

## 4.4 Рекомендуемая последовательность первичной настройки

1. Создайте ресурс и выберите схему подключения. Для он-прем поставки учитывайте, что доступный в панели функционал аналогичен схеме «Модуль».
2. Заполните основные настройки и описание.
3. Добавьте основной домен и при необходимости домены-алиасы.
4. Настройте SSL-сертификат либо автоматический выпуск сертификата, если функция доступна.
5. Добавьте один или несколько источников и проверьте параметры их доступности.
6. Настройте белый и чёрный списки и геоограничения при необходимости.

7. Переведите трафик на сервисные адреса согласно выбранной схеме.
8. Проверьте «Обзор», «Статистику по трафику» и «Логи запросов».
9. После накопления данных создавайте пользовательские правила, начиная с узких и наблюдаемых условий.

# 5 Настройка защищаемого ресурса

## 5.1 Общая структура настроек

Настройки выбранного ресурса сгруппированы по вкладкам. Состав вкладок зависит от схемы подключения, варианта поставки и функций, включенных для учетной записи.

| Вкладка | Назначение |
|---|---|
| Основные настройки | Имя и описание ресурса, включение основных механизмов защиты и параметров проксирования. |
| Домены и SSL | Управление основным доменом, доменами-алиасами, сертификатами и приватными ключами. |
| Источники | Адреса backend-серверов, режимы работы, веса и параметры временного исключения источника. |
| Белый список | IP-адреса и подсети, для которых применяется доверенная обработка согласно настройкам сервиса. |
| Чёрный список | IP-адреса и подсети, трафик которых должен быть заблокирован. |
| Геоограничения | Разрешение или блокирование трафика по странам. |

## 5.2 Основные настройки

Вкладка «Основные настройки» содержит идентификационные параметры ресурса и переключатели, определяющие базовую модель обработки трафика.

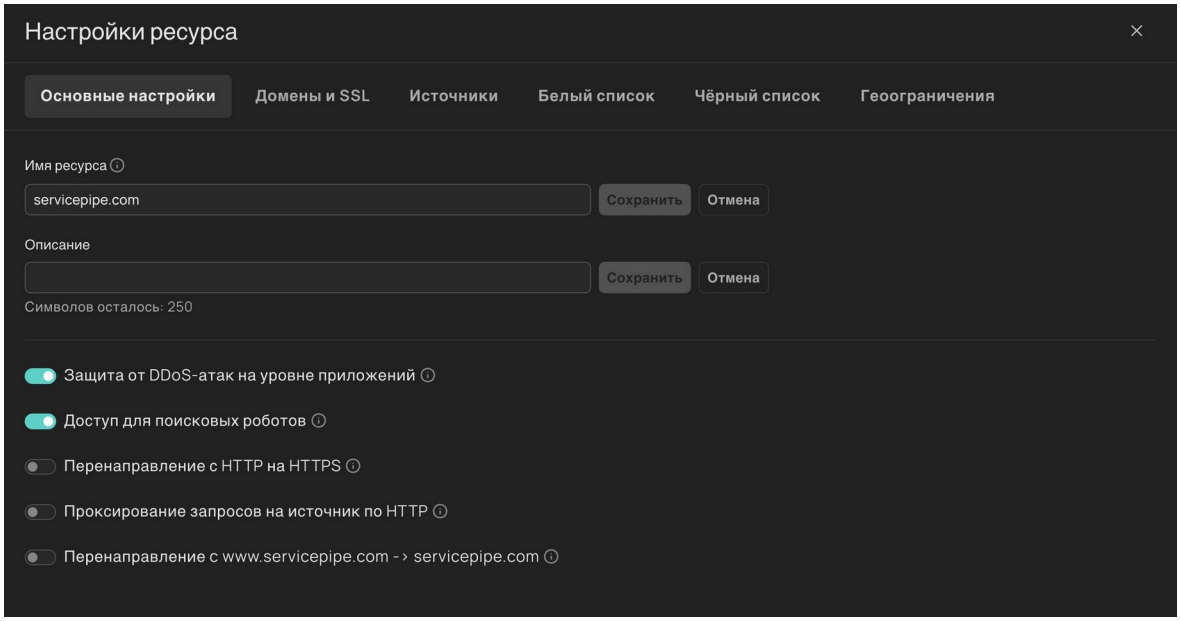


*Рисунок 1 - Вкладка «Основные настройки» ресурса*

| Поле / переключатель | Обязательность | Назначение и правила |
|---|---|---|
| Имя ресурса | Да | Отображаемое имя ресурса. Используется в списках, фильтрах и уведомлениях. При изменении следует сохранить однозначную связь имени с приложением и окружением. |
| Описание | Нет | Назначение ресурса, владелец, окружение или иная эксплуатационная информация. Максимальная длина - 250 символов. |
| Защита от DDoS-атак на уровне приложений | Нет | Включает механизмы выявления и обработки атак прикладного уровня для ресурса. |
| Доступ для поисковых роботов | Нет | Разрешает обработку полезных поисковых роботов согласно механизмам распознавания сервиса. |
| Перенаправление с HTTP на HTTPS | Нет | При включении HTTP-запросы перенаправляются на защищенную схему HTTPS. Перед включением должен быть готов действующий сертификат. |
| Проксирование запросов на источник по HTTP | Нет | Определяет использование HTTP при передаче разрешенного запроса от сервиса к источнику. При выключенном состоянии может использоваться защищенная схема в соответствии с конфигурацией. |
| Перенаправление с www.<name> на <name> | Нет | Включает перенаправление с домена с префиксом www на основной домен без префикса. Применимо, когда оба имени корректно настроены и разрешены сертификатом. |

**Важно. Набор переключателей может различаться для схем «Прокси», «Модуль» и «Гибрид», а также для ресурсов с внешним NGINX или отдельной функцией журналирования. Для он-прем поставки доступный в панели функционал аналогичен схеме «Модуль». Ориентируйтесь на фактически отображаемые элементы интерфейса.**

Для изменения основных настроек:

1. Откройте ресурс и перейдите в «Настройки -> Основные настройки».
2. Измените имя или описание при необходимости.
3. Установите требуемые положения переключателей.
4. Нажмите «Сохранить».
5. Проверьте уведомление об успешном сохранении и затем проконтролируйте трафик в разделе «Обзор».

## 5.3 Домены и SSL

### 5.3.1 Назначение вкладки

Вкладка «Домены и SSL» определяет имена, по которым принимается трафик ресурса, и сертификаты, используемые для TLS-соединений. Для ресурса выделяется основной домен; дополнительно можно создать домены-алиасы.

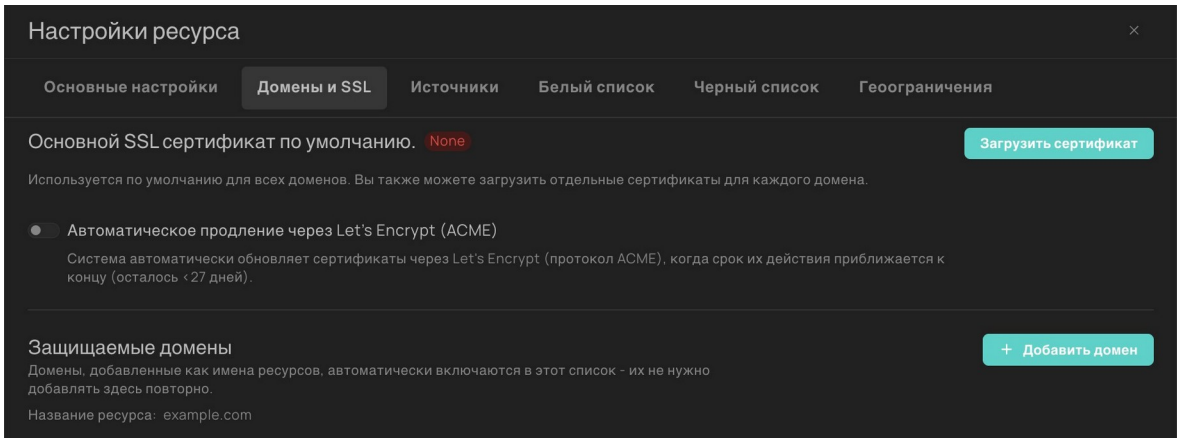


*Рисунок 2 - Состояние сертификата и список доменов ресурса*

### 5.3.2 Основной сертификат

| Элемент | Назначение |
|---|---|
| Статус сертификата | Показывает наличие и состояние сертификата, а также доступные действия. |
| Автоматическое продление Let’s Encrypt | При доступности функции позволяет использовать автоматически выпускаемый и продлеваемый сертификат. |
| Срок действия | Дата окончания действия текущего сертификата. Следует контролировать заранее, чтобы избежать недоступности HTTPS. |
| Загрузить / заменить сертификат | Открывает форму ввода цепочки сертификатов и приватного ключа. |

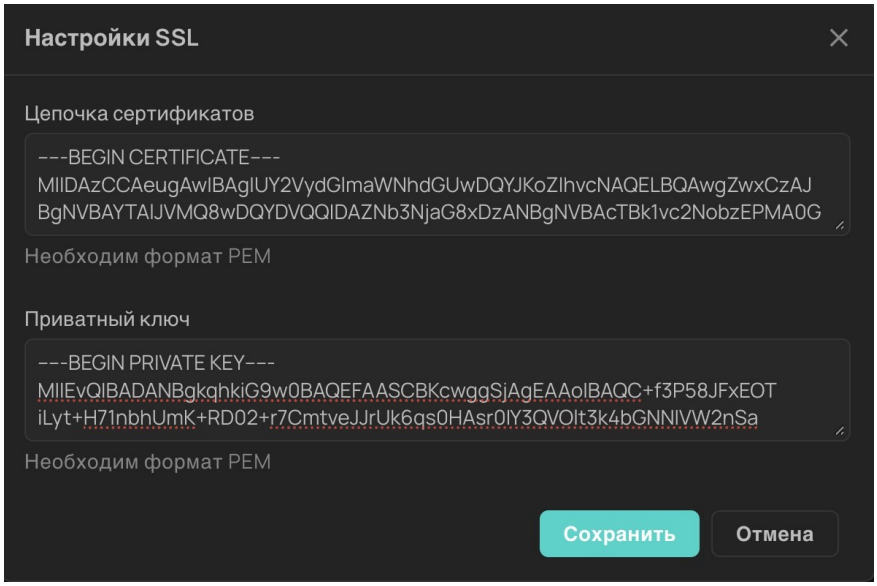


*Рисунок 3 - Форма загрузки сертификата и приватного ключа*

| Поле | Обязательность | Назначение и правила заполнения |
|---|---|---|
| Цепочка сертификатов (PEM) | Да | Сертификат домена и промежуточные сертификаты в формате PEM. Блоки должны быть расположены в корректном порядке. |
| Приватный ключ RSA (PEM) | Да | Приватный ключ, соответствующий сертификату. Значение является чувствительным и должно передаваться только через защищенный интерфейс. |

**Проверка перед сохранением.** Убедитесь, что приватный ключ соответствует сертификату, сертификат покрывает основной домен и все требуемые алиасы, цепочка не содержит лишних блоков, а срок действия не истек.

### 5.3.3 Добавление защищаемого домена

Чтобы добавить домен или домен-алиас, нажмите «Добавить домен» и заполните форму.

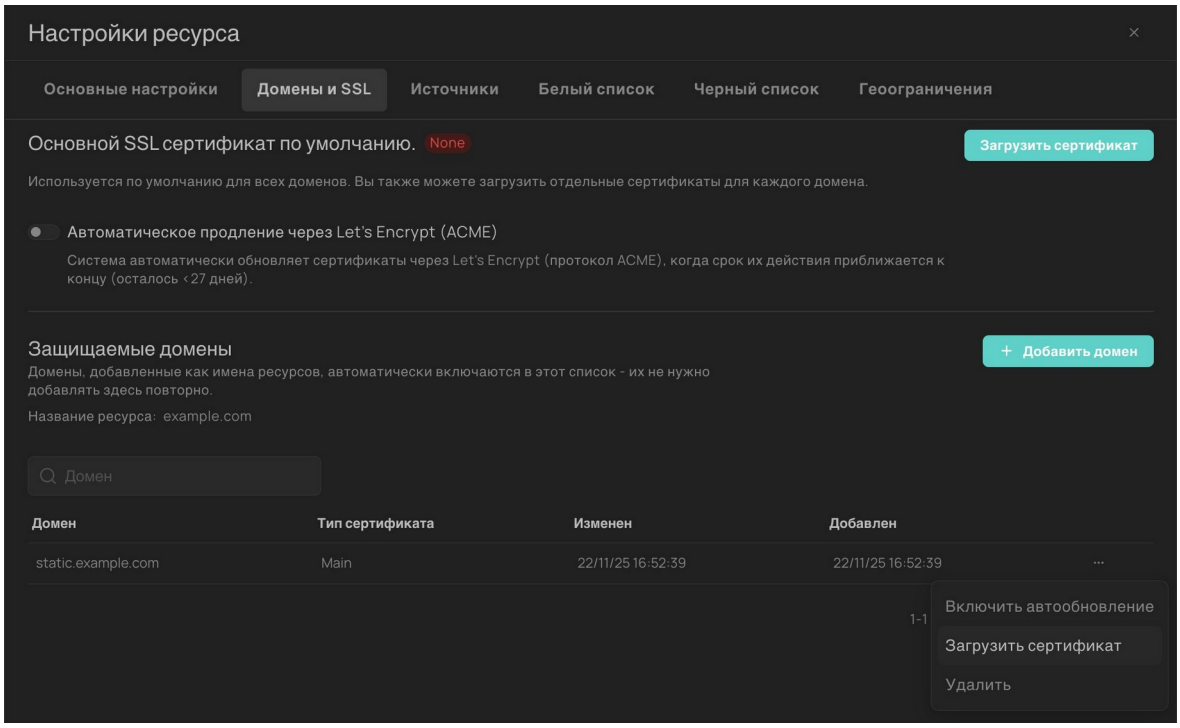


*Рисунок 4 - Форма добавления защищаемого домена*

| Поле | Обязательность | Назначение и правила |
|---|---|---|
| Домен | Да | Полное доменное имя, по которому будет приниматься трафик. Допускаются поддерживаемые интерфейсом IDN- и wildcard-имена. Не указывайте схему, путь или порт. |

| Поле | Обязательность | Назначение и правила |
|---|---|---|
| Сертификат домена | Зависит от конфигурации | Для алиаса можно использовать основной сертификат, если он покрывает домен, либо загрузить отдельный сертификат и ключ. |

После создания домена в списке доступны действия:

- загрузить или заменить сертификат домена;
- переключить домен на использование основного сертификата, если он покрывает это имя;
- удалить домен-алиас после подтверждения.

**Важно.** Удаление домена из панели не изменяет автоматически внешние DNS-записи. Перед удалением убедитесь, что пользователи и интеграции больше не направляют запросы на этот домен.

## 5.4 Источники

### 5.4.1 Назначение источников

Источник - backend-узел заказчика, на который Servicepipe Cybert передает разрешенные запросы. Для отказоустойчивости можно добавить несколько источников и назначить им режимы и веса.

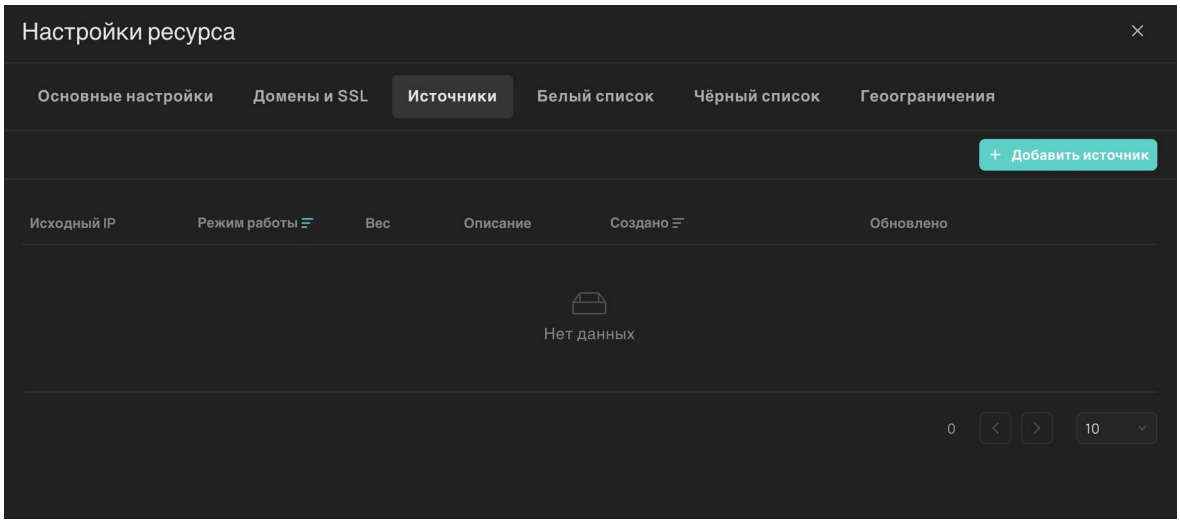


*Рисунок 5 - Список источников ресурса*

### 5.4.2 Добавление и редактирование источника

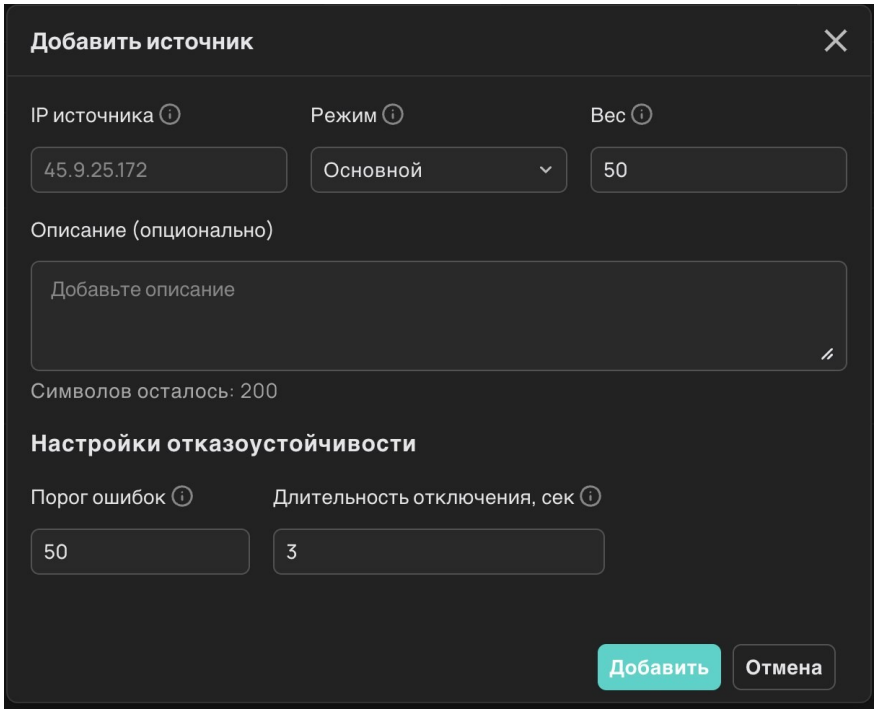


*Рисунок 6 - Форма добавления источника*

| Поле | Обязательность | Назначение и правила заполнения |
|---|---|---|
| IP-адрес | Да | IPv4-адрес backend-сервера. В режиме редактирования поле недоступно; для замены адреса создайте новый источник и выведите старый из эксплуатации. |
| Режим | Да | «Основной» - принимает штатный трафик; «Резервный» - используется в резервном сценарии; «Отключён» - сохраняется в конфигурации, но не используется. |
| Вес | Да | Положительное число, определяющее относительную долю трафика между источниками одинакового режима. Значение должно быть больше 0. |
| Описание | Нет | Назначение узла, площадка, окружение или контакт ответственной команды. Максимальная длина - 200 символов. |
| Порог ошибок | Да | Количество или порог неуспешных ответов, после которого источник временно исключается из обработки. Значение должно быть больше 0. |
| Время отключения, сек. | Да | Период временного исключения источника после достижения порога ошибок. Значение должно быть больше 0. |

Порядок добавления источника:

1. Откройте «Настройки -> Источники».
2. Нажмите «Добавить источник».

3. Введите IPv4-адрес и выберите режим.
4. Укажите вес, описание, порог ошибок и время отключения.
5. Сохраните источник.
6. Проверьте, что источник отображается в списке в требуемом режиме, а разрешенные запросы достигают backend-сервера.

**Рекомендация.** Перед включением нового источника проверьте сетевую доступность, правила межсетевого экрана, ожидаемый Host, TLS-настройки и готовность приложения принимать трафик от инфраструктуры Servicepipe.

## 5.5 Белый список

### 5.5.1 Назначение и список записей

Белый список предназначен для хранения доверенных IP-адресов и подсетей. Конкретный эффект записи зависит от общей конфигурации защиты и интеграций, поэтому добавлять следует только адреса, владелец и назначение которых подтверждены.

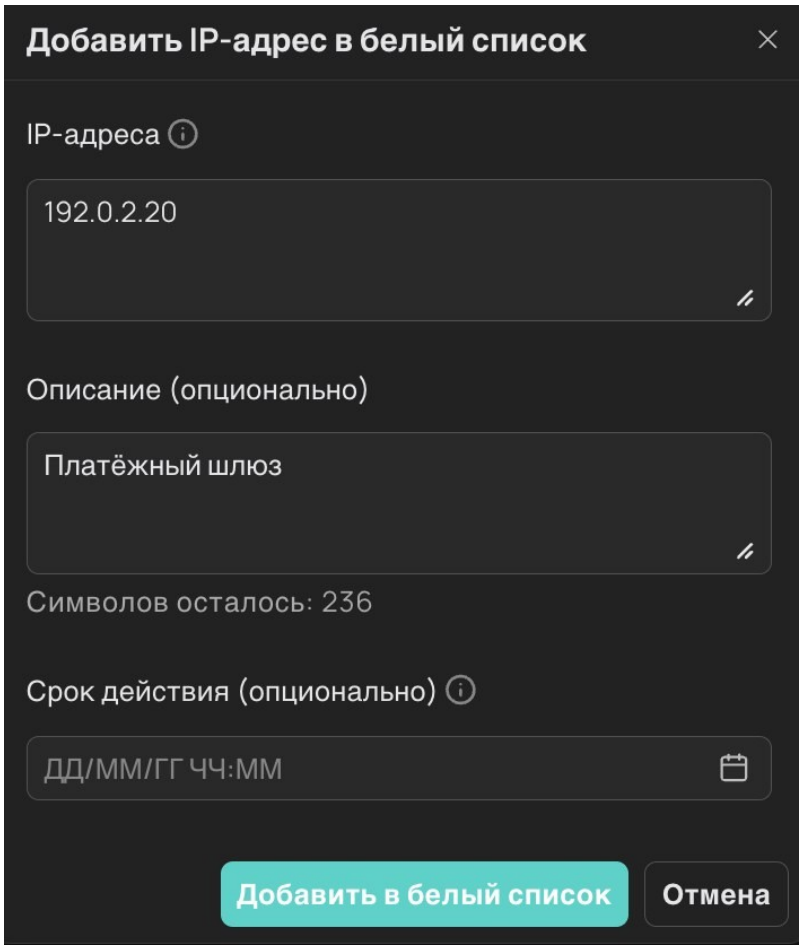


*Рисунок 7 - Форма добавления записи в белый список*

| Поле | Обязательность | Назначение и правила заполнения |
|---|---|---|
| IP-адреса / подсети | Да | Один или несколько IPv4-адресов либо подсетей. Значения вводятся через запятую в поддерживаемом интерфейсом формате. При редактировании существующей записи адрес не изменяется. |
| Описание | Нет | Причина добавления, владелец, заявка или срок пересмотра. Максимальная длина - 250 символов. |
| Срок действия | Нет | Будущая дата и время автоматического прекращения действия записи. В интерфейсе используется формат вида DD/MM/YY HH:mm. |

**Ограничение массовой операции.** За один запрос можно передать до 2000 адресов. Общий объем списка может достигать 60 000 адресов. При частичном результате изучите сообщение интерфейса: корректные значения могут быть сохранены, а ошибочные - перечислены отдельно.

### 5.5.2 Добавление, изменение и удаление

1. Откройте «Настройки -> Белый список».
2. Нажмите «Добавить».
3. Введите IP-адреса или подсети, добавьте описание и при необходимости срок действия.
4. Сохраните запись и проверьте результат импорта.
5. Для изменения откройте запись и скорректируйте описание либо срок действия.
6. Для исключения адреса удалите соответствующую запись после подтверждения.

**Рекомендация.** Для временных интеграций всегда задавайте срок действия. В описании фиксируйте номер заявки или ответственную команду, чтобы запись можно было обоснованно пересмотреть.

## 5.6 Чёрный список

Чёрный список используется для явного блокирования запросов от отдельных IP-адресов и подсетей. Записи следует создавать на основании подтвержденного инцидента или утвержденной политики доступа.

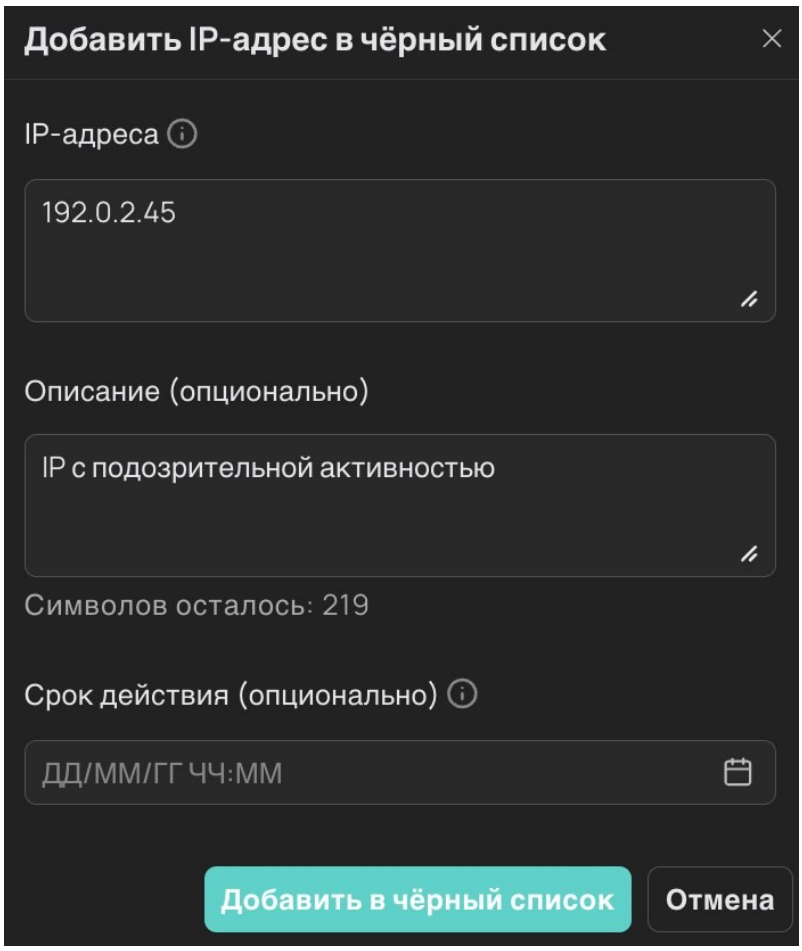


*Рисунок 8 - Форма добавления записи в чёрный список*

| Поле | Обязательность | Назначение и правила заполнения |
|---|---|---|
| IP-адреса / подсети | Да | Один или несколько IPv4-адресов либо подсетей через запятую. Для подсетей поддерживаются маски, разрешенные интерфейсом; локальные и недопустимые диапазоны отклоняются. В режиме редактирования адрес не изменяется. |
| Описание | Нет | Основание блокирования, источник данных, номер инцидента или ответственный сотрудник. Максимальная длина - 250 символов. |
| Срок действия | Нет | Будущая дата и время автоматического снятия блокировки. Для временных мер рекомендуется заполнять обязательно. |

**Важно.** Перед массовым блокированием подсети оцените риск блокировки легитимных пользователей, партнеров, облачных площадок и средств мониторинга. Для широких диапазонов предпочтительны узкие пользовательские правила с дополнительными условиями.

Ограничения массового добавления и логика частичного результата аналогичны белому списку: до 2000 адресов за операцию и до 60 000 адресов в списке. В подсказке интерфейса для чёрного списка указаны поддерживаемые маски IPv4 от /8 до /30 и отдельные адреса /32.

## 5.7 Геоограничения

Геоограничения позволяют задать политику доступа по стране, определенной для источника запроса. Настройка применяется ко всему ресурсу, поэтому ее следует использовать с учетом аудитории, VPN, мобильных операторов и международных интеграций.

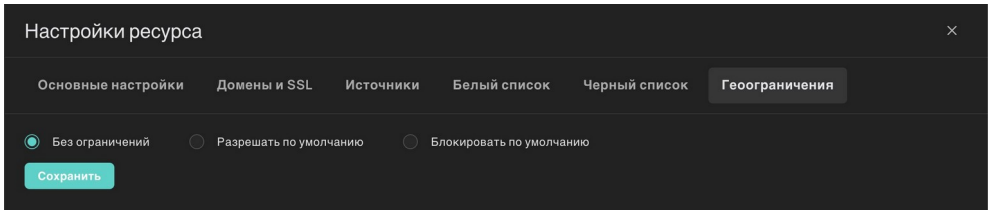


*Рисунок 9 - Выбор режима геоограничений*

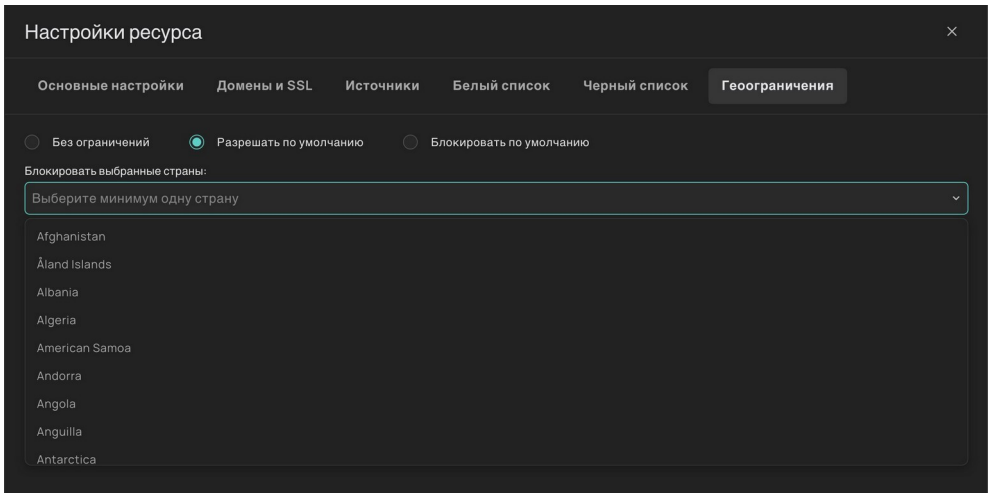


*Рисунок 10 - Выбор стран для геоограничений*

| Режим | Поле стран | Результат |
|---|---|---|
| Без ограничений | Не требуется | Страна источника не используется как самостоятельное основание для разрешения или блокирования. |
| Разрешить выбранные страны | Обязательно выбрать одну или несколько стран | Разрешается трафик только из выбранных стран; остальной трафик ограничивается. |
| Заблокировать выбранные страны | Обязательно выбрать одну или несколько стран | Блокируется трафик из выбранных стран; остальные страны не ограничиваются этой настройкой. |

Порядок настройки:

1. Откройте «Настройки -> Геоограничения».
2. Выберите один из трех режимов.
3. Для разрешающего или блокирующего режима выберите страны в поле множественного выбора.

4. Сохраните изменения.
5. Проверьте статистику по странам и журналы запросов, чтобы убедиться в ожидаемом результате.

**Примечание.** Географическая принадлежность IP-адреса определяется по используемой сервисом базе. Она не гарантирует фактическое физическое местонахождение пользователя, особенно при использовании VPN, прокси, CGNAT и облачных платформ.

# 6 Мониторинг, статистика и аналитика

## 6.1 Общие принципы работы с периодом и данными

Разделы мониторинга предназначены для оценки интенсивности и состава трафика, результата работы механизмов защиты, доступности источников и времени обработки запросов. Данные отображаются для выбранного ресурса и временного интервала.

| Элемент | Назначение |
|---|---|
| Период | Определяет временной интервал, за который строятся показатели. На обзорных экранах доступны быстрые периоды 1 час, 4 часа, 24 часа, 7 дней и 30 дней. |
| Произвольный интервал | Позволяет задать начало и окончание периода в пределах ограничений конкретного раздела. |
| Обновить | Повторно запрашивает данные с учетом текущего периода и фильтров. |
| Легенда графика | Включает или скрывает отдельные серии для удобства сравнения. |
| Наведение на точку | Показывает точное время и значение метрики. |
| Фильтры | Ограничивают статистику по действиям, классам источника, причинам и другим измерениям. |

**Примечание.** Агрегированные значения предназначены для анализа динамики. Для расследования конкретного запроса используйте раздел «Логи запросов», где доступны индивидуальные атрибуты.

## 6.2 Обзор ресурса

Подраздел «Обзор» показывает ключевые показатели ресурса и основные графики за выбранный период. Он используется для быстрого ответа на вопросы: изменился ли объем трафика, выросло ли число блокировок, появились ли ошибки источника и требуется ли детальный анализ.

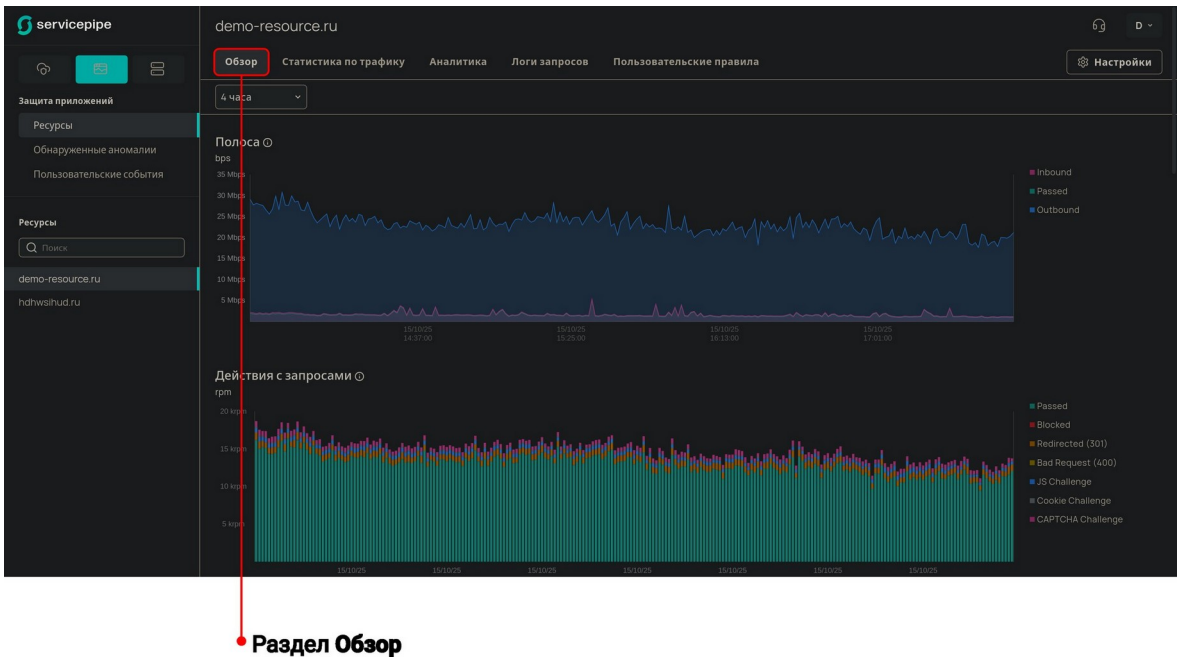


*Рисунок 11 - Обзор показателей защищаемого ресурса*

| Группа показателей | Как использовать |
|---|---|
| Действия защиты | Сравнивайте разрешенные, заблокированные и направленные на проверку запросы. Резкое изменение соотношения требует проверки правил и источников трафика. |
| Класс источника | Оценивайте доли ботов, вероятных ботов, вероятных людей и людей. |
| Полоса | Сопоставляйте входящую и исходящую нагрузку, а также разрешенный и заблокированный трафик. |
| Коды ответа | Контролируйте 2xx, 3xx, 4xx и 5xx, отдельно анализируя ответы платформы и источника. |
| Время обработки | Отслеживайте общую задержку и время ответа источника; рост времени без роста нагрузки может указывать на деградацию backend. |

Рекомендуемый порядок первичной диагностики по обзору:

1. Проверьте общий объем запросов и полосу.
2. Сопоставьте разрешенные, заблокированные и проверяемые запросы.
3. Оцените распределение классов источников.
4. Проверьте коды ответа платформы и источника.
5. Сопоставьте изменения с временем ответа источника и общей обработкой.
6. При необходимости перейдите к детальной статистике, аналитике и журналам.

## 6.3 Статистика по трафику

### 6.3.1 Назначение и структура

Подраздел «Статистика по трафику» содержит набор временных графиков. Каждый график отражает отдельную сторону обработки запросов и позволяет сравнить серии за один период.

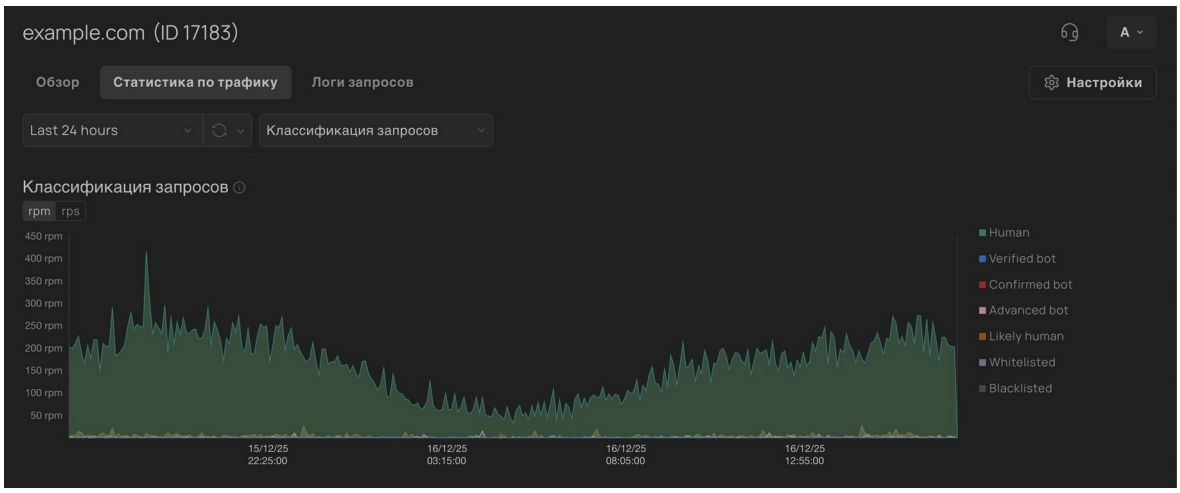


*Рисунок 12 - Раздел «Статистика по трафику»*

| График | Содержание и назначение |
|---|---|
| Действия над запросами | Количество запросов, пропущенных, заблокированных, перенаправленных или направленных на Cookie-, JS- и CAPTCHA-проверки. |
| Статистика CAPTCHA | Количество выданных, успешно решенных и разрешенных после CAPTCHA запросов. |
| Класс источника | Распределение трафика по классам: бот, вероятно бот, вероятно человек, человек. |
| Полоса | Входящий, исходящий, пропущенный и заблокированный объем данных. |
| Время ответа источника | Распределение запросов по интервалам времени ответа backend-сервера. |
| Коды ответа источника | Классы 2xx, 3xx, 4xx и 5xx, полученные от источника. |
| Ошибки источника 5xx | Отдельная детализация кодов 500, 501, 502, 503 и 504. |
| География | Распределение запросов по странам или связанным географическим метрикам. |
| TCP | Доступные метрики транспортных соединений. |
| Общее время обработки | Полное время обработки запроса в доступной сервису части цепочки. |
| Коды ответа платформы | Классы HTTP-кодов, возвращенных клиенту платформой защиты. |

**Интерпретация.** Одновременный рост 5xx источника и времени ответа источника обычно требует проверки backend. Рост блокировок при стабильной доступности источника требует анализа причин действий и пользовательских правил. Это диагностические признаки, а не автоматический вывод о причине.

### 6.3.2 Работа с графиками

1. Выберите период.
2. Оставьте включенными только серии, которые требуется сравнить.

3. Наведите указатель на интересующую точку для просмотра значения.
4. Зафиксируйте время изменения показателя.
5. Перейдите в «Аналитика» с тем же периодом для поиска основных источников изменения.
6. Откройте «Логи запросов» и задайте более узкий интервал для просмотра отдельных запросов.

## 6.4 Аналитика

### 6.4.1 Назначение раздела

Раздел «Аналитика» показывает распределения и наиболее значимые значения по отдельным измерениям. Он используется для ответа на вопрос, какие источники, запросы, страны или клиенты сформировали наблюдаемую нагрузку. Максимальный период анализа в интерфейсе - 31 день.

| Фильтр | Назначение |
|---|---|
| Действие | Ограничивает данные выбранным результатом обработки, например пропуском, блокированием или проверкой. |
| Класс источника | Ограничивает выборку классом «Бот», «Вероятно бот», «Вероятно человек» или «Человек». |
| Причина действия | Выбирает запросы, для которых действие было применено по конкретной причине или механизму. |
| Период | Временной интервал не более 31 дня. Для точного расследования рекомендуется использовать минимально достаточный период. |

### 6.4.2 Аналитические срезы

| Срез | Что показывает | Практическое применение |
|---|---|---|
| IP-адреса | Источники с наибольшим числом запросов или выбранной метрикой. | Поиск единичных активных клиентов, кандидатов для журнала или списка доступа. |
| Подсети | Агрегацию по сетевым диапазонам. | Выявление распределенной активности в пределах провайдера или площадки. |
| Запросы / пути | Наиболее часто используемые URI. | Поиск целевых endpoint-ов, форм, API и страниц, подвергающихся автоматизированной активности. |
| User-Agent | Наиболее распространенные значения User-Agent. | Выявление массовых клиентов и проверка согласованности с другими признаками. |
| Страны | Распределение по географии. | Оценка соответствия аудитории и подготовка геоограничений. |
| ASN / сети | Автономные системы и сетевые владельцы. | Анализ активности облачных, хостинговых и операторских сетей. |

**Важно.** Топ по одному признаку не является достаточным основанием для блокирования. Сопоставьте IP, подсеть, ASN, путь, User-Agent, класс источника, действие и конкретные записи журнала.

## 6.5 Логи запросов

### 6.5.1 Назначение и вкладки

Раздел «Логи запросов» предназначен для поиска и исследования отдельных запросов. В интерфейсе используются две вкладки: «Весь трафик» и журнал запросов, для которых оценивались или применялись политики защиты. Доступный период хранения в интерфейсе - последние две недели.

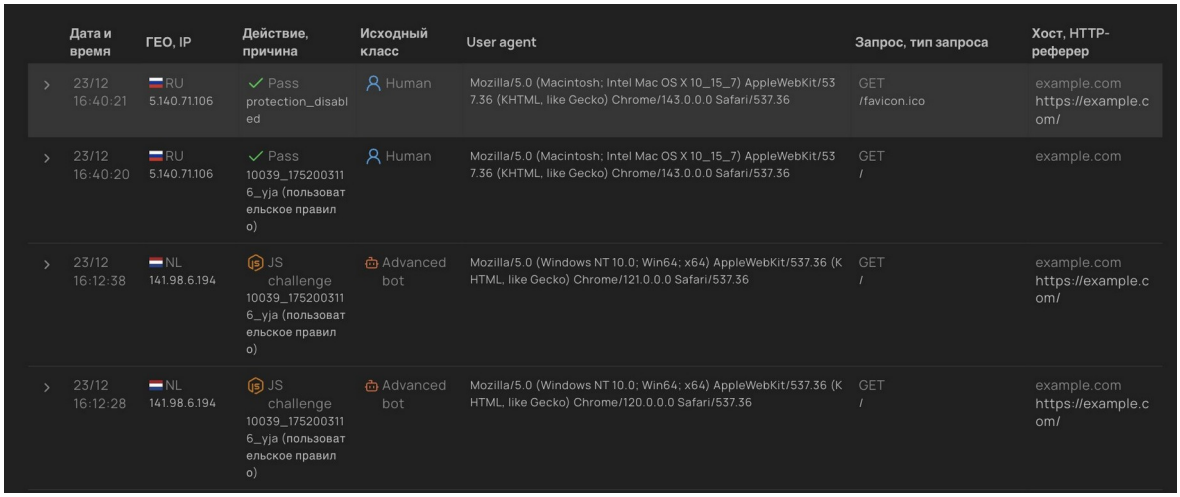


*Рисунок 13 - Таблица и карточка запроса в журнале*

### 6.5.2 Фильтры журнала всего трафика

| Фильтр | Назначение / формат |
|---|---|
| ID запроса | Поиск конкретного запроса по уникальному идентификатору. |
| User-Agent | Полное или поддерживаемое интерфейсом частичное значение клиентского заголовка. |
| IP источника | IPv4/IPv6-адрес клиента в формате, доступном сервису. |
| Host | Домен, к которому был направлен запрос. |
| Referer | Страница-источник перехода. |
| Метод | HTTP-метод: GET, POST, PUT, DELETE, PATCH и другие поддерживаемые значения. |
| Путь | URI без имени хоста; используется для поиска обращений к конкретному endpoint. |
| Query string | Параметры после знака вопроса. Не вводите секреты в фильтр при демонстрации или совместном доступе. |
| Страна | Страна, определенная для IP-адреса источника. |
| Схема | HTTP или HTTPS в зависимости от доступных данных. |
| Код ответа | Код, возвращенный клиенту. |
| Код ответа источника | Код, полученный от backend-сервера. |

| Фильтр | Назначение / формат |
|---|---|
| Версия HTTP | Например HTTP/1.1, HTTP/2 или HTTP/3 при наличии данных. |
| IP источника приложения | Backend-адрес, на который был направлен запрос. |
| Порт источника приложения | Backend-порт. |
| Время ответа источника | Время, затраченное на получение ответа от backend. |
| Общее время запроса | Полное время обработки запроса в доступной сервису части цепочки. |

### 6.5.3 Фильтры журнала политик защиты

| Фильтр | Назначение |
|---|---|
| ID запроса / ID сессии | Связывает конкретный запрос и последовательность действий одного клиента. |
| User-Agent, IP, Host, Referer | Основные сетевые и HTTP-признаки источника. |
| Класс источника | Бот, вероятно бот, вероятно человек или человек. |
| Действие | Итоговый результат обработки запроса. |
| Причина | Механизм или условие, по которому было выбрано действие. |
| ID правила | Идентификатор сработавшего пользовательского или системного правила. |
| Страна, Netname, ASN, подсеть | Географические и сетевые атрибуты источника. |
| SP hashes | Сервисные отпечатки запроса, доступные для технического анализа. |
| JA3 | TLS-отпечаток клиента при наличии данных. |
| Тип запроса | Классификация запроса по доступному сервису типу. |
| Метод / путь | HTTP-метод и URI. |
| Bot score | Числовая оценка, используемая классификацией автоматизированной активности. |

### 6.5.4 Просмотр карточки запроса

Для открытия подробностей выберите строку журнала. Карточка запроса содержит доступные атрибуты клиента, соединения, HTTP-запроса, результата защиты, ответа платформы и источника. Набор полей может различаться в зависимости от схемы подключения, варианта поставки и типа запроса.

При расследовании рекомендуется зафиксировать:

- ID запроса и точное время;
- IP-адрес, подсеть, ASN и страну;
- Host, метод, путь и Query string;
- User-Agent, Referer и доступные отпечатки;
- класс источника, действие, причину и ID правила;
- код ответа клиенту и код ответа источника;
- время ответа источника и общее время обработки.

### 6.5.5 Экспорт и отправка журнала

Интерфейс позволяет сформировать выгрузку журнала или отправить ее на указанный адрес электронной почты. Для одной операции экспорта выбирается период не более 24 часов; результат ограничен доступным объемом и правами пользователя. В интерфейсе отображается до 10 000 записей по результату запроса.

1. Выберите вкладку журнала.
2. Установите период не более 24 часов и необходимые фильтры.
3. Проверьте пример результата в таблице.
4. Запустите экспорт или отправку на электронную почту.
5. Дождитесь уведомления о принятии операции и используйте полученный файл в соответствии с политикой хранения данных.

**Безопасность данных.** Журналы могут содержать IP-адреса, URI, заголовки и другие сведения о запросах. Ограничивайте доступ к выгрузкам, не пересылайте их в общедоступные каналы и удаляйте после завершения расследования согласно правилам организации.

# 7 Пользовательские правила

## 7.1 Общая структура и порядок применения

Раздел «Пользовательские правила» позволяет задавать дополнительные политики обработки трафика конкретного ресурса. Правила сгруппированы по назначению: ограничение интенсивности, применение действий защиты, сбор JS score и классификация ботов.

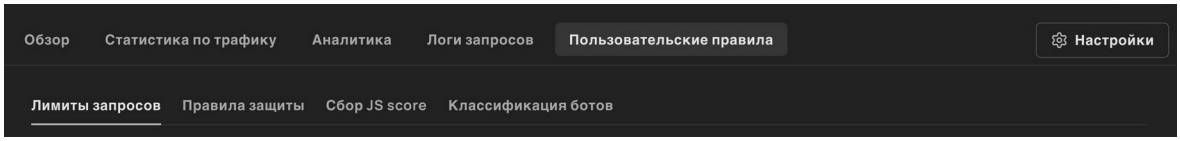


*Рисунок 14 - Вкладки раздела «Пользовательские правила»*

| Вкладка | Назначение |
|---|---|
| Лимиты запросов | Простое ограничение количества запросов к одному или нескольким URI за заданный период с последующей временной блокировкой. |
| Правила защиты | Гибкие условия по признакам запроса, лимитам и состоянию DDoS с выбором действия для классов источников. Здесь же создается специальное правило защиты API. |
| Сбор JS score | Определение областей трафика, в которых клиенту должен выдаваться JavaScript для получения оценки. |
| Классификация ботов | Настройка порогового значения JS bot score для общей или условной классификации. |

Для каждого списка правил обычно доступны следующие операции:

- создание нового правила;
- включение или отключение существующего правила;
- редактирование условий и параметров;
- изменение позиции в порядке выполнения, если тип правила поддерживает порядок;
- удаление после подтверждения.

**Важно.** Перед включением правила оцените его область действия на реальных данных. Ошибка в пути, операторе или слишком широком условии может затронуть легитимных пользователей. Начинайте с узкой области и контролируйте результат по статистике и журналам.

## 7.2 Лимиты запросов

### 7.2.1 Назначение

Правила «Лимиты запросов» предназначены для быстрого ограничения частоты обращений к конкретным путям. Правило считает запросы, соответствующие одному из заданных URI, и при превышении лимита блокирует источник на установленный срок.

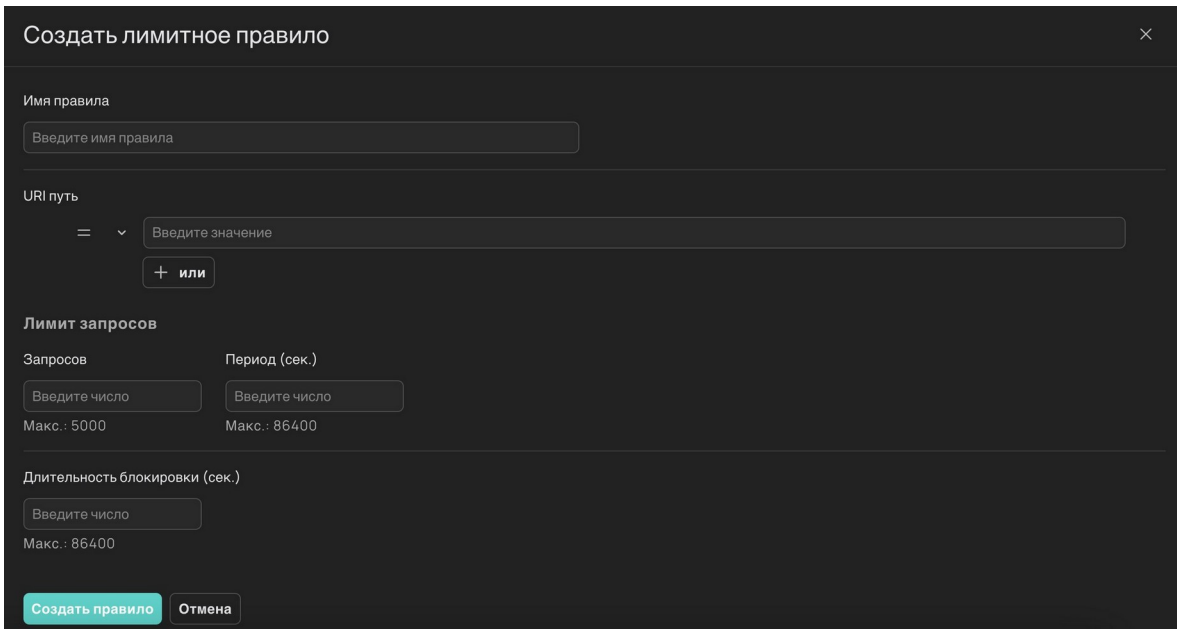


*Рисунок 15 - Форма создания правила «Лимиты запросов»*

### 7.2.2 Поля формы

| Поле | Обязательность | Назначение и правила заполнения |
|---|---|---|
| Название правила | Нет | Человекочитаемое имя. Максимальная длина - 50 символов. Рекомендуется указывать защищаемый endpoint и назначение, например «login-rate-limit». |
| URI | Да, не менее одного | Путь, к которому применяется лимит. Для каждого элемента выбирается оператор «Равно» или «Начинается с». Максимальная длина значения - 200 символов. |
| Добавить URI | Нет | Создает дополнительное условие пути. Несколько URI внутри правила объединяются логикой «ИЛИ»: запрос должен соответствовать хотя бы одному. |
| Запросов | Да | Максимально допустимое количество запросов за выбранный период. Значение должно быть положительным; интерфейс указывает верхнее ограничение до 5000. |
| Период, сек. | Да | Окно подсчета запросов в секундах. Значение должно быть положительным; интерфейс указывает верхнее ограничение до 86400 секунд. |
| Время блокировки, сек. | Да | Срок временной блокировки после превышения лимита. Значение должно быть положительным; интерфейс указывает верхнее ограничение до 86400 секунд. |
| Состояние правила | Да | Включенное правило участвует в обработке; отключенное хранится в конфигурации, но не применяется. |

**Логика URI.** Оператор «Равно» подходит для одного точного endpoint. Оператор «Начинается с» охватывает вложенные пути и должен использоваться осторожно: значение «/api/» затронет все запросы в соответствующей ветке.

### 7.2.3 Создание правила

1. Откройте ресурс и перейдите в «Пользовательские правила -> Лимиты запросов».
2. Нажмите «Добавить правило».
3. При необходимости задайте название.
4. Добавьте один или несколько URI и выберите для каждого оператор.
5. Укажите количество запросов, период подсчета и время блокировки.
6. Проверьте состояние правила и сохраните форму.
7. В журнале запросов проконтролируйте срабатывания на тестовом трафике и отсутствие блокировки ожидаемых клиентов.

### 7.2.4 Примеры настройки

| Сценарий | URI и оператор | Пример лимита | Комментарий |
|---|---|---|---|
| Защита формы входа | Равно: /login | 20 запросов за 60 сек., блокировка 300 сек. | Подходит для точного пути; значения следует согласовать с реальной моделью входа. |
| Ограничение ветки API | Начинается с: /api/search/ | 120 запросов за 60 сек., блокировка 120 сек. | Охватывает все endpoint-ы внутри ветки. |
| Несколько эквивалентных путей | Равно: /signin; Равно: /auth/login | 30 запросов за 60 сек. | Оба пути учитываются одним правилом по логике «ИЛИ». |

## 7.3 Правила защиты

### 7.3.1 Назначение и приоритет

«Правила защиты» позволяют сопоставлять запросы по сетевым, HTTP- и поведенческим признакам, учитывать лимиты и состояние DDoS-атаки, а затем назначать действие для соответствующих классов источника. Правила обрабатываются последовательно; применяется первое подходящее правило.

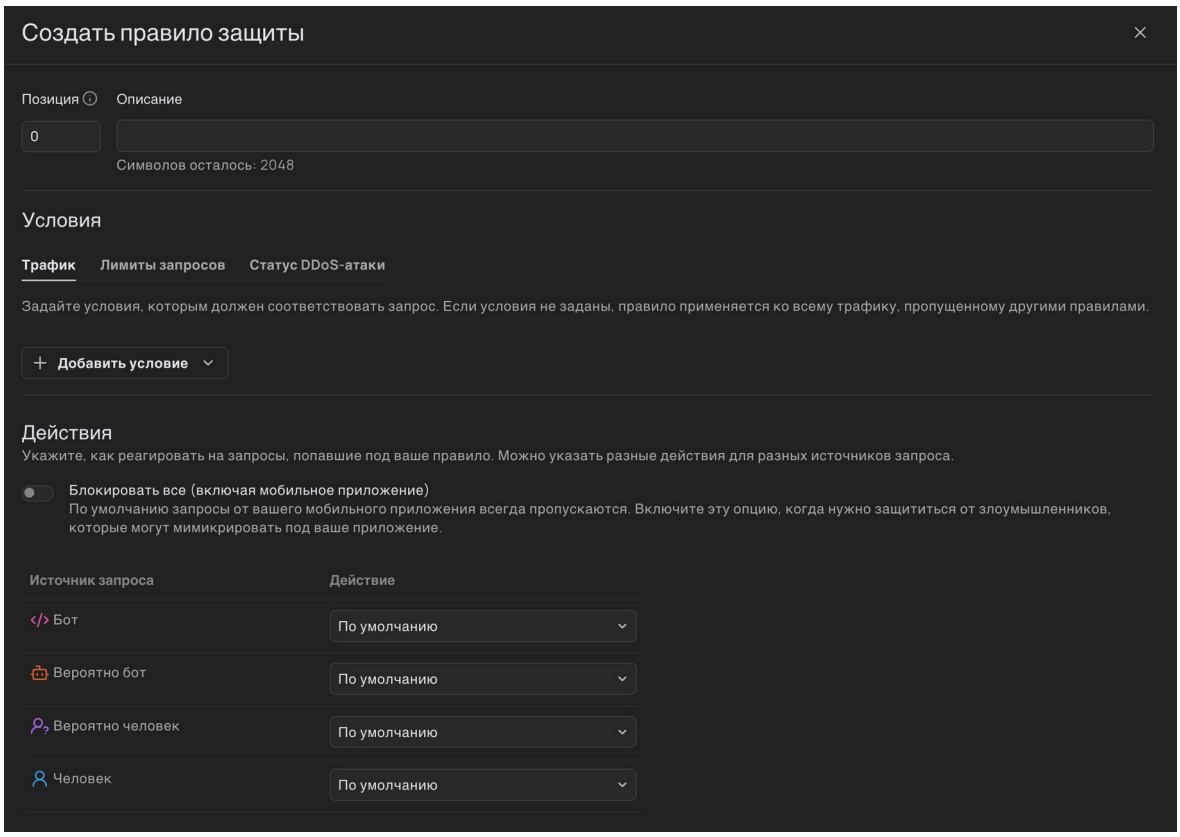


*Рисунок 16 - Общая форма правила защиты*

| Поле | Обязательность | Назначение |
|---|---|---|
| Позиция | Да | Место правила в последовательности. Меньшее значение соответствует более ранней проверке. |
| Описание | Нет | Назначение, основание и область действия правила. Максимальная длина - 2048 символов. |
| Состояние | Да | Включает или отключает применение правила. |
| Трафик | Зависит от сценария | Набор условий по сетевым и HTTP-признакам. При отсутствии условий область действия может быть широкой. |
| Лимиты запросов | Нет | Глобальный и/или индивидуальный для IP лимит, а также выбор применения действия до или после превышения. |
| Статус DDoS-атаки | Да | Ограничивает правило режимом «Всегда», «Пока нет атаки» или «Во время атаки». |
| Действия | Да | Определяют обработку запроса целиком либо отдельно для каждого класса источника. |

**Правило без условий.** Если форма допускает сохранение правила без условий трафика, оно может соответствовать всем запросам в выбранном состоянии DDoS. Такое правило следует размещать только после более узких правил и использовать осознанно.

### 7.3.2 Условия на вкладке «Трафик»

Каждое условие состоит из параметра, оператора и значения. Доступные операторы зависят от типа параметра. Несколько условий в одном блоке используются совместно согласно логике, показанной в интерфейсе; при создании проверяйте визуальные связки «И» и «ИЛИ».

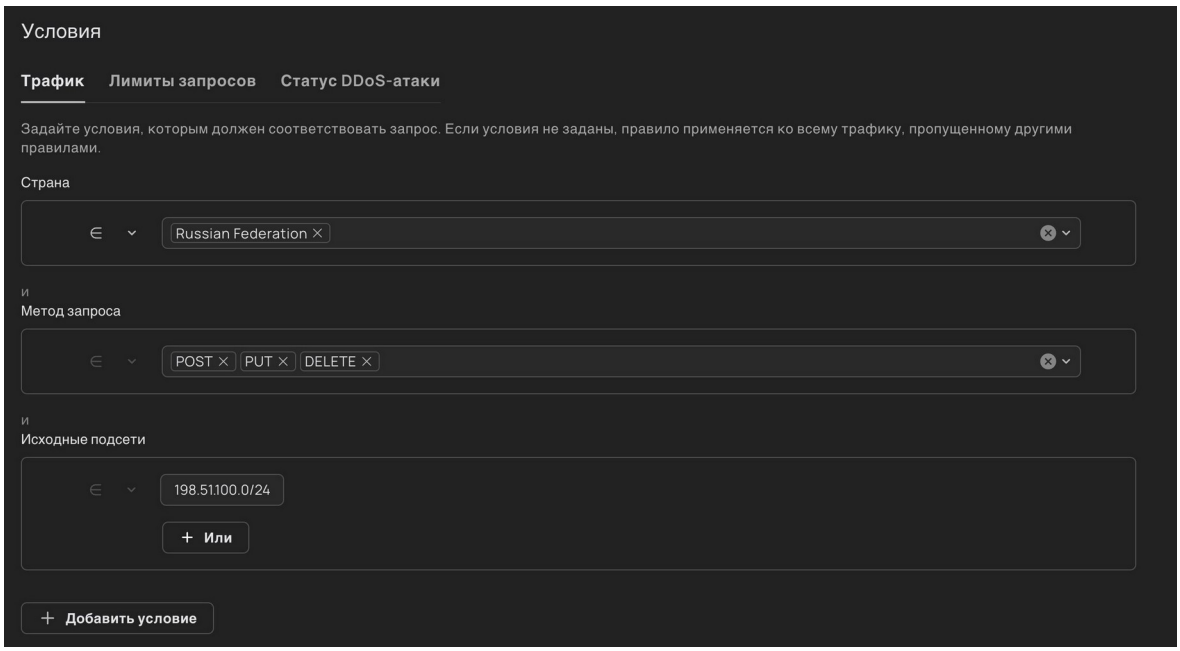


*Рисунок 17 - Добавление условий трафика в правило защиты*

| Параметр | Что сопоставляется | Типичные значения |
|---|---|---|
| Страна | Географическая страна IP-адреса источника. | Коды или названия стран из справочника интерфейса. |
| ASN | Номер автономной системы источника. | Числовой ASN. |
| Query string | Строка параметров URL после знака вопроса. | Пары параметров или фрагменты строки. |
| Путь URL | Полный путь запроса без домена. | /login, /api/v1/orders. |
| Сегмент пути URL | Отдельная часть пути. | api, admin, checkout. |
| Content-Type | Значение заголовка типа содержимого. | application/json, multipart/form-data. |
| Cookie (или) | Совпадение хотя бы одной указанной cookie. | Имя и шаблон значения. |
| Cookie (и) | Одновременное совпадение всех указанных cookie. | Набор имен и значений. |
| Заголовок | HTTP-заголовок запроса. | Имя заголовка и ожидаемое значение. |
| Имя хоста | Заголовок Host / защищаемый домен. | example.ru, api.example.ru. |
| Хостинговая подсеть | Признак принадлежности IP к хостинговой инфраструктуре. | Логическое значение. |

| Параметр | Что сопоставляется | Типичные значения |
|---|---|---|
| Метод запроса | HTTP-метод. | GET, POST, PUT, DELETE, PATCH и др. |
| Referer | Источник перехода. | URL или шаблон домена/пути. |
| Хэши | Сервисные составные отпечатки запроса. | Значения, полученные из журналов и аналитики. |
| Запрос от нового пользователя | Признак новой для системы сессии/пользователя. | Да / Нет. |
| Исходные подсети | IP-адрес или CIDR источника. | 192.0.2.0/24, 2001:db8::/32 - в пределах поддерживаемого формата. |
| User-Agent | Строка клиентского приложения. | Браузер, библиотека, бот или шаблон. |
| X-Forwarded-For | Значение заголовка цепочки прокси. | IP-адрес или фрагмент заголовка. |

### 7.3.3 Операторы условий

| Оператор в интерфейсе | Смысл |
|---|---|
| Входит в / Не входит в | Значение присутствует или отсутствует в заданном наборе. |
| Равно / Не равно | Точное совпадение или несовпадение. |
| Содержит / Не содержит | Искомый фрагмент присутствует или отсутствует в строке. |
| Начинается с / Не начинается с | Проверяется начало строки. |
| Заканчивается на / Не заканчивается на | Проверяется окончание строки. |
| Любое | Условие соответствует любому непустому или доступному значению согласно типу параметра. |
| Пустое / Не пустое | Проверяется отсутствие либо наличие значения. |

**Точность условий.** Для путей и заголовков сначала используйте точное сравнение. Операторы «Содержит» и «Начинается с» расширяют область действия и требуют проверки на примерах из журнала.

### 7.3.4 Лимиты запросов внутри правила защиты

Вкладка «Лимиты запросов» позволяет сделать совпадение правила зависимым от интенсивности трафика. Поддерживаются общий счетчик и счетчик для отдельного IP-адреса.

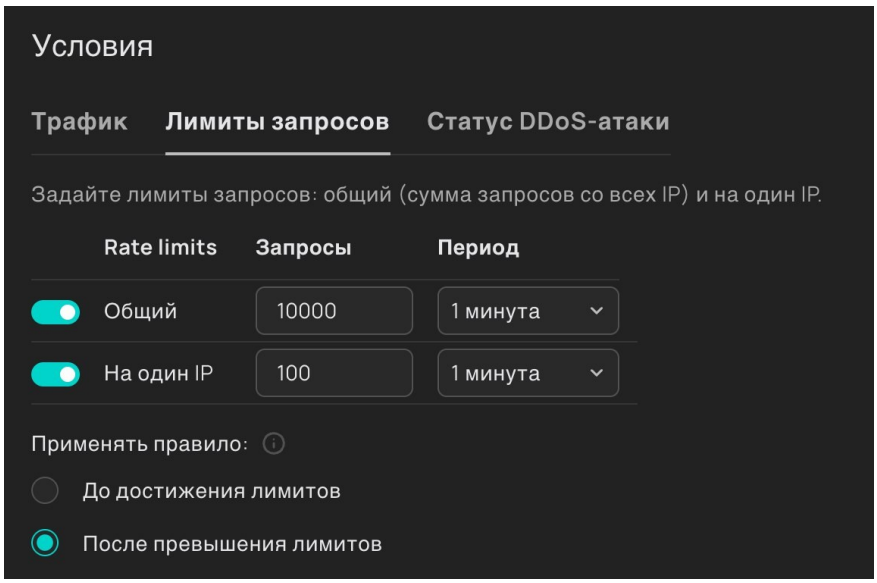


*Рисунок 18 - Настройка лимитов запросов в правиле защиты*

| Элемент | Назначение |
|---|---|
| Общий лимит | Считает все запросы, соответствующие условиям правила, независимо от IP источника. |
| Лимит на IP | Считает запросы отдельно для каждого IP-адреса. Подходит для ограничения одного клиента. |
| Количество | Порог запросов за период. Должен быть положительным. |
| Период | Доступные интервалы: 1 секунда, 10 секунд, 1 минута, 5 минут и 10 минут. |
| Применять до превышения | Действие правила применяется, пока счетчик находится ниже порога. |
| Применять после превышения | Действие применяется после достижения/превышения порога согласно логике интерфейса. |

**Выбор счетчика.** Общий лимит полезен для защиты ресурсоемкого endpoint от суммарной нагрузки, а лимит на IP - для ограничения одного клиента. Одновременное использование обоих счетчиков следует проверять на тестовом трафике.

### 7.3.5 Состояние DDoS-атаки

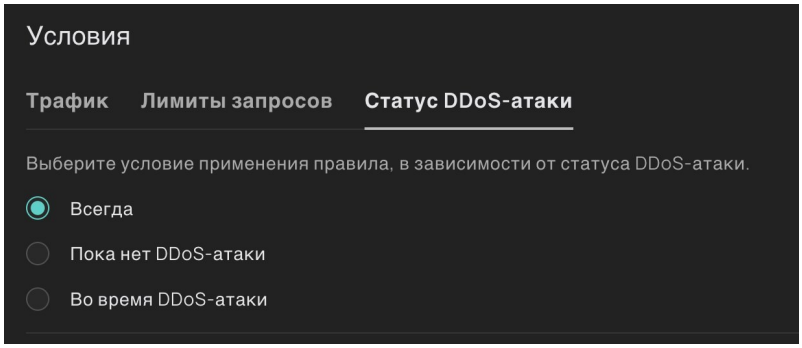


*Рисунок 19 - Выбор состояния DDoS для правила*

| Режим | Когда правило проверяется |
|---|---|
| Всегда | Независимо от наличия зафиксированной DDoS-атаки. |
| Пока нет атаки | Только в штатном состоянии ресурса. |
| Во время атаки | Только когда система определила состояние DDoS-атаки для соответствующего контекста. |

### 7.3.6 Действия правила

На вкладке действий можно назначить единое блокирование всего соответствующего трафика либо определить отдельное действие для каждого класса источника.

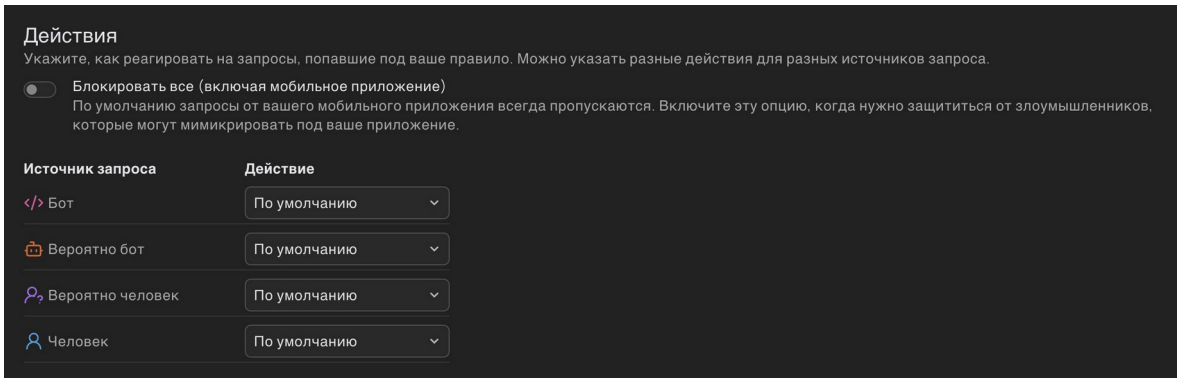


*Рисунок 20 - Настройка действий по классам источников*

| Класс источника | Смысл |
|---|---|
| Бот | Высокая вероятность автоматизированной активности. |
| Вероятно бот | Признаки автоматизации преобладают, но уверенность ниже. |
| Вероятно человек | Признаки легитимного пользователя преобладают, но требуется осторожность. |
| Человек | Высокая вероятность легитимной пользовательской активности. |

| Действие | Результат |
|---|---|
| По умолчанию | Сохраняется стандартная обработка, определенная профилем защиты и другими механизмами. |
| Пропустить | Запрос разрешается без применения более строгого действия этого правила. |
| Блокировать | Запрос отклоняется. |
| JS-проверка | Клиенту предлагается выполнить JavaScript-проверку. Уровень: «Простой», «Обычный» или «Сложный». |
| Cookie-проверка | Клиенту выдается проверка, связанная с установкой и последующим подтверждением cookie. |
| CAPTCHA | Клиенту показывается CAPTCHA. Уровень: «Простой», «Продвинутый» или «Сложный». |

| Действие | Результат |
|---|---|
| Блокировать весь трафик, включая мобильное приложение | Единое блокирование всех запросов, соответствующих правилу, без разделения по классам источников. Используется только для однозначно вредоносной области. |

**Осторожно.** Действия «Пропустить» и «Блокировать весь трафик» имеют сильное влияние. Не используйте «Пропустить» для широких условий без оценки обхода других механизмов защиты; не применяйте полное блокирование к общим путям без тестирования.

### 7.3.7 Создание и проверка правила защиты

1. Откройте «Пользовательские правила -> Правила защиты».
2. Нажмите «Добавить правило защиты».
3. Задайте позицию и понятное описание.
4. На вкладке «Трафик» добавьте минимально необходимый набор условий.
5. При необходимости настройте общий или индивидуальный лимит.
6. Выберите состояние DDoS-атаки.
7. Назначьте действия по классам источника либо единое действие.
8. Сохраните правило в отключенном состоянии, если требуется предварительная проверка конфигурации.
9. Включите правило в согласованное окно изменений.
10. Проверьте статистику действий и журнал запросов; при нежелательном результате немедленно отключите правило.

### 7.3.8 Изменение порядка

Позиция определяет последовательность проверки. Узкие исключения и правила для конкретных endpoint-ов обычно располагаются выше общих правил. После изменения позиции следует повторно проверить конфликтующие условия.

| Порядок | Пример |
|---|---|
| 1. Узкое разрешающее исключение | Доверенная интеграция к одному API-пути из подтвержденной подсети. |
| 2. Специальное защитное правило | Ограничение формы входа или платежного endpoint. |
| 3. Общая политика ветки | Действия для /api/ или /account/. |
| 4. Широкая политика ресурса | Правило без пути либо с общим условием. |

## 7.4 Специальное правило защиты API

### 7.4.1 Назначение

Специальное правило защиты API ограничивает прямой доступ к выбранным API-путям. Запрос разрешается только при наличии подтвержденного предварительного посещения веб-страницы ресурса в течение заданного времени. Правило предназначено для endpoint-ов, которые должны вызываться из пользовательского веб-сценария, а не напрямую автоматизированным клиентом.

**Ограничение.** Для одного ресурса может быть создано не более одного специального правила защиты API. Оно имеет фиксированный приоритет и обрабатывается перед обычными правилами защиты.

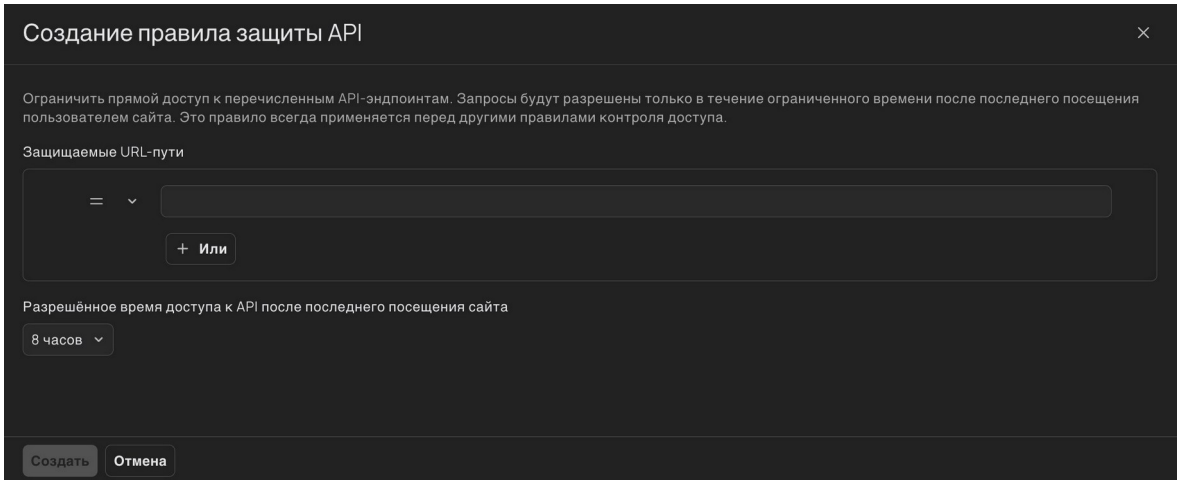


*Рисунок 21 - Форма специального правила защиты API*

### 7.4.2 Поля формы

| Поле | Обязательность | Назначение и правила заполнения |
|---|---|---|
| Защищаемые URL-пути | Да, не менее одного | Пути API, для которых требуется подтвержденное посещение веб-страницы. Для каждого пути выбирается точное совпадение или совпадение по началу. Несколько путей объединяются логикой «ИЛИ». |
| Оператор пути | Да | «Равно» защищает один точный endpoint; «Начинается с» распространяет правило на всю ветку. |
| Разрешенное время | Да | Период после посещения веб-страницы, в течение которого клиент может обращаться к защищаемому API. |
| Пользовательское время | Условно | Используется при выборе собственного значения. Максимум - 1440 минут. |
| Состояние правила | Да | Включает или отключает действие специального правила. |

| Доступные значения времени | Комментарий |
|---|---|
| 5, 15 или 30 минут | Для коротких пользовательских сценариев с быстрым вызовом API после открытия страницы. |
| 1, 2, 3, 4, 6, 8, 12 или 24 часа | Для длительных сессий и приложений, где повторные вызовы API выполняются в течение рабочего периода. |
| Пользовательское значение | Задается в минутах, но не более 1440 минут. |

### 7.4.3 Порядок настройки

1. Откройте «Пользовательские правила -> Правила защиты».
2. Выберите создание специального правила защиты API.
3. Добавьте один или несколько путей и выберите оператор для каждого.
4. Установите разрешенное время после посещения страницы.
5. Сохраните правило и включите его в согласованное окно изменений.
6. Проверьте два сценария: штатный вызов API после открытия страницы и прямой вызов API без предварительного посещения.
7. Проконтролируйте результат по журналу запросов и убедитесь, что мобильные и серверные интеграции, которым нужен прямой API-доступ, не затронуты.

**Важно.** Не включайте правило для API, которое штатно вызывается мобильным приложением, серверной интеграцией, мониторингом или партнером без предварительного посещения веб-страницы. Для таких клиентов используйте отдельную архитектуру доступа или более точные условия.

## 7.5 Сбор JS score

### 7.5.1 Назначение

Правила «Сбор JS score» определяют, для какого трафика клиенту должен выдаваться JavaScript, собирающий признаки браузера и формирующий оценку. Само правило не задает разрешение или блокирование: полученное значение используется дальнейшей классификацией и другими механизмами защиты.

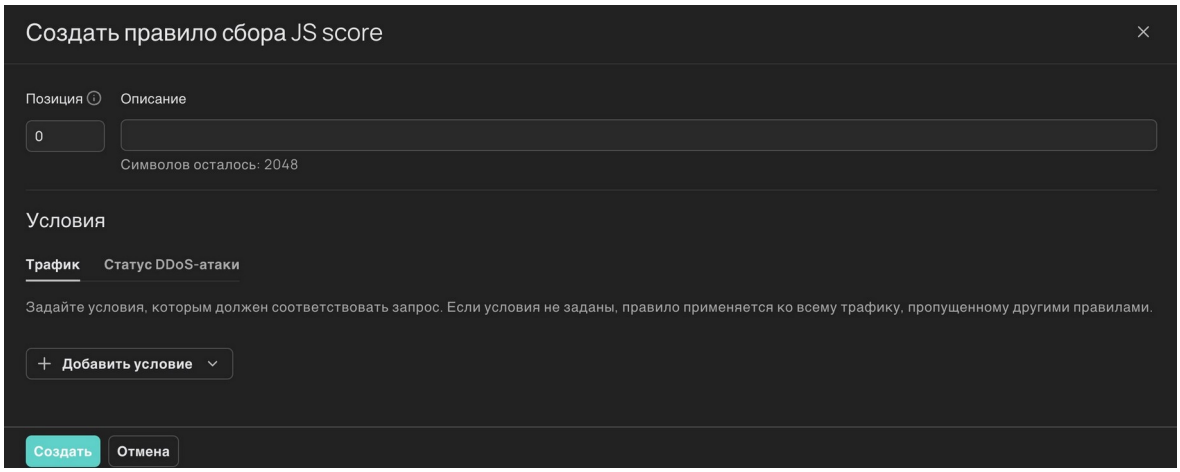


*Рисунок 22 - Форма правила сбора JS score*

### 7.5.2 Поля и условия

| Поле / блок | Обязательность | Назначение |
|---|---|---|
| Позиция | Да | Порядок проверки правила среди других правил сбора JS score. |
| Описание | Нет | Назначение и область действия. Максимальная длина - 2048 символов. |
| Условия трафика | Нет | Параметры и операторы, аналогичные доступным в правилах защиты. Без условий правило может охватывать весь подходящий трафик. |

| Поле / блок | Обязательность | Назначение |
|---|---|---|
| Статус DDoS-атаки | Да | «Всегда», «Пока нет атаки» или «Во время атаки». |
| Состояние | Да | Включение или отключение правила. |

Набор параметров и операторов условий соответствует описанному в разделе 7.3.2. Рекомендуется ограничивать выдачу JavaScript HTML-страницами и пользовательскими маршрутами, на которых браузер ожидаемо выполняет сценарий.

### 7.5.3 Ограничения применения

**Не применять.** Не создавайте правило сбора JS score для AJAX-запросов, API-endpoint-ов, статических файлов, изображений, шрифтов, служебных health-check и других запросов, в ответе на которые JavaScript не может быть корректно выполнен пользователем.

Подходящие области для сбора JS score:

- HTML-страницы входа, регистрации и восстановления доступа;
- страницы каталога, поиска и оформления заказа;
- страницы личного кабинета, на которых браузер выполняет JavaScript;
- начальные страницы пользовательского сценария перед обращением к защищаемому API.

Порядок создания правила:

1. Откройте «Пользовательские правила -> Сбор JS score».
2. Нажмите «Добавить правило».
3. Укажите позицию и описание.
4. Добавьте условия, ограничивающие правило HTML-трафиком и нужными путями.
5. Выберите состояние DDoS-атаки.
6. Сохраните и включите правило.
7. Проверьте наличие JS score в журнале для ожидаемых браузерных запросов и отсутствие выдачи скрипта на API/статике.

## 7.6 Классификация ботов

### 7.6.1 Назначение и порог

Правила «Классификация ботов» задают порог JS bot score, при котором трафик относится к автоматизированному. Порог может быть общим для ресурса или применяться только при совпадении дополнительных условий.

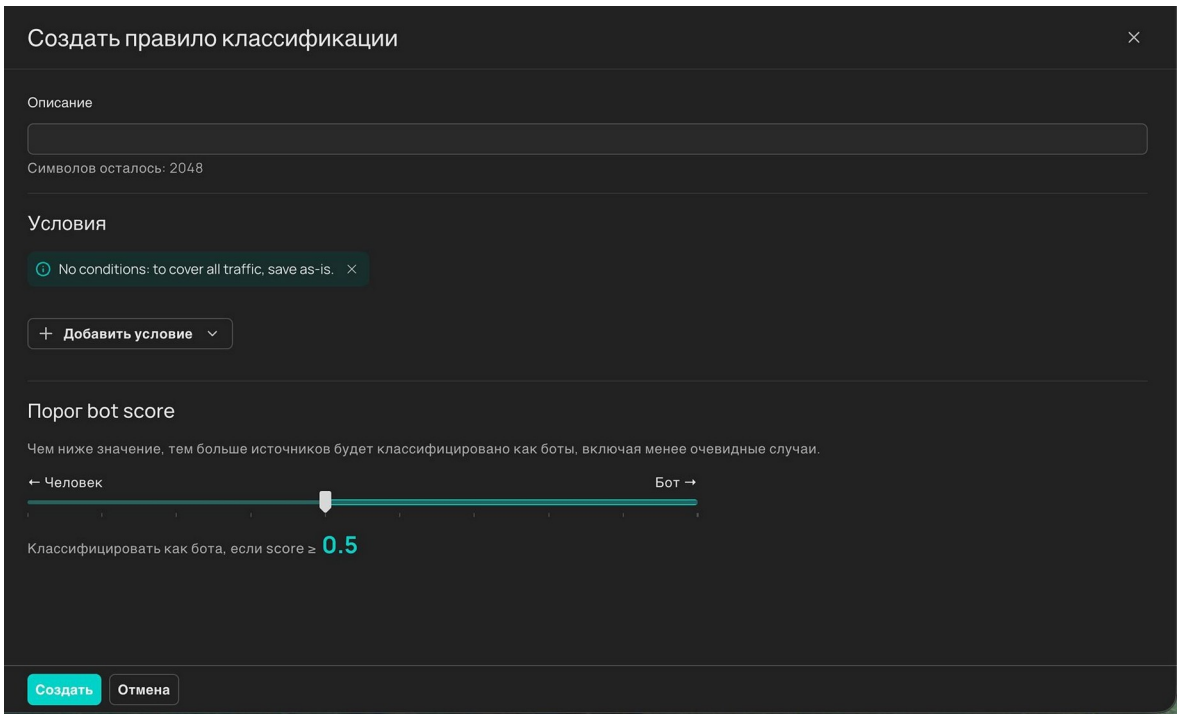


*Рисунок 23 - Форма правила классификации ботов*

| Поле / блок | Обязательность | Назначение и правила |
|---|---|---|
| Описание | Нет | Назначение правила. Максимальная длина - 2048 символов. |
| Условия | Нет | Ограничивают область действия. Если условия отсутствуют, правило применяется ко всему трафику, для которого доступен JS bot score. |
| Порог Bot score | Да | Значение от 0 до 1 с шагом 0,1. В интерфейсе минимально выбираемое значение - 0,1; типовое исходное значение формы - 0,5. |
| Состояние | Да | Включение или отключение правила. |

### 7.6.2 Логика выбора порога

Если одному запросу соответствуют несколько включенных правил классификации, применяется наиболее строгий порог - минимальное подходящее значение. Поэтому условные правила должны только ужесточать общую настройку и не должны создавать неоднозначные исключения.

| Пример | Подходящие пороги | Применяемый порог |
|---|---|---|
| Общее правило 0,5 и правило для /login со значением 0,3 | 0,5 и 0,3 | 0,3 для /login; 0,5 для остального трафика. |
| Два правила без условий 0,6 и 0,4 | 0,6 и 0,4 | 0,4 для всего трафика. Такая конфигурация избыточна. |
| Условное правило не совпало | Только общее правило 0,5 | 0,5. |

**Интерпретация порога.** Чем ниже порог, тем больше клиентов будут классифицированы как боты. Снижение порога повышает строгость, но увеличивает риск ложной классификации. Изменяйте порог постепенно и подтверждайте результат по журналам и пользовательским метрикам.

### 7.6.3 Создание и проверка правила

1. Откройте «Пользовательские правила -> Классификация ботов».
2. Нажмите «Добавить правило».
3. Введите описание.
4. Для общего правила оставьте условия пустыми; для отдельной области добавьте путь, Host, страну, ASN или другие поддерживаемые условия.
5. Установите порог на шкале от 0 до 1.
6. Сохраните и включите правило.
7. Сопоставьте изменение распределения классов источников с логами и бизнес-показателями.
8. При росте ложных срабатываний повысьте порог или сузьте условия.

## 7.7 Рекомендации по сопровождению правил

| Практика | Рекомендация |
|---|---|
| Именование и описание | Указывайте защищаемый сценарий, владельца, номер изменения и ожидаемый результат. |
| Минимальная область | Начинайте с точного Host/пути/метода и добавляйте расширение только после наблюдения. |
| Порядок | Размещайте узкие исключения и специальные сценарии выше общих политик. |
| Тестирование | Проверяйте штатного пользователя, вредоносный сценарий, API-клиент, мобильное приложение и мониторинг, если они затрагиваются. |
| Наблюдение | После включения контролируйте действия защиты, классы источников, ошибки, время ответа и журнал. |
| Откат | Сохраняйте возможность быстро отключить правило; не удаляйте предыдущую конфигурацию до завершения проверки. |
| Периодический пересмотр | Удаляйте устаревшие исключения и дублирующие правила, проверяйте временные причины и владельцев. |

# 8 Обнаруженные аномалии

## 8.1 Назначение раздела

Раздел «Обнаруженные аномалии» содержит периоды нетипичного или вредоносного трафика, зафиксированные системой для защищаемых ресурсов. Он используется для ретроспективного анализа атаки, определения основных источников и сопоставления с действиями защиты.

**Примечание.** Раздел отображается только для учетных записей, которым доступна соответствующая функция. Отсутствие раздела не означает отсутствие защиты ресурса.

## 8.2 Список аномалий

| Поле | Назначение |
|---|---|
| ID | Уникальный идентификатор аномалии. Используется при расследовании и обращении в техническую поддержку. |
| Начало | Дата и время начала зафиксированного периода. |
| Окончание | Дата и время завершения. Для продолжающейся аномалии окончание может отсутствовать или обновляться. |
| Ресурс | Защищаемый ресурс, для которого зафиксирована аномалия. |
| Максимальная скорость блокировок | Наибольшее агрегированное значение блокируемых запросов за единицу времени в период аномалии. |
| Всего заблокировано | Суммарное количество заблокированных запросов за период. |

Для поиска нужной записи используйте доступные фильтры по периоду, ресурсу и идентификатору.

## 8.3 Карточка аномалии

При выборе аномалии открывается подробная страница с временными границами, ресурсом, графиками трафика и аналитическими топами. Конкретный набор виджетов зависит от доступных данных и версии интерфейса.

| Блок | Содержание |
|---|---|
| Сводка | Начало, окончание, ресурс, максимальная скорость и суммарные значения. |
| Динамика запросов | Изменение входящих, разрешенных и заблокированных запросов во времени. |
| Действия защиты | Распределение по блокировке, пропуску и дополнительным проверкам. |
| Классы источников | Доли ботов, вероятных ботов, вероятных людей и людей. |

| Блок | Содержание |
|---|---|
| Страны | Основные страны, сформировавшие трафик аномалии. |
| IP-адреса и подсети | Наиболее активные источники и сетевые диапазоны. |
| Запросы / пути | Наиболее часто запрашиваемые URL-пути. |
| User-Agent / ОС | Основные клиентские строки и определенные операционные системы. |

## 8.4 Порядок анализа аномалии

1. Зафиксируйте ID, ресурс, начало и окончание аномалии.
2. Определите время пика и сравните входящий, разрешенный и заблокированный трафик.
3. Проверьте действия защиты и классы источников.
4. Изучите топы стран, IP-адресов, подсетей, путей и User-Agent.
5. Перейдите в «Логи запросов» и задайте узкий интервал вокруг пика.
6. Найдите типичные и пограничные примеры запросов, зафиксируйте причину действия и ID правила.
7. Проверьте коды и время ответа источника, чтобы исключить одновременную деградацию backend.
8. При необходимости скорректируйте списки или пользовательские правила и контролируйте результат.

**Важно.** Не делайте вывод о вредоносности только по стране, ASN или User-Agent. Для изменения политик используйте совокупность признаков и примеры запросов из журнала.

# 9 Пользовательские события

## 9.1 Назначение

«Пользовательские события» позволяют задать порог по выбранной метрике и фиксировать периоды, когда значение становится больше или меньше порога. Функция используется для контроля нагрузки, действий защиты, кодов ответа и времени обработки.

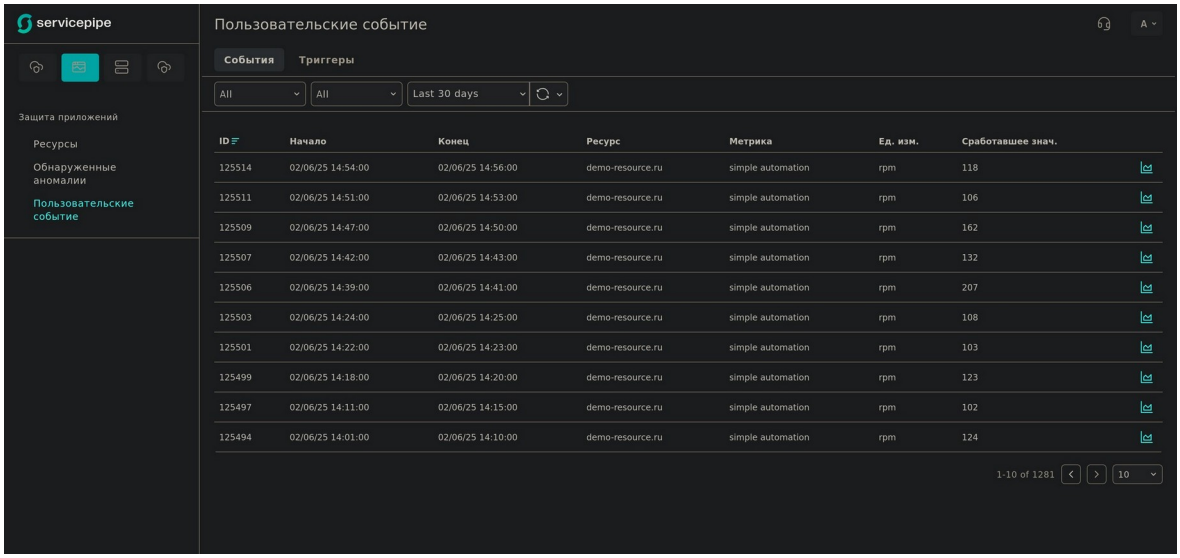


*Рисунок 24 - Список пользовательских событий*

## 9.2 Создание условия события

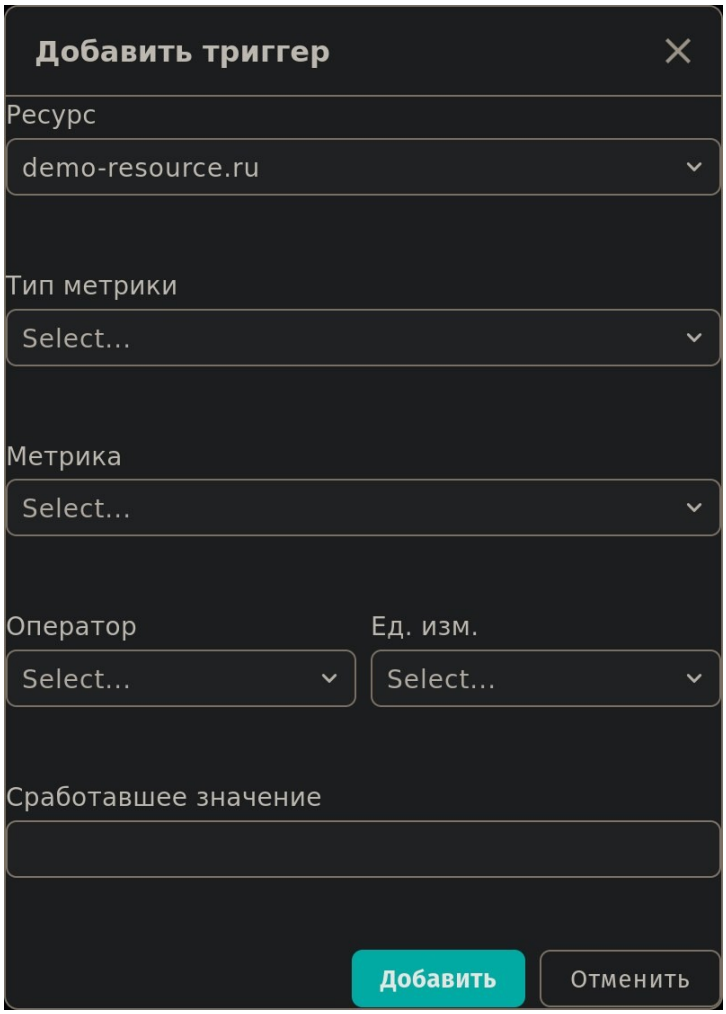


*Рисунок 25 - Форма создания пользовательского события*

| Поле | Обязательность | Назначение и правила |
|---|---|---|
| Ресурс | Да | Защищаемый ресурс, для которого контролируется метрика. |
| Тип метрики | Да | Группа показателей: полоса, действия над запросами, CAPTCHA, коды ответа, время обработки, класс источника и другие доступные типы. |
| Метрика | Да | Конкретный показатель внутри выбранного типа. Набор изменяется динамически после выбора типа метрики. |
| Условие | Да | «Больше» или «Меньше» заданного порога. |
| Единица измерения | Да | Для полосы - Кбит/с или Мбит/с; для количества запросов - RPS или RPM. Доступные единицы зависят от метрики. |
| Порог | Да | Числовое значение, при пересечении которого фиксируется событие. Должно быть неотрицательным и соответствовать масштабу выбранной единицы. |

## 9.3 Группы метрик

| Тип метрики | Доступные показатели |
|---|---|
| Полоса | Заблокированная, пропущенная, входящая и исходящая полоса. |
| Действия над запросами | Заблокировано, Cookie-проверка, JS-проверка, CAPTCHA, пропущено, перенаправлено, некорректный запрос. |
| Статистика CAPTCHA | Разрешено после CAPTCHA, выдано CAPTCHA, успешно решено. |
| Коды ответа платформы | Классы 2xx, 3xx, 4xx и 5xx. |
| Общее время обработки | Запросы в доступных временных интервалах/корзинах. |
| Время ответа источника | Запросы в доступных интервалах времени ответа backend. |
| Класс источника | Бот, вероятно бот, вероятно человек, человек. |
| Ошибки источника 5xx | Коды 500, 501, 502, 503 и 504. |
| Коды ответа источника | Классы ответов 2xx, 3xx, 4xx и 5xx от backend. |

## 9.4 Порядок создания и проверки

1. Откройте «Защита приложений -> Пользовательские события».
2. Нажмите «Добавить событие».
3. Выберите ресурс.
4. Выберите тип метрики и конкретную метрику.
5. Установите условие «Больше» или «Меньше».
6. Выберите единицу измерения и введите порог.
7. Сохраните условие.
8. Проверьте его в списке и сопоставьте с графиком соответствующей метрики.
9. После срабатывания откройте карточку события и проанализируйте тот же период в статистике и журналах.

**Рекомендация.** Порог следует выбирать по историческим данным ресурса. Слишком низкое значение создает частые события, слишком высокое - не фиксирует значимую деградацию. Начните с наблюдаемого рабочего максимума и корректируйте после периода эксплуатации.

# 10 Проверки клиентов

## 10.1 Назначение проверок

Servicepipe Cybert может использовать дополнительные проверки, когда имеющихся признаков недостаточно для однозначного решения. Проверка позволяет подтвердить способность клиента выполнять браузерный сценарий и уточнить классификацию.

| Проверка | Назначение и особенности |
|---|---|
| JS-проверка | Выполнение JavaScript в браузере. Может иметь уровни «Простой», «Обычный» и «Сложный». Не подходит для клиентов без JavaScript. |
| Cookie-проверка | Проверка способности клиента получить и вернуть служебную cookie. Может затронуть клиентов, которые блокируют cookie. |
| CAPTCHA | Интерактивная проверка пользователя. Уровни в правилах: «Простой», «Продвинутый», «Сложный». |

## 10.2 Когда клиент может увидеть проверку

- действие назначено системным профилем защиты для текущего класса источника;
- сработало пользовательское правило защиты;
- изменилось состояние DDoS-атаки и начало действовать правило, привязанное к этому состоянию;
- клиент не имеет необходимой служебной cookie либо требуется обновить результат проверки;
- значение JS score или другие признаки требуют дополнительного подтверждения.

## 10.3 Диагностика проблем с проверками

| Симптом | Что проверить |
|---|---|
| Проверка показывается слишком часто | Срок действия служебных cookie, повторные правила, смену IP/браузера, блокирование cookie, очистку хранилища браузера, корректность времени. |
| Проверка не завершается | Поддержку JavaScript и cookie, расширения блокировки, корпоративный прокси, доступность служебных доменов и отсутствие ошибок в браузере. |
| Проверка появляется у API-клиента | Область правил сбора JS score и защиты; исключите API, AJAX и статические пути из браузерных проверок. |
| CAPTCHA затрагивает легитимных пользователей | Условия правила, классы источников, порог классификации, географию и сетевые признаки. |
| Мобильное приложение блокируется | Наличие действия «Блокировать весь трафик, включая мобильное приложение», поддержку Cookie/JS и отдельные пути мобильного API. |

# 11 Типовые сценарии использования

## 11.1 Подключение веб-ресурса по схеме «Прокси»

1. Создайте ресурс и выберите схему «Прокси».
2. Заполните имя и описание.
3. Добавьте основной домен и необходимые алиасы.
4. Настройте действующий сертификат либо автоматический выпуск, если доступен.
5. Добавьте основной и при необходимости резервный источники.
6. Настройте сетевой доступ источников от инфраструктуры Servicepipe.
7. Выполните требуемое изменение DNS или маршрутизации по данным интеграции.
8. Проверьте HTTPS, коды ответа, Host и доступность статического и динамического содержимого.
9. Откройте «Обзор» и «Логи запросов», убедитесь в поступлении данных.
10. После стабилизации трафика настройте дополнительные списки и пользовательские правила.

## 11.2 Добавление резервного источника

1. Откройте «Настройки -> Источники».
2. Добавьте новый IP-адрес в режиме «Резервный».
3. Заполните вес, описание, порог ошибок и время отключения.
4. Проверьте сетевую доступность и корректность ответа с требуемым Host.
5. Согласуйте тест временного отключения основного источника.
6. После теста верните штатную конфигурацию и зафиксируйте результат.

## 11.3 Ограничение запросов к форме входа

1. По аналитике и журналам определите точный путь формы входа и нормальную частоту запросов.
2. Создайте правило «Лимиты запросов».
3. Выберите оператор «Равно» для пути /login или фактического endpoint.
4. Установите лимит, период и время блокировки с учетом повторных попыток пользователя и приложений.
5. Включите правило и выполните тест ниже и выше порога.
6. Проверьте, что легитимный вход, восстановление пароля, SSO и мониторинг не затронуты.

## 11.4 Защита API, вызываемого из веб-страницы

1. Подтвердите, что API не используется напрямую мобильными, серверными и партнерскими клиентами.
2. Создайте специальное правило защиты API.
3. Добавьте точный путь или ветку API.
4. Установите разрешенное время после посещения страницы.
5. Проверьте штатный веб-сценарий и прямой запрос без посещения страницы.
6. Контролируйте журнал по ID правила и корректируйте область при ложных блокировках.

### 11.5 Временное разрешение доверенного адреса

1. Получите подтвержденный IP-адрес, основание и требуемый срок.
2. Откройте «Настройки -> Белый список».
3. Добавьте IP, описание с номером заявки и срок действия.
4. Проверьте результат импорта.
5. После завершения работ убедитесь, что запись истекла или удалите ее вручную.

### 11.6 Расследование роста 5xx

1. На «Обзоре» зафиксируйте начало и масштаб роста ошибок.
2. В «Статистике по трафику» сравните 5xx платформы и источника, время ответа источника и общий трафик.
3. В «Аналитике» определите основные пути и источники запросов.
4. В «Логах запросов» отфильтруйте код ответа источника 500-504 и откройте примеры.
5. Проверьте IP источника, порт, время ответа и наличие повторяемого пути.
6. Сопоставьте с изменениями приложения и состоянием источников.
7. При необходимости временно отключите проблемный источник или скорректируйте его режим в согласованном порядке.

### 11.7 Уточнение классификации на чувствительном пути

1. Включите сбор JS score на HTML-странице, предшествующей чувствительному действию.
2. Накопите данные и изучите распределение Bot score для легитимных и вредоносных сценариев.
3. Создайте условное правило классификации для нужного Host/пути.
4. Установите более строгий порог небольшим шагом.
5. Проверьте изменение классов и действий в журнале.
6. При ложных срабатываниях повысите порог либо добавьте дополнительные условия.

### 11.8 Анализ обнаруженной аномалии

1. Откройте аномалию и зафиксируйте временной диапазон.
2. Определите пик и основные действия защиты.
3. Изучите топы IP, подсетей, стран, путей и User-Agent.
4. Перейдите в журнал на период вокруг пика.
5. Соберите несколько типовых примеров с ID запросов.
6. Решите, требуется ли временный черный список, узкое правило защиты или изменение лимита.
7. После изменения наблюдайте метрики и документируйте результат.