Руководство оператора
Интеллектуальный сетевой экран для защиты веб-приложений iBatyr WAF 2.15

г.Астана

ОГЛАВЛЕНИЕ

1. Функциональные возможности iBatyr WAF

Основные функции iBatyr WAF:

- Защита от основных видов атак на веб-приложения из перечня OWASP Top 10.
- Защита от логических атак на приложения, в том числе от атак на механизмы аутентификации и контроля сессий, а также атак на бизнес-логику.
- Контроль безопасности использования защищаемого приложения, включая контроль действий пользователей.

Интерфейс управления:

- Управление осуществляется по протоколу HTTP с использованием специализированного Веб-интерфейса.
- В целях интеграции с другими решениями, управление может осуществляться также с использованием REST API.
- Ограничение доступа пользователей только к определенным группам приложений (режим Multitenancy).
- Веб-интерфейс обеспечивает версионность конфигурационных настроек системы: в т.ч. базовых конфигурационных настроек, настроек модулей анализа, моделей нормального функционирования приложений, правил принятия решений.
- Интерфейс поддерживает механизмы аутентификации и авторизации пользователей. Ролевая модель предусматривает разграничение доступа для трех групп: администраторы (можно выполнять любые действия), аналитики (можно менять только настройки безопасности), операторы (только мониторинг и работа с событиями безопасности).
- Действия пользователей веб-интерфейса, включая внесенные изменения, сохраняются во внутреннем журнале аудита системы.

Возможности iBatyr WAF:

- Работа с использованием сигнатурного метода:
  - Наличие набора встроенных сигнатур в комплекте поставки.
  - Поддержка распространенного открытого формата веб-сигнатур ModSecurity.
- Противодействие переборным атакам и повторяющимся запросам:
  - Возможность ограничения количества запросов, направляемых приложению в единицу времени.
  - Возможность индивидуальной настройки параметров противодействия переборным атакам для отдельных логических действий в приложении.
  - Возможность блокировки периодических однотипных запросов от одного источника (противодействие ботам).
- Работа на основе позитивных моделей приложения.
- Возможность гибкой настройки различных типов моделей для каждого из защищаемых приложений, в том числе:
  - модели валидации протокола HTTP;

  - модели синтаксического анализа запросов и ответов с поддержкой различных видов сжатия, кодирования и способов передачи данных с различными уровнями вложенности (в частности, XML, JSON, BASE64, GZIP);
  - модели источников – определение характеристик источника на основе параметров запроса;
  - модели определения логических действий (бизнес-действий) в приложении, параметров логических действий и их значений, последовательностей действий, проверки успешности действий;
  - модели защиты от переборных атак и атак типа «умный DoS» на уровне отдельных логических действий и произвольных параметров действия;
  - модели пользователей, их идентификации, аутентификации и контроля сессий.
- Наличие готовых моделей валидации протокола HTTP и синтаксического анализа запросов для типового веб-приложения в комплекте поставки:
  - Возможность разделения запросов к статическому и динамическому контенту на основе анализа заголовков и статистических моделей для минимизации времени обработки статического контента, а также экономии ресурсов, требуемых аналитику для разбора событий (запросы к статическим ресурсам не отображаются в консоли мониторинга).
  - Наличие автоматического алгоритма рекурсивного синтаксического разбора параметров запроса.
  - Наличие автоматического алгоритма построения модели маршрутизации запросов для веб-приложения.
  - Наличие автоматического алгоритма построения синтаксических моделей параметров действий веб-приложения.
  - Наличие автоматического алгоритма оценки отклонения параметров действий Веб-приложения от статистической нормы.
- Обнаружение аномалий и значимых событий:
  - Возможность обнаружения аномалий или значимых данных как в HTTP-запросах, так и в HTTP-ответах.
  - Возможность обнаружения аномалий работы приложения на основе сопоставления значений параметров HTTP-запросов/ответов с сигнатурами атак.
  - Возможность обнаружения аномалий или значимых данных в работе приложения на основе настроенных позитивных моделей приложения (совпадение с моделью или наоборот – отклонение от нее).
  - Обнаружение аномалий и значимых параметров непосредственно внутри вложенных данных, передаваемых по протоколу HTTP без ограничений на количество уровней вложенности.
  - Возможность обнаружения аномалий, свидетельствующих о возможных попытках атак, осуществляемых «методом грубой силы» (bruteforce).
  - Возможность обнаружения аномалий или значимых данных в процессе работы механизмов идентификации, аутентификации, авторизации пользователей и контроля пользовательских сессий.
  - Возможность обнаружения аномалий нарушения бизнес-логики приложения или контроля выполнения бизнес-логики путем использования соответствующей позитивной модели работы приложения.
- Подавление ложных срабатываний:

  - Наличие механизма предварительного («раннего») подавления ложных срабатываний, чтобы исключить возможность их влияния на сформированные правила принятия решений.
  - Наличие функции упрощенного («быстрого») подавления ложных срабатываний оператором iBatyr WAF непосредственно при просмотре описания выявленной аномалии.
  - Возможность тонкой настройки подавления ложных срабатываний различных механизмов определения аномалий в привязке к отдельным параметрам запроса/ответа или бизнес действиям.

- Принятие решений:
  - Наличие настраиваемого модуля принятия решений, позволяющего выделять значимые события информационной безопасности и принимать решения относительно дальнейших действий в отношении HTTP-транзакций (запрос/ответ).
  - Управление правилами принятия решений на основе данных об источнике (IP-адрес, пользователь, ID сессии) и цели HTTP-транзакции (приложение, бизнес-действие), а также обнаруженных в ней аномалиях или значимых данных.
  - Поддерживаются следующие возможные решения: блокировать HTTP-транзакцию, пропустить HTTP-транзакцию, пометить HTTP-транзакцию, модифицировать ответ, добавить источник HTTP-запроса в список.
  - Управление правилами принятия решений (создание, удаление, перегруппировка) с помощью графического конфигуратора через интерфейс управления.
- Машинное обучение:
  - Автоматическое определение и описание статического контента на основе анализа статистики запросов к защищаемым приложениям.
  - Автоматическое построение рекурсивной модели синтаксического анализа данных запросов и ответов с поддержкой различных видов сжатия, кодирования и способов передачи данных с произвольным уровнем вложенности (в частности, XML, JSON, BASE64, GZIP, SOAP).
  - Автоматическое построение модели маршрутизации запросов для веб-приложения.
  - Автоматическое построение моделей логических действий в приложении и моделей параметров этих действий, а также последовательностей (цепочек) логических действий.
  - Оценка отклонения параметров логических действий в веб-приложении от статистической нормы.
  - Возможности по выполнению автоматического обучения в следующих режимах:
    - непрерывное обучение в процессе функционирования;
    - периодический запуск заданий по обучению по установленному расписанию;
    - ручной однократный запуск заданий по обучению.
  - Результаты автоматического обучения полностью интерпретируемы и корректируемы оператором (настройки, выполненные по результатам автоматического обучения, выглядят в интерфейсе управления аналогично настройкам, выполненным вручную).
  - Возможность инкрементного обучения (только для изменений, произошедших с момента предыдущего обучения), а также частичной ручной корректировки результатов обучения для отдельных статических ресурсов, элементов модели синтаксического анализа, логических действий и т.п. без необходимости проводить полное обучение заново.
- Мониторинг и аудит событий информационной безопасности:

- Выводится обобщенная статистика по следующим параметрам: статусы HTTP-ответа сервера, решение по транзакции (заблокировать/пропустить), задержки обработки запросов приложением и WAF, уровень враждебности среды.
- Сообщения об обнаруженных и/или заблокированных атаках на приложения выводятся в агрегированном виде, агрегация происходит по приложениям, типам обнаруженных аномалий и времени возникновения аномалий.
- Для событий безопасности агрегируется информация об источниках атак, в том числе по IP адресам, по географическому распределению источников по странам, по номерам автономных систем.
- Возможность автоматического оповещения пользователей системы о событиях безопасности с использованием электронной почты, гибкая настройка оповещений из веб-интерфейса.
- Возможность автоматической генерации отчетов в формате *.PDF, содержащих статистику событий информационной безопасности за заданные промежутки времени, в том числе регулярные отчеты с периодичностью «раз в сутки», «раз в неделю», «раз в месяц».
- Возможность передачи данных в режиме реального времени в систему мониторинга и корреляции событий информационной безопасности (SIEM).

2. Вход в систему

Для доступа к iBatyr WAF необходимо открыть любой браузер актуальной версии и в адресной строке ввести адрес iBatyr WAF.

Если на WAF не включена мультитенантная модель, откроется окно (см. рисунок 1) с вводом учётных данных пользователя.

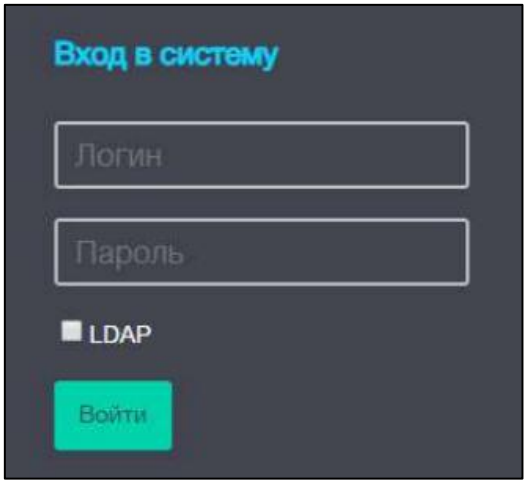

Рисунок 1 – Окно авторизации

Если на WAF включена мультитенантная модель, откроется окно (см. рисунок 2), где в дополнение к полям с вводом логина и пароля, есть еще поле с вводом имени тенанта.

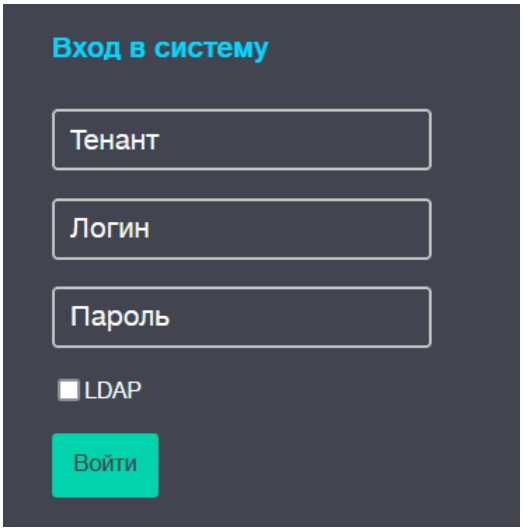

Рисунок 2 – Окно авторизации с тенантом

Подробнее о мультитенантной модели можно прочитать в разделе 6.

При первой авторизации пользователю будет предложено поменять пароль (см. рисунок 3).

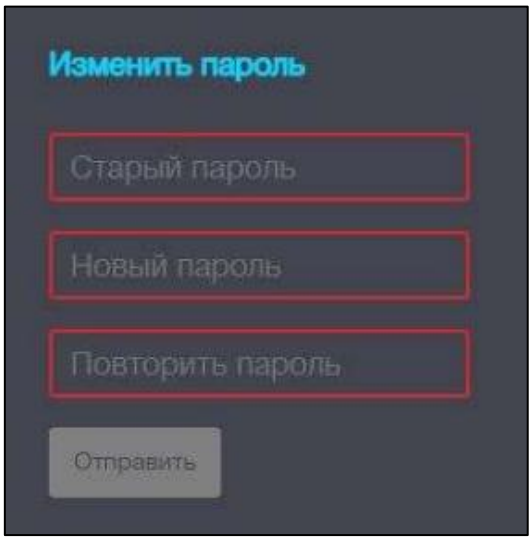

Рисунок 3 – Окно смены пароля

В случае ввода неверной пары «логин – пароль» в окне авторизации высветится сообщение об ошибке (см. рисунок 4).

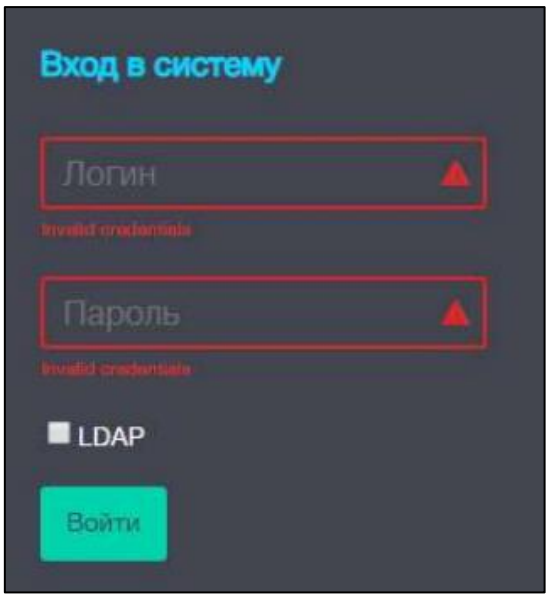

Рисунок 4 – Сообщение об ошибке авторизации

В случае успешной авторизации откроется окно «Обзор» iBatyr WAF (см. рисунок 5).

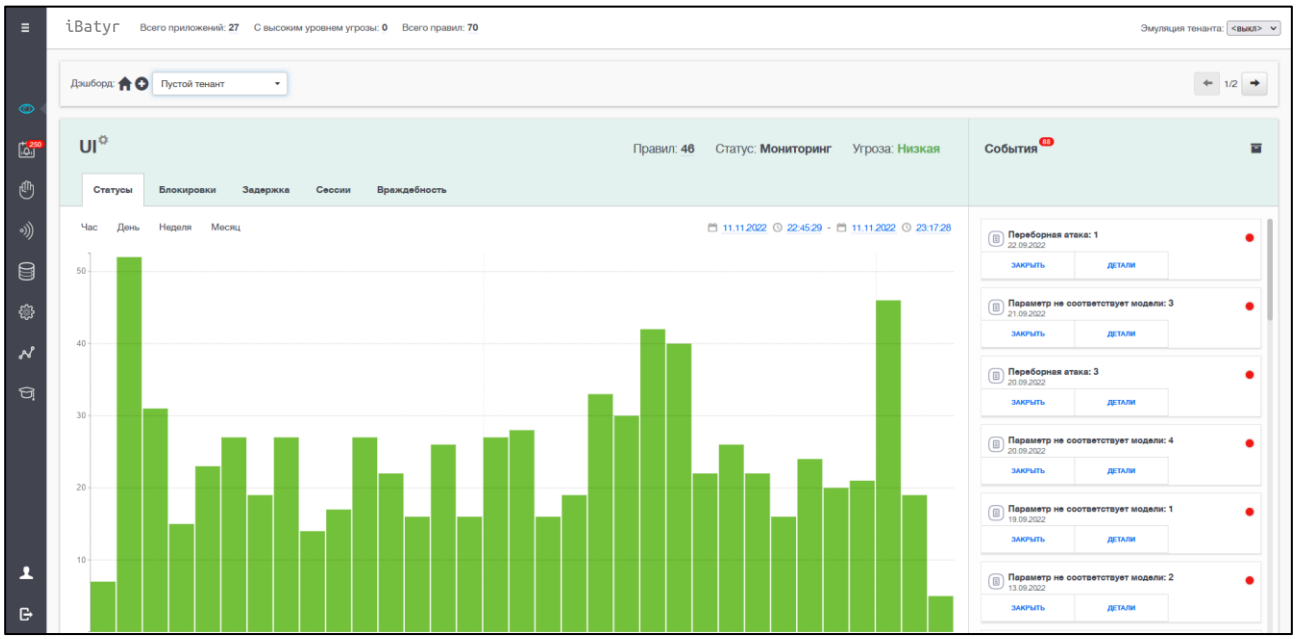

Рисунок 5 – Окно «Обзор»

3. Знакомство с интерфейсом

Для того чтобы свернуть и развернуть меню элементов управления необходимо нажать на иконку в левом верхнем углу (см. рисунок 6).

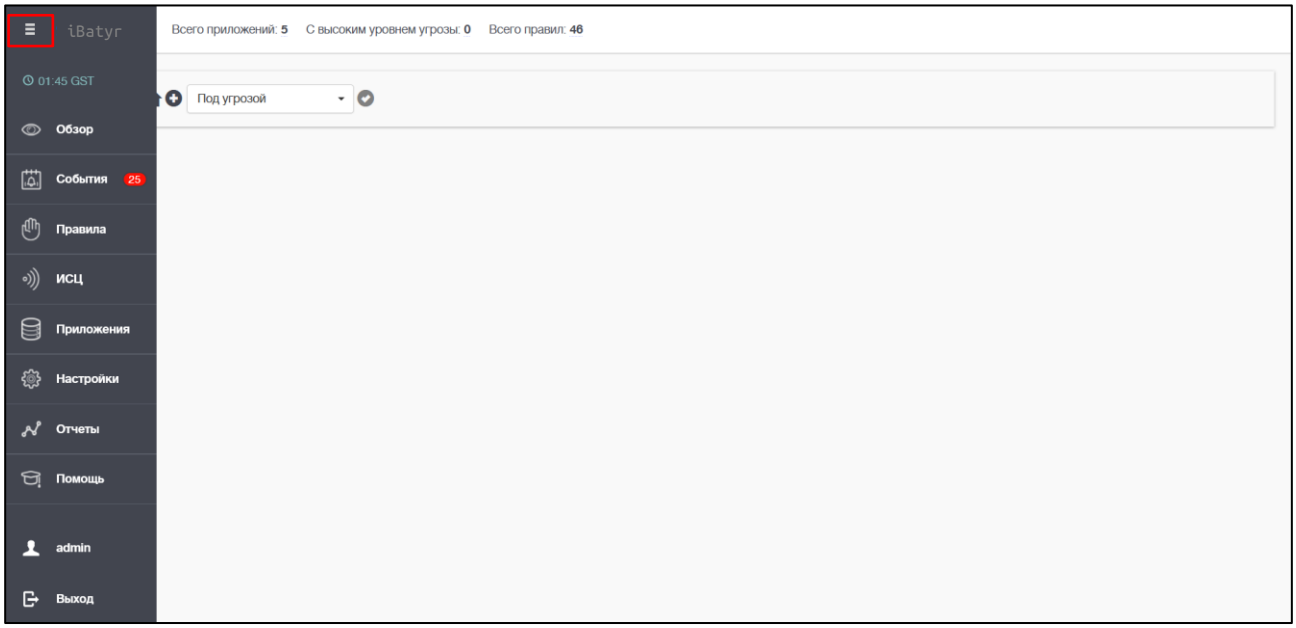

Рисунок 6 – Начальный экран с наименованием колонок

3.1. Окно «Обзор»

Окно «Обзор» позволяет просматривать графики с различными статистиками по каждому из приложений, оценивать динамику нагрузки на приложение, а также динамику количества произошедших событий разного уровня опасности за определённый временной интервал.

Окно «Обзор» является домашней страницей, оно открывается по умолчанию после аутентификации в интерфейсе.

При нажатии на иконку «Обзор» откроется окно со следующими органами управления (см. рисунок 7).

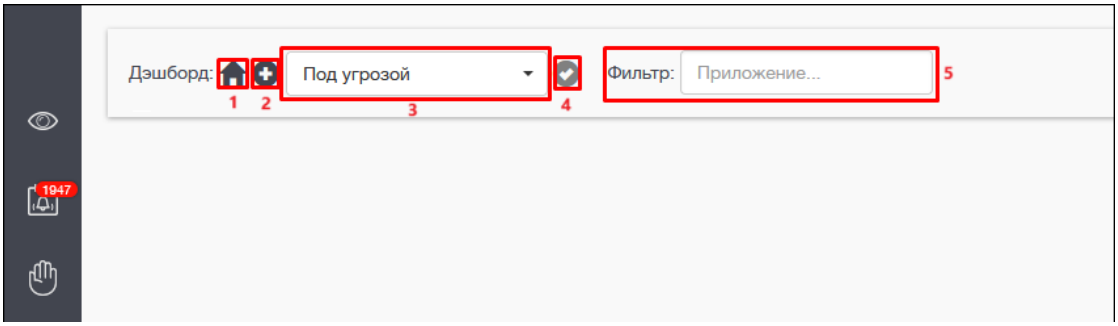

Рисунок 7 – Окно «Обзор»

Где:

1. – переключиться на домашний набор приложений (дешборд).
2. – создать новый набор из заведенных на WAF приложений.

3. Окно выбора – выводит список всех имеющихся наборов приложений.
4. – сделать текущий набор домашним. Данный набор приложений будет открываться по умолчанию при переходе в раздел «Обзор». «Домашним» можно сделать либо набор, созданный пользователем, либо набор «под угрозой».

При выборе пользовательского набора приложений появляются дополнительные органы управления (см.

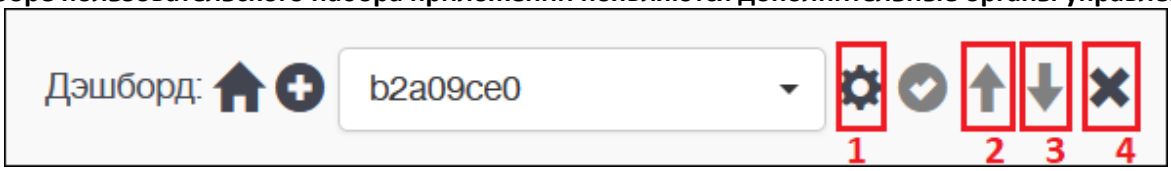

Рисунок 8).

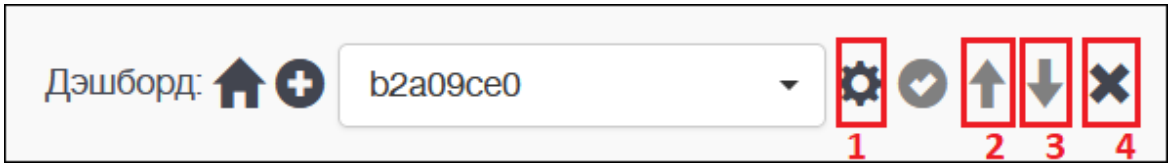

Рисунок 8 – Дополнительные иконки

1. – открыть/закрыть панель настройки выбранного в списке набора приложений. Открытая панель настроек представлена на рисунке 9.
2. – сдвинуть вверх положение выбранного набора в списке.
3. – сдвинуть вниз положение выбранного набора в списке.
4. – удалить выбранный набор. Удалить можно только пользовательский набор.

После добавления нового набора, его можно редактировать нажатием иконки . При нажатии данной иконки открывается окно добавления приложений в набор (см. рисунок 9).

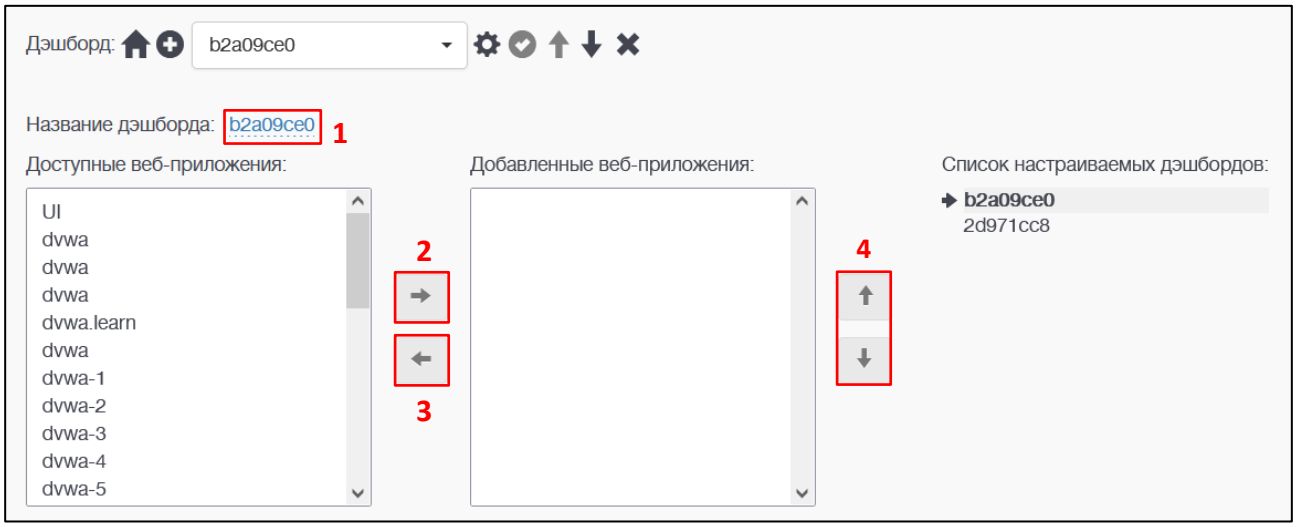

Рисунок 9 – Панель настройки дэшборда

1. Название дэшборда – при нажатии на имя набора приложений, его можно будет изменить. Для того чтобы применить изменения, необходимо нажать на появившуюся при входе в режим редактирования наименования иконку . Чтобы отменить изменения, необходимо нажать на иконку .

2. – переместить выбранные веб-приложения из списка доступных в список добавленных. В последствии, при открытии данного набора будет выводиться статистика приложениям из добавленного списка.
3. – переместить выбранные веб-приложения из списка добавленных в список доступных.
4. – изменить положение приложение в списке добавленных веб-приложений.

Примечание: одно и то же защищаемое веб-приложение может одновременно присутствовать в нескольких наборах (дэшбордах).

После создания нового набора с активным веб-приложением или выбора уже имеющегося набора появятся графики со статистиками приложений (см. рисунок 10).

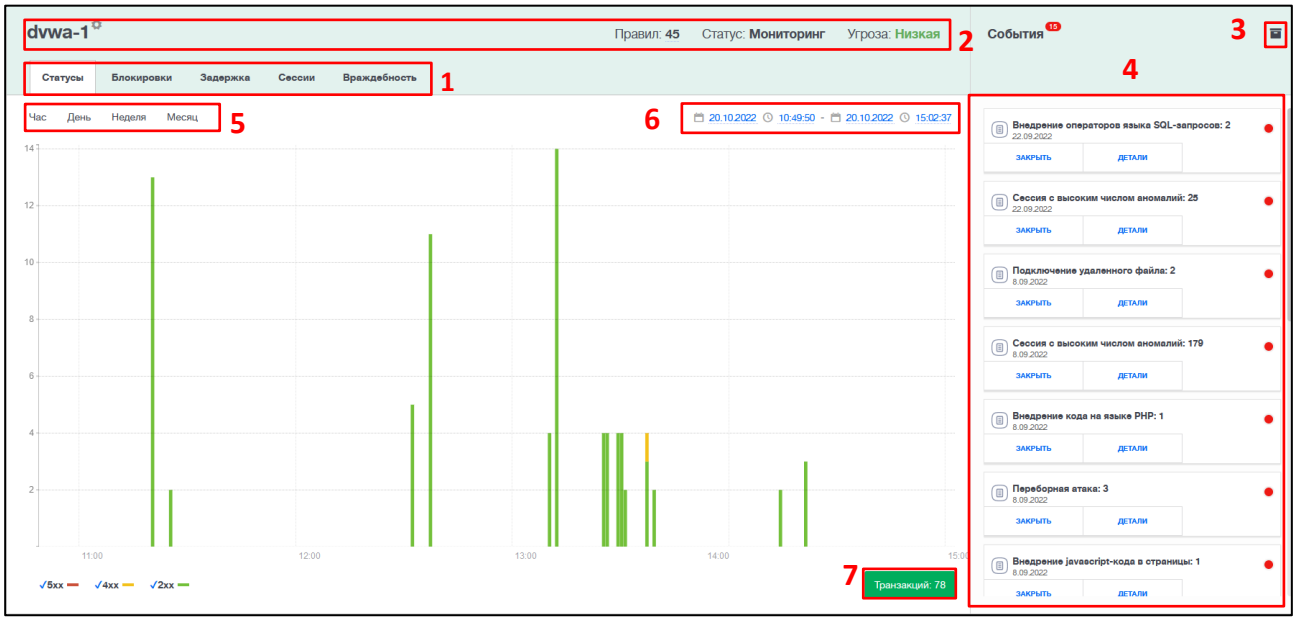

Рисунок 10 – График со статистикой приложения

1. Здесь представлены виды аналитических графиков, которые строит iBatyr WAF на основе анализа проходящего через него трафика. На графиках с несколькими типами значений (например, статусы, см. рисунок 10) можно подсвечивать нужный тип, кликая мышкой на нужный параметр в легенде графика. При наведении курсора на конкретный столбец диаграммы или точку графика – появляется всплывающее окно с параметрами графика в конкретной точке.

   – Статусы – на графиках этой вкладки отображается количество транзакций (вертикальная ось) за единицу времени (горизонтальная ось) в разбивке по кодам HTTP-ответов. Выделены следующие группы HTTP-транзакций:

   - 2xx – транзакции с кодами ответов 1xx, 2xx, 3xx. Отображаются зеленым цветом.
   - 4xx – транзакции с кодами ответа 4xx: ошибки клиента (например, 404 – запрос несуществующей страницы или 403 – запрос, требующий авторизации). Также в эту категорию попадают запросы без ответа, например, заблокированные запросы. Отображаются желтым цветом.
   - 5xx – транзакции с кодами ответа 5xx: ошибки сервера. Наличие таких ошибок свидетельствует о некорректной работе веб-сервера, им необходимо уделять особое внимание. Отображаются красным цветом.

- Блокировки – Отображают решения, принятые системой относительно транзакций. По вертикальной оси отображается количество транзакций, по горизонтальной оси – время регистрации транзакции. Транзакции разделены на группы:
  - Пропущено – транзакция пропущена.
  - Заблокировано – заблокирован запрос.
  - Модифицировано – заблокирован ответ.
- Задержка – Отображает среднюю задержку при обработке транзакции на iBatyr WAF, а также среднюю задержку обработки запроса защищаемым приложением от времени .
- Сессии – график зависимости количества активных сессий от времени.
- Враждебность – график зависимости отношения количества заблокированных транзакций к общему числу транзакций от времени.

Примечание: на графиках не отображаются данные о транзакциях, попавших под фильтр запросов к статическим ресурсам. Подробнее о статических ресурсах и настройку их фильтрации написано в разделе 8.

2. Информация о приложении – содержит название приложения, данные о количестве правил, распространяющихся на это приложение, режим блокировок, а также уровень угрозы. По мимо этого в строке отображается:
   - Режим блокировок (Статус) может принимать значения «Мониторинг» - если активная защита на данном приложении выключена, и «Защита» - если активная защита включена.
   - Уровень угрозы может принимать значения высокий, средний и низкий, в зависимости от отношения количества заблокированных транзакций к общему количеству транзакций.
3. Актуальные события – при нажатии на данную иконку откроется окно «События» с актуальными событиями по данному веб-приложению.
4. События – содержит информацию по последним событиям: наименование сработавшего правила, время обновления события и индикатор уровня угрозы (высокий – красный, средний – желтый, низкий – зеленый). Число, указанное в красном овале над надписью «События», соответствует количеству не просмотренных событий. Пиктограмма с изображением архивной коробки позволяет перейти в представления «События» в раздел «Архив». В каждом событии доступна кнопка «Детали», для просмотра подробной информации по каждому событию. Для пользователей с правами «Администратор» и «Аналитик» доступна также кнопка «Закрыть», позволяющая отправить событие в архив, т.е. пометить как отработанное.
5. Иконки периода – для быстрого изменения периода можно воспользоваться кнопками «Час», «День», «Неделя» или «Месяц», что позволит вывести выбранный в пункте 1 график за указанный период.
6. Период - более тонкая настройка периода отображения.
7. Транзакции – содержит данные о количестве транзакций, и перенаправляет в представление «Приложения».

Примечание: период на графике так же можно выбрать, выделив нужный промежуток мышкой. Для этого необходимо нажать левую кнопку мыши в начале интересующего периода, провести курсор до конца периода и отпустить левую кнопку мыши.

3.2. Окно «События»

Окно «События» (см. рисунок 11) позволяет просматривать события безопасности по всем защищаемым веб-приложениям, или по каждому в отдельности, фильтровать их по уровню критичности и периоду их действия.

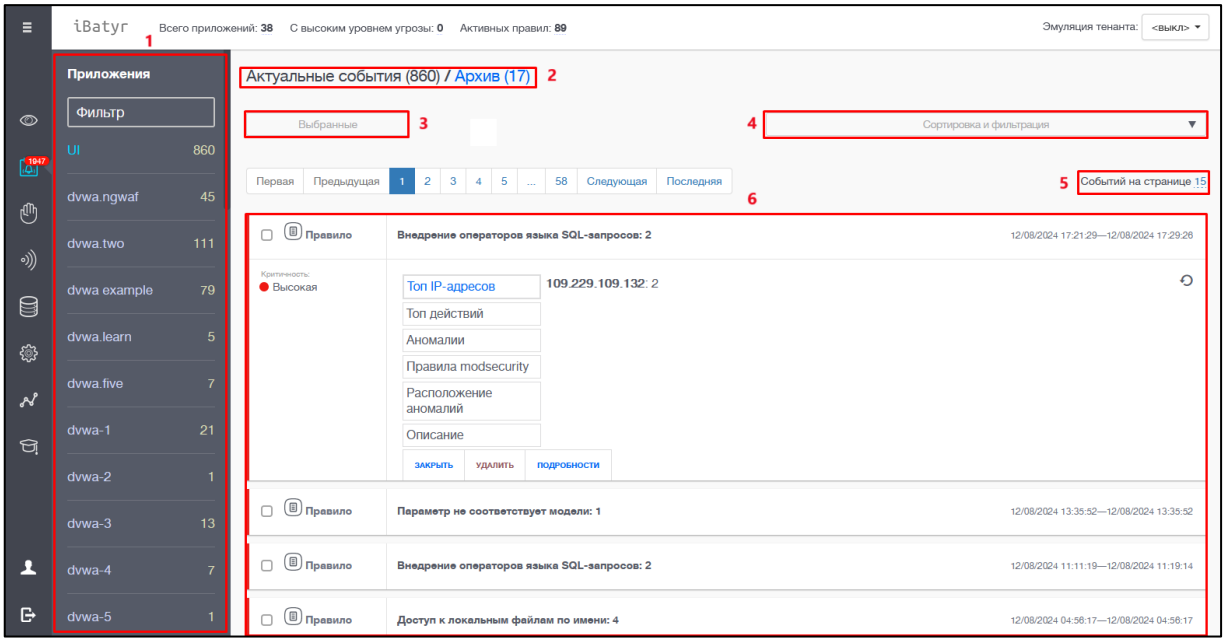

Рисунок 11 – Окно «События»

1. Список приложений – здесь находится список всех доступных пользователю приложений. Справа от названия приложения располагается количество актуальных для него событий.
2. Актуальные события / Архив – переключение между двумя интерпретациями окна «События».
   2.1. Актуальные события – события безопасности, которые еще не были закрыты или просмотрены пользователями.
   2.2. Архив – события безопасности, которые были закрыты или просмотрены пользователями, и система переместила их в архив.
3. Групповые действия – если навести курсор, на выделенное в пункте 3 поле, откроется список групповых действий (см. рисунок 12).

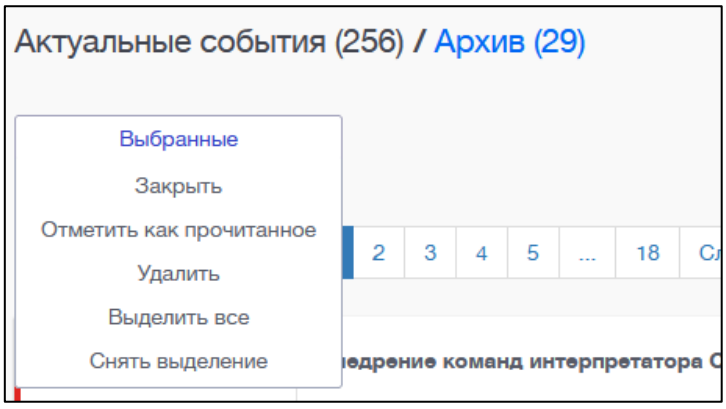

Рисунок 12 – Групповые действия

Администратору и Аналитику доступны следующие действия:

- Закрыть – позволяет перенести приложение в архив;
- Отметить, как прочитанное – переносит событие в конец списка;
- Удалить – удалить событие (удаленное событие не перемещается в архив);
- Выделить всё – отметить все события в активных событиях;
- Снять выделение – снять все отметки.

На iBatyr WAF имеется возможность выделять события, щелкнув на квадратик справа от названия правила (см. рисунок 13).

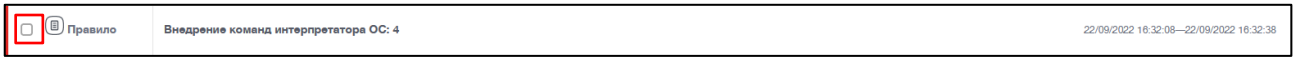

Рисунок 13 – Выделение события

4. Сортировка и фильтрация – при нажатии, на выделенное в четвертом пункте поле, откроется скрытое меню (см. рисунок 14) с настройками направления сортировки и параметрами фильтрации.

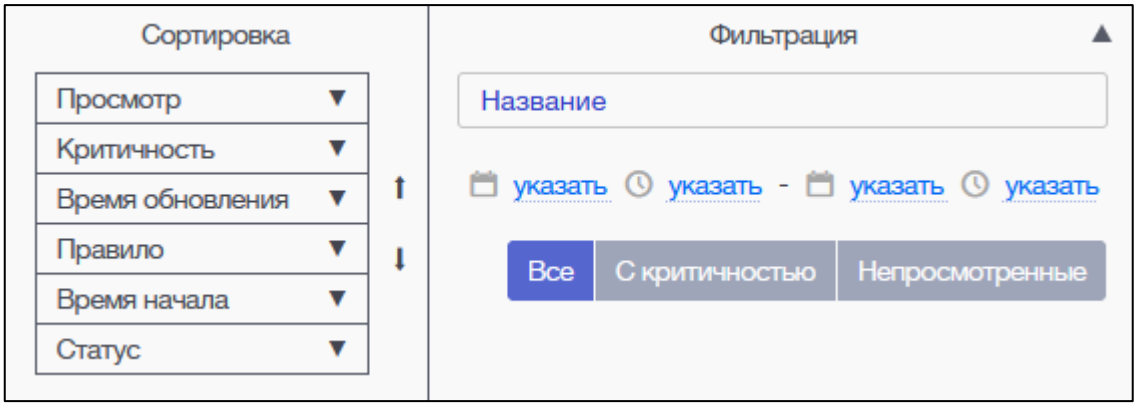

Рисунок 14 – Меню «Сортировка и фильтрация»

Для изменения направления сортировки по определенному параметру необходимо нажать на пиктограмму с изображением треугольной стрелки, находящейся в одной строке с параметром « ▼/▲ ».

Для изменения приоритета параметров при сортировке необходимо выбрать нужный параметр и переместить его с помощью стрелок справа от параметров « ⬇/⬆ ».

Для фильтрации событий необходимо в правой части меню «Сортировка и фильтрация» выбрать критерии фильтрации: ввести название правила или ключевые слова для поиска и/или указать дату и время происхождения событий, и/или выбрать один из параметров «Все»/ «С критичностью»/ «Непросмотренные».

Свернуть меню «Сортировка и фильтрация» можно нажатием на черный треугольник в правом верхнем углу меню.

5. События на странице – количество отображаемых событий на странице можно изменить, щелкнув по числу в строке «Событий на странице:». В появившемся окне (см. рисунок 15) ввести нужное число событий на страницу. Чтобы изменения применились, необходимо нажать на появившуюся при входе в режим редактирования наименования иконку ☑ (применить изменения). Чтобы отменить изменения, необходимо нажать на иконку ✖ (отменить изменения).

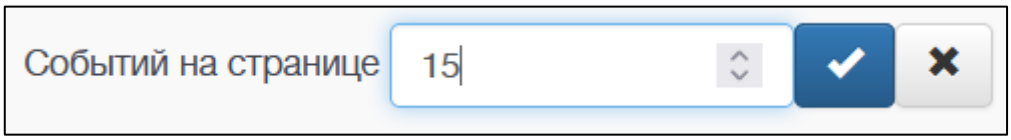

Рисунок 15 – Количество событий на странице

6. События безопасности - события представлены отсортированным списком, каждое событие слева имеет индикатор критичности события (см. рисунок 16):
   - красный для события с высокой критичностью;
   - жёлтый для события со средней критичностью;
   - зелёный для события с низкой критичностью;
   - серый, если критичность для события не задана.

Рисунок 16 – Список событий

Каждая строка события содержит поле для отметки, название сработавшего правила, количество транзакций, период, за который произошли события. При нажатии на строку события открывается общая информация по событию (см. рисунок 17).

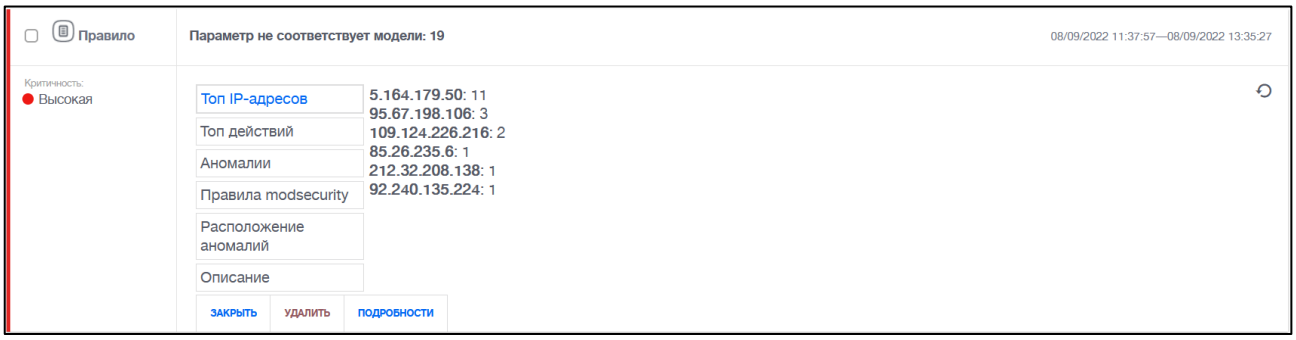

Рисунок 17 – Общая информация по событию

На iBatyr WAF имеется возможность предварительного просмотра информации по событию. Для этого необходимо кликнуть по соответствующей строке просмотра информации. На выбор есть следующие варианты.

- Топ IP-адресов – показывает топ 10 IP адресов с количеством транзакций в данном событии в порядке убывания.
- Топ действий – показывает топ 10 действий с количеством транзакций в данном событии в порядке убывания (если для транзакций в данном событии не было сопоставлено ни одно действие, будет показано сообщение «Не найдено»).
- Аномалии – показывает топ 10 аномалий, которые были обнаружены в транзакциях из данного события.

- Правила Modsecurity – показывает топ 10 идентификаторов сигнатур Modsecurity, которые были обнаружены в транзакциях данного события (описание поиска сигнатур Modsecurity по идентификатору описано в разделе 22).
- Расположение аномалий – показывает топ 10 расположений аномалий в транзакциях, в которых обнаружены аномалия.
- Описание – выводит описание правила, из сработок которого было создано данное событие (создание описания указано в разделе 21).

Так же возможны три действия с выбранным событием:

- Закрыть – переносит выбранное событие в архив. Данная иконка доступна в интерфейсах пользователя с ролью Администратора, Аналитика или «Только для чтения».
- Удалить – доступна только роли Администратора. При нажатии на кнопку «Удалить» появится окно с запросом подтверждения удаления, после чего событие будет удалено без возможности восстановления.
- Подробности – просмотр подробной информации. Данная иконка доступна в интерфейсах пользователя с ролью Администратора, Аналитика или «Только для чтения».

Для просмотра подробной информации о событии необходимо кликнуть на него, и в появившемся поле нажать иконку «Подробности», описанную выше. В результате откроется окно с полной информацией по событию (см. рисунок 18).

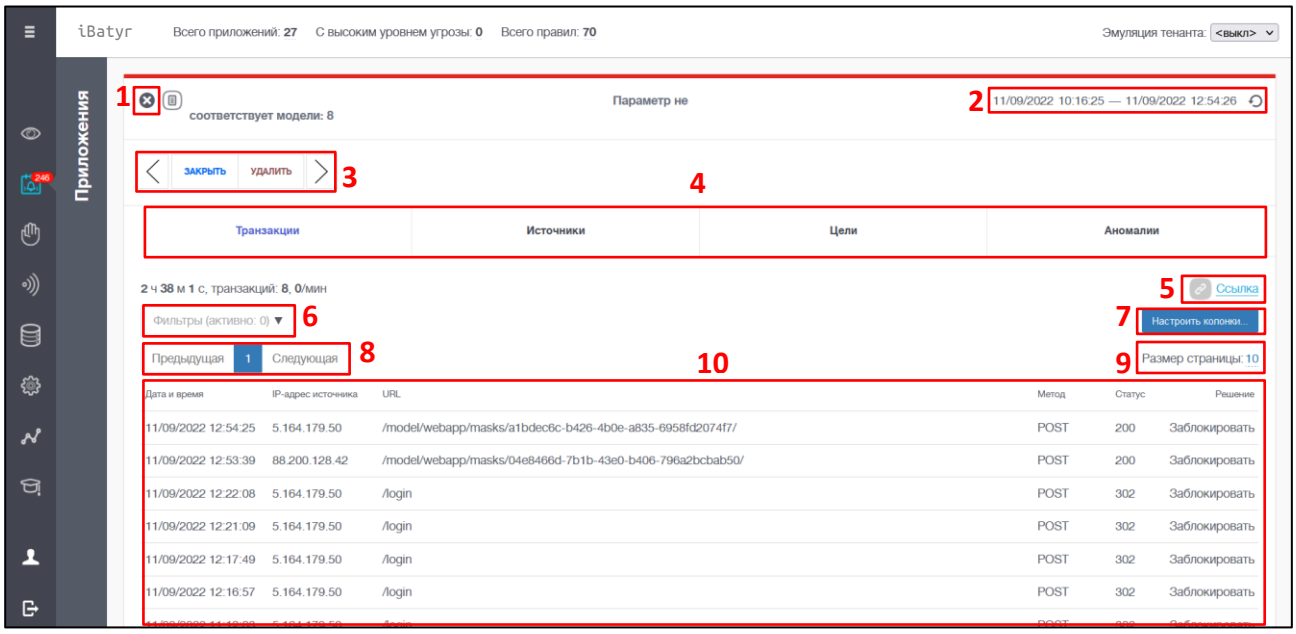

Рисунок 18 – Общая информация по событию

1. Выйти из события – выход из окна «Подробности» в окно «События». Просмотренное событие помещается в конец списка актуальных событий и отмечается как прочитанное. На рисунке 19 представлено непрочитанное правило сверху и прочитанное снизу.

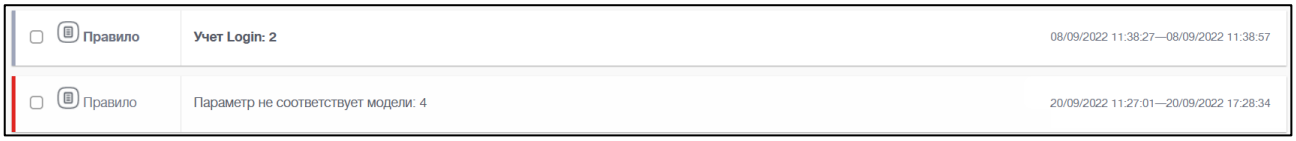

Рисунок 19 – Общая информация по событию

2. Период события – в данном поле указан период, за который собирались транзакции для данного события. Справа от периода имеется иконка (Обновить), которая позволяет отобразить последние изменения данных в данном событии.
3. Иконки управления просмотром событий – имеются четыре управляющие иконки:

- Предыдущее событие «<» – открывает предыдущее событие безопасности.
- Закрыть – переносит выбранное событие в архив. Данная иконка доступна в интерфейсах пользователя с ролью Администратора, Аналитика или «Только для чтения».
- Удалить – доступна только в интерфейсе Администратора. При нажатии на кнопку «Удалить» появится окно с запросом подтверждения удаления, после чего событие будет удалено без возможности восстановления.
- Следующее событие «>» – открывает следующее событие безопасности.

4. Аналитика – для анализа транзакций, попавших в событие, помимо журнала транзакций, который открывается по умолчанию, имеются следующие вкладки.

- Источники – на данной вкладке находятся статистики, относящиеся к IP адресам и пользователям (см. рисунок 20).

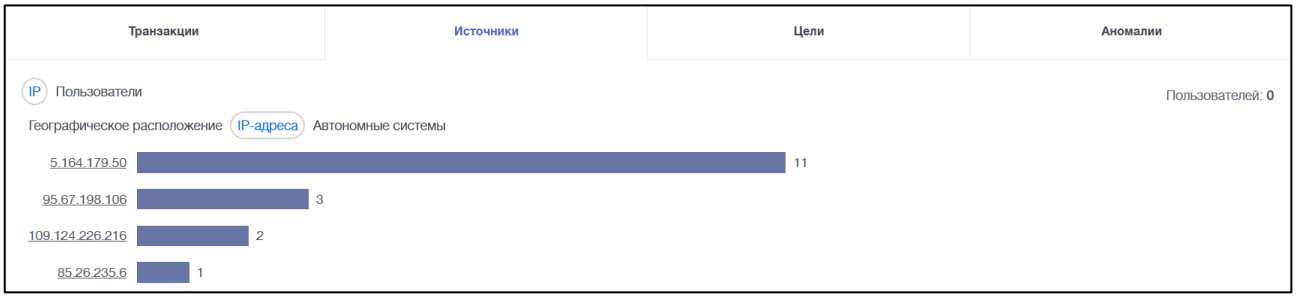

Рисунок 20 – Вкладка «Источники»

На данной вкладке есть возможность просмотреть:

- Географическое расположение – топ стран, которым принадлежат IP-адреса источников транзакций;
- IP-адреса – топ адресов, транзакции которых попали под данное событие;
- Автономные системы – топ автономных систем, которым принадлежат IP адреса;
- Пользователи - топ пользователей, транзакции которых попали под данное событие (для извлечения идентификаторов пользователей из HTTP-транзакций необходимо настроить сессионный идентификатор «извлечение имени пользователя». Описание его настройки находится в разделе 18.1).
- Цели – на данной вкладке расположена статистика по топу действий позитивной модели Бизнес-логики (см. рисунок 21).

Рисунок 21 – Вкладка «Цели»

Примечание: некоторые значения в этих статистиках подчеркнуты, например, IP-адреса (см. рисунок 20) или действия (см. рисунок 21). Если нажать на какое-нибудь значение, то откроется журнал транзакций, отфильтрованный по выбранному значению.

- Аномалии – на данной вкладке расположены топ аномалий, под которые попали транзакции из данного события (так как транзакция, попавшая под событие, может иметь несколько аномалий от различных модулей, здесь можно встретить не только аномалии от модуля, характерного для события (см. рисунок 22).

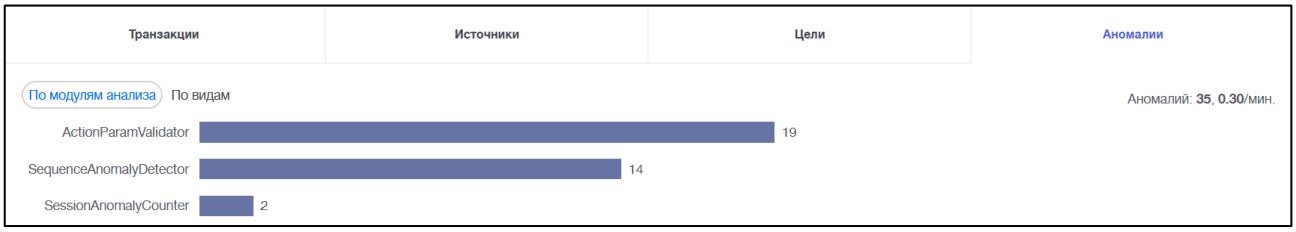

Рисунок 22 – Вкладка «Аномалии»

На данной вкладке есть возможность просмотреть:

  – Статистику по аномалиям от различных модулей анализатора, под которые попали транзакции из данного события. Описание модулей можно найти в разделе 17;
  – Статистику по видам аномалий, под которые попали транзакции из данного события.

5. Ссылка – при нажатии на данную иконку в буфер обмена копируется ссылка на выбранное событие.
6. Фильтры – при нажатии на иконку «Фильтры» появляется возможность выбрать один или несколько фильтров из выпадающего списка (рисунок 23).

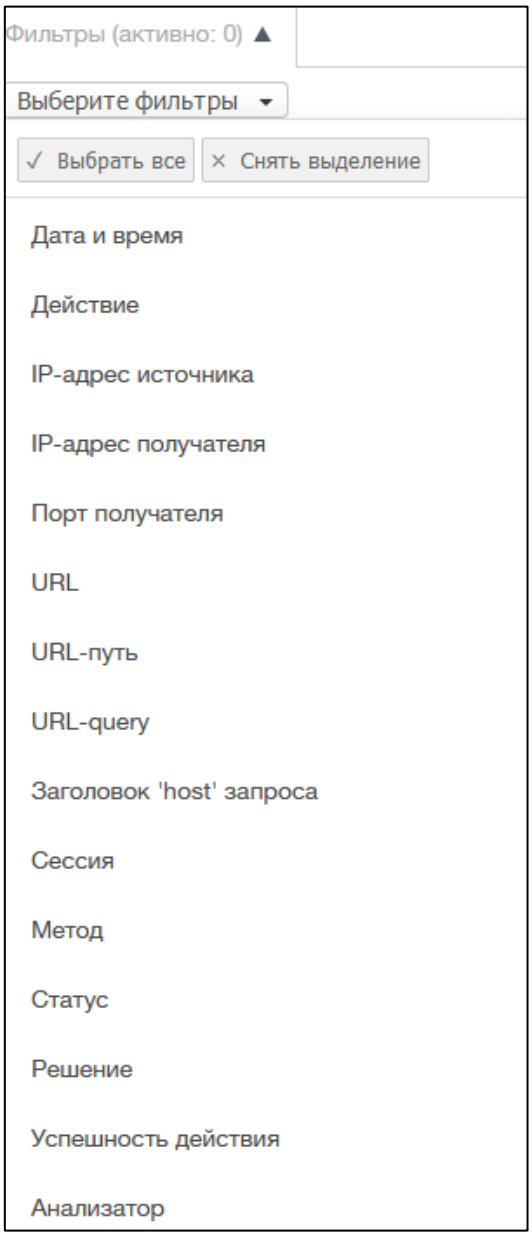

Рисунок 23 – Список фильтров

Описание фильтров и окон их настройки в таблице 1.

Таблица 1 – Описание фильтров

Фильтр	Описание
Дата и время	Выбор, для фильтрации, периода, за который необходимо вывести транзакции, попавшие в событие
Действие	Выбор, для фильтрации, одного, или нескольких действия\действий, под которое\которые попали транзакции из выбранного события. Действие выбирается из выпадающего списка с функцией поиска. Создание действий описано в разделе 15
Правило реагирования	Выбор для фильтрации правила реагирования, под которое попали транзакции из выбранного события. Правило выбирается из выпадающего меню с функцией поиска

Фильтр	Описание
IP-адрес источника	Вывод транзакций выбранного события, в которых параметр «src_ip» совпал с введенным вручную IP-адресом источника (клиента). После ввода одного IP-адреса можно нажать на иконку «➕», чтобы появилось дополнительное поле для ввода IP-адреса. При нажатии на иконку «➖» будет удалена строка, напротив которой находится данная иконка
IP-адрес получателя	Вывод транзакций выбранного события, в которых параметр «dst_ip» совпал с введенным вручную IP-адресом получателя (сервера). После ввода одного IP-адреса можно нажать на иконку «➕», чтобы появилось дополнительное поле для ввода IP-адреса. При нажатии на иконку «➖» будет удалена строка, напротив которой находится данная иконка
Порт получателя	Вывод транзакций выбранного события, в которых параметр «dst_port» совпал с введенным вручную портом получателя (сервера). Иконками «^\v» можно увеличивать и уменьшать значение, введенное в поле. После ввода одного порта можно нажать на иконку «➕», чтобы появилось дополнительное поле для ввода IP-адреса. При нажатии на иконку «➖» будет удалена строка, напротив которой находится данная иконка
URL	Вывод транзакций выбранного события, в которых параметр «URL» (заголовок «URL» содержит в себе все значения заголовков «PATH» и «QUERY») содержит введенное вручную значение поля данного фильтра
URL-путь	Вывод транзакций выбранного события, в которых параметр «PATH» содержит введенное вручную значение поля данного фильтра
URL-query	Вывод транзакций выбранного события, в которых параметр «QUERY» содержит введенное вручную значение поля данного фильтра
Заголовок 'host' запроса	Вывод транзакций выбранного события, в которых параметр «HOST» совпадает с введенным вручную значение поля данного фильтра
Сессия	Вывод транзакций выбранного события, в которых идентификатор сессии совпадает с введенным вручную значением поля фильтра. Данный фильтр будет работать только если настроена сессионная модель. Инструкция по настройке сессионной модели находится в разделе 18
Метод	Выбор для фильтрации одного или нескольких методов, под который\которые попали транзакции из выбранного события. Метод выбирается из выпадающего списка
Статус	Выбор для фильтрации одного или нескольких вариантов статуса, который\которые пришли в ответ на транзакции из выбранного события
Решение	Выбор для фильтрации одного или несколько из предложенных вариантов решений по транзакциям из списка
Успешность действия	Выбор для фильтрации одного или нескольких из предложенных вариантов успешности действия по транзакциям из списка. Описание и настройка успешности действий описана в разделе 15
Анализатор	Выбор для фильтрации анализатора, который выдавал решение по транзакции из выбранного события

7. Настроить колонки – при нажатии на данную иконку откроется окно с настройкой отображения полей таблицы транзакций. Данное окно представлено на рисунке 24.

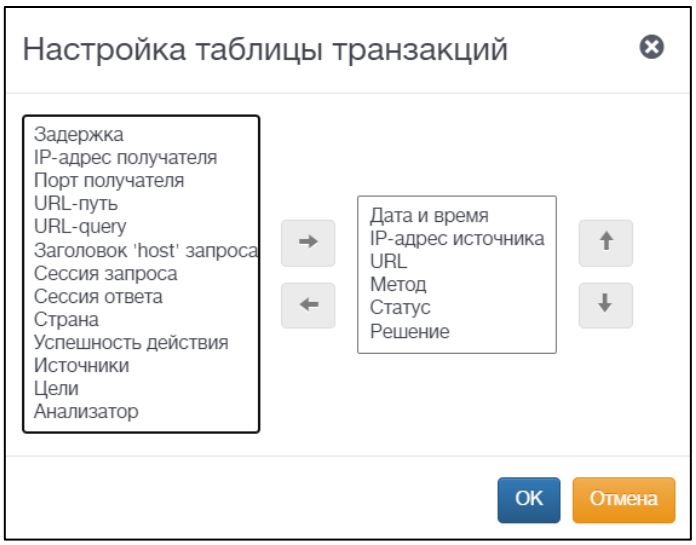

Рисунок 24 – Окно с настройкой отображения полей таблицы транзакций

В списке справа отображаются список возможных параметров для отображения, а слева расположен список уже отображаемых параметров. Чтобы переместить в параметр из списка возможных в список отображаемые, его необходимо выделить и нажать на иконку «→». Чтобы убрать параметр из списка отображаемых, необходимо выделить параметр и нажать на иконку «←». Для того, чтобы изменить очередность необходимо выделить параметр и воспользоваться иконками «↓» и «↑».

Описание возможных параметров представлено в таблица 2.

Таблица 2 – Описание параметров

Параметр	Описание
Задержка	Отображает временное значение задержки ответа от WAF
IP-адрес источника	Отображает значение параметра src_ip (IP-адрес клиента)
IP-адрес получателя	Отображает значение параметра dst_ip (IP-адрес сервера)
Порт получателя	Отображает значение параметра dst_port (порт сервера)
URL	Отображает значение параметра URL
URL-путь	Ображает значение параметра PATH
URL-query	Отображает значение параметра QUERY
Заголовок 'host' запроса	Отображает значение параметра HOST
Сессия запроса	Отображает 128 символьный идентификатор сессии запроса (необходима настроенная сессионная модель)
Сессия ответа	Отображает 128 символьный идентификатор сессии ответа (необходима настроенная сессионная модель)
Страна	Отображает иконку флага страны, которой по базам принадлежит IP-адрес клиента
Успешность действия	Отображает значение успешности действия, под которое попала данная транзакция (необходима настройка успешности действия)

Параметр	Описание
Источники	Отображает все источники, под которые попала данная транзакция (описание источников в разделе 13)
Цели	Отображает все цели, под которые попала данная транзакция (описание целей в разделе 14)
Анализатор	Отображает анализатор, который отвечал за анализ данной транзакции
Дата и время	Отображает дату и время, в которое данная транзакция пришла на WAF
Метод	Отображает метод, с которым была отправлена данная транзакция
Статус	Отображает статус ответа сервера на данную транзакцию
Решение	Выводит решение, выданное анализатором на данную транзакцию

8. Страницы и перемещение по ним – отображает количество страниц с учетом заданного количества транзакций на странице (задается в пункте 9). Перемещаться между страницами можно с помощью иконок «Предыдущая \ Следующая», или выбрав номер страницы.
9. Размер страницы – количество отображаемых транзакций на странице можно изменить, щелкнув по числу в строке «Размер страницы:». В появившемся окне (см. рисунок 25) ввести нужное число транзакций на странице. Иконками «\» можно увеличивать и уменьшать, с шагом 5, значение, введенное в поле. Чтобы изменения применились, необходимо нажать на появившуюся при входе в режим редактирования наименования иконку «применить изменения» ✔. Чтобы отменить изменения, необходимо нажать на иконку «отменить изменения» ✖.

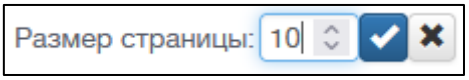

Рисунок 25 – Размер страницы

10. Транзакции – в выделенном окне представлены транзакции, попавшие в данное событие. Каждую из транзакций можно просмотреть, кликнув на нее дважды левой кнопкой мыши (подробнее о просмотре транзакций можно прочитать в разделе 7).

3.3. Окно «Правила»

Окно «Правила» (см. рисунок 26) позволяет просматривать, создавать, редактировать, включать и выключать правила по всем защищаемым веб-приложениям или по каждому в отдельности, фильтровать их по категориям (тегам) и по выводимому ими решению (заблокировать, пропустить, пометить).

2 1

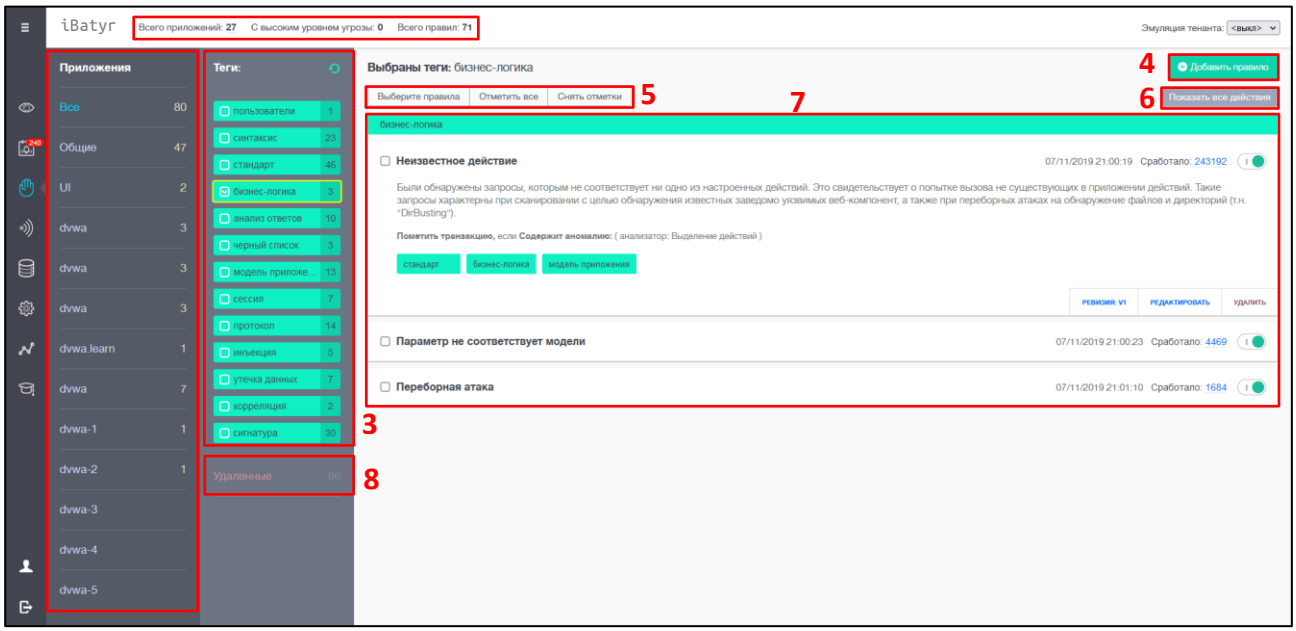

Рисунок 26 – Окно «Правила»

1. В выделенной области находится информация по количеству приложений на инсталляции, информация по количеству приложений с высоким угрозы и информация по общему количеству правил на инсталляции.
2. Список приложений – содержит список всех доступных пользователю приложений. Справа от названия приложения располагается количество созданных для него правил. При нажатии на приложение выводятся правила, созданные для данного приложения.
3. Теги – блок содержит список ключевых слов (тегов), используемых в правилах. Справа от тега указано количество правил, в которых он установлен. При выборе тега выводятся все правила, в которых он установлен. Для того чтобы выбрать тег, достаточно нажать на строку с названием тега; чтобы сбросить выделение тега, на него необходимо нажать повторно или нажать для сброса всех тегов.
4. Добавить правило – при нажатии на данную кнопку открывается окно создания правила, как показано на рисунке 27 (механизм создания правила описан в разделе 21).

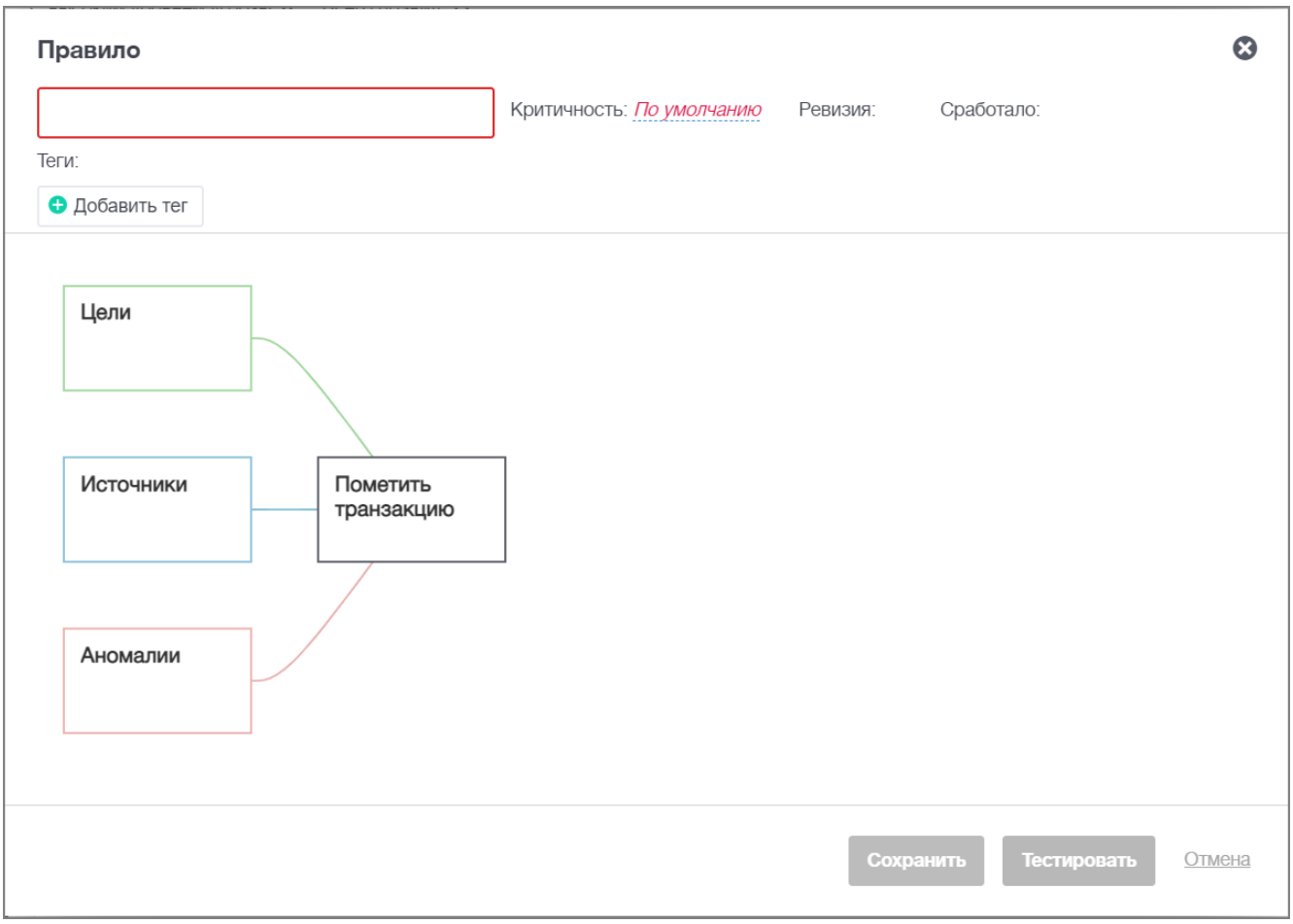

Рисунок 27 – Окно создания правила

5. Массовые действия – блок позволяет выполнять операции над множеством правил. Для того чтобы отметить все правила, необходимо нажать на кнопку «Отметить всё». Для того чтобы снять все выделения, необходимо нажать на кнопку Снять отметки. Также имеется возможность точечно отмечать, или снимать выделения, данный механизм описан в пункте 7. При наведении курсора мыши на кнопку Выберите правила открывается всплывающее меню массовых действий (см. рисунок 28).

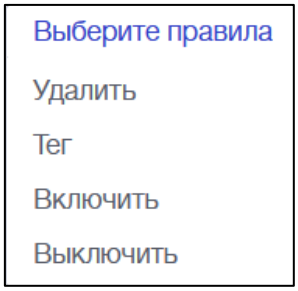

Рисунок 28 – Всплывающее меню массовых действий

В данном окне есть возможность выбрать следующие действия:

- удалить – удаляет все выделенные правила;
- тег – добавить тег ко всем выделенным правилам;
- включить – включить все выделенные правила;
- выключить – выключить все выделенные правила.

6. Фильтр по действиям с транзакциями в правилах – с помощью данного фильтра можно вывести правила по действиям с попавшими под них транзакциями (блокировать, пометить, пропустить). По умолчанию выводятся все действия, но при наведении на фильтр появляется всплывающие окно с выбором действий (см. рисунок 29).

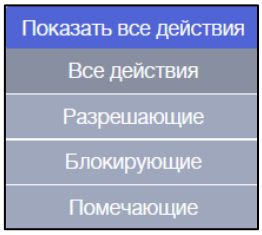

Рисунок 29 – Фильтр по действиям с транзакциями в правилах

7. Область с правилами – в выделенной области находятся правила, попавшие под заданные фильтры (по умолчанию выводятся все правила). Слева от названия правила имеется поле для выделения правила (где выделенное правило:) для последующих массовых действий. В правом верхнем углу блока правила есть переключатель, позволяющий включать и выключать правило (правило включено , правило выключено). При нажатии на правило левой кнопкой мыши открывается общая информация о правиле (см. рисунок 30): краткое описание правила, теги правила, дата создания, количество срабатываний, данные о ревизии (т.е. о версионности правила). Администратору и Аналитику также доступно включение/выключение, редактирование, удаление правила, а также перемещение правила в списке. Оператору доступна только общая информация о правиле.

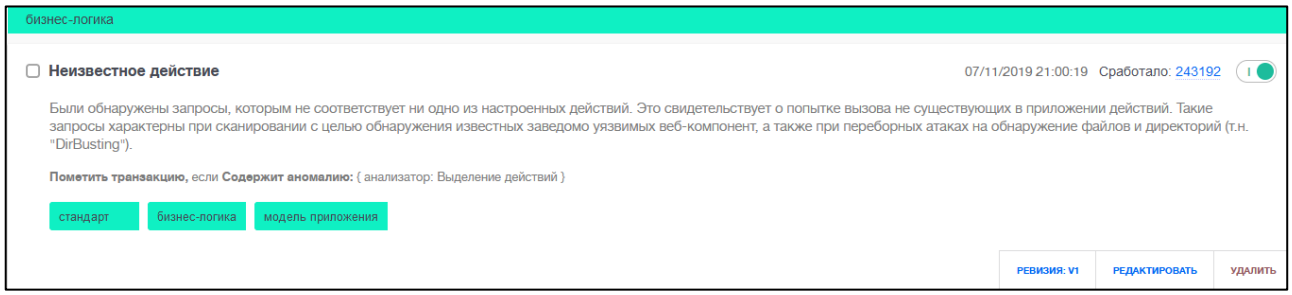

Рисунок 30 – Общая информация о правиле

После нажатия кнопки «Удалить» правило перемещается в раздел «Удалённые». После нажатия «Редактировать» откроется окно «Правило» (см. рисунок 31). Подробное описание создания и редактирования правил находится в разделе 21.

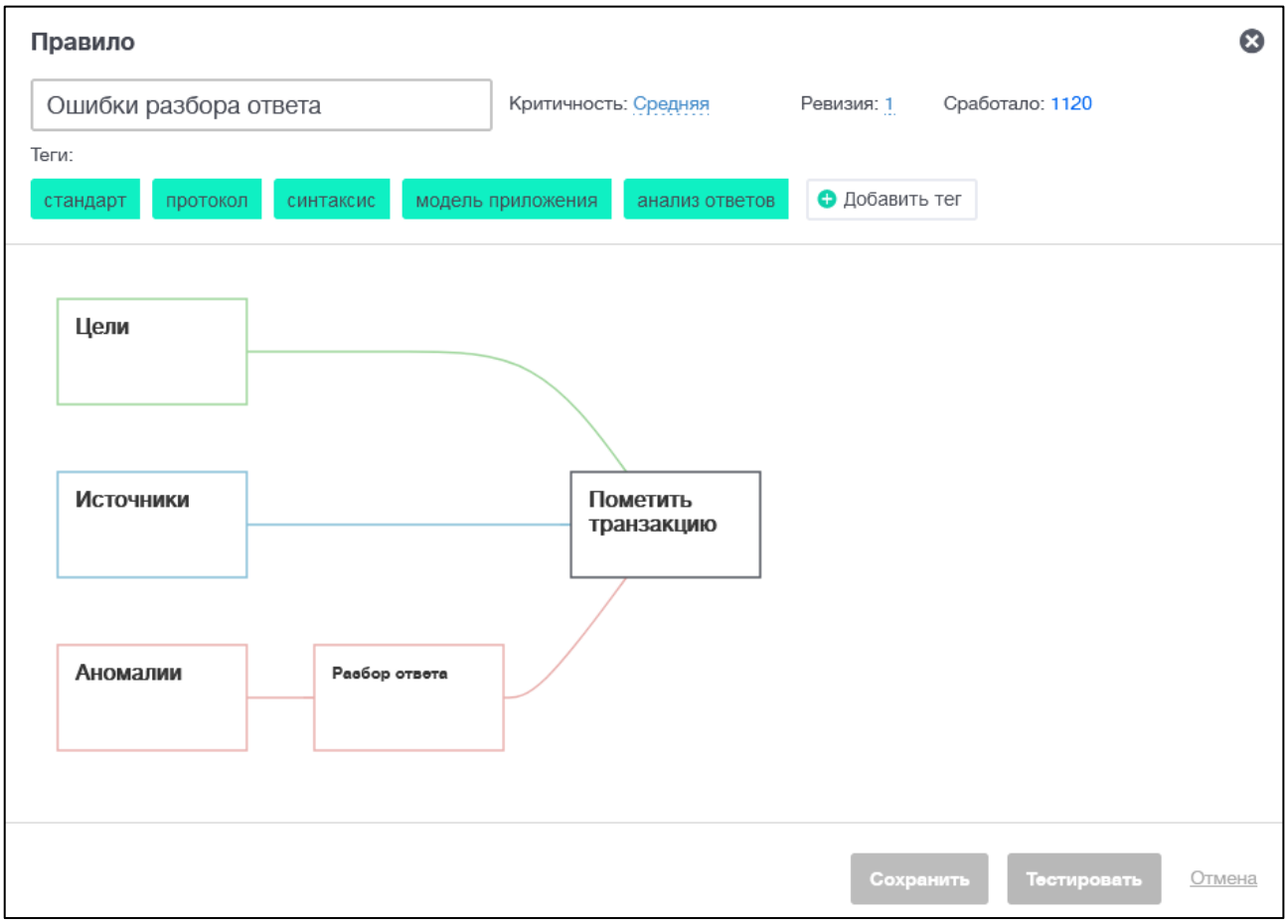

Рисунок 31 – Редактирование правила

Правила расположены в порядке убывания приоритета, т.е. трафик, попадающий под действие двух правил, будет обработан в соответствии с правилом, расположенным выше в списке. Для перемещения правила необходимо навести курсор на левый угол блока правила, затем щелкнуть по появившимся трём вертикальным точкам и, удерживая левую клавишу мыши, перемещать правило.

8. Удаленные правила – при нажатии на данную кнопку откроется окно со всеми удаленными правилами (см. рисунок 32).

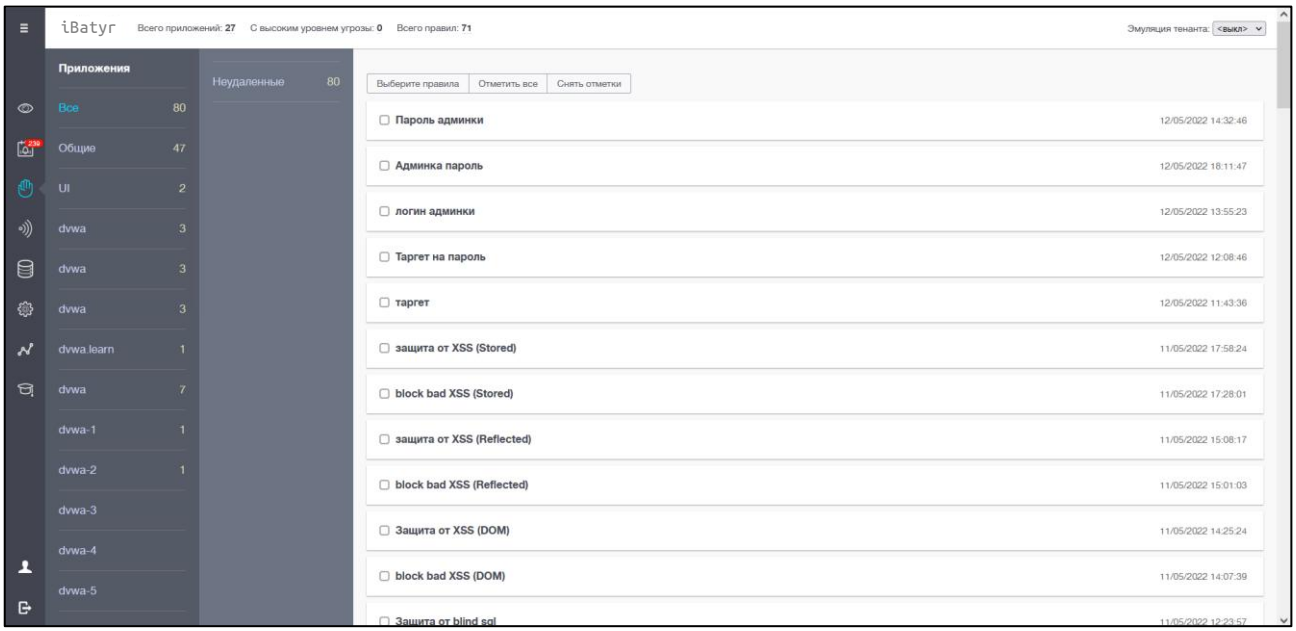

Рисунок 32 – Удаленные правила

Удаленные правила можно восстановить как массово (правила выбираются по аналогии с описанным выше механизмом), так и точечно, кликнув на правило правой кнопкой мыши и нажав кнопку «Восстановить».

Примечание: правила восстанавливаются в выключенном режиме, не забудьте включить правило, если это необходимо.

3.4. Окно «Источники, списки, цели»

Окно «Источники, списки, цели» позволяет просматривать, создавать, редактировать и удалять источники, списки и цели по всем защищаемым веб-приложениям, или по каждому в отдельности. Данное окно состоит из трех вкладок:

- Источники;
- Списки;
- Цели.

Первая вкладка, которая открывается при нажатии на строку меню «Источники, списки, цели» - вкладка с созданием и редактированием источников (см. рисунок 33).

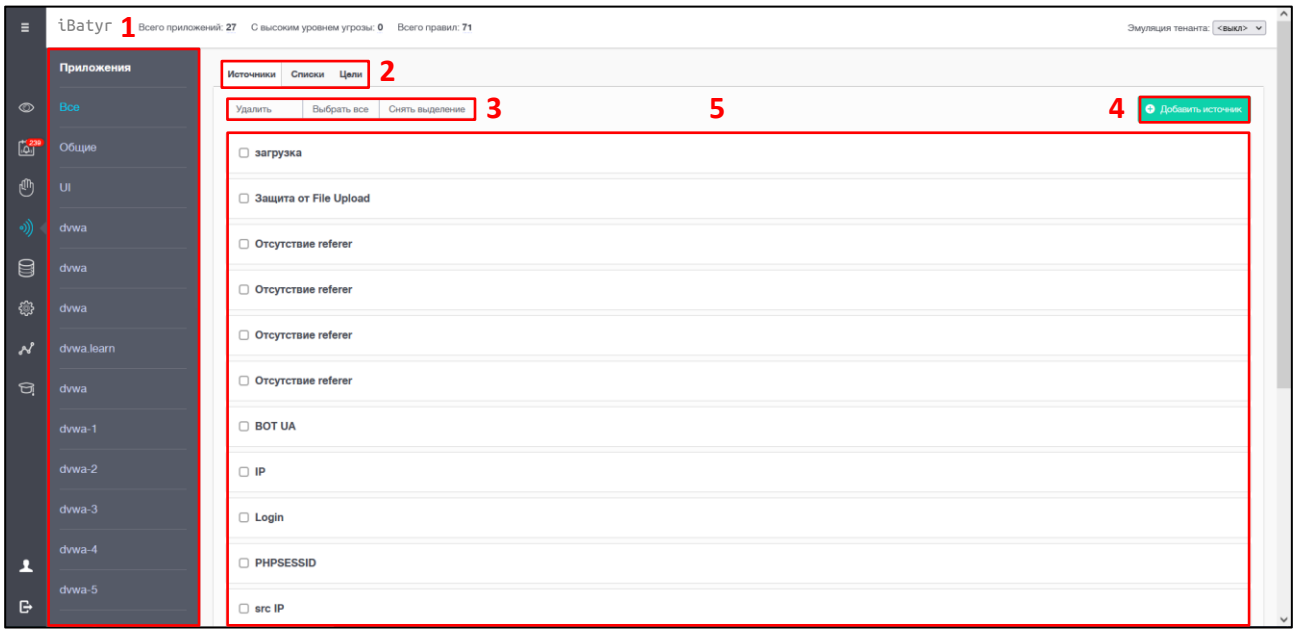

Рисунок 33 – Окно «Источники, списки, цели»

1. Список приложений – в данном блоке представлен список всех доступных пользователю приложений. При нажатии на приложение выводятся источники, работающие только для выбранного приложения.
2. Источники, списки, цели – блок вкладок позволяет перемещаться между вкладками.
3. Массовые действия – в отмеченной области находятся массовые действия с источниками. Для того чтобы отметить все источники, необходимо нажать на кнопку Выбрать все. Для того чтобы снять все отметки, необходимо нажать на кнопку Снять выделение. Также имеется возможность точечно отмечать или снимать выделения, данный механизм описан в пункте 5. При нажатии на кнопку Удалить будут удалены все выделенные источники.
4. Добавить источник – при нажатии на данную кнопку открывается окно создания источника (см. рисунок 34). Подробнее механизм создания источника описан в разделе 13.

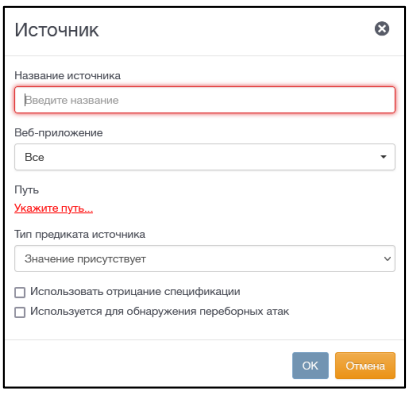

Рисунок 34 – Окно создание источника

При переходе в меню настроек предиката появляется выбор значений предиката (см. рисунок 35) Возможные значения с описанием дополнительных параметров представлены в таблице 13.

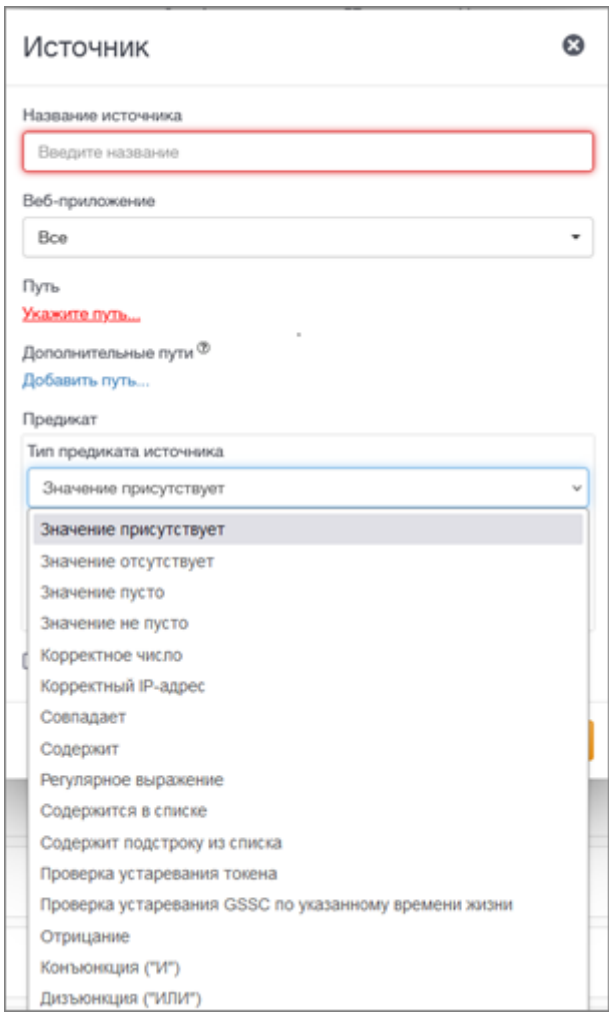

Рисунок 35 – Выпадающий список выбора предиката источника

5. Область с источниками – в выделенной области находятся источники. Слева от названия источника имеется поле для выделения источника (где выделенный источник выглядит как:). При нажатии на источник левой кнопкой мыши открывается общая информация о источнике (см. рисунок 36).

Рисунок 36 – Общая информация о источнике

В открывшимся окне имеется краткое описание источника и следующие с ним действия (см. рисунок 37):

- Редактировать – открывает окно редактирования источника (подробнее о редактировании\изменении источника написано в разделе 13);
- Удалить – безвозвратно удаляет выбранный источник.

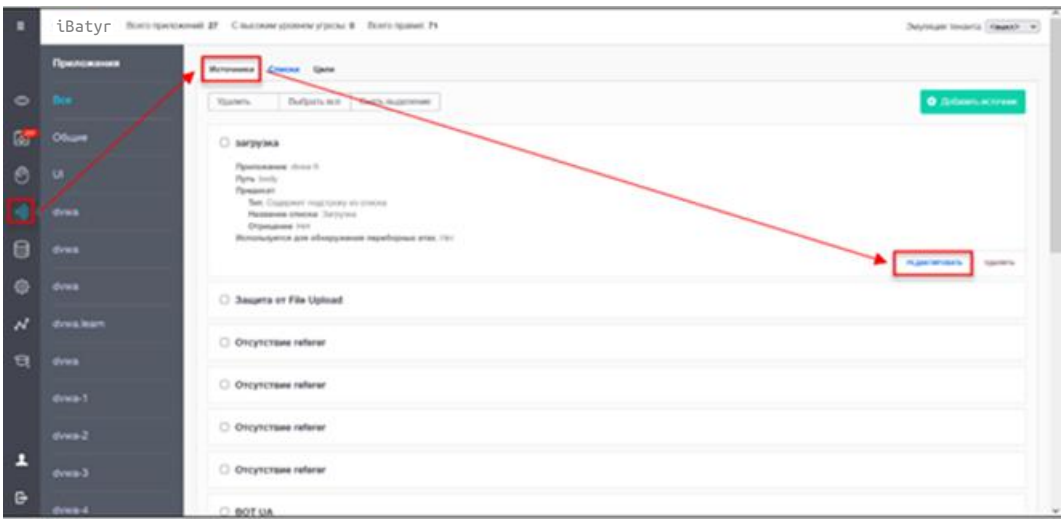

Рисунок 37 – Редактирование источника

Примечание: на iBatyr WAF имеется стандартный источник с названием «src_ip», который обычно используется для создания детекторов переборных атак. Данный источник нельзя удалять.

Вторая вкладка – списки. Данная вкладка позволяет фильтровать, создавать, редактировать и удалять списки (см. рисунок 38).

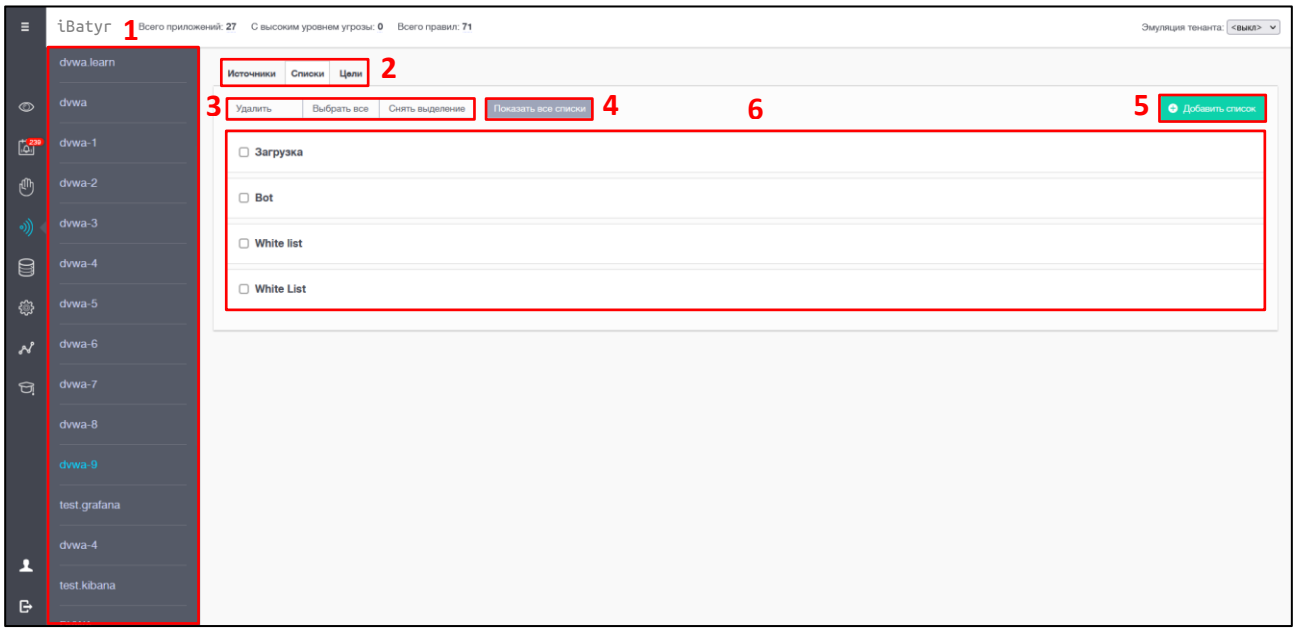

Рисунок 38 – Вкладка «Списки»

1. Список приложений – блок содержит список всех доступных пользователю приложений. При нажатии на приложение выводятся списки, работающие только для выбранного приложения.
2. Источники, списки, цели – блок вкладок позволяет перемещаться между вкладками.
3. Массовые действия – в отмеченной области находятся массовые действия с списками. Для того чтобы отметить все списки, необходимо нажать на кнопку Выбрать все. Для того чтобы снять все отметки, необходимо нажать на кнопку Снять выделение. Также имеется возможность точечно отмечать или снимать выделения, данный механизм описан в пункте 6. При нажатии на кнопку Удалить будут удалены все выделенные списки.

4. Фильтр по назначению списков – с помощью данного фильтра можно вывести списки с определенными назначениями. По умолчанию выводятся все списки, независимо от их назначения, но при наведении на фильтр появляется всплывающие окно с выбором действий (см. рисунок 39).

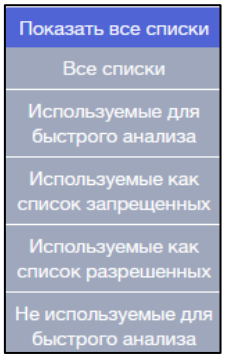

Рисунок 39 – Фильтр по назначению списков

5. Добавить список – при нажатии на данную кнопку открывается окно создания списка (см. рисунок 40). Подробнее механизм создания списков описан в разделе 12.1.

Рисунок 40 – Фильтр по назначению списков

6. Область со списками – в выделенной области находятся списки. Слева от названия правила имеется поле для выделения списка (где выделенный список ☑). При нажатии на список левой кнопкой мыши открывается общая информация о списке (см. рисунок 41).

Рисунок 41 – Общая информация о списке

В открывшимся окне имеется краткое описание списка и следующие с ним действия:

- Пополнить из файла – открывает окно загрузки файла с элементами источника (подробнее о редактировании\изменении списка написано в разделе 12);
- Редактировать – открывает окно редактирования списка (подробнее о редактировании\изменении списка написано в разделе 12);
- Удалить – безвозвратно удаляет выбранный список.

Третья вкладка – цели. Данная вкладка позволяет создавать, редактировать и удалять цели (см. рисунок 42).

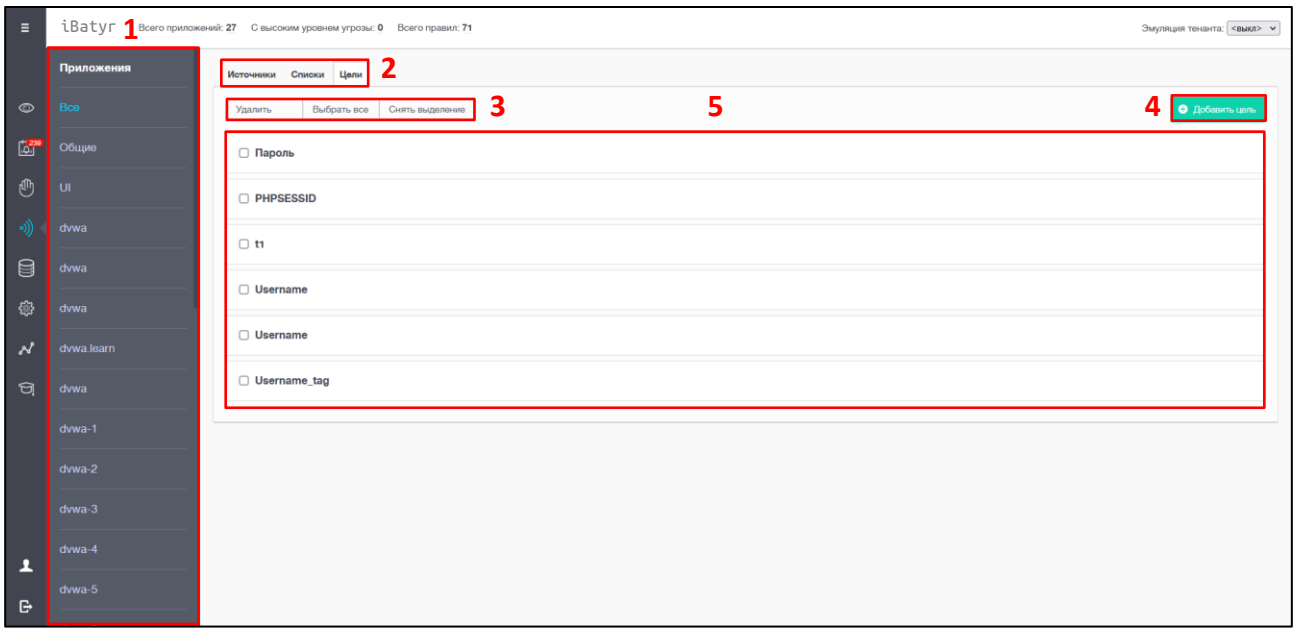

Рисунок 42 – Вкладка «Цели»

1. Список приложений – блок содержит список всех доступных пользователю приложений. При нажатии на приложение выводятся цели, работающие только на данном приложении.
2. Источники, списки, цели – блок вкладок позволяет перемещаться между вкладками.
3. Массовые действия – в отмеченной области находятся массовые действия с целями. Для того чтобы отметить все цели, необходимо нажать на кнопку Выбрать все. Для того чтобы снять все отметки, необходимо нажать на кнопку Снять выделение. Также имеется возможность точечно отмечать, или снимать выделения, данный механизм описан в пункте 5. При нажатии на кнопку Удалить будут удалены все выделенные цели.
4. Добавить цель – при нажатии на данную кнопку открывается окно создания цели (см. рисунок 43). Подробнее механизм создания целей описан в разделе 14.

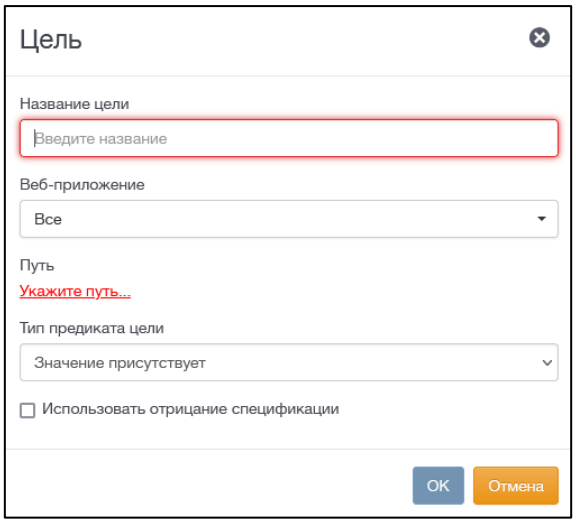

Рисунок 43 – Окно создания цели

5. Область с целями – в выделенной области находятся цели. Слева от названия цели имеется поле для выделения (цель выделена ☑). При нажатии на цель левой кнопкой мыши открывается общая информация о цели (см. рисунок 44).

Рисунок 44 – Общая информация о цели

В открывшимся окне имеется краткое описание цели и следующие с ней действия (см. рисунок 45):

- Редактировать – открывает окно редактирования цели (подробнее о редактировании\изменении цели написано в разделе 14).
- Удалить – безвозвратно удаляет выбранные цели.

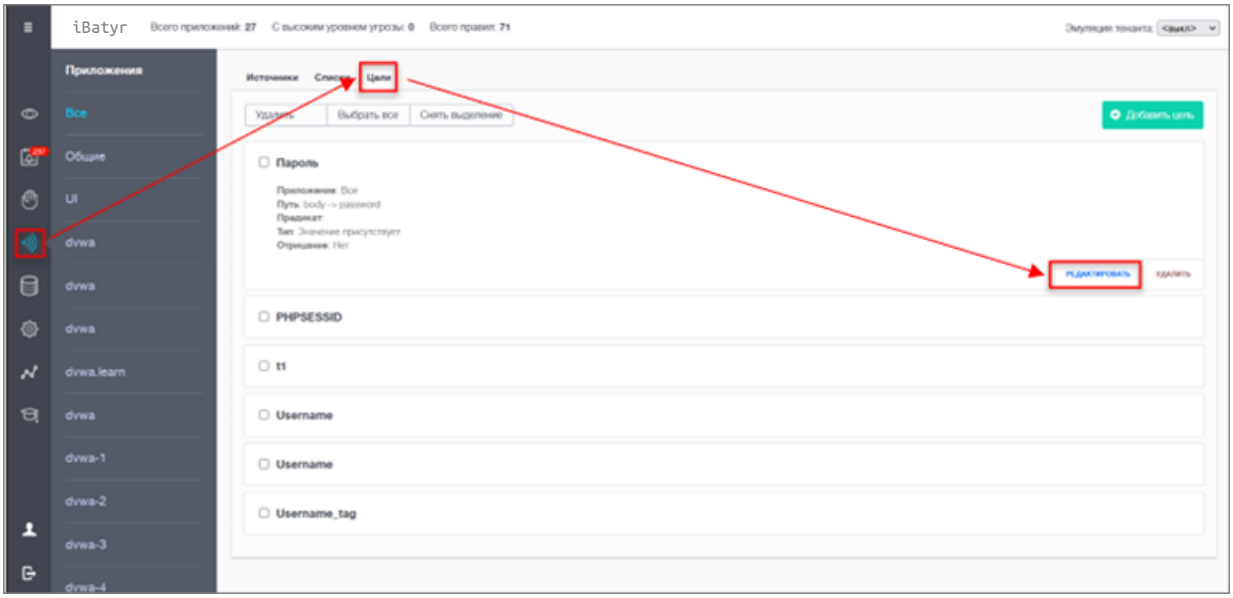

Рисунок 45 – Редактирование цели

3.5. Окно «Приложения»

Окно «Приложения» используется для мониторинга за трафиком и настройки моделей защиты веб-приложений. Для перехода к данному окну, необходимо нажать кнопку «Приложения» в элементах управления. В открывшемся окне (см. рисунок 46) WAF предложит добавить приложение (подробнее о добавлении приложения можно прочитать в разделе 5), или выбрать одно из уже созданных (между приложениями можно перемещаться в любой момент, кликнув по названию другого приложения в выделенной области).

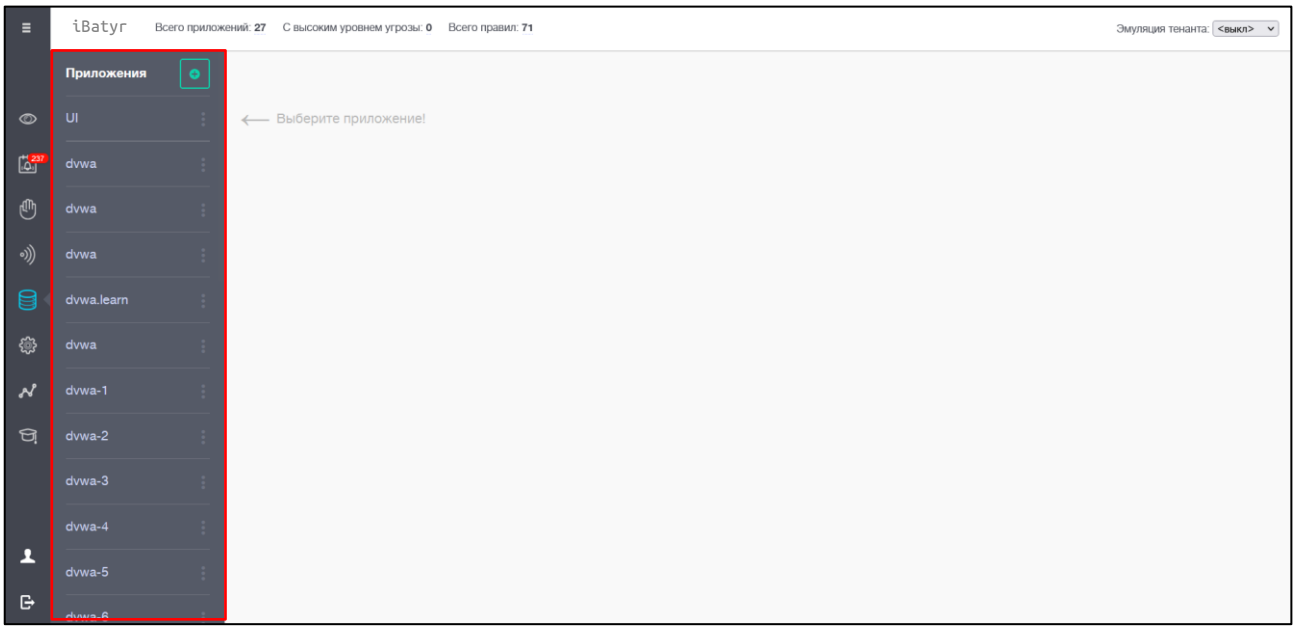

Рисунок 46 - Окно «Приложения»

3.5.1. Вкладка «Транзакции»

После выбора приложения открывается по умолчанию вкладка «Транзакции» (см. рисунок 47), на которой выводятся транзакции выбранного веб-приложения. Данная вкладка служит для анализа проходящего через WAF трафика. По умолчанию, для транзакций установлено семплирование, равное 10 (настройки семплирования можно найти в разделе 0). Это означает, что каждая транзакция обрабатывается на WAF, но на вкладку «Транзакции» выводится только каждая 10 из нормальных транзакций. В противовес нормальным, заблокированные и помеченные транзакции под семплирование не попадают и сохраняются все.

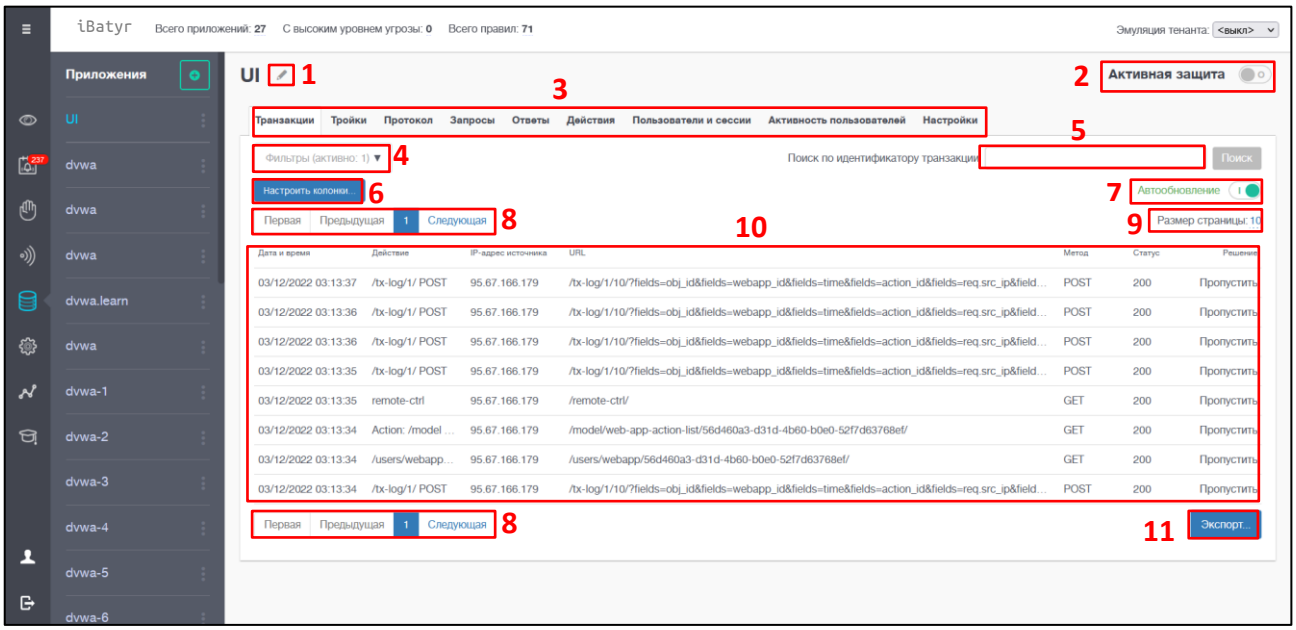

Рисунок 47 – Вкладка «Транзакции»

1. Редактирование названия – пиктограмма с изображением карандаша, при нажатии на которую, открывается окно редактирования названия приложения (см. рисунок 48).

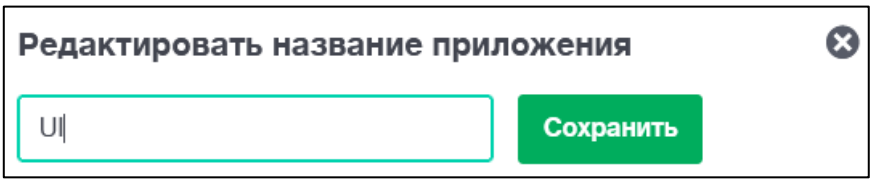

Рисунок 48 – Окно редактирования названия приложения

2. Активная защита – переключатель режима защиты приложения. Имеется два режима:
   - Мониторинг - активная защита выключена. Решение о блокировке транзакций выводится в интерфейсе, но не применяется.
   - Активная защита - активная защита включена. Принятые решения о блокировке применяются к транзакциям.
3. Область переключения между вкладками.
4. Фильтры - при нажатии на кнопку «Фильтры» появляется возможность выбрать один или несколько фильтров из выпадающего списка. Настройка фильтров транзакций рассмотрена в разделе 3.2.
5. Поиск по идентификатору транзакции – WAF дает каждой транзакции свой индивидуальный идентификатор, который указывается в данных по транзакции и в сообщении о блокировке. Для поиска транзакции достаточно просто вставить в поле ID транзакции. Поиск транзакции осуществляется только в рамках приложения, которому она принадлежит. Поиск из других приложений работать не будет!
6. Настроить колонки – при нажатии на данную кнопку откроется окно с настройкой отображения полей таблицы транзакций (см. рисунок 49). Настройка колонок, отображаемых транзакций, рассмотрена в разделе 3.2.

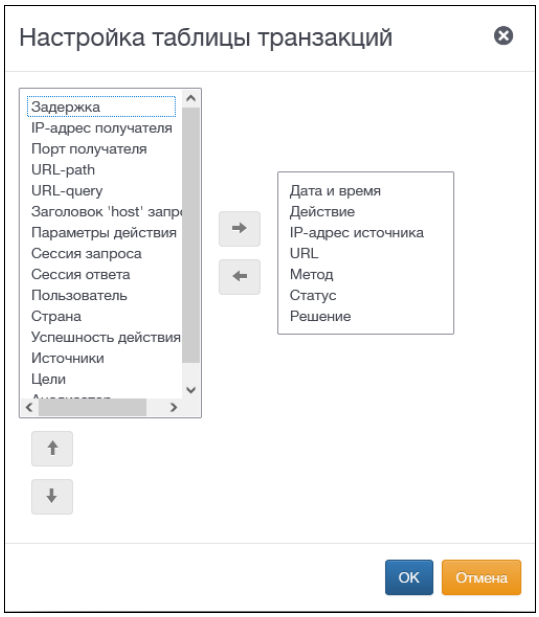

Рисунок 49 – Настройка таблицы транзакций

7. Автообновление – переключатель автоматического обновления отображаемых транзакций.
8. Страницы и перемещение по ним – отображает количество страниц с учетом заданного количества транзакций на странице (задается в пункте 9). Перемещаться между страницами можно с помощью кнопок Предыдущая \ Следующая, или выбрав номер страницы.

9. Размер страницы – количество отображаемых транзакций на странице. Изменить количество отображаемых транзакций можно, щелкнув по числу в строке «Размер страницы:». В появившемся окне (см. рисунок 50) ввести нужное число транзакций на странице. Кнопками ^\v можно увеличивать и уменьшать, с шагом 5, значение, введенное в поле. Чтобы изменения применились, необходимо нажать на появившуюся при входе в режим редактирования кнопку ✔ (Применить изменения). Чтобы отменить изменения, необходимо нажать на кнопку ✖ (Отменить изменения).

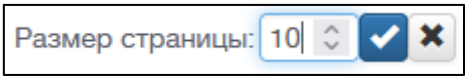

Рисунок 50 – Размер страницы

10. Блок с транзакциями – в данном блоке отображаются транзакции, с учетом заданных фильтров, настроенных колонок и количества транзакций на странице. Подробнее работа с транзакциями описана в разделе 7.
11. Экспорт – позволяет экспортировать транзакции, с учетом заданных фильтров, настроенных колонок. После нажатия на данную кнопку, появится дополнительное поле (см. рисунок 51) с вводом количества транзакций для экспорта (можно так же выбрать все, нажав на иконку в соответствующей области). При повторном нажатии на кнопку «Экспорт» появится диалоговое окно, в котором можно скачать CSV-файл.

Рисунок 51 – Экспорт транзакций

3.5.2. Вкладка «Тройки»

На данной вкладке (см. рисунок 52) находится список «троек» – совокупностей доменного имени веб-приложения, IP-адреса и порта WAF, на которые поступает трафик. Тройки позволяют сопоставлять трафик, приходящий на WAF с конкретным защищаемым приложением.

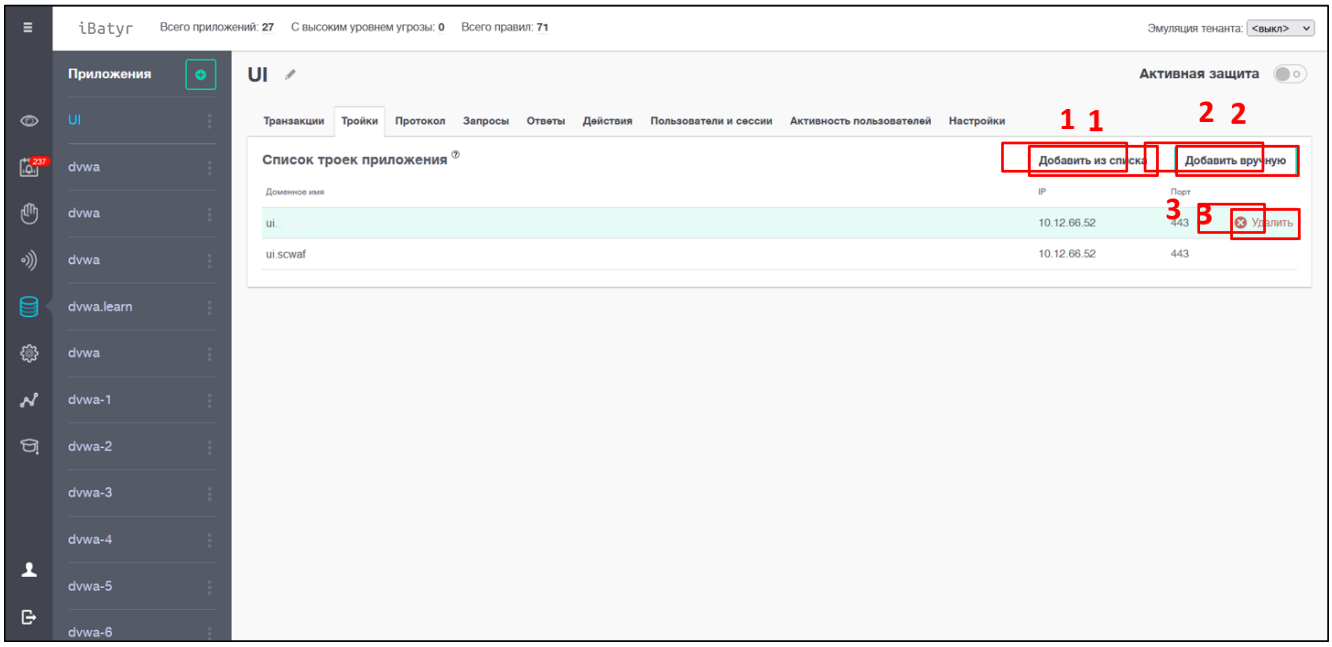

Рисунок 52 – Вкладка «Тройки»

1. Добавить из списка – при нажатии на данную кнопку появится вкладка, на которой можно увидеть те адреса\имена, трафик с которых был зафиксирован на WAF (см. рисунок 53).

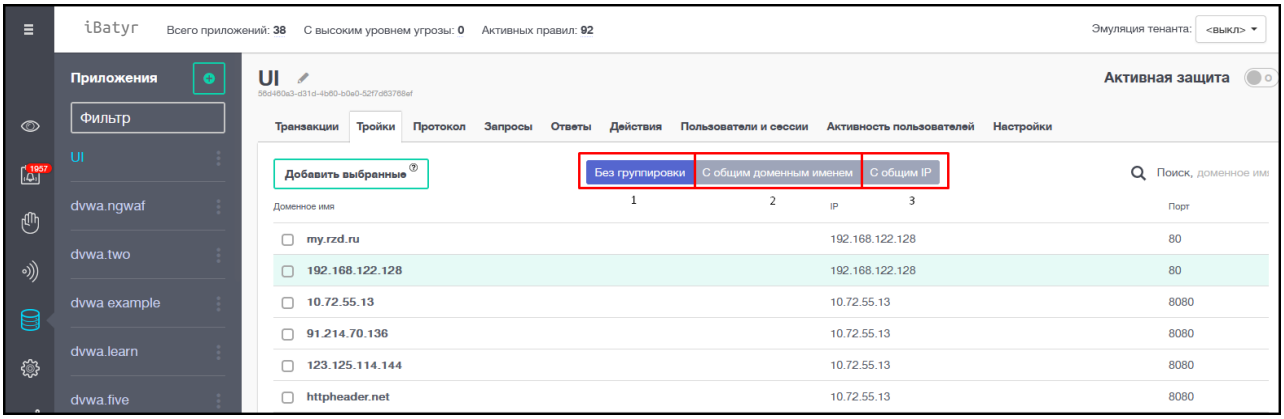

Рисунок 53 - Добавление из списка

2. Добавить вручную – при нажатии на данную кнопку появится окно с вводом доменного имени, адреса и порта.
3. Удалить – данная кнопка появляется при наведении курсора мыши на уже добавленные «троки». Позволяет безвозвратно удалить строку с «тройками».

Отредактировать «тройки» нельзя. Более подробная информация по добавлению троек представлена в разделе 5.2.

3.5.3. Вкладка «Протокол»

На данной вкладке (см. рисунок 54) находятся настройки позитивной модели валидации протокола.

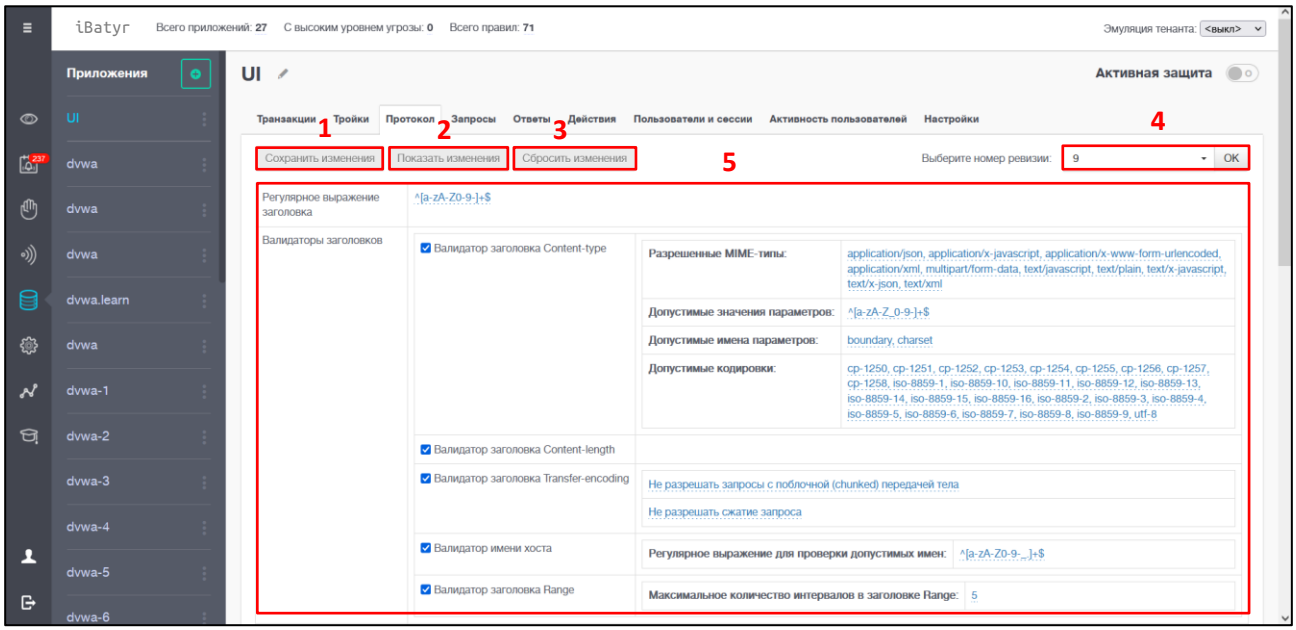

Рисунок 54 – Вкладка «Протокол»

1. Сохранить изменения – кнопка становится активной, после внесения изменений в настройки протокольной валидации в блоке 5. Сохраняет внесенные изменения и создает новую ревизию.

2. Показать изменения – кнопка становится активной, после внесения изменений в настройки протокольной валидации в блоке 5. Сравнивает введенные значения с актуальной ревизией и в диалоговом окне показывает изменения.
3. Сбросить изменения – кнопка становится активной, после внесения изменений в настройки протокольной валидации в блоке 5. Сбрасывает значения полей до актуальной ревизии.
4. Выберите номер ревизии – имеется возможность переключения между ревизиями настроек. После выбора ревизии, отличной от актуальной, можно нажать на кнопку OK для просмотра настроек выбранной ревизии. Для того чтобы применить выбранную ревизию, необходимо нажать на кнопку Откатить.
5. В выделенном блоке находятся настройки протокольной валидации. Подробнее см. раздел 9.

3.5.4. Вкладки «Запрос» и «Ответ»

На данных вкладках находятся настройки позитивной модели «Дерево разбора» (см. рисунок 55). Вкладки «Запрос» и «Ответ» идентичны по возможным настройкам.

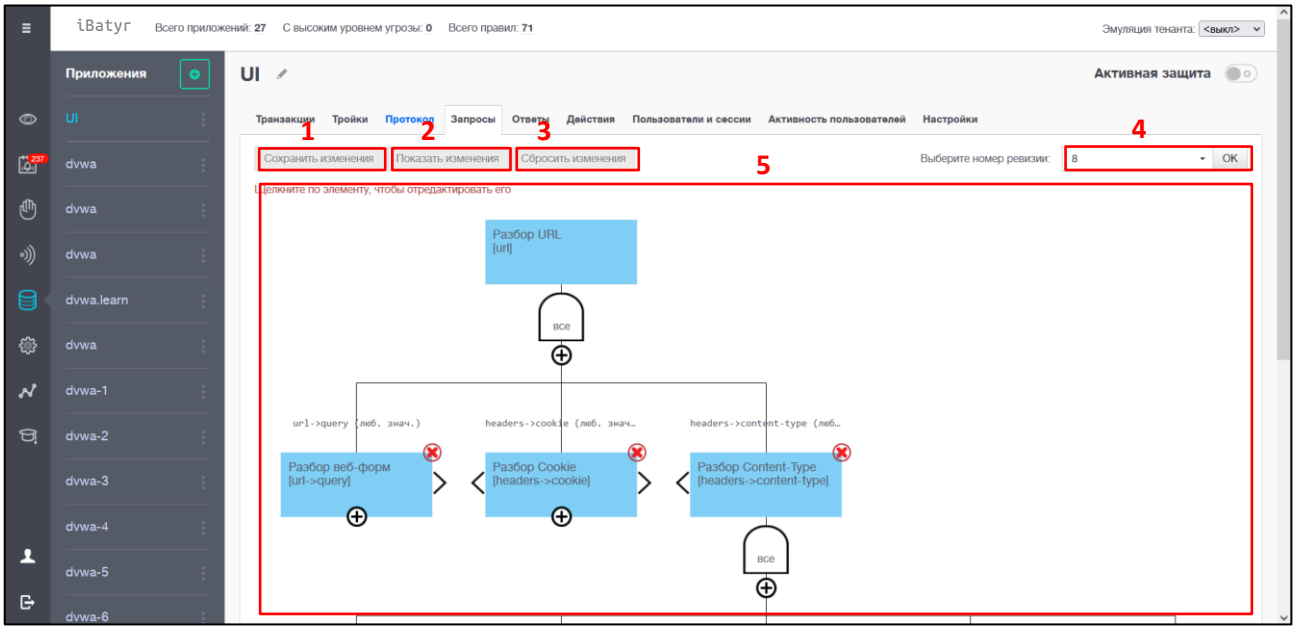

Рисунок 55 – Вкладка «Запросы»

1. Сохранить изменения – кнопка становится активной, после внесения изменений в настройки дерева разбора в блоке 5. Сохраняет внесенные изменения и создает новую ревизию.
2. Показать изменения – кнопка становится активной, после внесения изменений в настройки дерева разбора в блоке 5. Сравнивает введенные значения с актуальной ревизией и в диалоговом окне показывает изменения.
3. Сбросить изменения – кнопка становится активной, после внесения изменений в настройки дерева разбора в блоке 5. Сбрасывает значения полей до актуальной ревизии.
4. Выберите номер ревизии – имеется возможность переключения между ревизиями настроек. После выбора ревизии, отличной от актуальной, можно нажать на кнопку OK для просмотра настроек данной ревизии. Для того чтобы применить выбранную ревизию, необходимо нажать на кнопку Откатить.
5. В выделенном блоке находятся настройки дерева разбора. Подробнее см. раздел 10.

3.5.5. Вкладка «Действия»

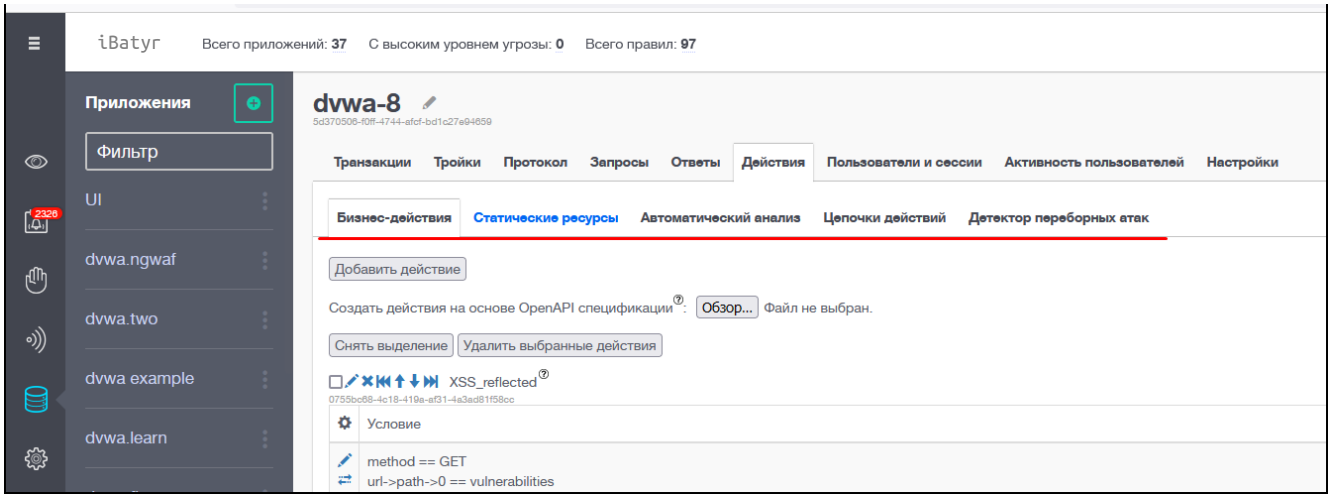

Рисунок 56 – Вкладка «Действия»

На данной вкладке содержатся тонкие настройки следующих модулей:

- Бизнес-действия – данная вкладка нужна для создания, редактирования и удаления действий (Раздел 3.5.5.1).
- Статические ресурсы – вкладка с созданием и удалением настроек фильтрации запросов к статическим ресурсам (Раздел 3.5.5.2).
- Автоматический анализ – вкладка с настройкой задач для самообучения некоторых модулей WAF (Раздел 3.5.5.3).
- Цепочки действий – вкладка для создания, редактирования и удаления цепочек действий (Раздел 3.5.5.4).
- Детектор переборных атак – на вкладке находятся два модуля обнаружения переборных атак (Действие\Источник и Действие\Источник\Цель) Раздел 3.5.5.5.

3.5.5.1. Вкладка «Бизнес-действия»

При переходе на вкладку «Действия» по умолчанию открывается вкладка «Бизнес-действия» (см. рисунок 57). Данная вкладка используется для создания и редактирования позитивной модели Бизнес-логики. Модель состоит из отдельных действий и их параметров, которые позволяют описывать на логическом уровне действия пользователей в веб-приложениях. Например, аутентификация, регистрация, поиск, оплата покупок, отправка формы и т.д.

Действия – это сопоставление HTTP-запросов с логикой работы веб-приложения. При создании действия можно использовать условия не только на URL запроса, но и на любые другие параметры запроса.

Модель Бизнес-логики может использоваться для детектирования и блокировки запросов, которые не соответствую данной модели. Помимо этого, созданные действия могут быть использованы для точечного подавления ложных срабатываний в качестве параметра в правиле для тонкой настройки детектора переборных атак, в качестве элементов модели Последовательности действий, в качестве параметров при настройке сессионной модели, а также других смежных с ней модулей.

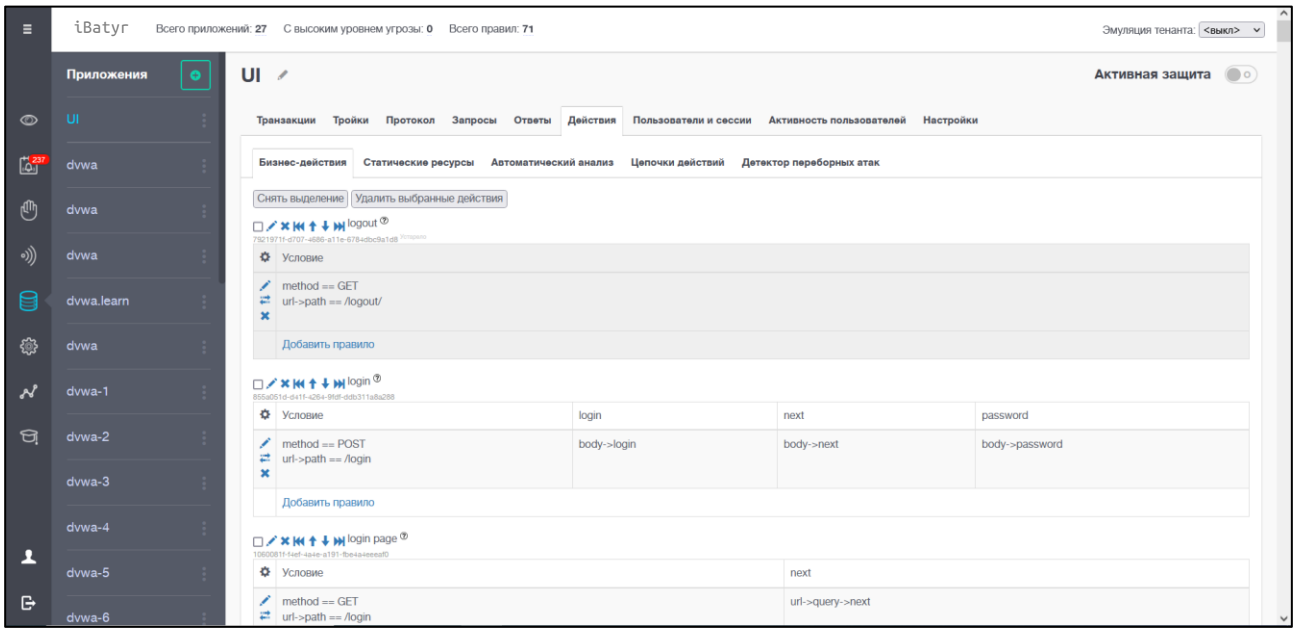

Рисунок 57 – Вкладка «Бизнес-действия»

Чтобы создать действие, необходимо перейти на вкладку «Бизнес-действия» и нажать на поле «Добавить действие» (см. рисунок 58).

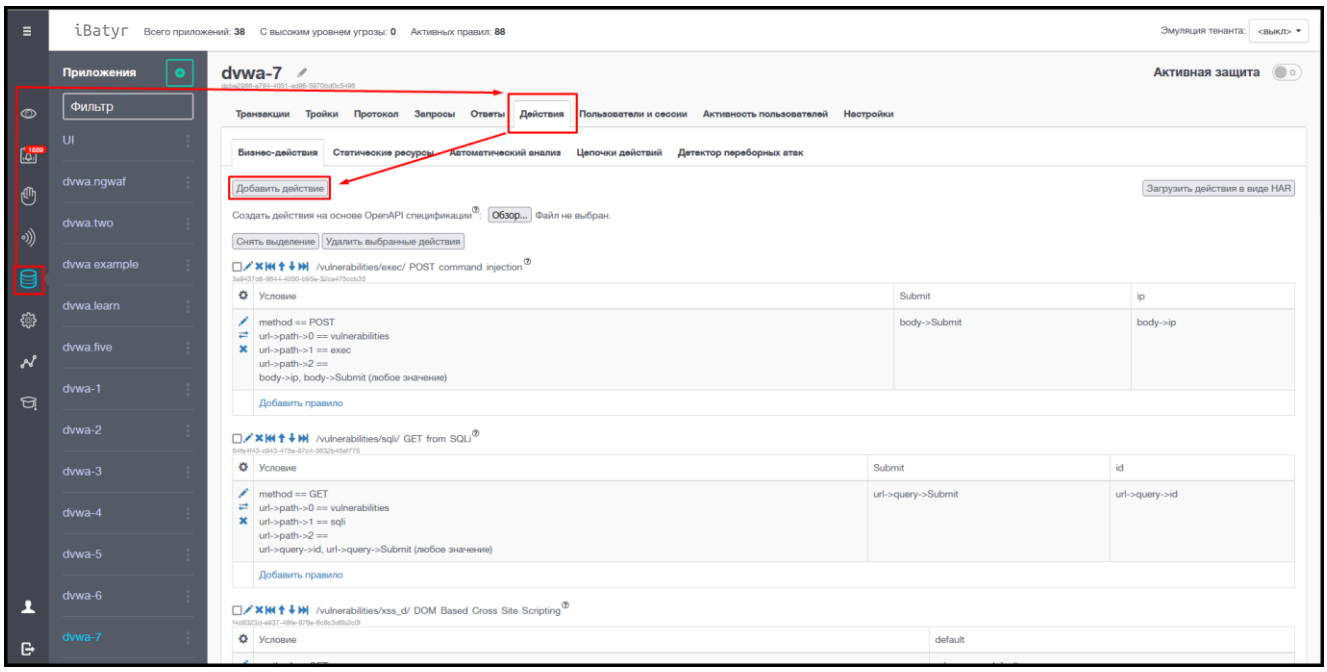

Рисунок 58 – Создание действия

При нажатии на данное поле открывается окно «Модель действия» (см. рисунок 59)

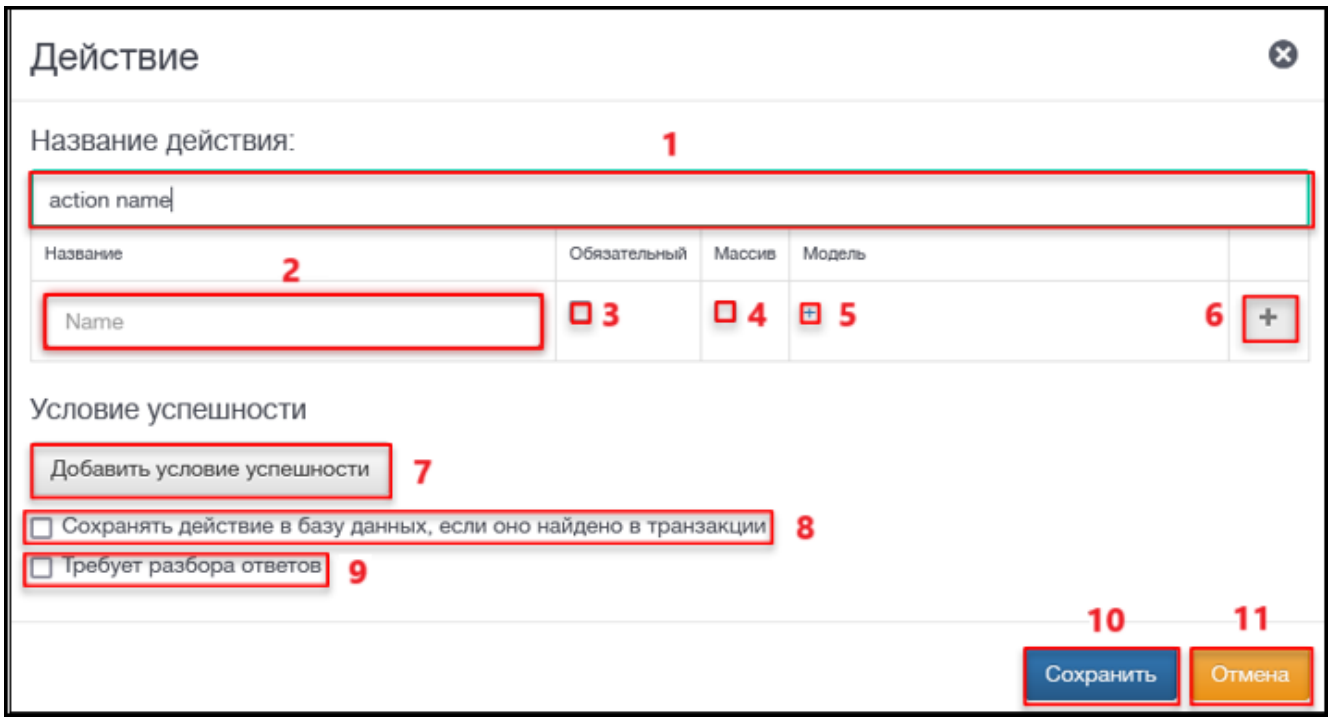

Рисунок 59 – Окно «Модель действия»

1. Название действия – поле для ввода названия действия.
2. Название – поле для ввода параметра действия. В качестве параметра действия можно выбрать один или несколько элементов дерева разбора, которые критичны в рамках данного действия.
3. Обязательный – бинарное поле, которое может принимать значения «Да», или «Нет» («☑», «☐» соответственно). Данное поле отвечает за обязательность наличия параметра для действия.
4. Массив – бинарное поле, которое может принимать значения «Да», или «Нет» («☑», «☐» соответственно). Данное поле отвечает за характеристику параметра, как массива данных.
5. Модель – при нажатии выделенной иконки открывается окно «Редактирование модели параметра»
6. В выделенной области находится иконка, при нажатии на которую добавляется ещё одна строка ввода параметра модели.
7. Добавить условие успешности – кнопка открывает окно «Редактирование условия успешности».
8. Сохранить действие в базу данных, если оно найдено в транзакции – бинарное поле, которое может принимать значения «Да», или «Нет» («☑», «☐» соответственно). Данное поле отвечает за сохранение действия в базу данных, если оно найдено в транзакции.
9. Требует разбора ответов – бинарное поле, которое может принимать значения «Да», или «Нет» («☑», «☐» соответственно). В случае если в действии используется условие успешности, данное поле необходимо включать обязательно.
10. Сохранить – кнопка сохраняет внесенные изменения.
11. Отменить – кнопка отменяет внесённые изменения.

Работа с действиями разобрана в разделе 15.

3.5.5.2. Вкладка «Статические ресурсы»

При загрузке страницы защищаемого веб-приложения происходит ряд запросов на загрузку файлов, таких как иконок, скрипты и таблицы стилей. Данного рода запросы также отображаются на WAF, что мешает корректному анализу трафика.

Фильтрацию запросов к статическим ресурсам необходимо настраивать для того, чтобы снизить нагрузку на анализаторы WAF и убрать неинформативный трафик, так как по умолчанию каждая транзакция падает в общий пул и анализируется (строится дерево разбора, проверяются сигнатуры и т.д.). Для того чтобы не анализировать транзакции к статическим ресурсам, и был разработан модуль «Статические ресурсы» (см. рисунок 60).

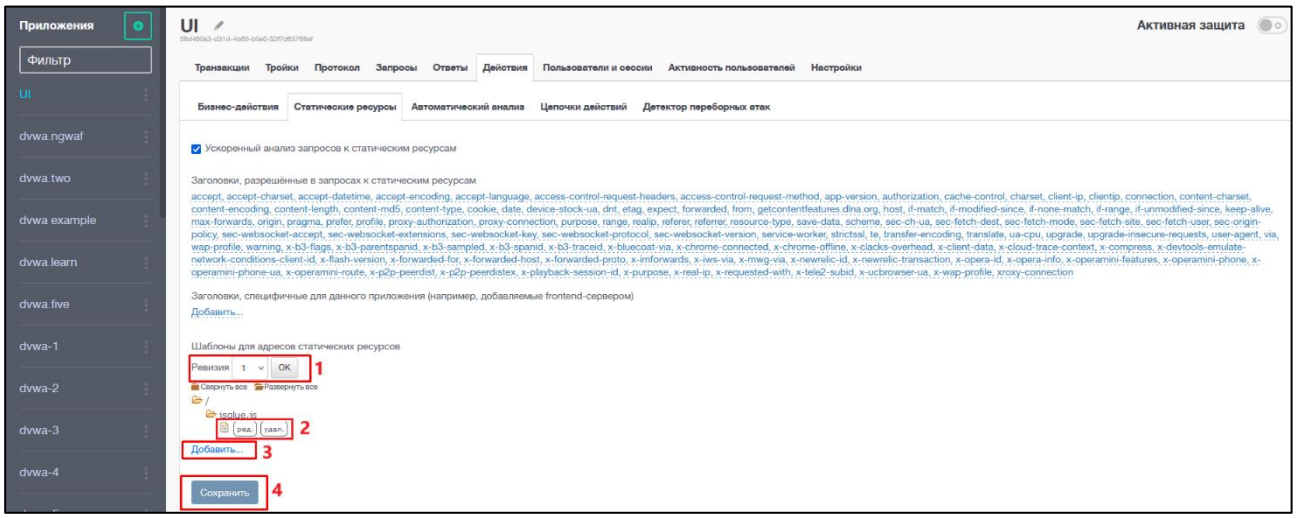

Рисунок 60 – Вкладка «Статические ресурсы»

1. Выпадающий список с кнопкой «ОК» позволяет переключаться между версиями добавленных статистических ресурсов.
2. Кнопки позволяют удалить или отредактировать созданный статистический ресурс.
3. При клике по иконке «Добавить…» открывается окно добавления шаблона, в котором имеется возможность добавления как пути к файлу целиком, так и задание последней его части регулярным выражением. Для добавления пути к файлу целиком, в появившемся окне необходимо ввести путь к файлу, затем нажать иконку «Добавить…», а после нажать на кнопку «Сохранить».
4. После добавления шаблона, необходимо сохранить изменения на странице, нажав кнопку «Сохранить».

Создание настроек фильтрации запросов к статическим ресурсам разобрано в разделе 8.

3.5.5.3. Вкладка «Автоматический анализ»

На WAF имеется возможность автоматического обучения некоторых модулей. Вкладка содержит данные о периодических заданиях. Представление разбито на две части: в верхней части представления расположено расписание периодических заданий, в нижней данные о выполненных заданиях (см. рисунок 61).

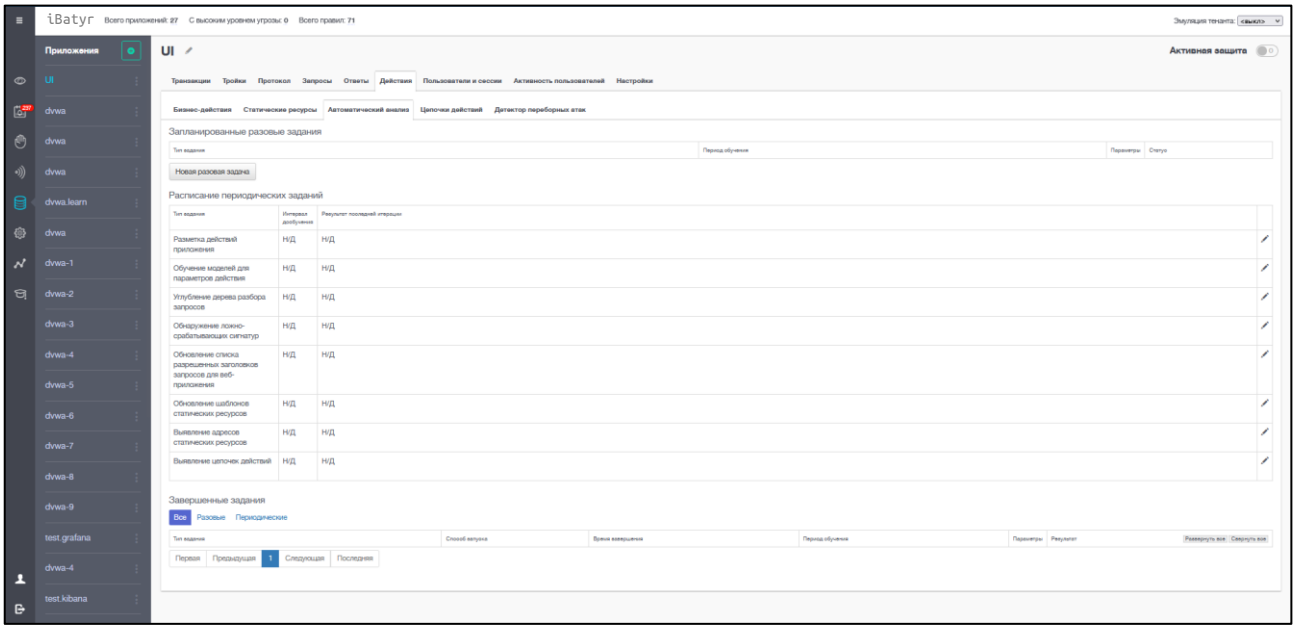

Рисунок 61 – Вкладка «Автоматический анализ»

В представлении можно создать новое разовое задание, для этого необходимо нажать «Новая разовая задача» в верхнем левом углу приложения, в появившемся окне (см. рисунок 62) выбрать один из восьми типов задач (см. таблица 3), а затем заполнить параметры задания. В расписании периодических заданий отображается тип задания, периодичность выполнения и результат последнего выполнения. По правому краю каждой строки таблицы периодических заданий расположена кнопка , позволяющая редактировать параметры задания. В блоке завершённых заданий есть возможность просмотра всех завершённых, периодических и разовых заданий. Все завершённые задания сортируются по времени завершения от новых до старых. Каждое задание подсвечивается зелёным или красным цветом в зависимости от результата: выполнено успешно – зеленый, задание завершилось неудачей – красный. В графе «Параметры» располагается пиктограмма , нажатие на которую открываются параметры задания. В графе «Результат» располагается пиктограмма «+», нажатие на которую разворачивает результаты выполнения задания.

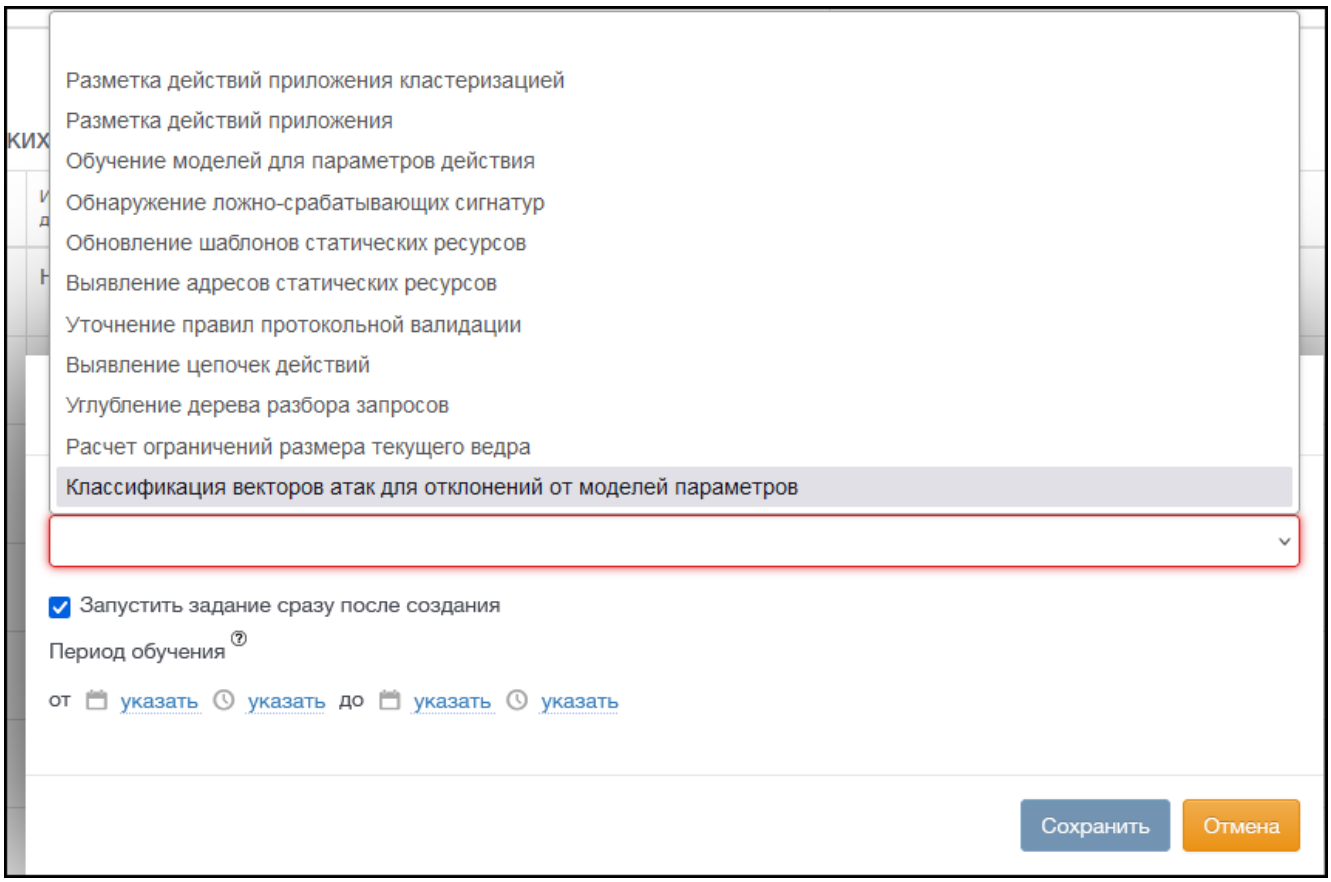

Рисунок 62 – Автоматические задачи

Таблица 3 – Автоматические задачи

Задача	Описание
Разметка действий приложений кластеризацией	Создает действия для приложения кластеризацией
Разметка действий приложения	Создает действия для приложения
Обучение моделей для параметров действия	Настраивает модель действий приложения
Углубление дерева разбора запросов	Автоматически углубляет модель дерева разбора запросов для данного приложения
Обнаружение ложно-срабатывающих сигнатур	Автоматически подавляет ложно срабатывающие сигнатуры на основе заданных параметров
Уточнение правил протокольной валидации	Обновляет список разрешенных заголовков запроса в протокольной валидации для выбранного приложения
Обновление шаблонов статических ресурсов	Обновляет настройки шаблонов фильтрации запросов к статическим ресурсам для выбранного приложения
Выявление адресов статических ресурсов	Добавляет пути к статическим ресурсам

Задача	Описание
Выявление цепочек действий	Создает цепочки действий для данного приложения
Расчет ограничений размера текущего ведра	На основании трафика рассчитывает оптимальные значения ведра с маркерами для детектора переборных атак
Классификация векторов атак для отклонений от моделей параметров	Определяет вектора

3.5.5.4. Вкладка «Цепочки действий»

Цепочки действий – позволяет создавать для отслеживания простые сценарные цепочки (см. рисунок 63). При нажатии на кнопку «Добавить новую цепочку» появляется окно «Цепочка действий», содержащая поля «Критическое действие», «Действие-пререквизит» и «Окно для действий в трассе». Для каждого созданного действия доступно редактирование, удаление и просмотр информации, при этом редактирование позволяет изменить только два параметра цепочки: «Действие-пререквизит» и «Окно для действий в трассе» (подробнее о создании цепочек действий написано в разделе 18.3). Отслеживание цепочек действий происходит в представлении «Автоматический анализ» вкладки «Действия» через задачу типа «Выявление паттернов в последовательностях действий».

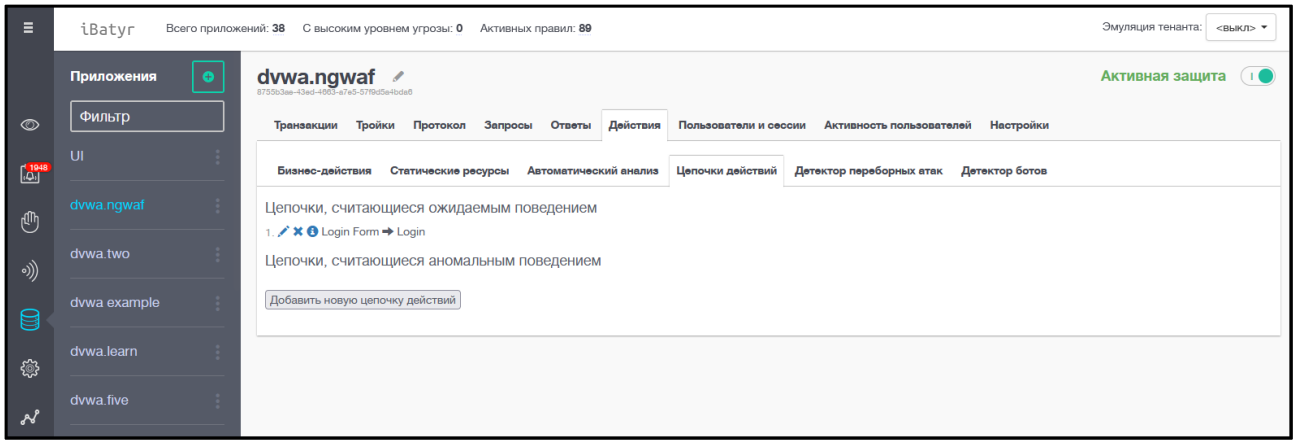

Рисунок 63 – Вкладка «Цепочки действий»

3.5.5.5. Вкладка «Детектор переборных атак»

Детектор переборных атак - способен обнаруживать переборные атаки - слишком частые обращения к отдельным действиям веб-приложения. Для этого Детектор переборных атак реализует алгоритм макетного ведра, обеспечивая таким образом ограничение допустимого числа запросов к веб-приложению за единицу времени (rate limiting). Субъектами, для которых вводятся ограничения на число запросов в единицу времени, являются источники. Вкладка «Детектор переборных атак» изображена на рисунке 64.

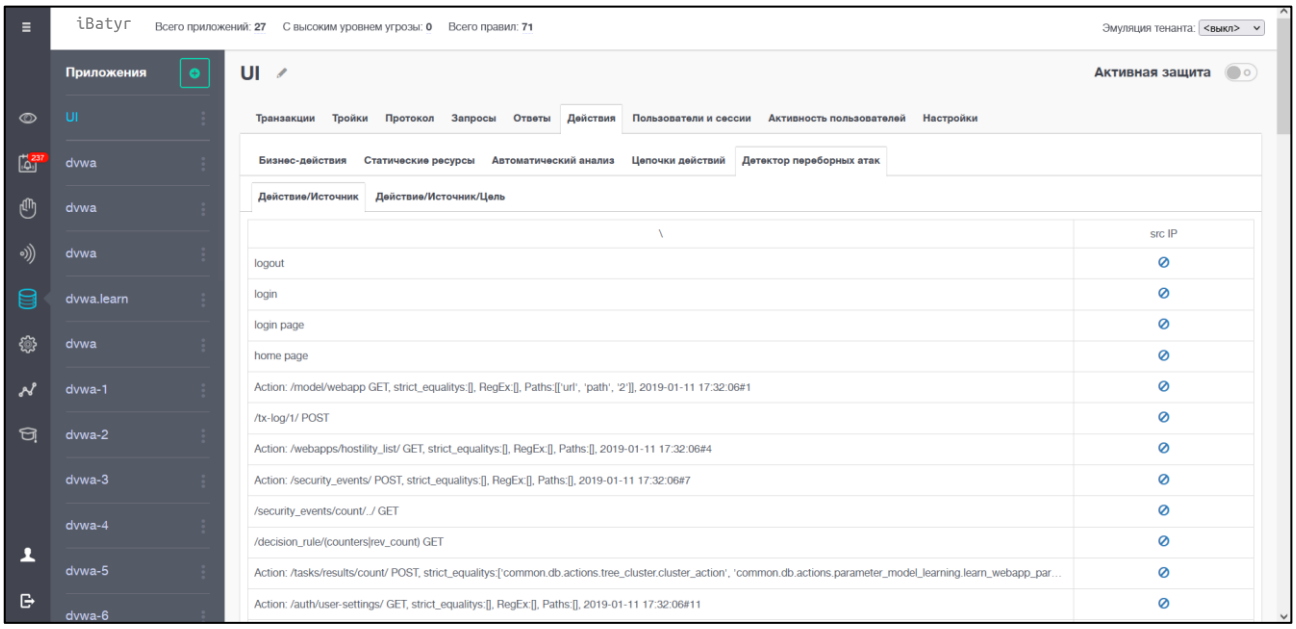

Рисунок 64 – Вкладка «Детектор переборных атак»

Подробное описание настроек детекторов переборных атак находится в разделе 16.

3.5.5.6. Вкладка «Детектор ботов»

Детектор ботов способен обнаруживать деятельность ботов на основе времени задержки ответа веб-приложения на запрос. Окно «детектора ботов» представлено двумя разделами: «Общие настройки» и «Настройки трафика» (см. рисунок 65).

Раздел «Общие настройки» - представляет собой настройки самого анализатора в части хранения информации о текущем наблюдаемом трафике.

Раздел «Настройки трафика» - представляет собой настройки порогов срабатывания алгоритма обнаружения ботов для трафика к отдельным действия веб-приложения и всего трафика с одного IP адреса к веб-приложению в целом.

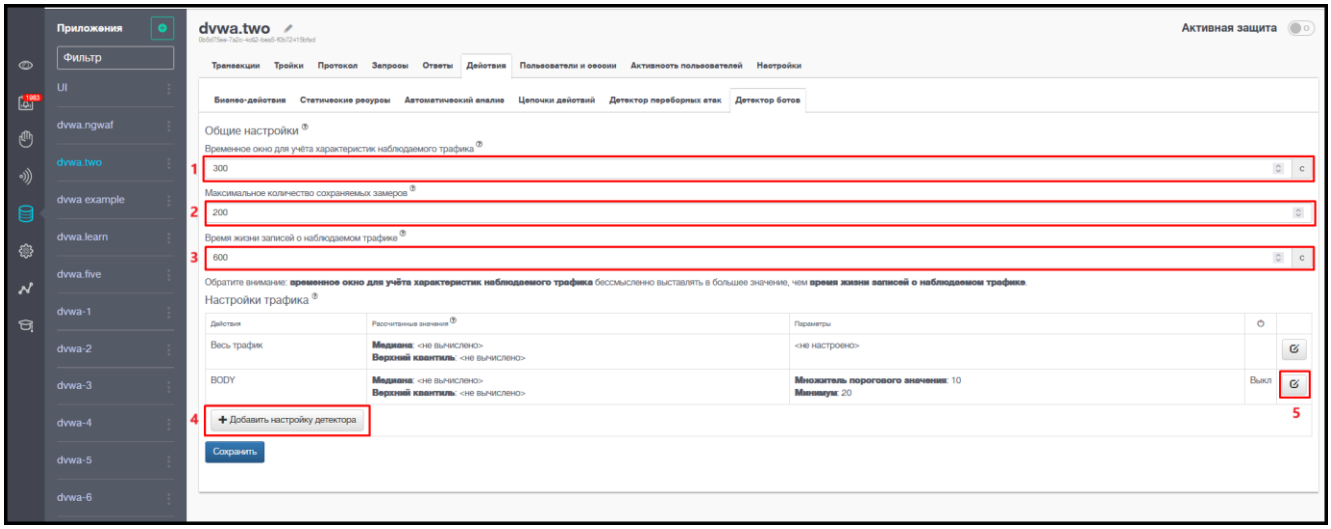

Рисунок 65 – Детектор ботов

1. Временное окно для учёта характеристик наблюдаемого трафика – характеристики актуального наблюдаемого трафика для алгоритма обнаружения ботов рассчитываются в пределах указанного

временного окна. Иными словами, для текущего трафика мы смотрим только на транзакции за последние N-секунд. Транзакции старше указанного возраста не принимаются в расчёт характеристик текущего трафика.

2. Максимальное количество сохраняемых замеров – для текущего наблюдаемого трафика (с одного IP-адреса к одному действию веб-приложения) хранятся временные замеры для ограниченного, указанного числа транзакций. Данное ограничение нужно, чтобы разумно ограничить объемы хранимой информации о наблюдаемом трафике в случае большого размера временного окна и высоких объемах трафика к веб-приложению.
3. Время жизни записей о наблюдаемом трафике – как долго хранятся записи о характеристиках текущего наблюдаемого трафика. Для каждой пары свой IP-адрес, действие веб-приложения характеристики наблюдаемого трафика хранятся в отдельных записях; если с некоторого IP-адреса на некоторое действие веб-приложения не будет запросов в течении указанного времени, то соответствующая запись будет удалена для экономии памяти.
4. Добавить настройку детектора – при нажатии кнопки открывается окно настройки детектора (см. рисунок 66).

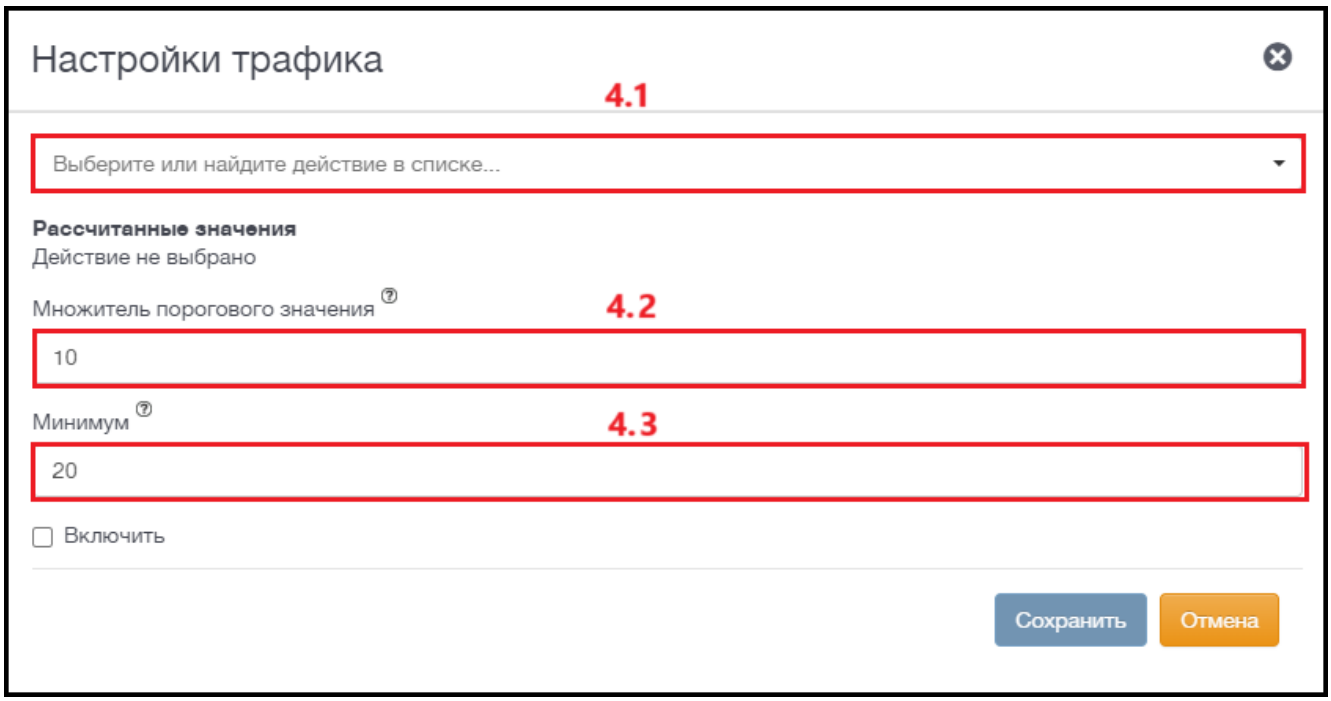

Рисунок 66 – Настройка детектора ботов

4.1. Необходимо выбрать действие, по которому детектором будет проверяться наличие ботов. Для выбранного действия автоматически рассчитываются значения «Медианы» и «Верхнего квантиля» (см. рисунок 67).

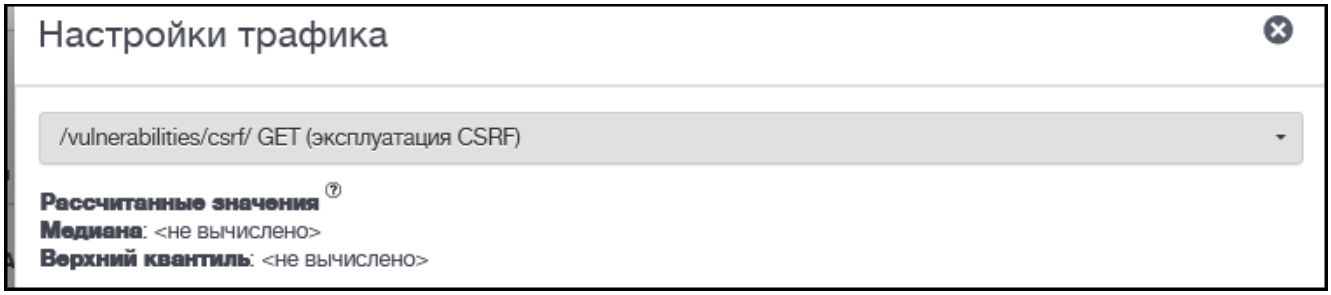

Рисунок 67 – Значения действия

4.2. Множитель порогового значения – определяет во сколько раз нужно превысить нормальное значение (вычисленное ранее на основе исторических данных по нормальному трафику веб-приложения) для обнаружения аномалии.

4.3. Минимум – алгоритм обнаружения ботов для отдельного IP адреса начнет применяться к наблюдаемому трафику только после того, как будет накоплено минимально необходимое число замеров характеристик трафика. Иными словами, IP адрес должен в течении указанного временного окна совершить минимум N запросов к конкретному действию веб-приложения (и запросов к веб-приложению в целом), прежде чем на основе этих транзакций станет возможно посчитать достоверные статистики и сравнить их с характеристиками нормального трафика для обнаружения аномалий.

5. Позволяет редактировать настройки трафика для каждого действия.

3.5.6. Вкладка «Пользователи и сессии»

Сессия – это механизм, реализованный для того, чтобы отличать запросы одного пользователя от другого. В самом протоколе HTTP нет такого понятия как механизм отслеживания сессий, для решения данной проблемы было принято решение использовать cookie, тела запроса, заголовков для передачи информации о сеансе. Классический вариант – когда клиент переходит в приложение, то ему выдается cookie уникально его идентифицирующая. После чего с каждым запросом данного клиента отправляется данная cookie. Для подобного рода cookie может быть установлено время жизни.

Сессионная модель — это механизм, позволяющий на WAF привязаться к вышеуказанным атрибутам для отслеживания сессий пользователей.

Примеры использования сессионной модели:

- Для ограничения доступа в личный кабинет неавторизованных пользователей;
- Для ограничения количества сессий одного пользователя по логину учетной записи;
- Для защиты от кражи сессионных идентификаторов.

На вкладке «Пользователи и сессии» реализован механизм добавления сессионных атрибутов (см. рисунок 68). Подробнее добавление сессионного атрибута описано в разделе 18.1.

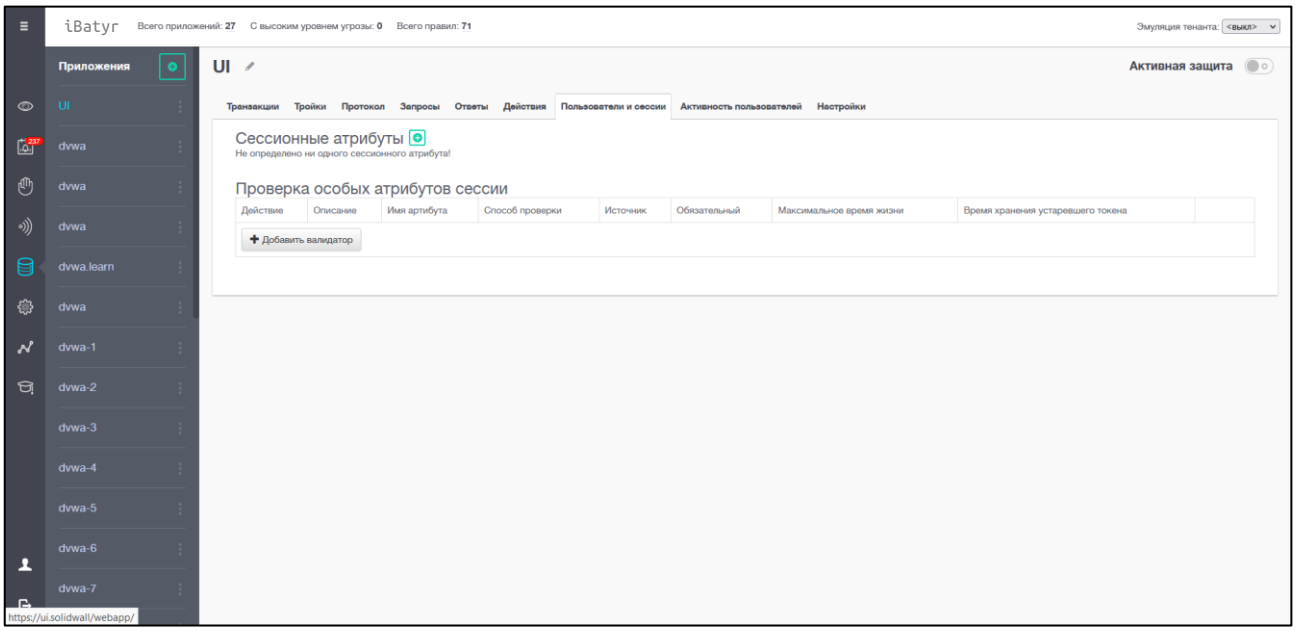

Рисунок 68 – Вкладка «Пользователи и сессии»

3.5.7. Вкладка «Активность пользователей»

На данной вкладке показана активность пользователей (см. рисунок 69) в рамках сессии в виде таблицы со следующими столбцами:

- Пользователь – в данном поле указывается значение сессионного идентификатора с типом атрибута «Извлечение имени пользователя».
- Зарегистрирован – указаны дата и время первого появления сессии пользователя.
- Последняя активность – указаны дата и время последнего появления сессии пользователя.
- Число накопленных аномалий – показывает количество накопленных аномалий за последнюю, или активную сессию пользователя.

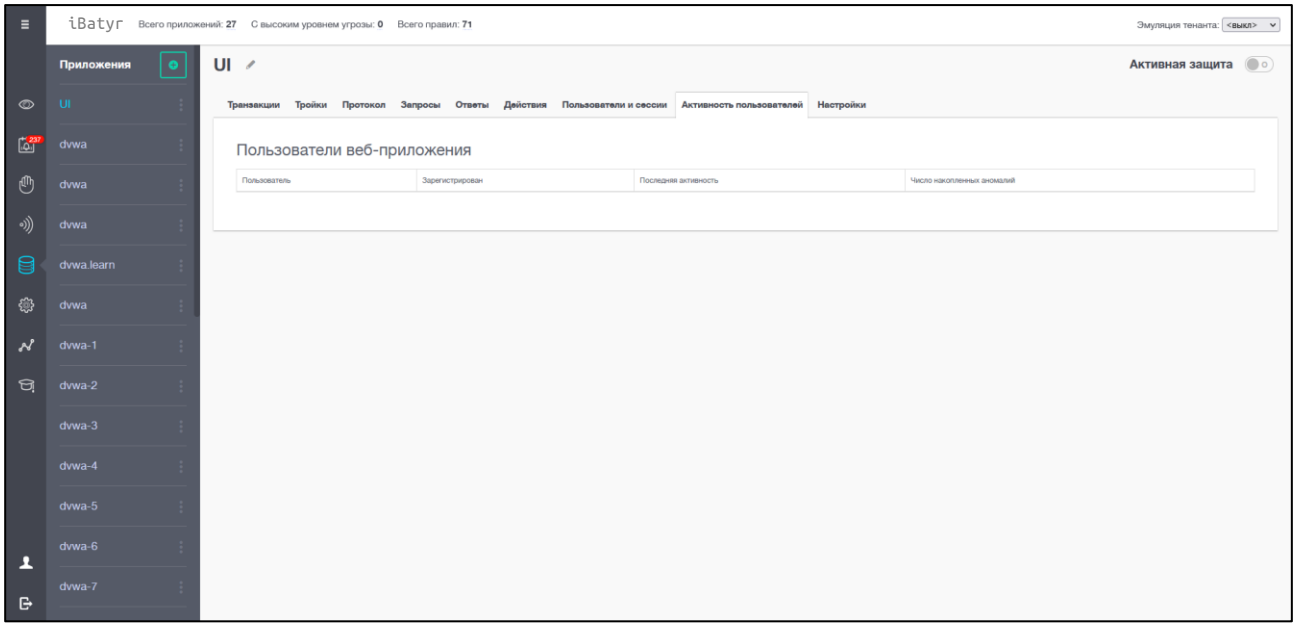

Рисунок 69 – Вкладка «Активность пользователей»

3.5.8. Вкладка «Настройки»

На вкладке «Настройки» выведены следующие настройки приложения (см. рисунок 70):

- Заголовки запроса, содержащие IP-адрес клиента – форма для указания заголовка запроса, в котором содержится реальный IP-адрес клиента. Данная настройка необходима, если перед WAF стоит прокси, например, балансировщик нагрузки или TLS-сервер. Прокси подменяет IP-адрес клиента защищаемого приложения на собственный адрес. Прокси, работающие на 7 уровне модели OSI, как правило, добавляют в запросы клиентов специальный заголовок, содержащий IP-адрес клиента. Например, заголовок x-real-ip.
- Кодировки символов, специфичные для данного приложения – форма для указания специфичных кодировок, используемых на защищаемом веб-приложении. Если на приложении имеются специфичные кодировки символов, и они не указаны в данной форме, будут возникать ошибки разбора запроса, что по умолчанию приводит к блокировке.
- Доверенные домены для данного приложения — это форма указания доменов, которые будут использоваться как белый список для модулей csrf и openredirect.
- Настройки для модулей анализатора – эти настройки применяются только в том случае, если соответствующие модули настроены на их использование. В данном случае выведена следующая настройка: строить дерево разбора для ответа – она отвечает за построение дерева разбора ответа на приложении (описание настройки модуля находится в разделе 0).
- Маскирование данных – замена символов в выбранных полях. Настройка маскирования описана в разделе 11.

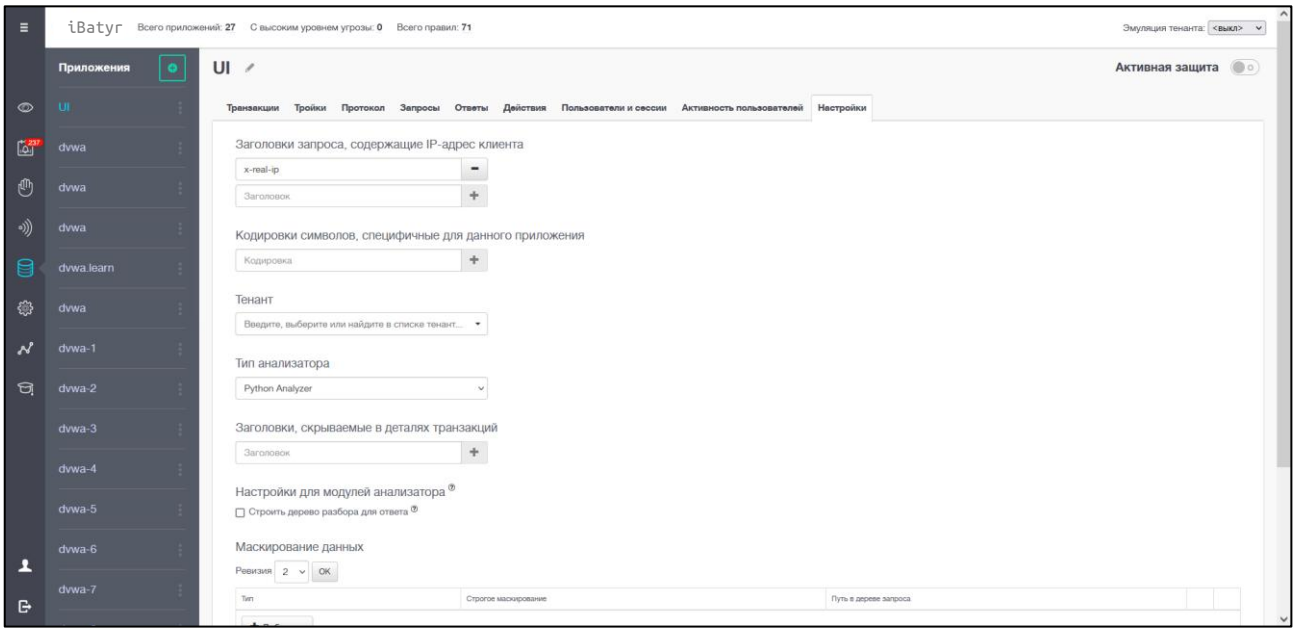

Рисунок 70 – Вкладка «Настройки»

Примечание: начиная с версии 2.12 появилась возможность включать модуль ModSecurity в настройках каждого приложения по отдельности. Для того, чтобы включить данный модуль на инсталляции без мультитенантной модели, достаточно обладать правами администратора. На мультитенантной инсталляции необходимо обладать правами супер-администратора, и открыть настройки приложения с выключенным тенантом.

3.6. Окно «Настройки»

Окно «Настройки» разделено на следующие вкладки (см. рисунок 71):

- Управление анализаторами – добавление и настройка анализаторов для инсталляции.
- Управление доступом – добавление и удаление пользователей. Также на данной вкладке имеется возможность редактирования прав пользователей.
- Подавление аномалий – на данной вкладке находятся настроенные на всей инсталляции подавления. Здесь их можно добавлять, удалять и редактировать.
- Настройки панели управления – настройки SMTP сервера, настройки парольной политики, настройки LDAP.
- Журнал – хранит записи о всех внесённых изменениях на инсталляции с указанием пользователя, который внес изменения.
- Конфигурации модулей – на данной вкладке можно обозначить конфигурацию, которую будет использовать модуль ModSecurity.
- Отслеживание сессий – список всех сессионных атрибутов, заведенных на инсталляции. Также включает в себя сессионные атрибуты, имеющиеся на WAF по умолчанию.
- Настройка тенантов – управление тенантами.
- Настройки аутентификации через nginx – на данной вкладке можно добавить пользователя защищаемого приложения, а также изменить пароли существующим, очистить сессии пользователей или удалить пользователей.

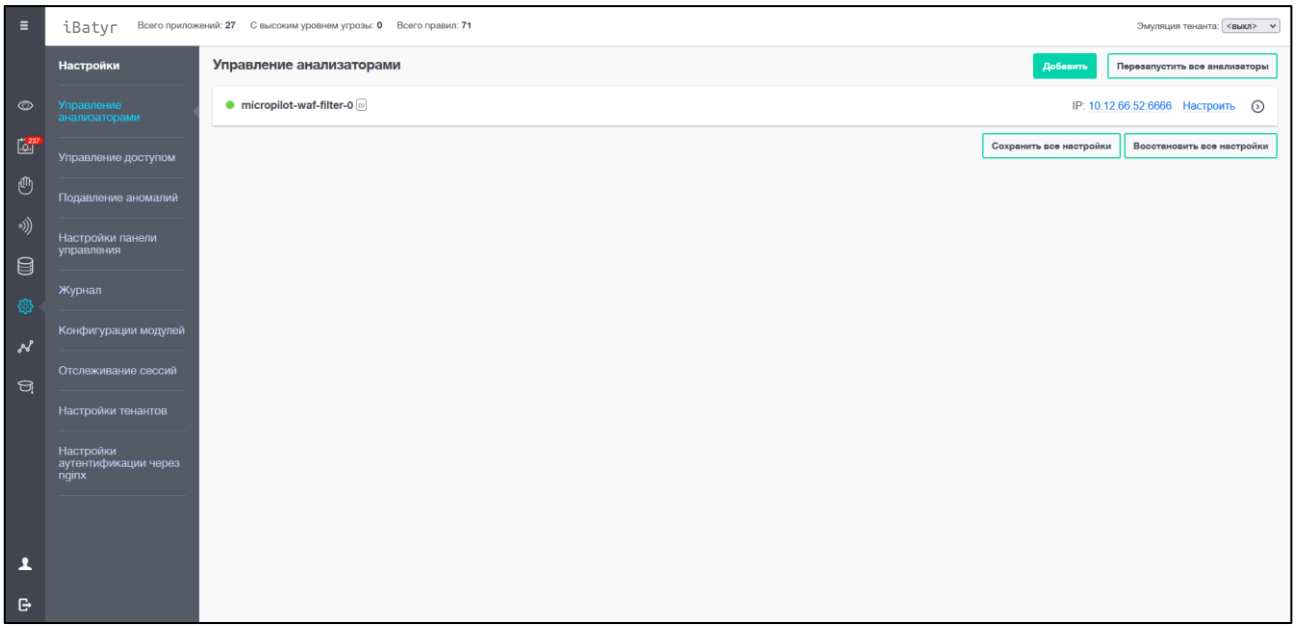

Рисунок 71 – Окно «Настройки»

Для перемещения по вкладкам достаточно нажать левой кнопкой мыши по соответствующему названию в выделенной области. По умолчанию при переходе к окну «Настройки» открывается вкладка «Управление анализаторами».

3.6.1. Вкладка «Управление анализаторами»

Управление анализаторами позволяет остановить или перезапустить отдельные модули анализатора для применения новых настроек, а также перезапустить анализатор. Данная вкладка доступна только пользователям с правами администратора. Вкладка «Управление анализаторами» (см. рисунок 72).

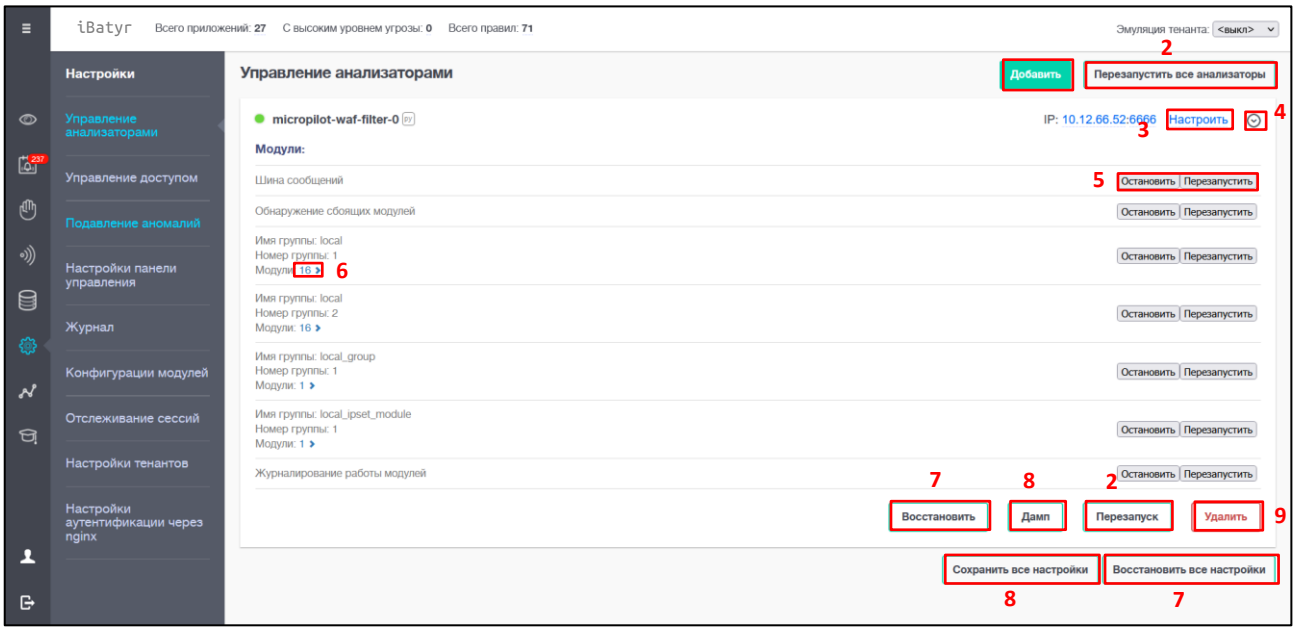

Рисунок 72 – Вкладка «Управление Анализаторами»

1. Добавить – при нажатии на данную кнопку открывается окно «Добавить анализатор» с полями, представленными в таблице 4.

Таблица 4 – Поля окна «Добавить анализатор»

Поле	Описание
Имя	Название для создаваемого анализатора
Хост	Поля для ввода IP-адреса или доменного имени узла, на котором расположен анализатор
Порт	Номер порта анализатора (по умолчанию 6666)
Тип анализатора	Выбор типа анализатора (Python Analyzer\ngWAF)
Создать конфигурацию на основе существующей	Чекбокс, отвечающий за перенос настроек анализатора с уже имеющегося. Если данная настройка выбрана, появятся два дополнительных поля. Анализатор – выбор анализатора, с которого переносить настройки; Ревизия – выбор ревизии настроек анализатора, которую необходимо перенести

2. Перезапустить – перезапускает анализатор. Кнопка «Перезапуск» перезапускает только выбранный анализатор, а кнопка «Перезапустить все анализаторы» перезапускает все анализаторы, которые есть на инсталляции.
3. Настроить – открывается окно настройки анализатора. Подробнее о настройках анализатора написано в разделе 17.

4. Данная кнопка открывает модули и действия с выбранным анализатором.
5. Остановить\перезапустить – действия с модулями анализатора.
6. Возле некоторых моделей имеется выделенная кнопка, позволяющая развернуть список модулей.
7. Восстановить – восстановление настроек анализатора из файла (файл с настройками выгружается в пункте 8). Кнопка «Восстановить» восстанавливает настройки только выбранного анализатора, а кнопка «Восстановить все настройки» восстанавливает настройки всех анализаторов, которые есть на инсталляции.
8. Дамп – делает резервную копию настроек анализатора, которая скачивается в виде файла в формате yaml. Резервная копия сохраняется в соответствии с настройками браузера для загружаемых файлов.
9. Удалить – безвозвратно удаляет выбранный анализатор и его настройки.

3.6.2. Вкладка «Управление доступом»

Администратору доступно добавление и удаление учёных записей пользователей WAF, а также изменение всех параметров учётной записи пользователя. Если на инсталляции включена мультитенантная модель, то в дополнение к ролям «Только для чтения», «Аналитик» и «Администратор» добавляется роль «Супер-администратор».

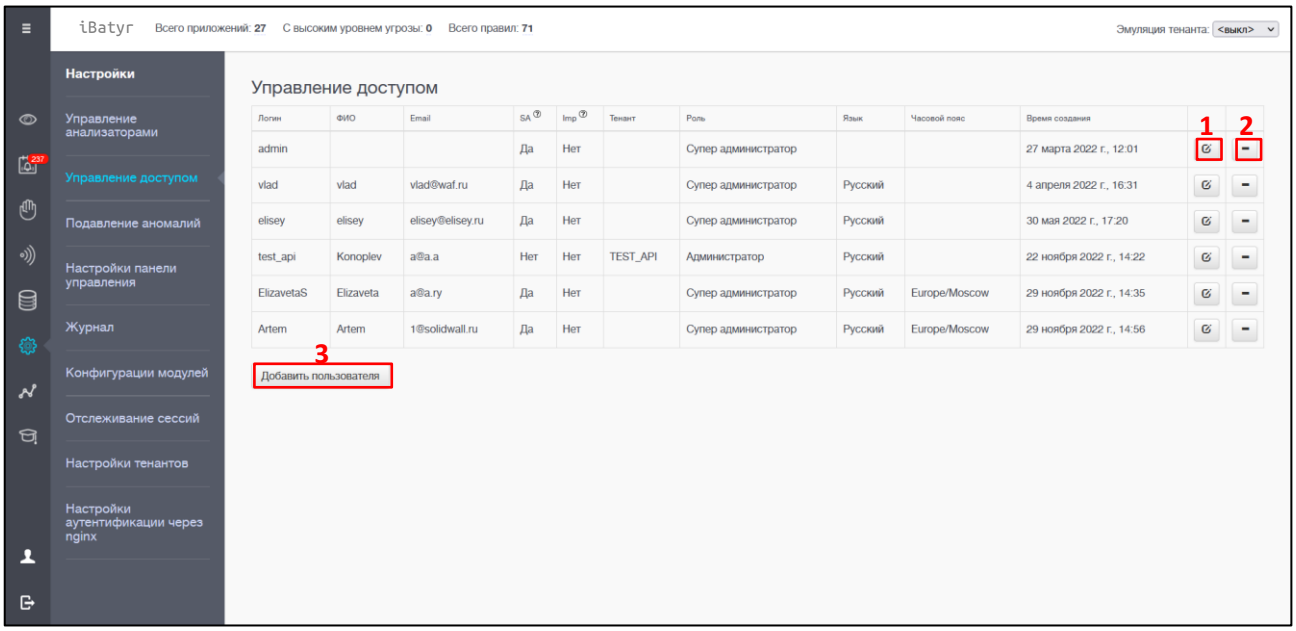

Рисунок 73 – Вкладка «Управление доступом»

1. Изменение – изменения параметров учётной записи пользователя, описание полей, которые можно изменить представлены в таблице 5.
2. Удаление – удаление учетной записи пользователя.
3. Добавить пользователя – при нажатии на данную иконку открывается окно заведения нового пользователя (см. рисунок 74). Описание полей данного окна представлено в таблице 5.

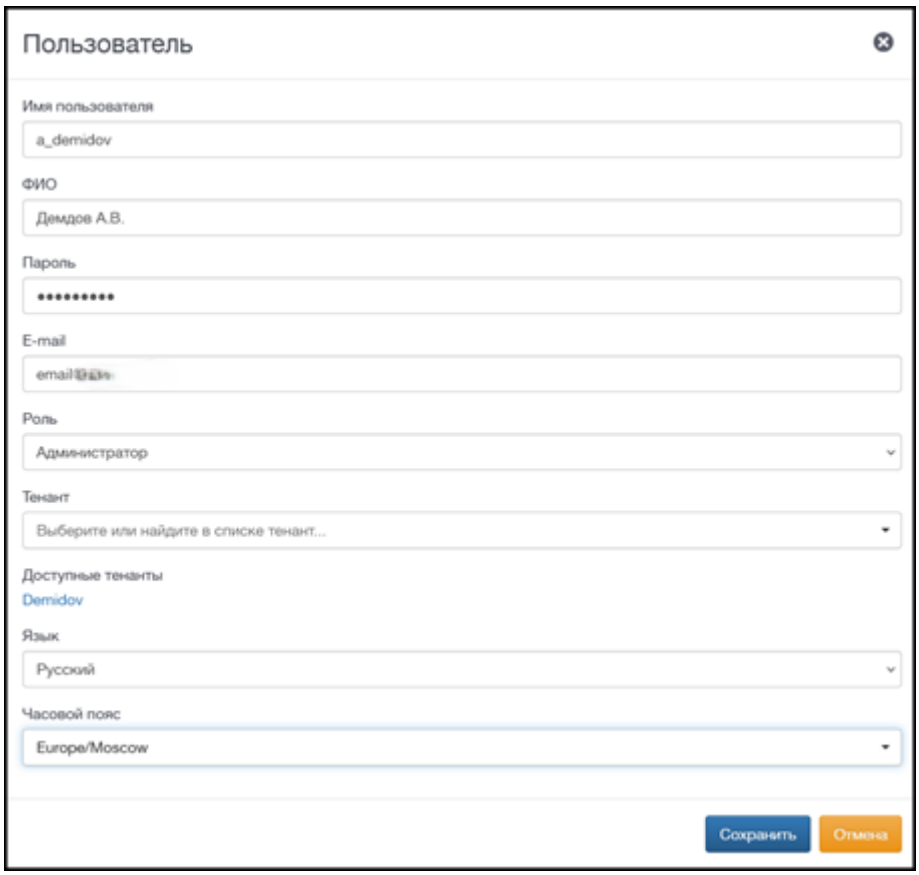

Рисунок 74 – Окно «Пользователь»

Таблица 5 – Описание полей окна «Пользователь»

Поле	Описание
Имя пользователя	Ввод имени пользователя, которое потом будет использовано в качестве логина
ФИО	Фамилия, имя и отчество пользователя
Пароль	Пароль от учетной записи
E-mail	Поле ввода e-mail пользователя
Роль	Выбор одной из трех, или четырех (если включена мультитенантная модель) ролей: Только для чтения – доступен только обзор транзакций, в рамках выбранного тенанта; Аналитик – доступно все, кроме изменения настроек на вкладке настроек в окне «Настройки» (кроме вкладки «Подавление аномалий»), в рамках выбранного тенанта; Администратор – доступны все настройки (кроме настроек анализатора и настроек тенантов), в рамках выбранного тенанта; Супер-администратор – доступны все настройки, в рамках всех тенантов на приложении
Тенант	Выбор одного тенанта из заведенных на инсталляции
Язык	Выбор языка интерфейса из предложенного списка

Поле	Описание
Часовой пояс	Выбор часового пояса. Время в транзакциях будет скорректировано под выбранный часовой пояс

Примечание: пользователи с правами «Супер-администратор» заводятся без указания тенанта, для всех остальных групп пользователей указание тенанта **обязательно,** в случае использования на WAF мульти-тенантной модели.

3.6.3. Вкладка «Подавление аномалий»

На данной вкладке находятся подавленные со всех приложений. Их можно удобно отфильтровать, внести в них изменения или же удалить (см. рисунок 75).

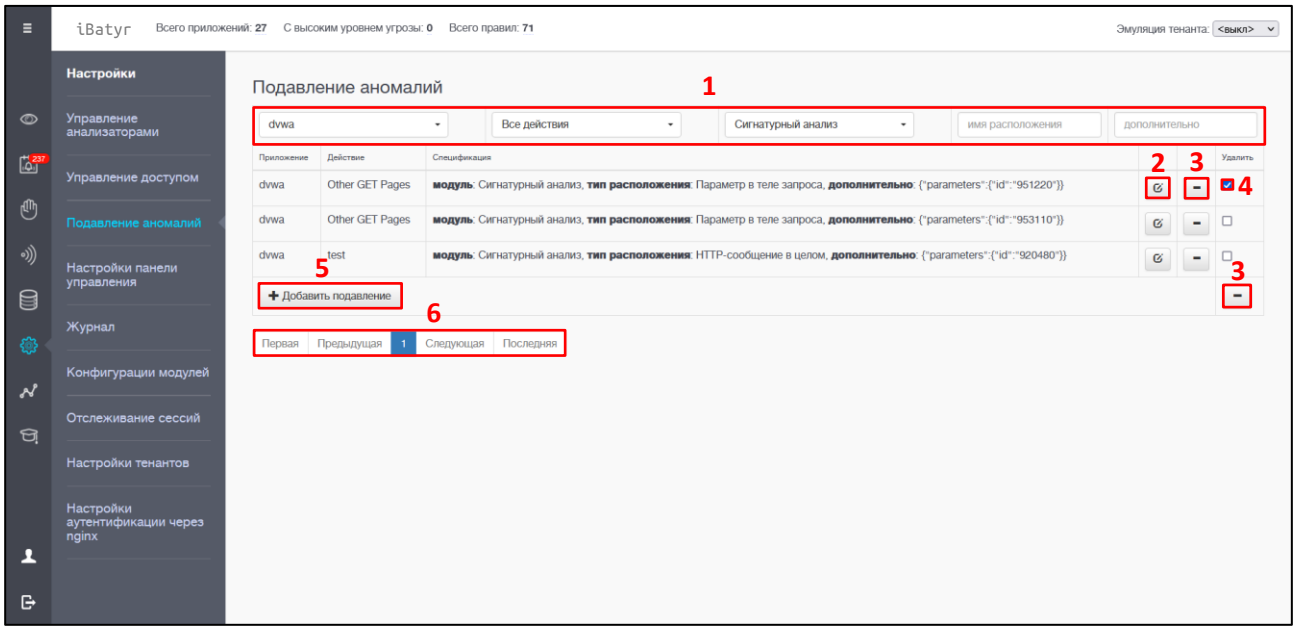

Рисунок 75 – Вкладка «Подавление аномалий»

1. Фильтры подавления аномалий – имеется пять фильтров:
   - Приложения – можно выбрать приложение из тех, которые заведены на инсталляции;
   - Действия – данный фильтр становится активен после выбора приложения. Можно выбрать одно из действий, созданных для выбранного приложения;
   - Выбор модуля анализатора – выбор модуля из выпадающего списка;
   - Имя расположения – ввод имени расположения аномалии;
   - Дополнительно – поле ввода дополнительных параметров.
2. Редактирование – при нажатии на данную кнопку открывается окно редактирования подавления (подробнее о подавлениях написано в разделе 23).
3. Удаление – удаляет выбранное подавление или выбранные подавления.
4. Чекбокс – позволяет выполнить массовое удаление выбранных подавлений.
5. Добавить подавление – открывает окно добавления подавлений (подробнее см. раздел 23);
6. Страницы и перемещение по ним – отображает количество страниц. Перемещаться между страницами можно с помощью кнопок Предыдущая \ Следующая, или выбрав номер страницы.

3.6.4. Вкладка «Настройки панели управления»

Вкладка «Настройка панели управления» включает в себя настройки почты, настройки аутентификации и настройки LDAP (см. рисунок 76).

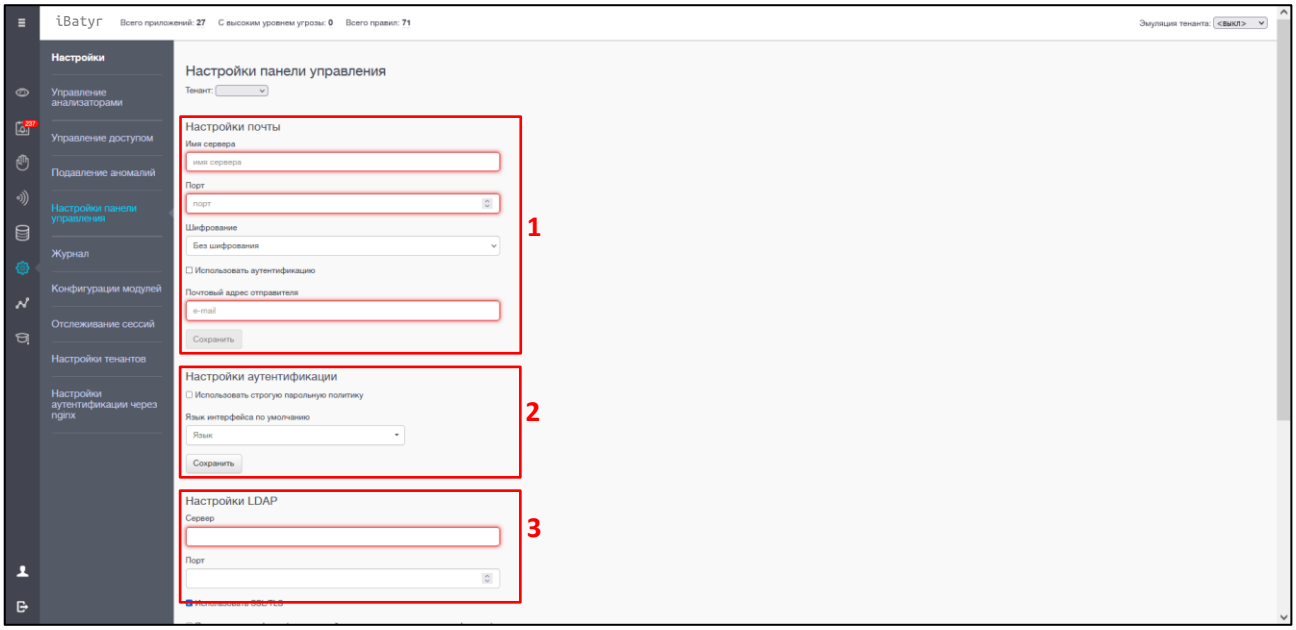

Рисунок 76 – Вкладка «Настройка панели управления»

На данной вкладке имеется возможность выбора тенанта, для которого будут применяться настройки.

1. Настройки почты позволяют настроить данные SMTP-сервера, используемого для отсылки уведомлений. Поля данной настройки описаны в таблице 6.

Таблица 6 – Поля настроек почты

Поле	Описание
Имя сервера	IP-адреса или имени сервера
Порт	Порт сервера
Шифрование	Выбор из трех вариантов: без шифрования, SSL\TLS, STARTTLS
Использовать аутентификацию	Чекбокс, в случае использования аутентификации появляются поля «Имя пользователя» и «Пароль»
Имя пользователя	Логин учетной записи почтового сервиса
Пароль	Пароль от учетной записи почтового сервиса
Почтовый адрес отправителя	Почтовый адрес, с которого будет отправляться корреспонденция

После заполнения данных полей станет активна кнопка «Сохранить».

2. Настройки аутентификации включают настройки парольной политики и настройки языка интерфейса по умолчанию. Поля данной настройки описаны в таблице 7.

Таблица 7 – Поля настроек аутентификации

Поле	Описание
Использовать строгую парольную политику	Чекбокс, в случае использования строгой парольной политики для паролей будут использованы следующие требования: Содержит сочетание букв верхнего и нижнего регистров (например, a-z, A-Z); Включает цифры и знаки пунктуации, например, 0-9, !@#$%^&*()_+|~-=\`{}[[ ]]:«;'<>?,./); Состоит из восьми и более символов
Язык интерфейса по умолчанию	Выбор языка интерфейса из предложенных вариантов по умолчанию

3. Настройки LDAP включает в себя настройки доменного имени или IP-адреса LDAP-сервера, порта LDAP-сервера, имени пользователя и пароля, а также объекта каталога, начиная с которого производится поиск. При установке отметки об использовании шифрования появляются дополнительные поля для настройки. Поля данной настройки описаны в таблице 8.

Таблица 8 – Поля настройки LDAP

Поле	Описание
Сервер	IP-адреса или имени сервера
Порт	Порт сервера
BaseDN	Ввод базы поиска
Фильтр	Фильтр поиска
Login	Ввод атрибута

3.6.5. Вкладка «Журнал»

Журнал позволяет отслеживать действия пользователей WAF. В верхней части окна расположено поле фильтров. Пиктограммы в столбце «Операция» имеют следующие значения:

- – произведено удаление параметров;
- – произведено добавление параметров;
- – параметры отредактированы.

Вкладка «Журнал» изображена на рисунке 77.

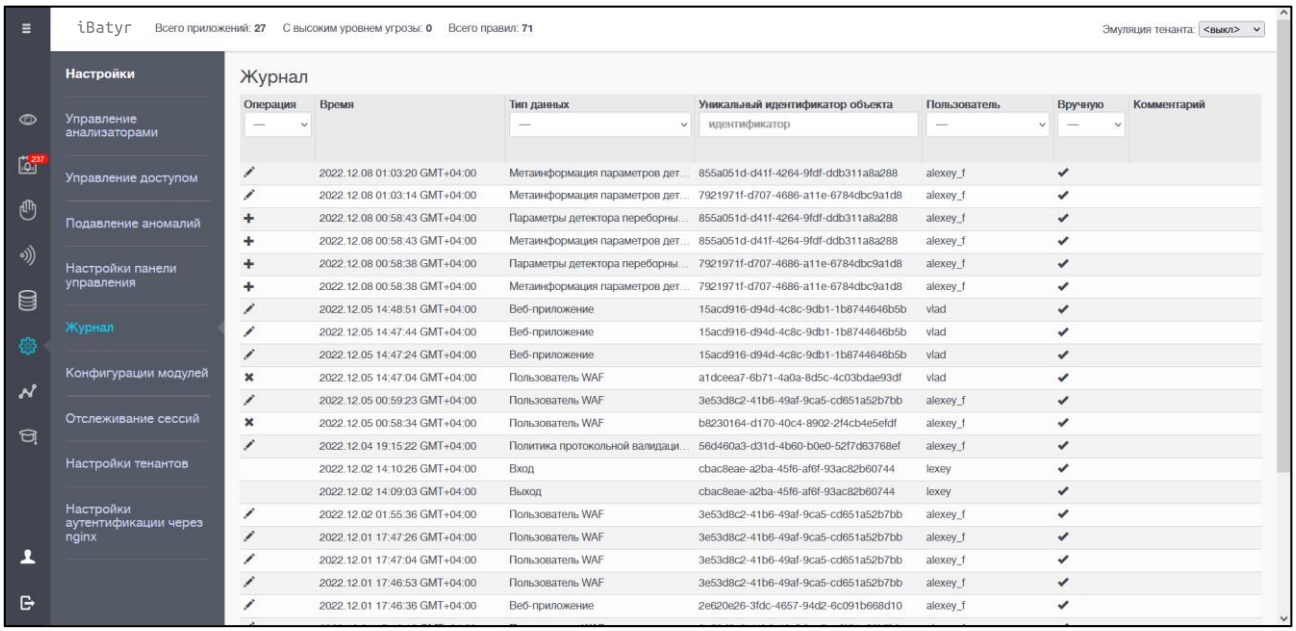

Рисунок 77 – Вкладка «Журнал»

3.6.6. Вкладка «Конфигурации модулей»

На данной вкладке можно обозначить конфигурацию, которую будет использовать модуль Modsecurity, для этого необходимо указать в поле «Конфигурация» настроек модуля имя этой конфигурации, а в поле «Ревизия» номер ревизии (см. рисунок 78). Подробнее о работе с Modsecurity написано в разделе.

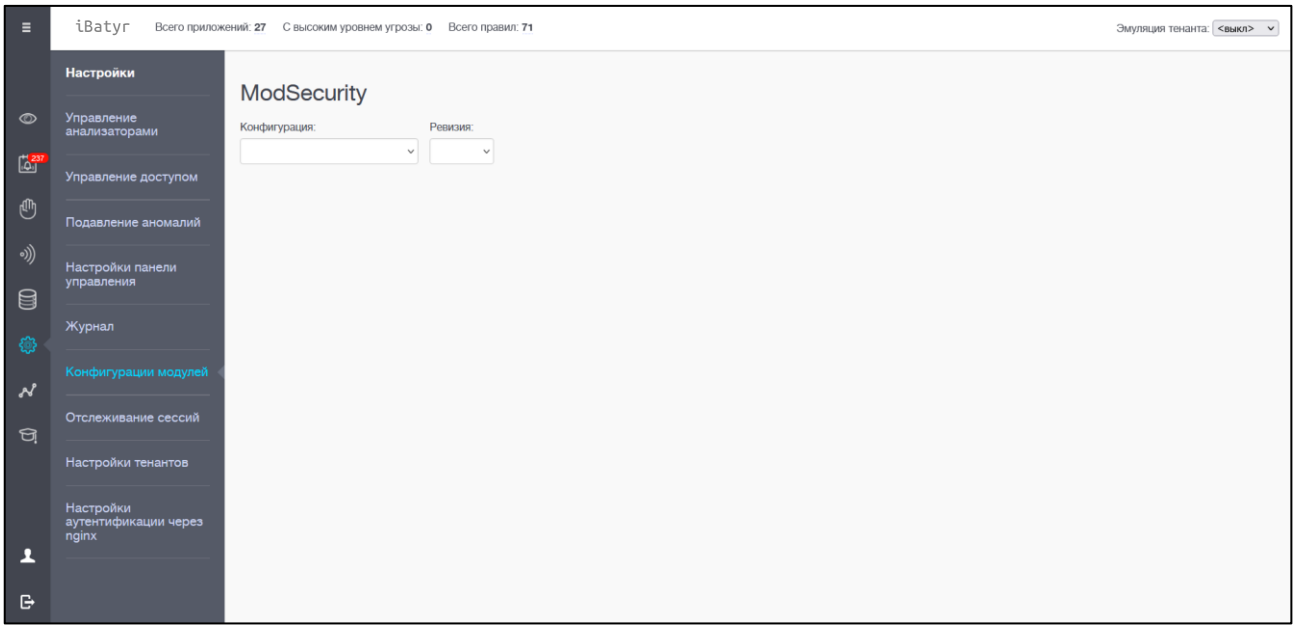

Рисунок 78 – Вкладка «Конфигурации модулей»

3.6.7. Вкладка «Отслеживание сессий»

На данной вкладке находятся все сессионные атрибуты, которые созданы на данной инсталляции. Также находятся сессионные атрибуты по умолчанию.

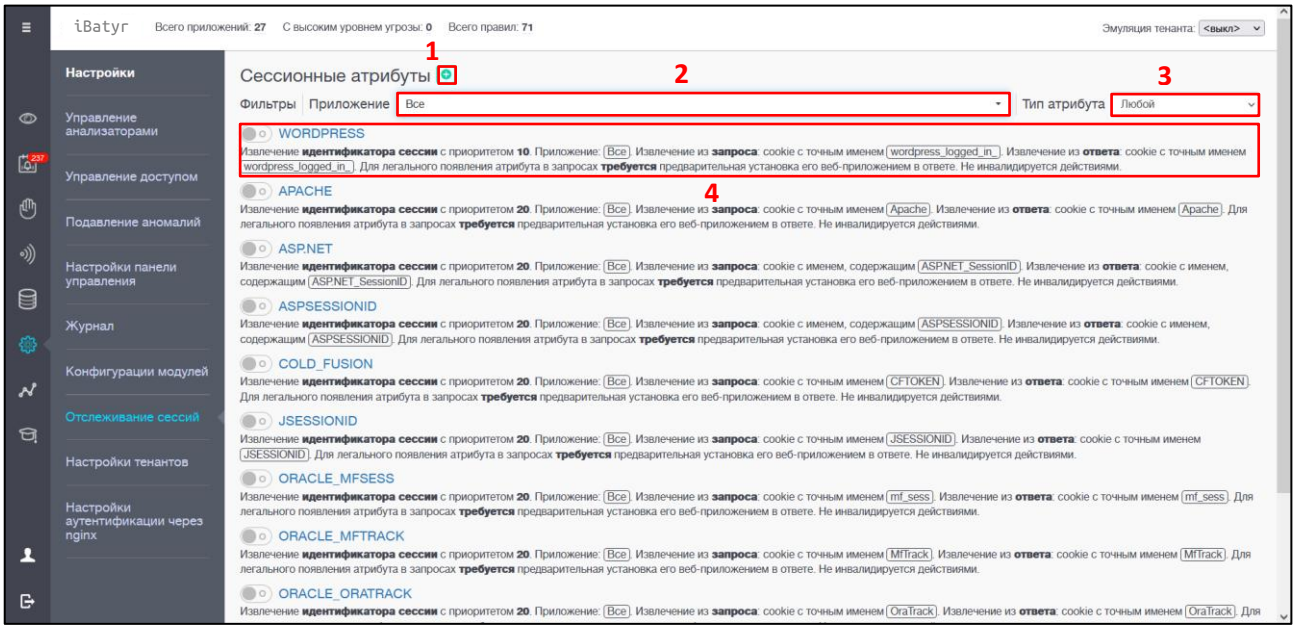

Рисунок 79 – Вкладка «Отслеживание сессий»

1. Добавление сессионного атрибута – при нажатии на выделенную кнопку открывается окно создания сессионного атрибута. Подробнее настройка сессионных атрибутов описана в разделе 18.1.
2. Фильтр по приложениям – выбор одного приложения из списка приложений, заведенных на тенанте или инсталляции.
3. Фильтр по типу атрибута – выбор одного из возможных вариантов типа атрибута.
4. В выделенной области находится сессионный атрибут с его описанием. Имеется возможность выключить  (останется в системе, но не будет использоваться в сессионной модели) или включить  сессионный атрибут. При наведении курсора мыши на название сессионного атрибута, появляется кнопка «Удалить», которая безвозвратно его удаляет. При нажатии левой кнопкой мыши на название сессионного атрибута, открывается окно редактирования настроек сессионного атрибута.

3.6.8. Вкладка «Настройки тенантов»

Данная вкладка доступна только если на приложении включена мультитенантная модель и только пользователям с правами «Супер-администратор». Здесь находятся все тенанты, заведенные на инсталляции (см. рисунок 80).

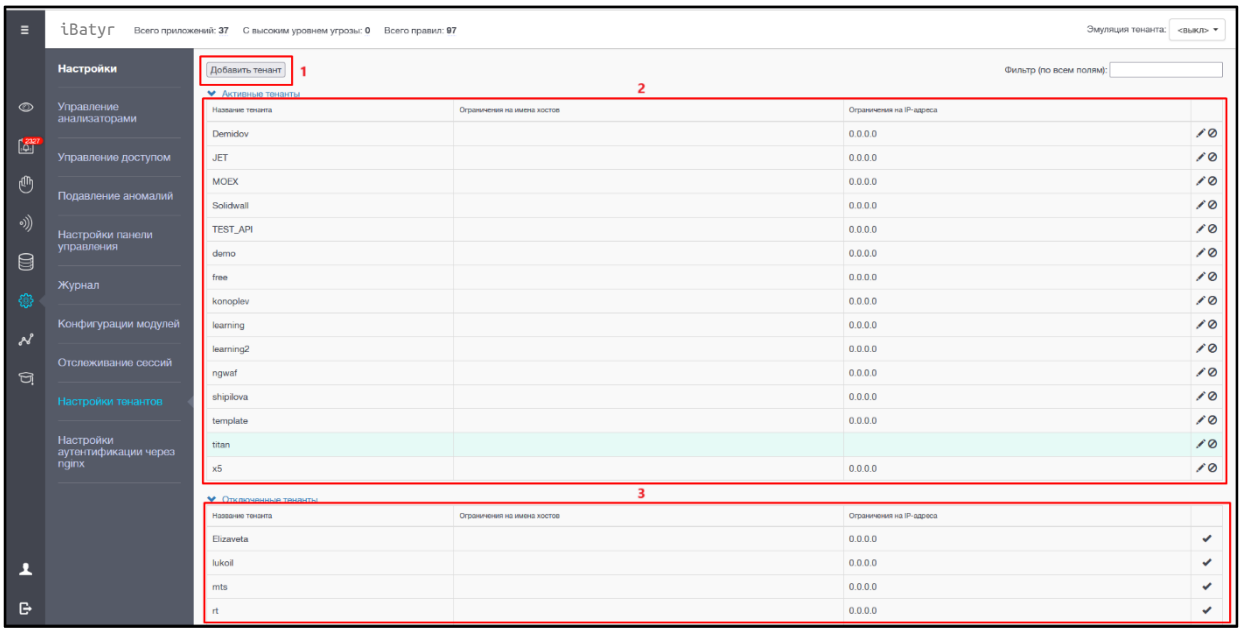

Рисунок 80 – Вкладка «Настройки тенантов»

1. Блок создания или редактирования тенанта. Имеются следующие поля (см. рисунок 81):
   - Название тенанта.
   - Ограничение на имена хостов (в случае отсутствия ограничения, можно не заполнять).
   - Ограничения на IP-адреса (в случае отсутствия ограничения, можно ввести 0.0.0.0).

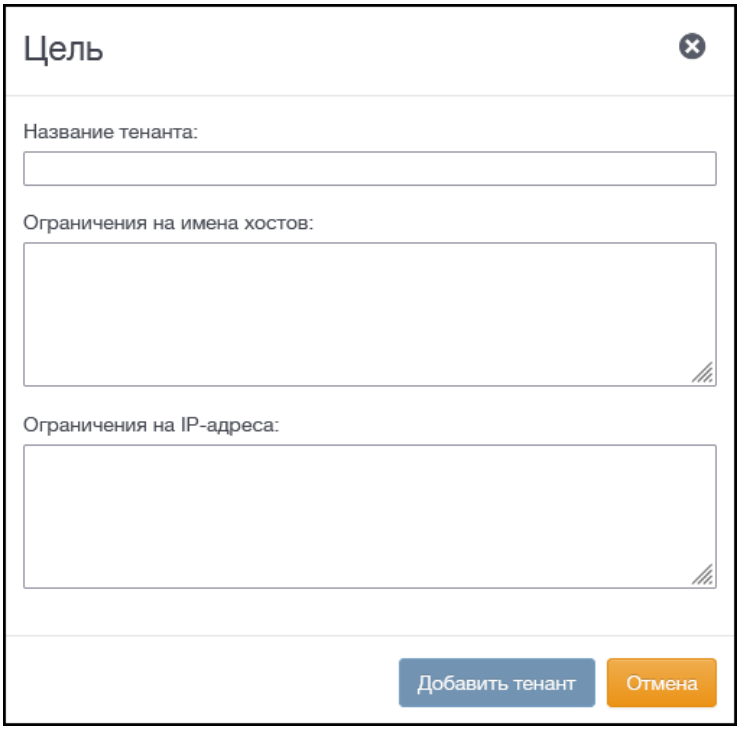

Рисунок 81 – Создание тенанта

2. В данном блоке отображаются все активные тенанты. Их можно отредактировать, нажав на кнопку напротив нужной строки, тогда настройки тенанта отобразятся в блоке 1. Также имеется возможность отключения тенанта нажатием кнопки , тогда тенант переносится в блок 3, а все приложения тенанта переходят в нераспределенные по тенантам.

3. В данном блоке находятся все отключённые тенанты. Тенанты невозможно удалить из веб-интерфейса.

3.6.9. Вкладка «Настройки аутентификации через nginx»

На вкладке можно добавить пользователя защищаемого приложения, а также изменить пароли существующим, очистить сессии пользователей или удалить пользователей (см. рисунок 82).

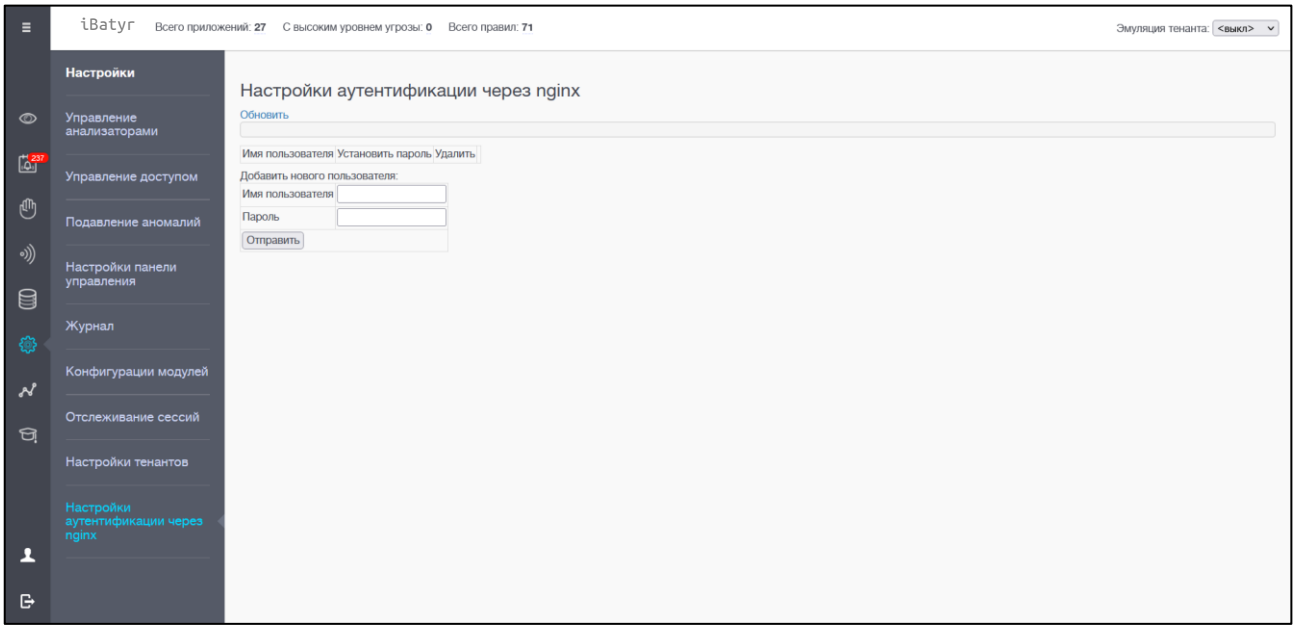

Рисунок 82 – Вкладка «Настройки аутентификации через nginx»

3.7. Окно «Отчеты»

На данной вкладке можно формировать отчеты о событиях безопасности для приложений инсталляции или тенанта. Каждый отчет содержит следующую информацию:

- Обзор – в данном разделе отчета содержится информация в графическом виде и содержит следующие подразделы:
  - Статусы – график в подразделе «Статусы» показывает статистику ответов веб-сервера по классам кодов состояния HTTP (англ. HTTP status code). Код состояния HTTP – это целое число из трёх десятичных цифр, которое обозначает результат выполнения запроса и определяет, какие действия ему предпринимать дальше. Набор кодов состояния является стандартом, и описан в соответствующих документах RFC. Первая цифра указывает на класс состояния.
  - Блокировки – данный график отображает статистику по решениям, принятым в отношении транзакций, поступающих на защищаемое приложение. Возможными вариантами решений являются следующие: пропустить транзакцию, заблокировать запрос, заблокировать (переписать) ответ.
  - Задержки – данный график показывает задержку отправки ответа защищаемым приложением после получения запроса. Такая статистика важна в том числе и с точки зрения информационной безопасности. Например, пики на графике задержки приложения могут свидетельствовать о попытках поиска или эксплуатации уязвимостей, нагружающих приложение необычным образом.

– Враждебность – данный график отображает интегральный показатель «враждебности», значение которого характеризует степень аномальности трафика приложения в данный момент времени. Показатель измеряется в процентах и вычисляется по следующей формуле:

```
1/2 * [(количество атак за последнюю минуту) / (количество транзакций за последнюю минуту) + (количество атак за последнюю минуту) / (максимальное количество атак за минуту в прошлом)]
```

- Общая статистика по трафику приложения - в данном разделе приводится общая статистика работы приложения. Включает в себя информацию о распределении транзакций по географическому расположению источников, по видам аномалий, по действиям приложения.
- События безопасности – включает информацию о событиях безопасности с количеством попавших под них транзакций.

Окно «Отчеты» представлено на рисунке 83.

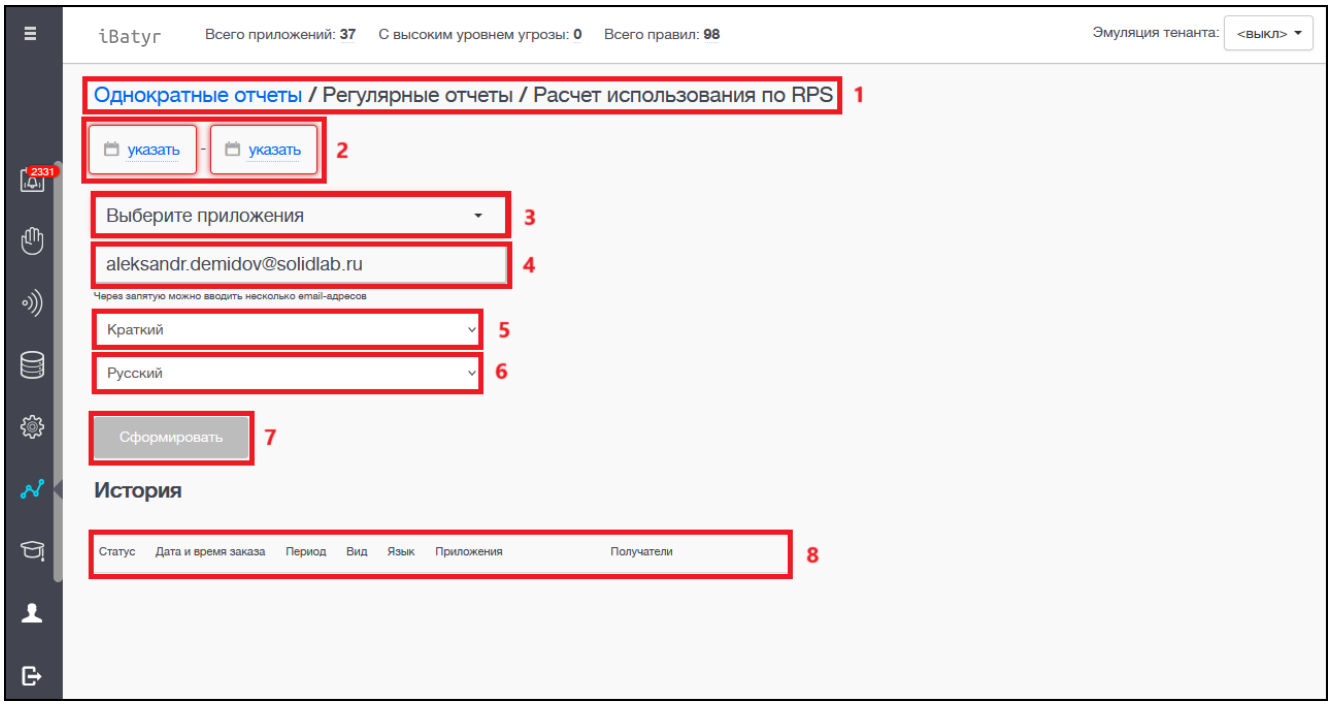

Рисунок 83 – Окно «Отчеты»

1. Однократные отчеты\Регулярные отчеты\Расчет по использованию RPS – выбор вида отчета. В случае выбора однократного отчета, отчет формируется однократно исходя из заданного в блоке 2 периода. В случае выбора регулярного отчета, отчет формируется отчет формируется автоматически в конце указанного периода (см. рисунок 84). В случае выбора «Расчета использования по RPS» отчет формируется на основе 95-го персентиля на основе данных о среднем значении RPS при разбиении заданного промежутка времени на 5-минутные интервалы и выбранного периода (см. рисунок 85).

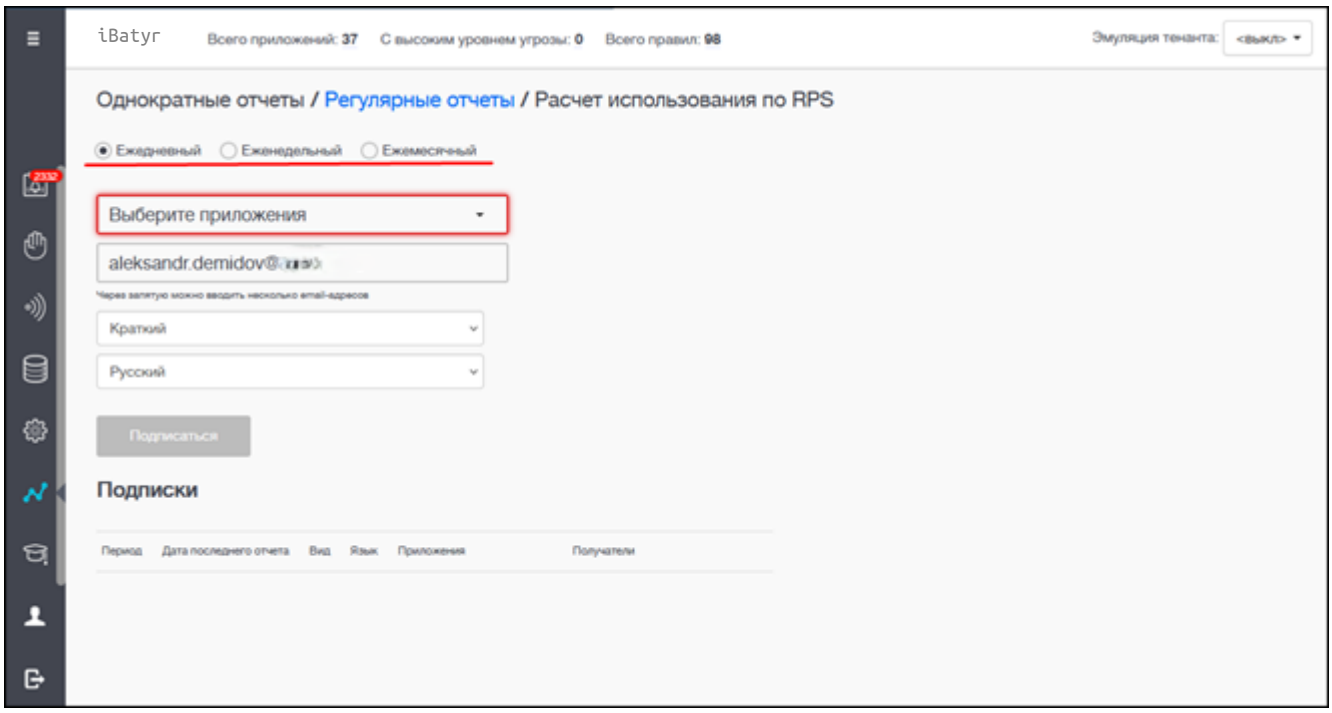

Рисунок 84 – Регулярные расчеты

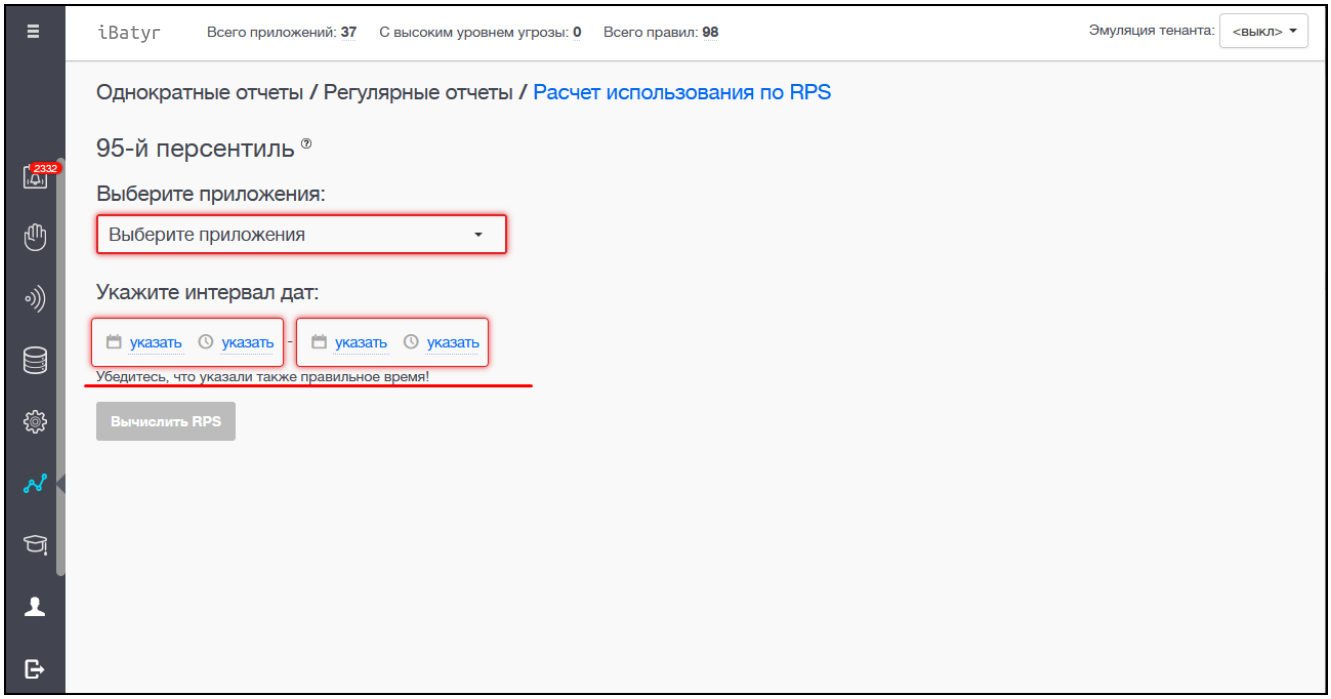

Рисунок 85 – Расчет использования по RPS

2. Период – задается период, за который будет формироваться отчет.
3. Выбор приложения – можно выбрать одно, или несколько приложений, по которым будет формироваться отчет.
4. Поле ввода e-mail – поле ввода одного или нескольких e-mail (через запятую), на которые будет отправляться сформированный отчет (в случае если настроен SMTP сервер).
5. Выбор формата отчета – есть два вида формата отчета:

   – Краткий – выводится только описанная выше информация.

– Полный – в дополнение к информации из краткого отчета более подробная статистика по событиям безопасности, обнаруженным системой на основе правил реагирования. Каждое событие безопасности включает в себя одно или несколько срабатываний правил реагирования одного типа. Период, за который однотипные срабатывания группируются в одно событие, определяется системой автоматически. Также событие может быть «закрыто» администратором вручную - в таком случае оно переносится в архив, а аналогичные срабатывания будут формировать уже новое событие. Для каждого события приводится следующая информация:

  - Название события. Например, это может быть название правила, срабатывание которого регистрировалось в рамках данного события.
  - Уровень. Уровень опасности события – «Инфо», «Низкий», «Средний», «Высокий» или «Критический».
  - Период (время жизни события), в течение которого однотипные срабатывания относились к данному событию.
  - Количество транзакций. Показывает какое количество транзакций было зарегистрировано в рамках данного события (сколько раз сработало правило).
  - Статистика по источникам события (IP-адреса, автономные системы, страны, пользователи).
  - Статистика по аномалиям (по видам аномалий и сработавшим анализаторам).
  - Статистика по целям (действиям) в приложении.

6. Язык – выбор языка, на котором будет формироваться отчет.
7. Сформировать – при нажатии на данную иконку начинает формироваться отчет по заданным параметрам. Не активна пока не выбрано приложение и период.
8. История – в данной области отображены последние из выгруженных отчетов. Также отсюда их можно скачать.

3.8. Окно «Помощь»

На данной вкладке располагается информация о версиях анализатора, Nginx и Suricata. Также там указаны даты обновления версий (см. рисунок 86).

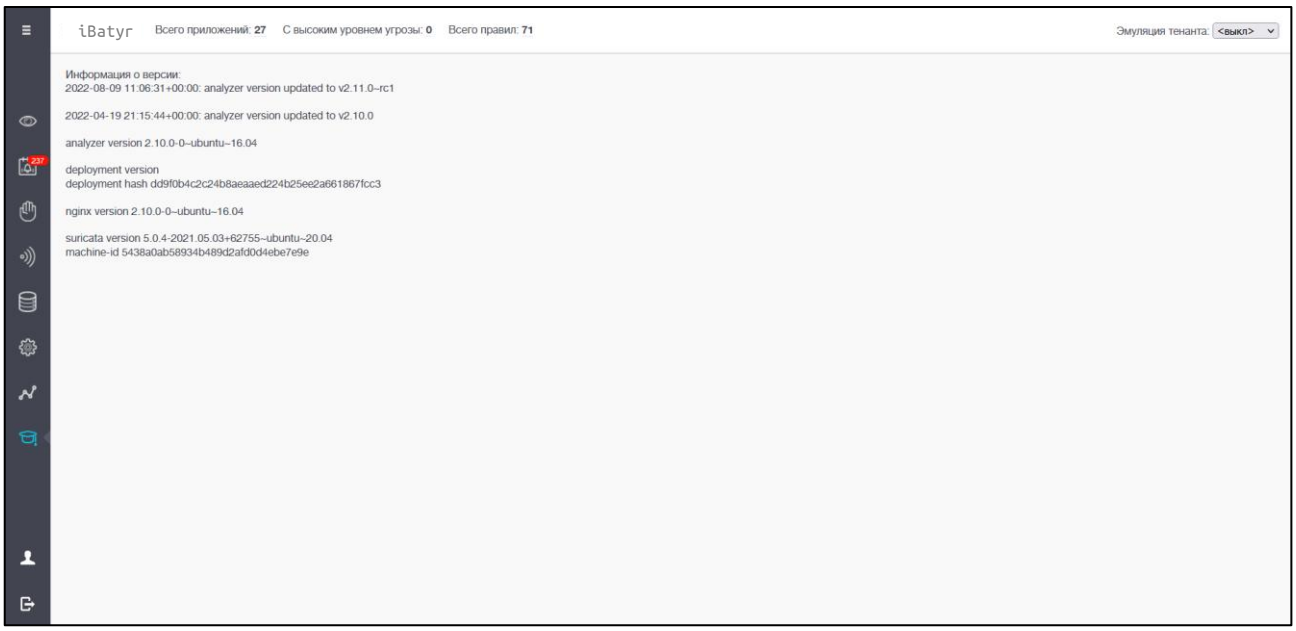

Рисунок 86 – Окно «Помощь»

3.9. Окно «Настройки учетной записи»

На данной вкладке можно изменить данные своей учетной записи, сменить пароль и настроить оповещение о срабатывании правил (см. рисунок 87).

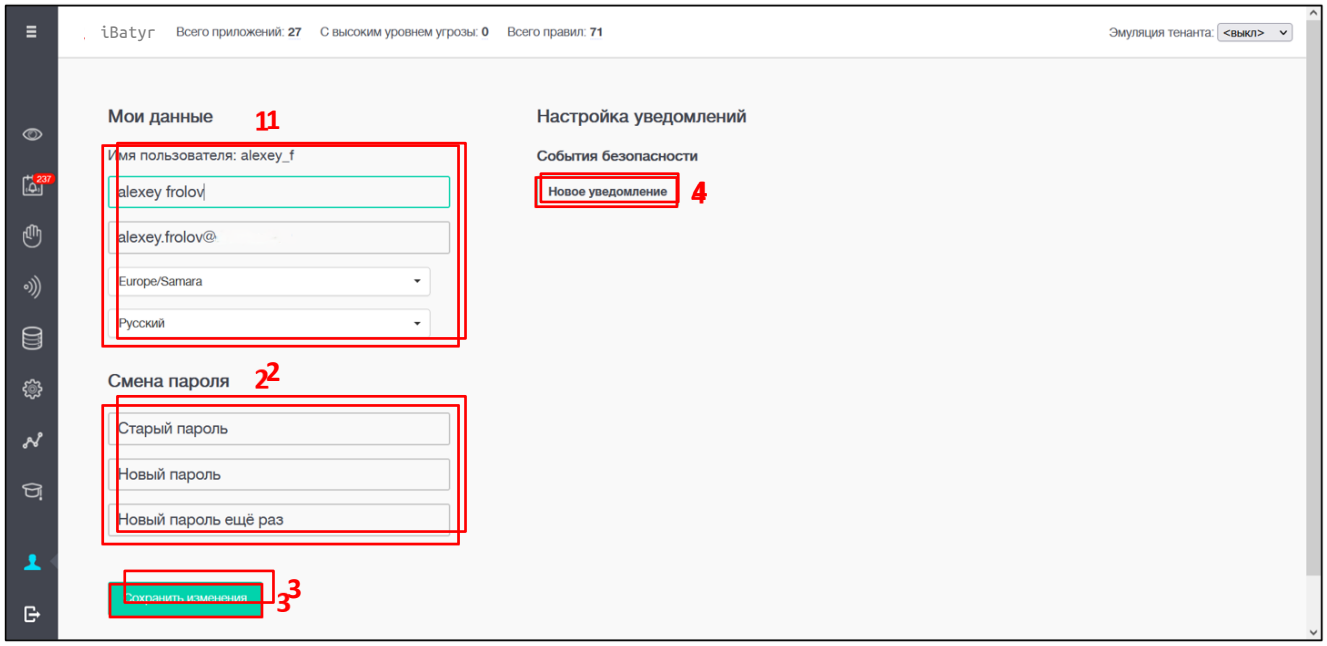

Рисунок 87 – Окно «Настройки учетной записи»

1. Мои данные – в данной области можно изменить ФИО, E-mail, часовой пояс и язык интерфейса для учетной записи, под которой вы работаете. После внесения изменений, если их необходимо сохранить, нужно нажать на иконку «Сохранить изменения» (блок 3).
2. Смена пароля – область смены пароля. Для смены пароля необходимо ввести свой старый пароль и дважды заполнить свой новый пароль. После внесения изменений, если их необходимо сохранить, нужно нажать на иконку «Сохранить изменения» (блок 3).
3. Сохранить изменения – сохраняет изменения, введенные в блоках 1 и 2.
4. Новое уведомление – при нажатии на выделенную иконку, открывается окно «Редактирования уведомления», в котором можно настроить уведомление по почте при срабатывании выбранного правила, как в рамках всей инсталляции, так и в рамках отдельных приложений.

4. Добавление конфигурационного файла NGINX

4.1. Настройка проксирования

Все файлы конфигурации должны храниться в каталоге /etc/ibatyr-nginx/sites-available. Ключи и TLS-сертификаты должны храниться в каталоге /etc/ibatyr-nginx/ssl. Новый конфигурационный файл рекомендуется создавать по имени приложения. Конфигурация файла состоит из блока\блоков **server**. Пример конфигурации:

```
server {
    include static/server.conf;
    listen 80;
    server_name example.com www.example.com;
    # WAF configuration.
    set $BACKEND http://192.168.1.100;
    location / {
        include static/waf.conf;
    }
}
server {
    include static/server.conf;
    listen 443 ssl;
    ssl_certificate ssl/cert.crt;
    ssl_certificate_key ssl/cert.key;
    server_name example.com www.example.com;
    # WAF configuration.
    set $BACKEND https://192.168.1.100:443;
    location / {
        include static/waf.conf;
    }
}
```

Директива **listen** содержит параметры с номером порта, на который будет проксироваться бэкенд. Параметр **ssl** у данной директивы указывает на то, что трафик должен быть доступен по HTTPS.

Директивы **ssl_certificate*** в своих параметрах содержат пути к файлам с ssl-сертификатами и ключами. Это необходимо для того, чтобы терминировать зашифрованный TLS трафик до его попадания на iBatyr WAF.

Директива **server_name** содержит доменные имена (заголовок **Host**), на которые будут идти запросы. Стоит отметить, что необходимо указать все доменные имена приложения, например, www.example.com, example.com. В противном случае часть запросов может быть обработана некорректно.

В параметре директивы **set $BACKEND** передается полный адрес бэкенда с указанием протокола и номера порта.

4.2. Применение конфигурации

После создания файла конфигурации на него необходимо создать символическую ссылку в каталог /etc/ibatyr-nginx/sites-enabled/ для активации конфигурации. Например, для файла конфигурации example.com это можно сделать с помощью команды:

```
ln -s /etc/ibatyr-nginx/sites-available/example.com /etc/ibatyr-nginx/sites-enabled/example.com
```

Далее необходимо обязательно проверить корректность синтаксиса командой:

```
ibatyr-nginx test
```

Положительный ответ представлен на рисунке 88.

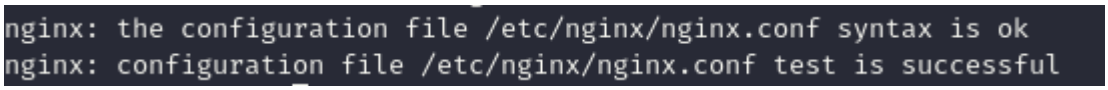

Рисунок 88 - Ответ на транзакцию

В случае получения положительного ответа можно применить конфигурацию (стоит отметить, что данный способ перезагрузки конфигурации NGINX не приводит к разрыву текущих соединений, и может быть применен на уже работающем в боевой среде сервере):

```
ibatyr-nginx reload
```

4.3. Проверка проксирования

Для проверки корректности настроенного проксирования необходимо сравнить ответы на запросы к защищаемому приложению направленные на бэкенд напрямую и через WAF. В обоих случаях ответы должны совпадать. Отправлять запросы можно любым удобным способом. Например, при помощи браузера, для чего необходимо настроить разрешение доменного имени проверяемого приложения в файле **hosts** операционной системы, или при помощи утилиты `curl` непосредственно в консоли сервера WAF.

5. Добавление приложений в веб-интерфейсе iBatyr WAF

5.1. Создание приложения

После того как выполнены настройки проксирования, необходимо завести само приложение в веб-интерфейсе iBatyr WAF.

Для этого зайдите на веб-интерфейс iBatyr WAF (например, https://ip_waf:8443/, авторизуйтесь, после чего выберите в левом навигационном меню «Приложения» -> «Добавить приложение». В появившемся окне укажите название приложения (см. рисунок 89).

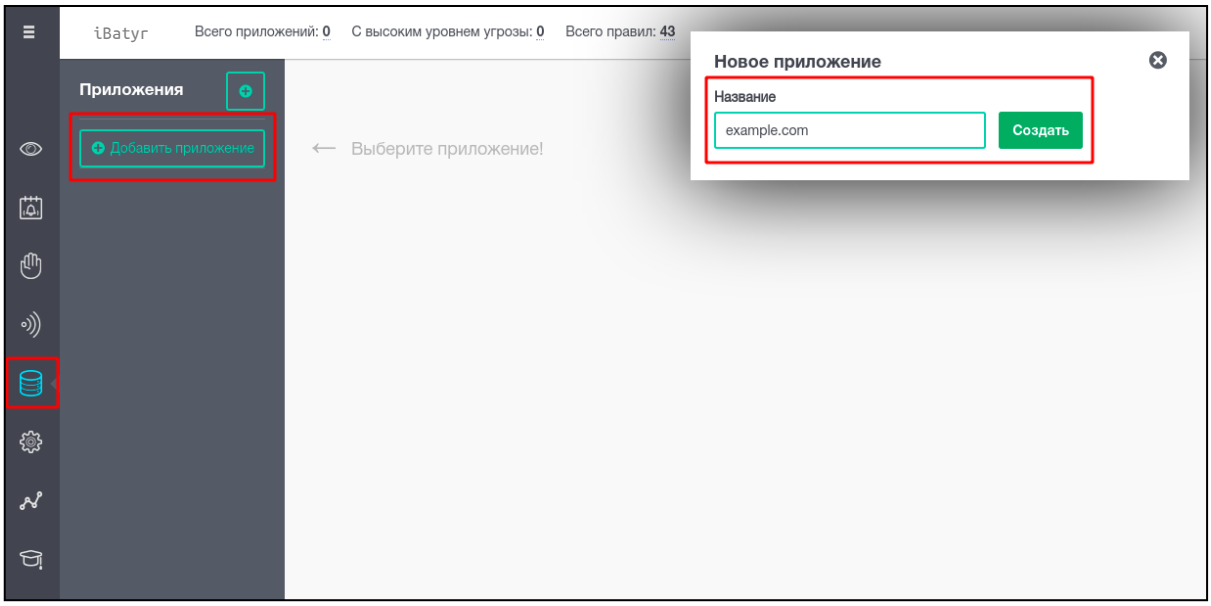

Рисунок 89 – Создание приложения.

5.2. Добавление «троек»

После того, как новое приложение было создано, для него необходимо указать «тройки» (см. рисунок 90).

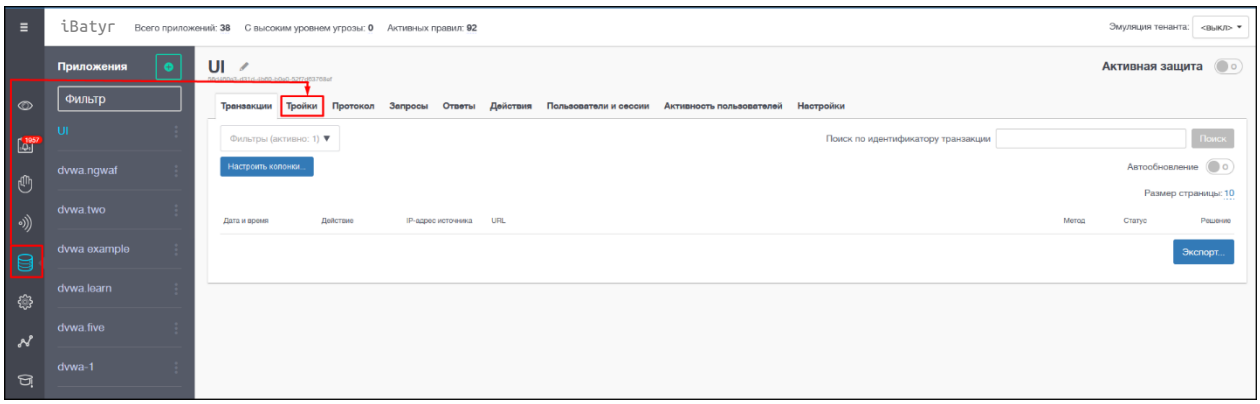

Рисунок 90 - «Тройки»

На данной вкладке находится список «троек» – совокупностей доменного имени веб-приложения, IP-адреса и порта WAF, на которые поступает трафик. «Тройки» позволяют сопоставлять трафик,

приходящий на WAF с конкретным защищаемым приложением. Добавить «тройки» можно двумя способами: «Добавить из списка» и «Добавить вручную» (см. рисунок 91).

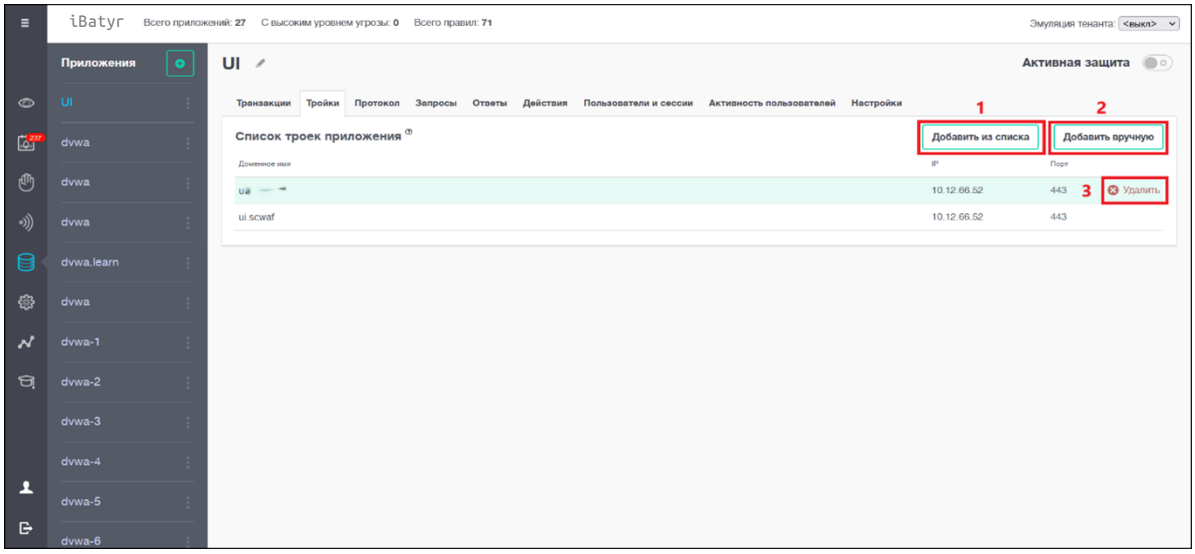

Рисунок 91 – Добавление «троек»

1. Добавить из списка – при нажатии на данную иконку появится вкладка, на которой можно увидеть те адреса\имена, трафик с которых был зафиксирован на WAF (см. рисунок 92).

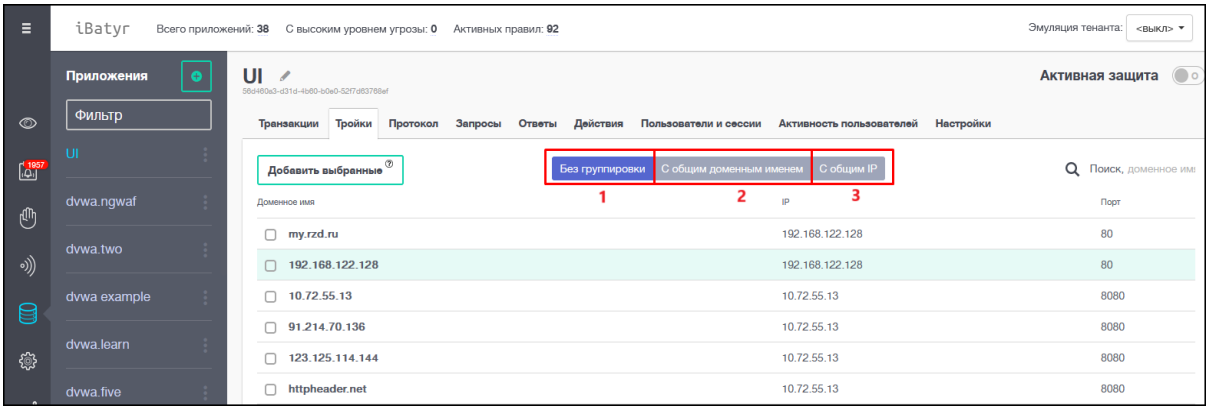

Рисунок 92 – Добавление «троек» из списка

1.1. Без группировки - по умолчанию в списке представлен перечень всех «троек», трафик с которых был зафиксирован на WAF, без группировки (см. рисунок 92).

1.2. С общим доменным именем – при нажатии на данную иконку, список будет представлен в виде значений, сгруппированных по доменному имени (см. рисунок 93).

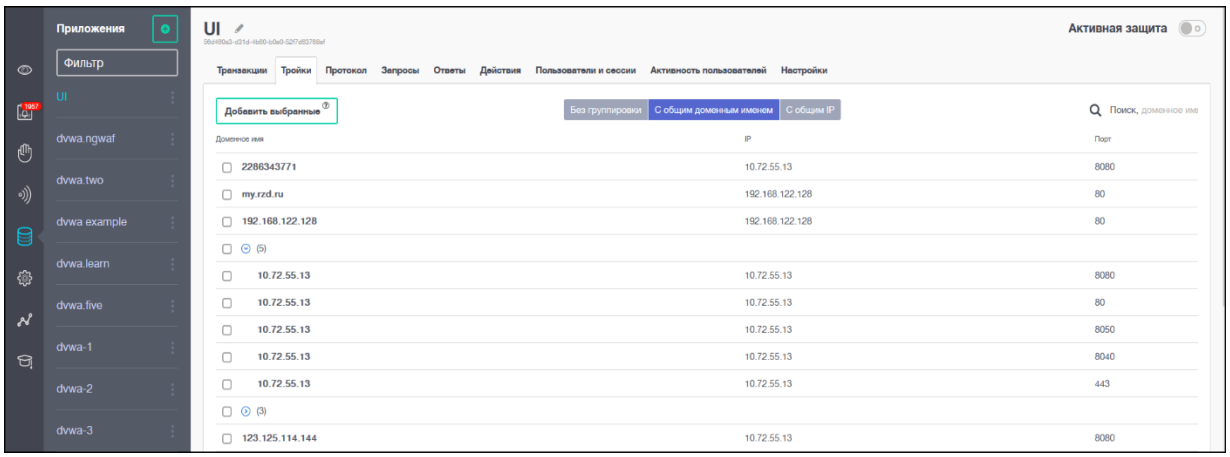

Рисунок 93 – С общим доменным именем

1.3. С общим IP – при нажатии на данную иконку, список будет представлен в виде значений, сгруппированных по доменному имени (см. Рисунок 94).

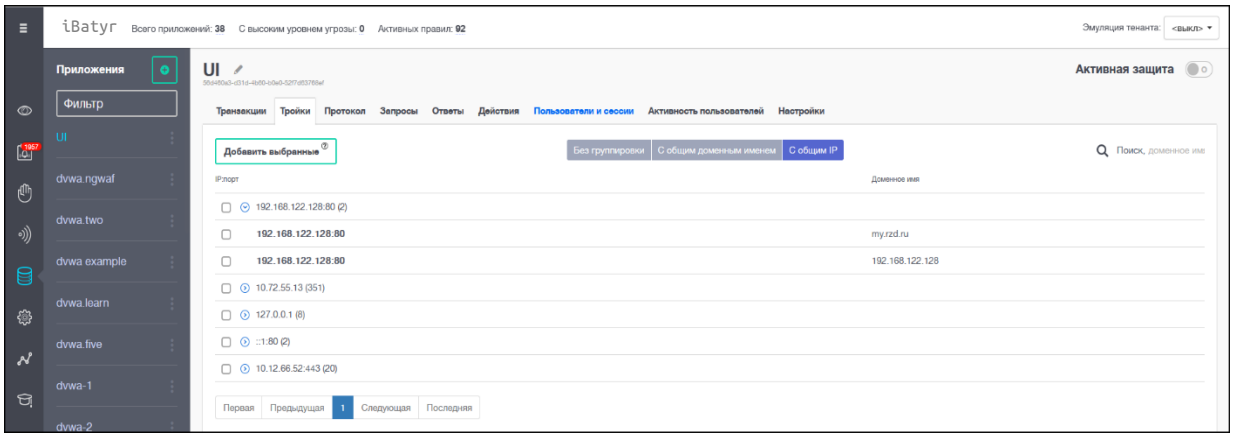

Рисунок 94 – С общим IP

2. Добавить вручную – при нажатии на данную иконку появится окно с вводом доменного имени, адреса и порта (см. рисунок 95).

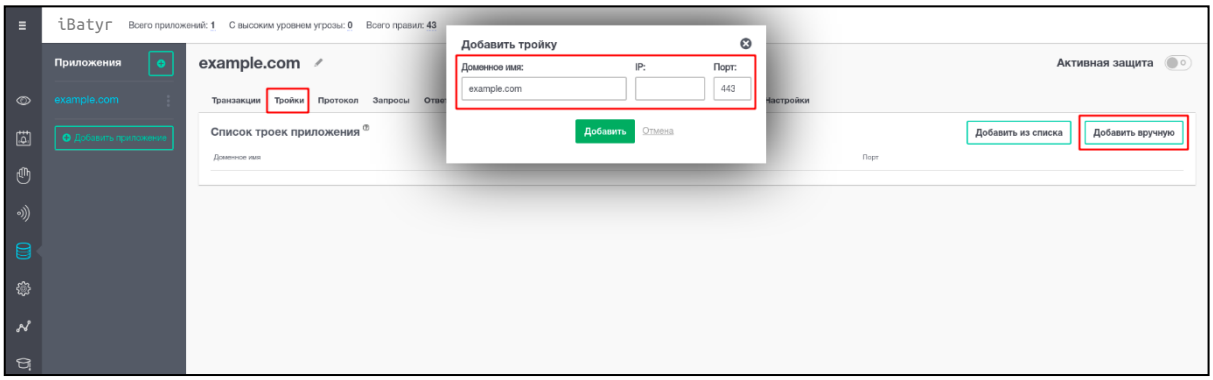

Рисунок 95 – Добавление «троек» вручную

Укажите доменное имя защищаемого приложения и порт для приема трафика на WAF. IP-адрес указывать не нужно. Данную операцию необходимо проделать для всех доменных имен и поддоменов, а также портов, которые были добавлены в файл конфигурации ibatyr-nginx (см. рисунок 96).

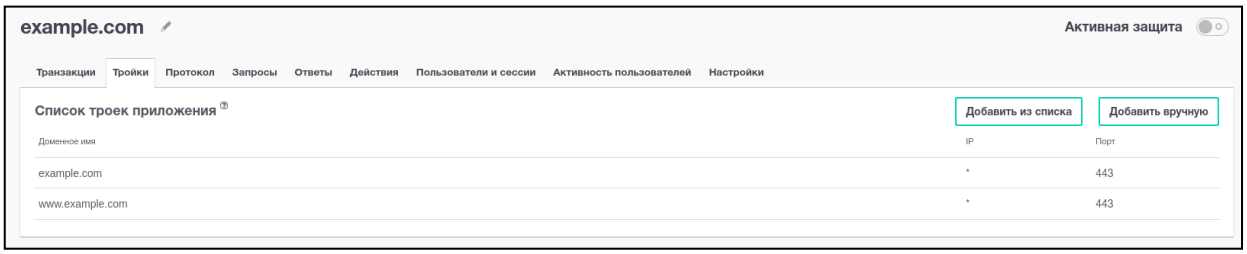

Рисунок 96 – Добавленные «тройки»

6. Настройка мультитенантной модели

Мультитенантная модель – предоставляет возможность распределения приложений инсталляции по отдельным и изолированным областям (тенантам). Источники, списки, цели, правила, сессионные атрибуты, созданные пользователем одного тенанта, не видны пользователям другого тенанта, за исключением атрибутов, настроенных на WAF по умолчанию (из коробки), а также атрибутов, созданных супер-администратором без указания тенанта.

Супер-администратору доступна возможность просматривать все приложения инсталляции, не зависимо от того, какому тенанту они принадлежат.

Для включения мультитенантной модели на инсталляции на узле управления (мастере в случае отказоустойчивой конфигурации) необходимо выполнить следующие команды:

```
sudo -u waf psql
update "user" set role = 'super_admin' where id = 1;

sudo systemctl restart ibatyr-dashbord
```

Для включения мультитенантной модели для отказоустойчивой конфигурации на мастере необходимо выполнить следующую команду:

```
sudo crm resource restart ibatyr-dashboard
```

7. Просмотр транзакций

Для просмотра деталей транзакции необходимо кликнуть по выбранной транзакции дважды левой кнопкой мыши (см. рисунок 97).

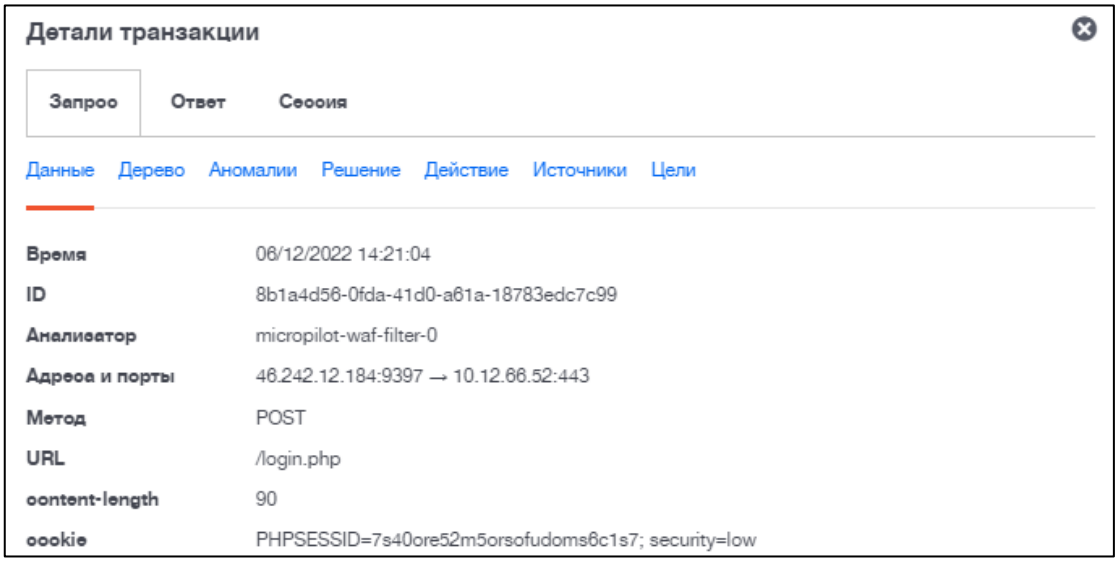

Рисунок 97 – Детали транзакции

Окно деталей транзакции делится на три вкладки: запрос, ответ и сессия, подробное описание которых дано в следующих разделах (см. разделы 7.1, 7.2 и 7.3).

7.1. Вкладка «Запрос»

На данной вкладке отображается подробная информация о запросе (см. рисунок 98). Также есть возможность обновить информацию о статических ресурсах на основе этой транзакции, нажав на кнопку Обновить настройки статических ресурсов на основе этой транзакции. Подробнее механизм статических ресурсов описан в разделе 8.

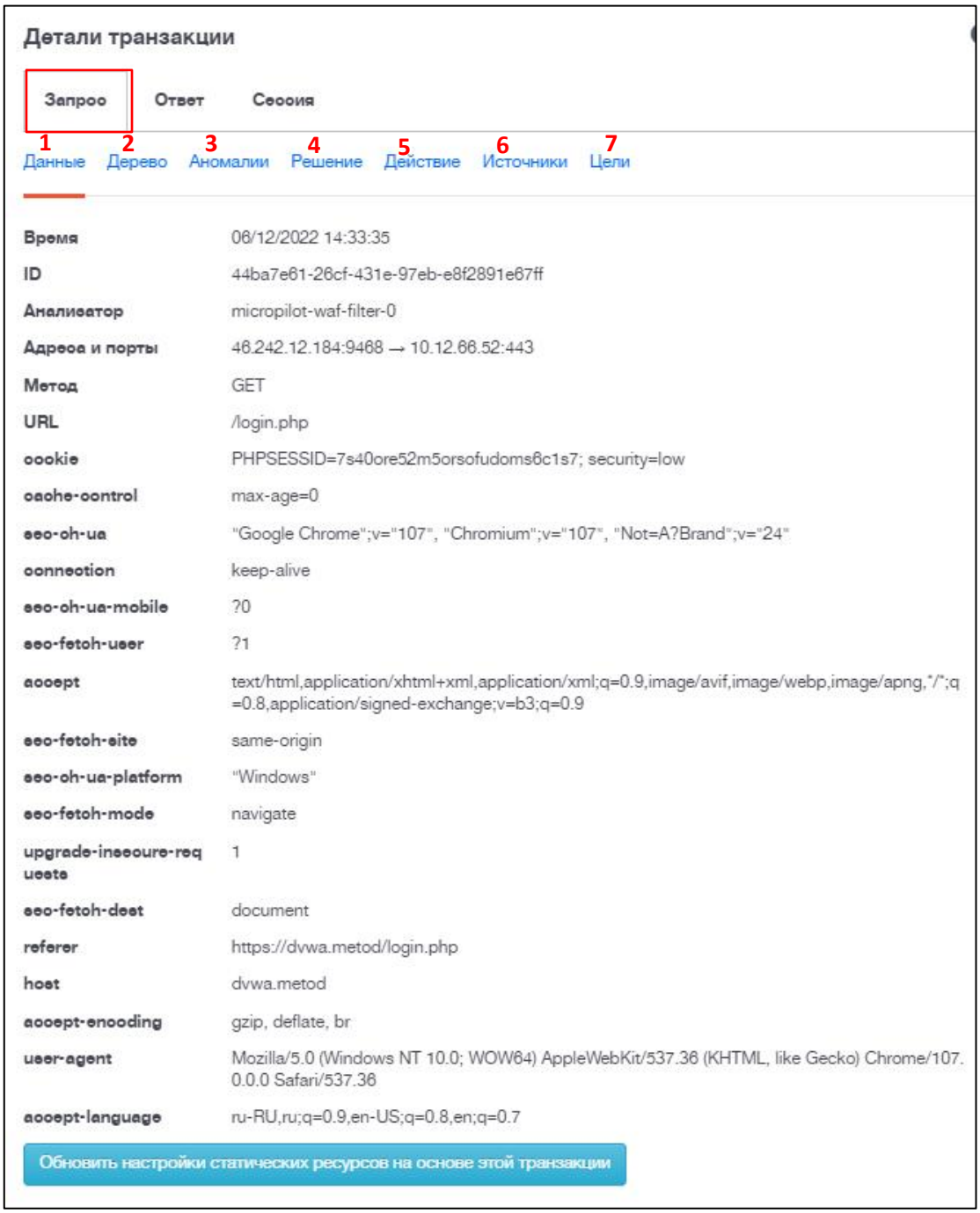

Рисунок 98 – Вкладка «Запрос»

1. Данные – текстовое представление запроса (см. рисунок 98).
2. Дерево – разобранное дерево запроса (см. рисунок 99). Данное представление создается моделью дерева разбора запроса. Для каждого элемента дерева можно посмотреть его значение нажав на пиктограмму с изображением глаза, как показано на рисунке 99. В данном окне можно свернуть и развернуть элементы дерева, нажав на «-» и «+» соответственно (см. рисунок 100). Также есть возможность дополнительно разобрать каждый элемент дерева. Настройки модели дерева разбора описаны в разделе 10.

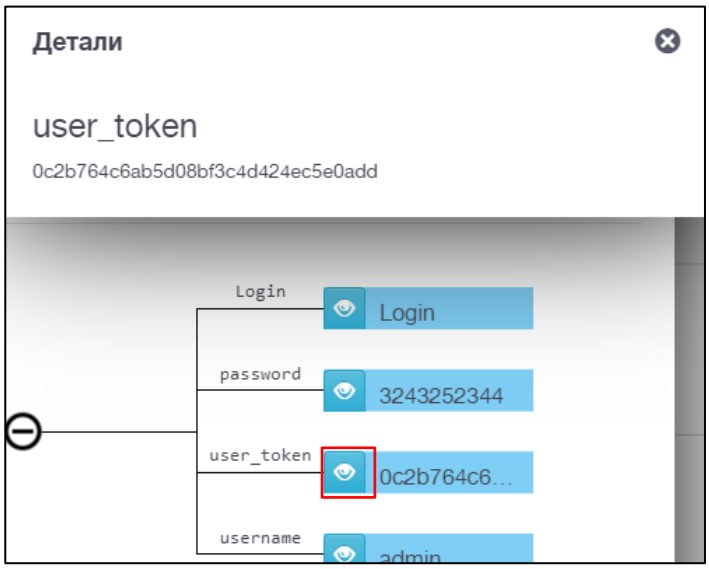

Рисунок 99 – Просмотр значения поля из дерева разбора

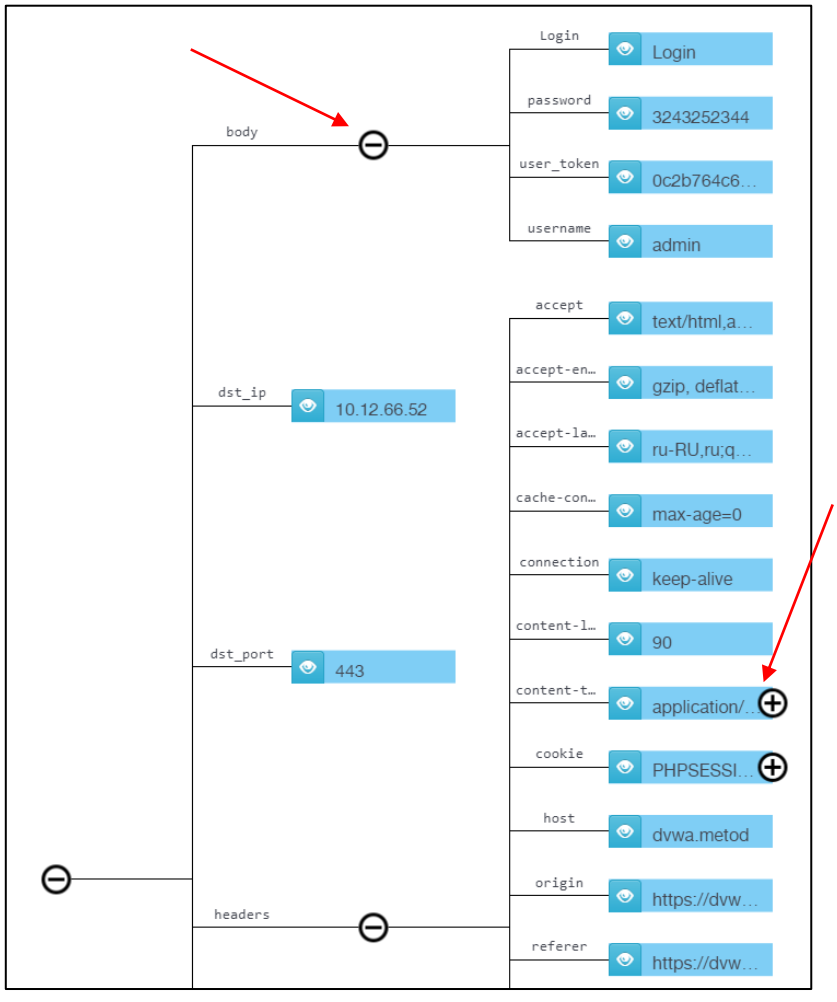

Рисунок 100 – Возможность сворачивать и разворачивать элементы дерева

3. Аномалии - в данном окне находятся аномалии, которые были обнаружены в данной транзакции (см. рисунок 101). При выборе аномалии доступна дополнительная информация о найденной аномалии. При ложных сработках можно подавить найденную аномалию, нажав на кнопку «Подавить эту

аномалию». При нахождении нескольких аномалий, можно подавить сразу все аномалии, нажав на кнопку «Подавить все аномалии».

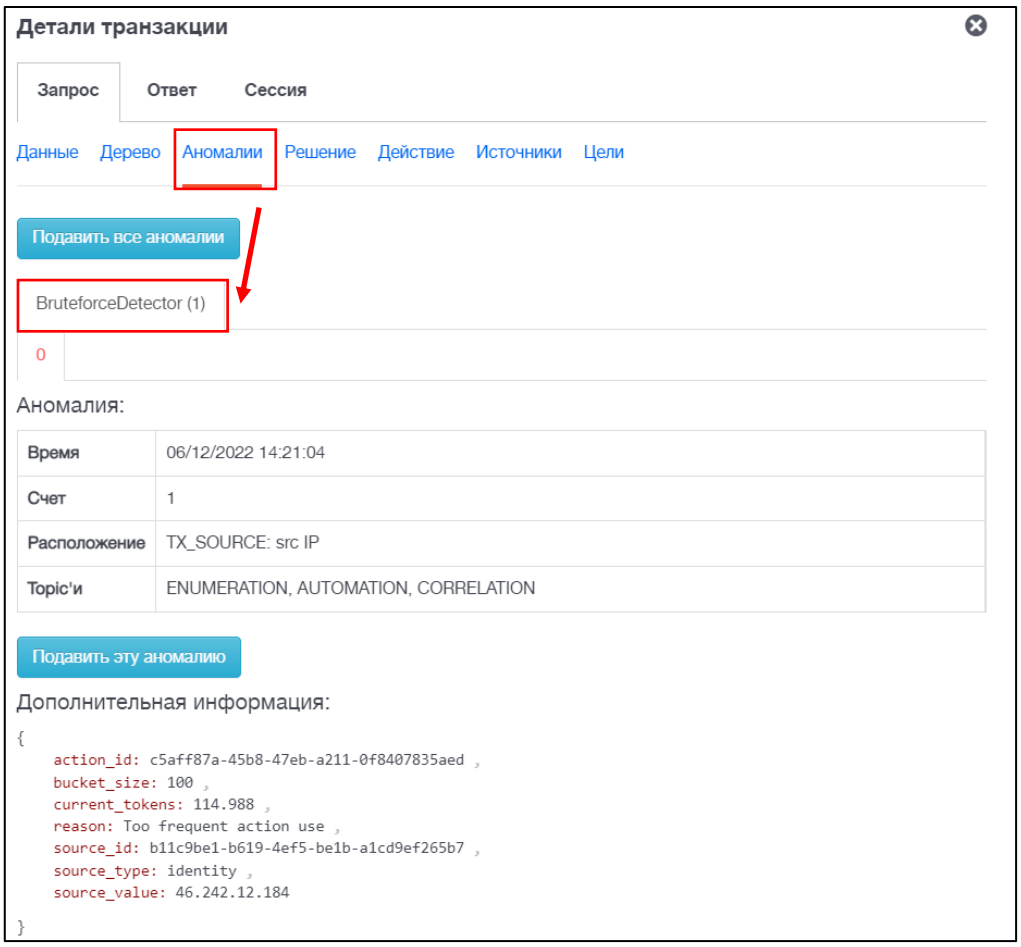

Рисунок 101 – Вкладка «Аномалии»

4. Решение - в данном окне можно увидеть подробную информацию о решении транзакции: время совершения транзакции, её ID, само решение о блокировке либо пропуске транзакции, измененное сообщение, правила, которые отработали для данной транзакции, и причину срабатывания правил (см. рисунок 102). В окне причины есть возможность просмотреть более подробную информацию, нажав на кнопку «[…]» для интересующего поля (см. рисунок 102).

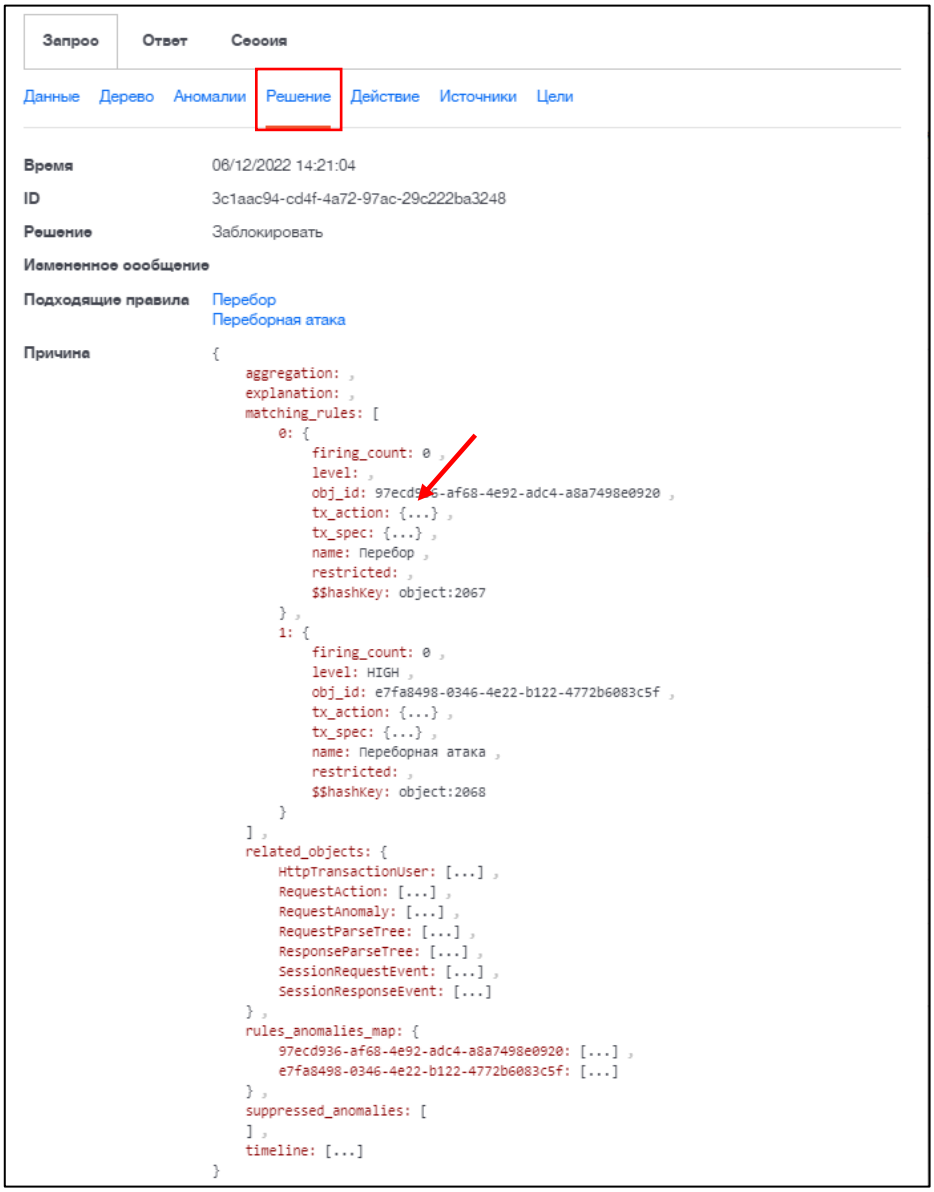

Рисунок 102 – Вкладка «Решение»

5. Действие - в данном окне находится действие и его параметры, которые подошли под данную транзакцию (см. рисунок 103). Здесь можно посмотреть значения параметров действия, которые указаны при настройке действия. Также имеется возможность полуавтоматического создания действия на основе этой транзакции (настройки действия описаны в разделе 15) с помощью кнопки «Создать действие на основе этой транзакции».

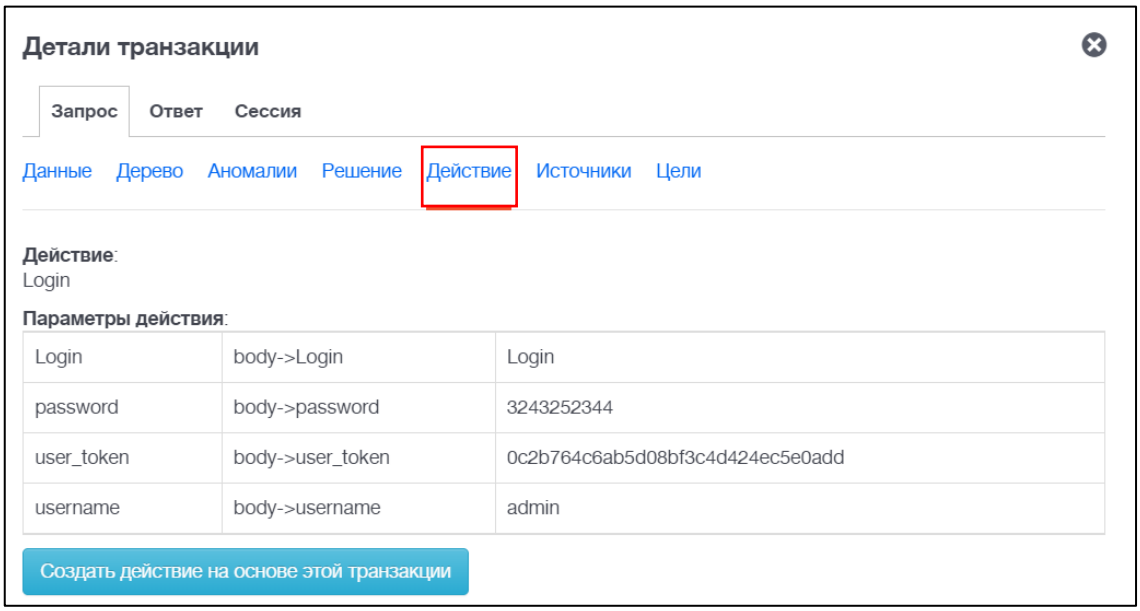

Рисунок 103 – Вкладка «Действие»

6. Источники - в данной вкладке отображаются найденные источники для данной транзакции и их значения (см. рисунок 104). Подробную информацию об источниках можно найти в разделе 13.

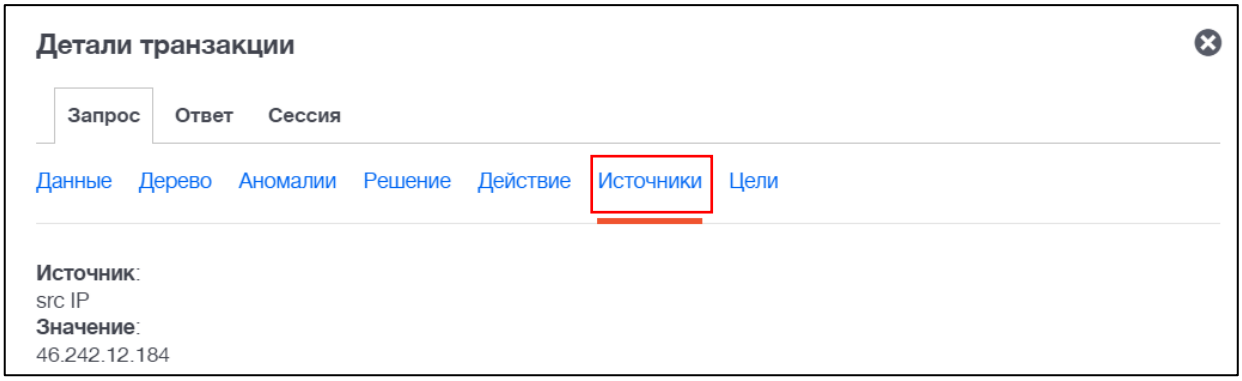

Рисунок 104 – Вкладка «Источники»

7. Цели - в данной вкладке отображаются найденные цели для данной транзакции и их значения (см. рисунок 105). Подробную информацию об целях можно найти в разделе 14.

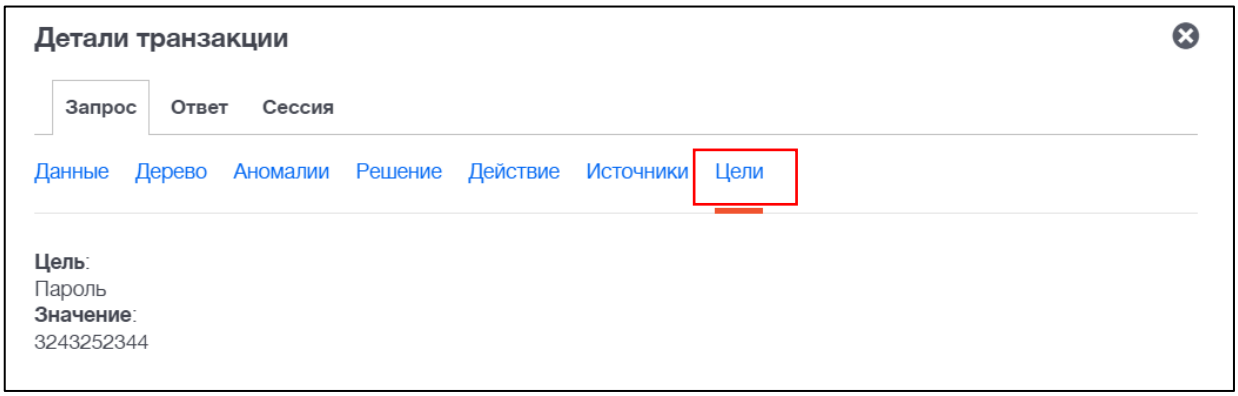

Рисунок 105 – Вкладка «Цели»

7.2. Вкладка «Ответ»

На данной вкладке отображается информация об ответе.

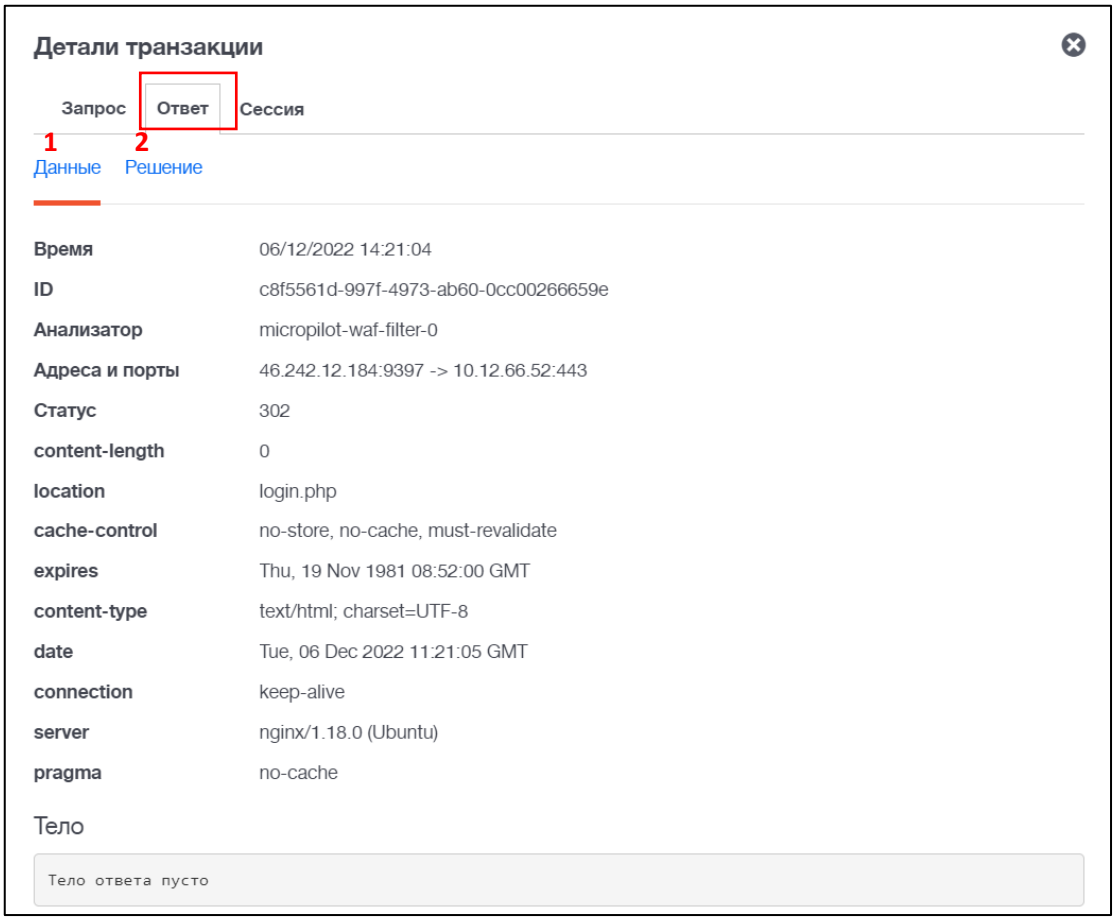

Рисунок 106 – Вкладка «Ответ»

1. Данные - в данной вкладке находятся поля ответа и их значения (см. рисунок 106).
2. Решение - в данной вкладке можно увидеть подробную информацию об решении ответа транзакции, а именно время ответа транзакции, её ID, само решение о блокировке либо пропуске ответа транзакции (стоит отметить, что транзакция может быть заблокирована как по решению запроса, так и по решению ответа (например, для атаки Open Redirect)), измененное сообщение правил, которые отработали для данной транзакции и причина (см. рисунок 107). В блоке причины есть возможность просмотреть более подробную информацию, нажав на соответствующую кнопку «[…]» для интересующего поля (см. рисунок 107).

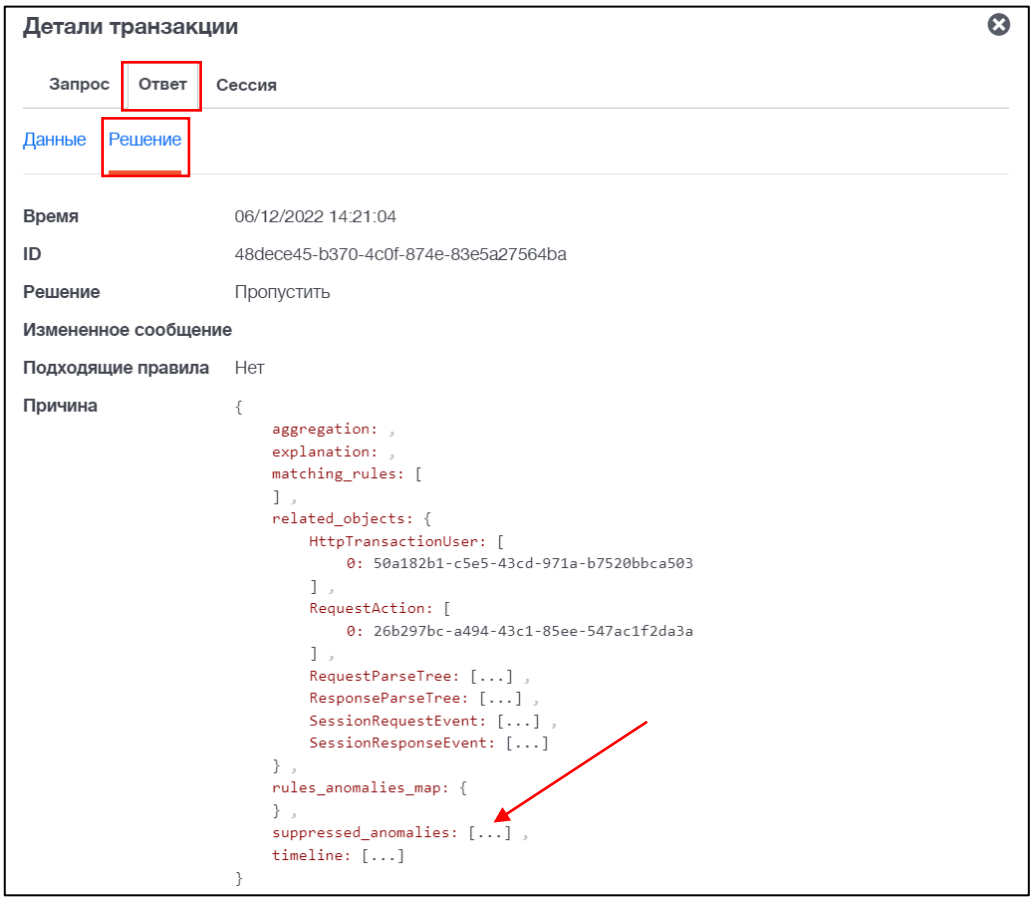

Рисунок 107 – Вкладка «Решение»

Примечание: на данной вкладке также может быть область с аномалиями. Например, аномалия от OpenRedirectDetector выдается на ответ.

7.3. Вкладка «Сессия»

На данной вкладке отображается информация о значении сессии запроса и сессии ответа, а также пользователь (см. рисунок 108). Данная вкладка появляется только если настроена сессионная модель (про настройку сессионной модели можно прочитать в разделе 18), и включен модуль LWSessionTracker (про настройку модуля можно прочитать в разделе 17.6). Поле «Пользователь» будет выводиться только в том случае, если настроен сессионный атрибут с типом атрибута «Извлечение имени пользователя» (про настройку сессионных атрибутов можно прочитать в разделе 18.1).

Рисунок 108 – Вкладка «Сессия»

8. Настройка фильтрации запросов к статическим ресурсам

При загрузке страницы защищаемого веб-приложения, также происходит ряд запросов на загрузку файлов, таких как иконки, скрипты и таблицы стилей. Данного рода запросы также отображаются на WAF, что повышает нагрузку на анализаторы. Для снижения нагрузки на WAF, а также для повышения эффективности анализа трафика был разработан модуль «Статические ресурсы», который позволяет настраивать фильтрацию запросов к статическим ресурсам, убирая неинформативный трафик.

Чтобы транзакции к статическим ресурсам пропускались на уровне nginx, на вкладке «Статические ресурсы» имеется переключатель «Ускоренный анализ запросов к статическим ресурсам» (см. рисунок 109).

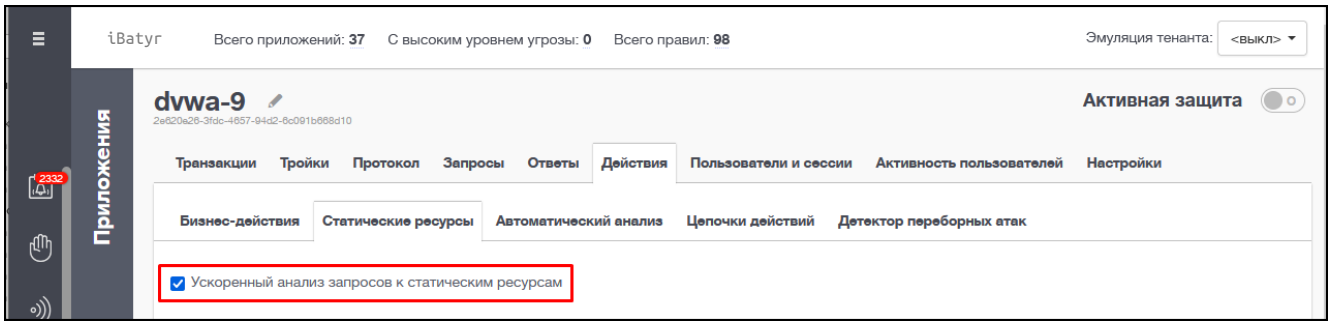

Рисунок 109 – Ускоренный анализ запросов к статическим ресурсам

На WAF имеется возможность создания статических ресурсов тремя способами, которые описаны пунктах 8.1 – 8.3.

8.1. Полуавтоматическое создание шаблонов фильтрации запросов к статическим ресурсам

На WAF имеется возможность поштучного добавления файлов в статические ресурсы из меню транзакций.

На вкладке «Приложения» -> «Транзакции» необходимо выбрать транзакцию с запросом статического ресурса (см. рисунок 110).

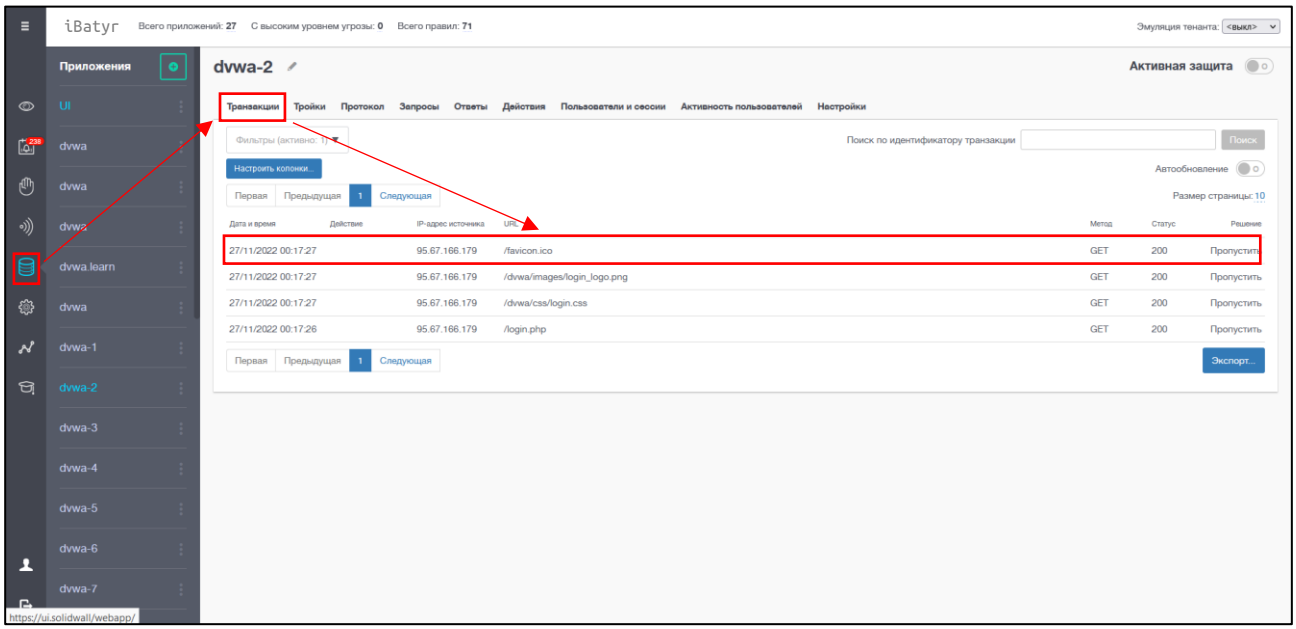

Рисунок 110 – Выбор транзакции

Двойным кликом по транзакции необходимо открыть ее описание. В открывшемся окне нажать «Обновить настройки статических ресурсов на основе этой транзакции». В появившемся диалоговом окне нажать «ОК» (см. рисунок 111).

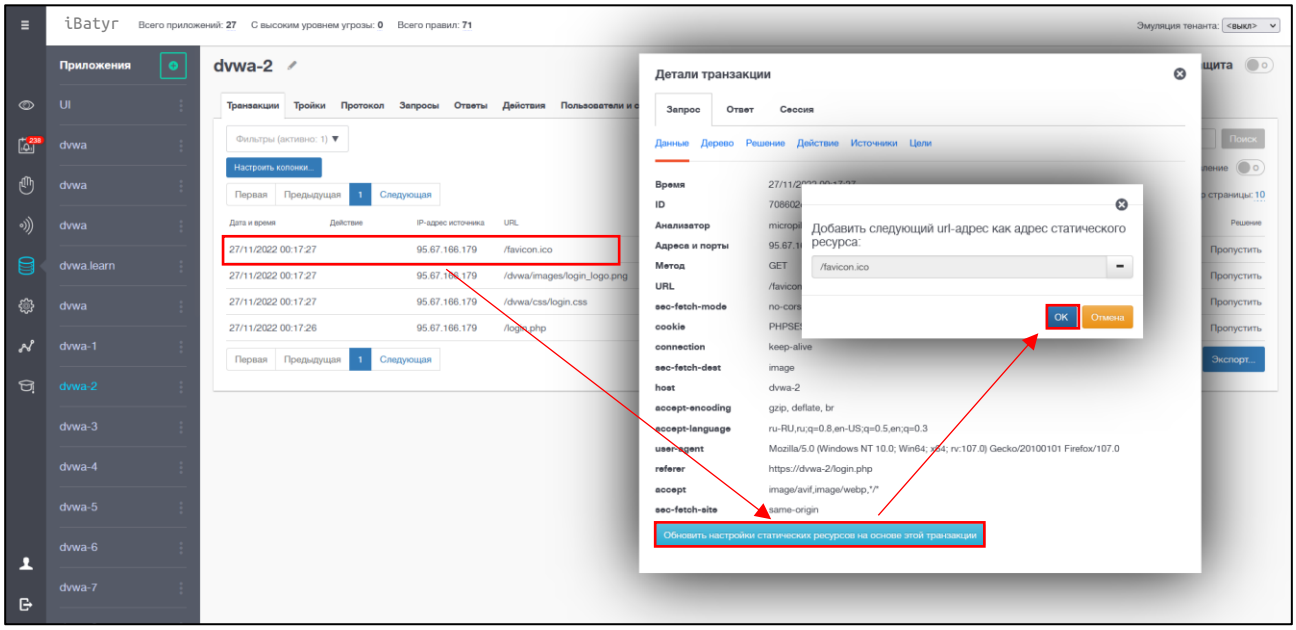

Рисунок 111 – Добавление статического ресурса

Для того чтобы проверить, что путь к данному файлу добавлен в настройку фильтрации запросов к статическим ресурсам, переходим на вкладку «Приложения» -> «Действия» -> «Статические ресурсы» (см. рисунок 112).

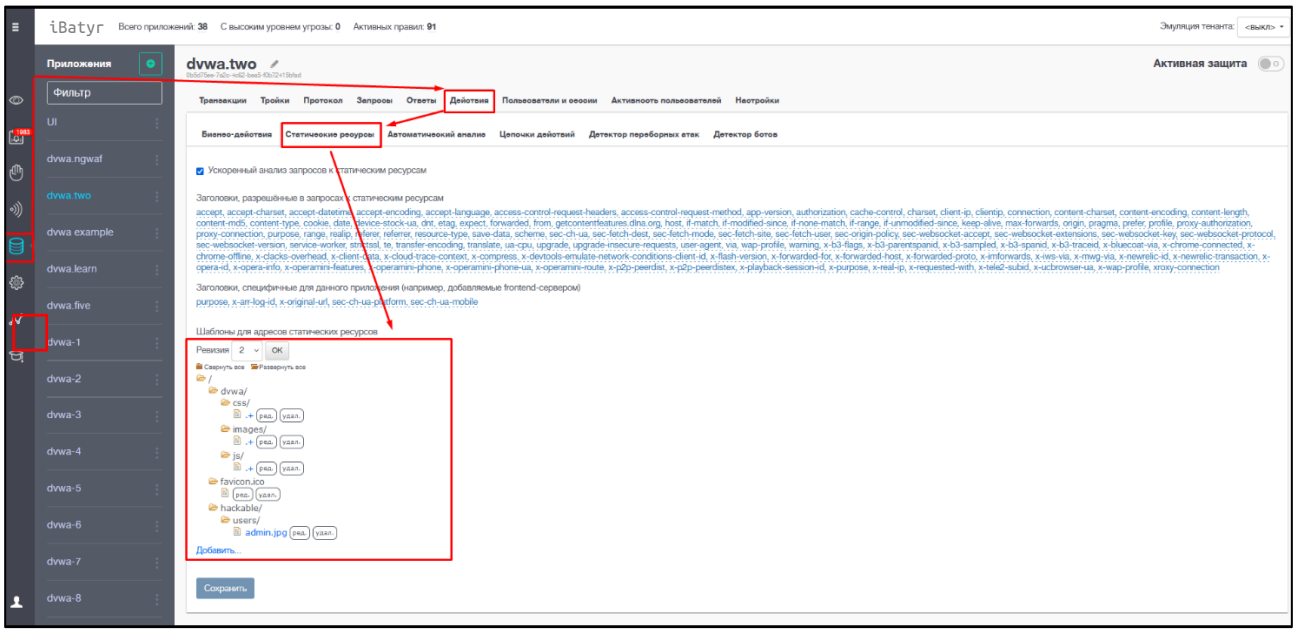

Рисунок 112 – Проверка добавления

8.2. Автоматическое создание шаблонов фильтрации запросов к статическим ресурсам

На WAF имеется возможность автоматического добавления запросов в статические ресурсы на основе машинного обучения. Данный модуль включен по умолчанию и его дополнительно можно настроить из веб-интерфейса WAF. Для этого необходимо перейти на вкладку «Приложения» -> «Действия» -> «Автоматический анализ» и отредактировать задание «Обновление шаблонов статических ресурсов» (см. рисунок 113).

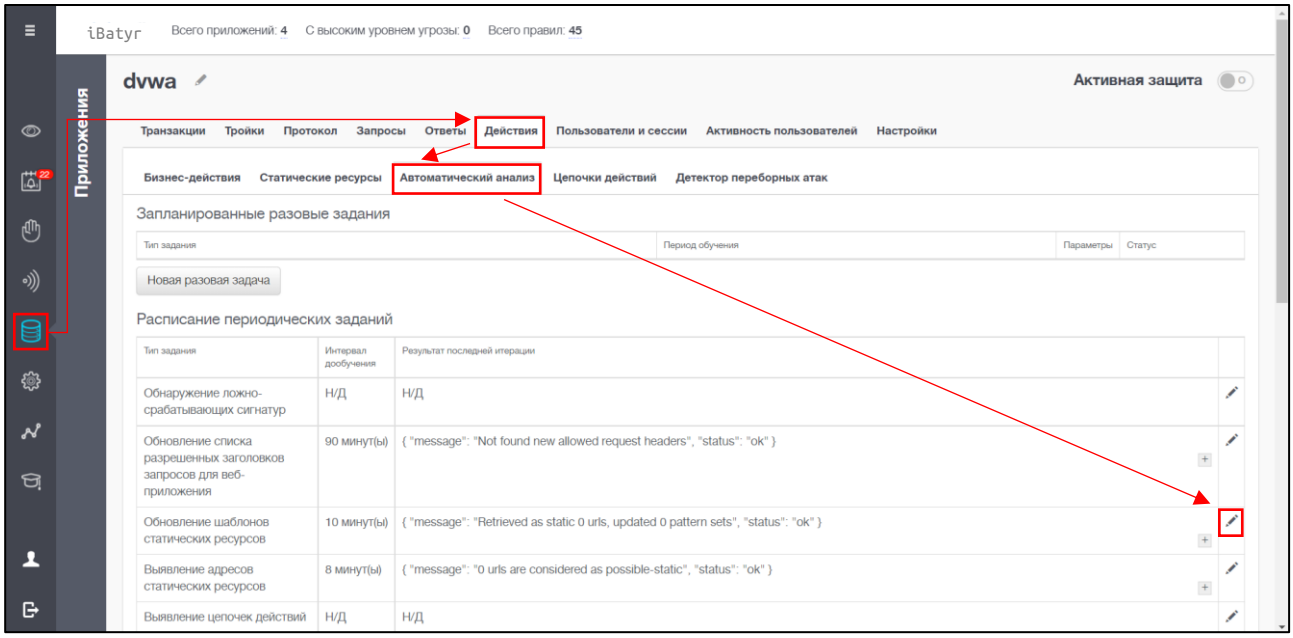

Рисунок 113 – Автоматический анализ

В открывшимся окне (см. рисунок 114) имеются два поля:

- Интервал обучения – интервал, за который считаются транзакции к статическим ресурсам;

- Минимальный размер выборки запросов от уникальных пользователей – порог количества запросов от уникальных (различных) пользователей, при достижении которого путь к статическому ресурсу записывается в настройки фильтрации запросов к статическим ресурсам.

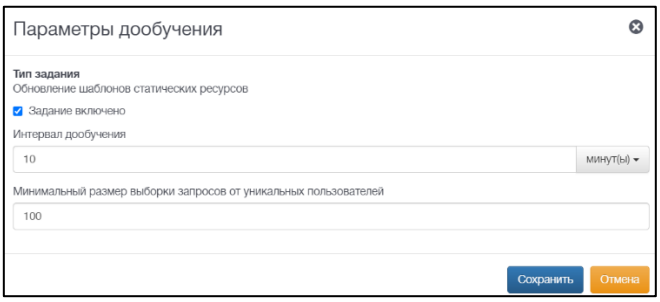

Рисунок 114 – Настройки задания «Обновление шаблонов статических ресурсов»

По умолчанию стоят значения 10 и 100 соответственно. Это означает, что настройки фильтрации запросов к статическим ресурсам будут изменены только тогда, когда у 100 разных пользователей за 10 минут встретится одинаковый запрос к статическому ресурсу.

8.3. Ручное создание шаблонов фильтрации запросов к статическим ресурсам

На WAF имеется возможность ручного добавления шаблонов фильтрации запросов к статическим ресурсам. Для того чтобы вручную добавить путь к статическому ресурсу, необходимо перейти на вкладку «Приложения» -> «Действия» -> «Статические ресурсы» и нажать на кнопку «Добавить» (см. рисунок 115).

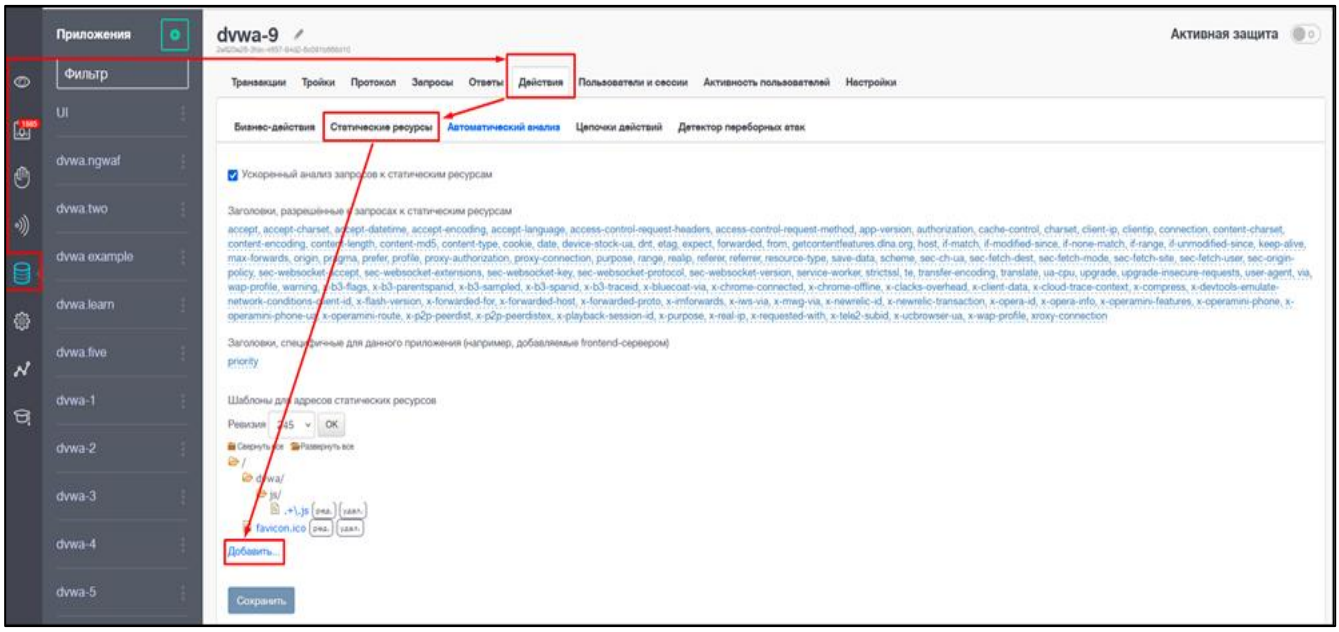

Рисунок 115 – Добавление статического ресурса

Открывшееся окно добавления шаблона позволяет добавить как пути к файлу целиком, так и задание последней его части регулярным выражением. Для добавления пути к файлу целиком, в появившемся окне необходимо ввести путь к файлу и нажать на кнопку «Добавить», а затем сохранить новый шаблон (см. рисунок 116).

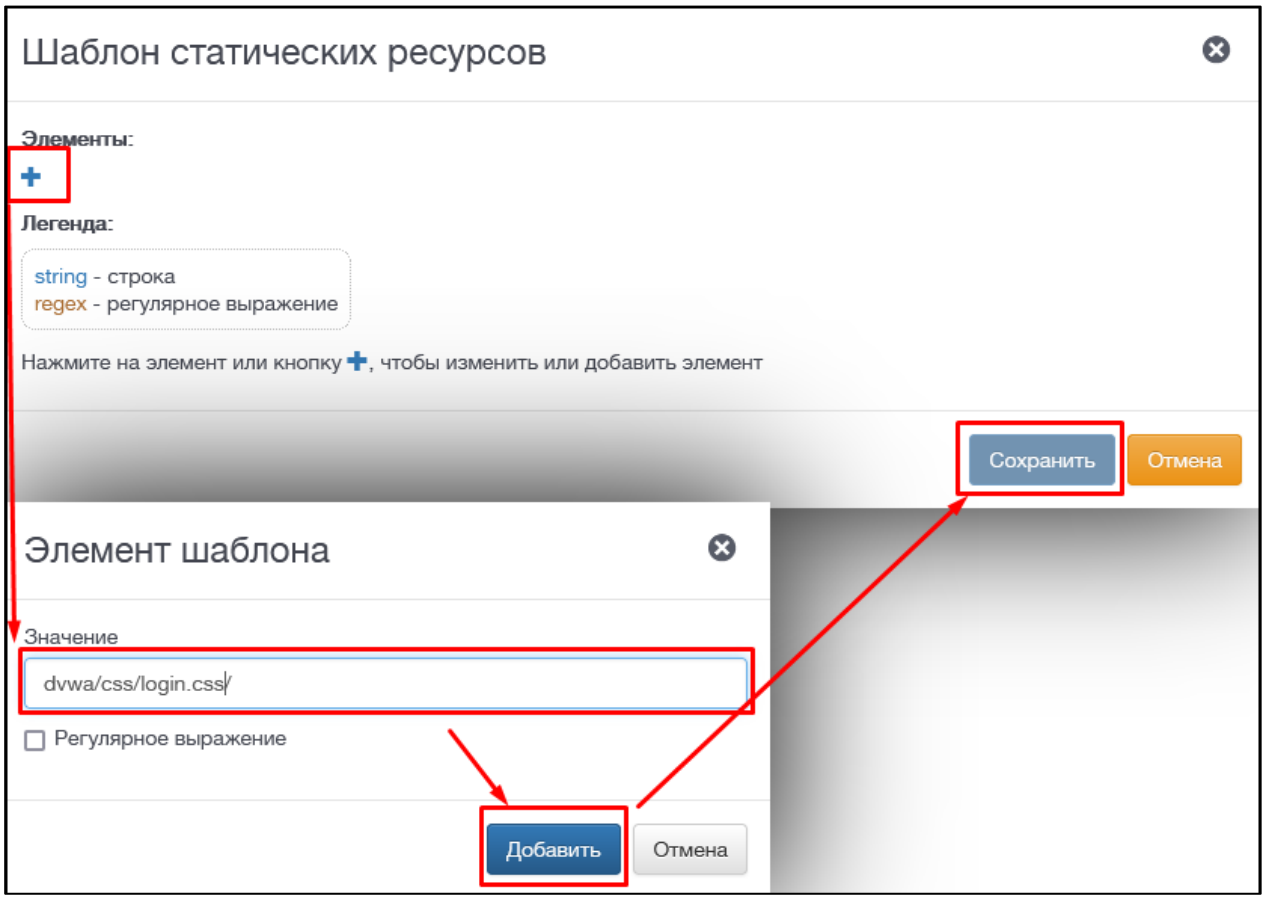

Рисунок 116 – Создание нового шаблона

Для добавления пути к файлу с использованием регулярного выражения в появившемся окне необходимо ввести путь к файлу, затем нажать на кнопку «Добавить», следующим шагом в это же окно добавить регулярное выражение и поставить отметку в поле «Регулярное выражение», повторно нажать «Добавить», после чего сохранить новый шаблон (см. рисунок 117).

Регулярное выражение также добавить сразу без добавления общей части. По мимо этого реализована возможность добавить несколько регулярных выражений.

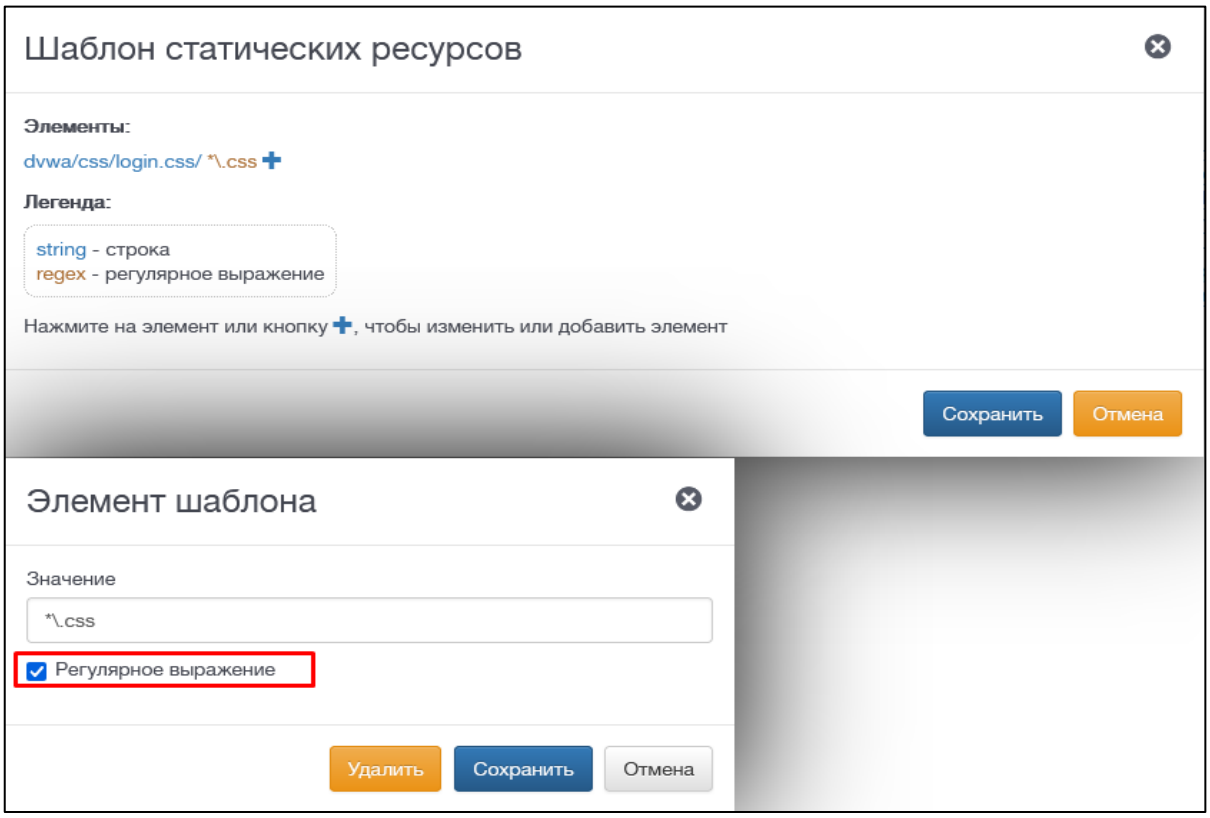

Рисунок 117 – Добавление регулярного выражения

После добавления шаблона, необходимо сохранить изменения на странице (см. рисунок 118).

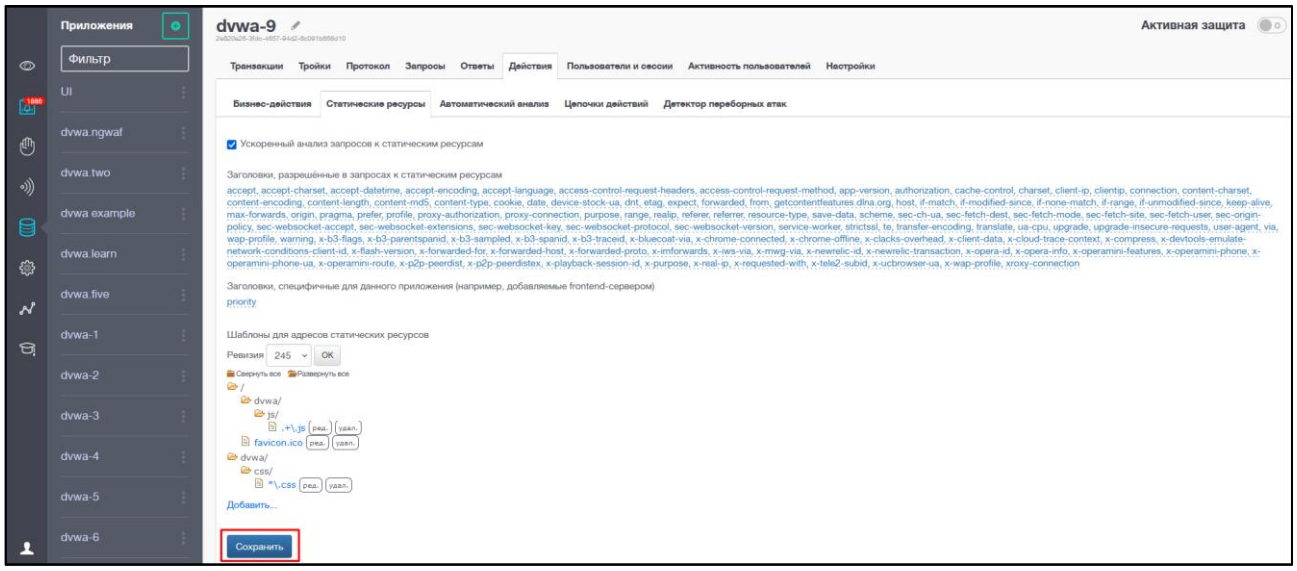

Рисунок 118 – Сохранение изменений

Примечание: при ручном добавлении шаблонов фильтрации запросов к статическим ресурсам, в отличие от автоматического и полуавтоматического, не происходит добавление заголовков в поле «Заголовки, разрешённые в запросах к статическим ресурсам». Поэтому их необходимо добавлять вручную. Запросы к статическим ресурсам с заголовками, которых нет в данном списке, будут отображаться в общем списке даже после создания шаблона фильтрации (даже если данные заголовки введены в протоколе).

8.4. Добавление и удаление заголовков, разрешенных при фильтрации запросов к статическим ресурсам

На вкладке «Статические ресурсы» имеется два поля, в которые можно добавить заголовки, разрешенные при фильтрации запросов к статическим ресурсам (см. рисунок 119).

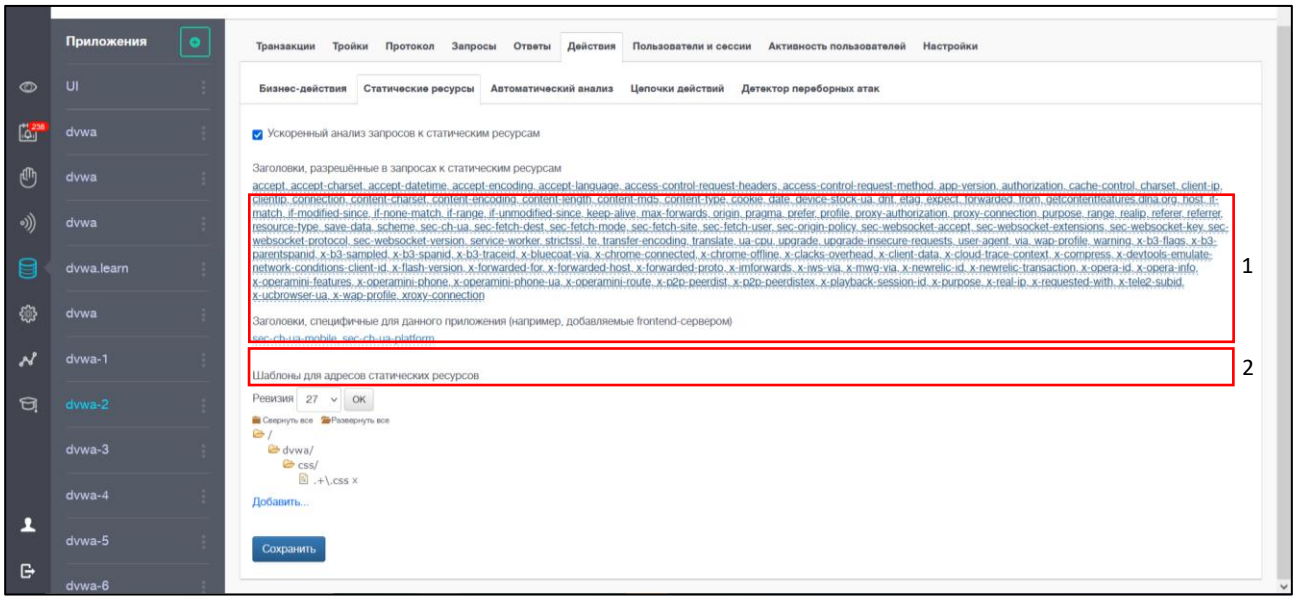

Рисунок 119 – Заголовки, разрешенные в запросах к статическим ресурсам

1. Заголовки, разрешенные в запросах к статическим ресурсам – в данном указываются заголовки, которые разрешены для использования в запросах к статическим ресурсам, и используются на всех приложениях тенанта, или инсталляции.
2. Заголовки, специфичные для данного приложения (например, добавляемые frontend-сервером) - в данном указываются заголовки, которые разрешены для использования в запросах к статическим ресурсам, и используются только на выбранном приложении. По умолчанию в данное поле добавляются заголовки автоматическом и полуавтоматическом добавлении шаблонов настройки фильтрации запросов к статическим ресурсам.

Для добавления заголовков, разрешенных в запросах к статическим ресурсам, нужно выбрать одно из двух полей, описанных выше, и нажать левой кнопкой мыши на его значения. В появившемся окне ввести название заголовка и нажать на кнопку «ОК». После добавления заголовка необходимо сохранить изменения на странице (см. рисунок 120).

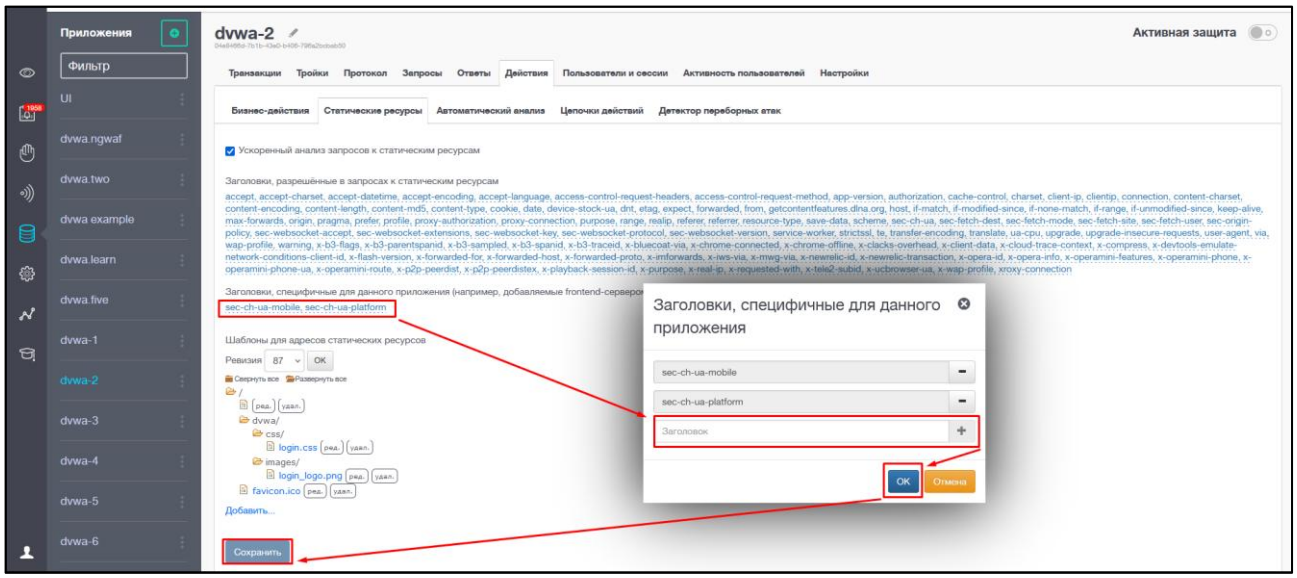

Рисунок 120 – Добавление заголовка, разрешенного в запросах к статическим ресурсам

Для добавления дополнительного поля ввода заголовка, необходимо нажать на иконку «➕».

Для удаления заголовков, разрешенных в запросах к статическим ресурсам, нужно выбрать одно из двух полей, описанных выше, и нажать левой кнопкой мыши на его значения. В появившемся окне нажать на иконку «➖» напротив заголовка, который необходимо удалить, и нажать на кнопку «ОК». После удаления заголовка необходимо сохранить изменения на странице (см. рисунок 121).

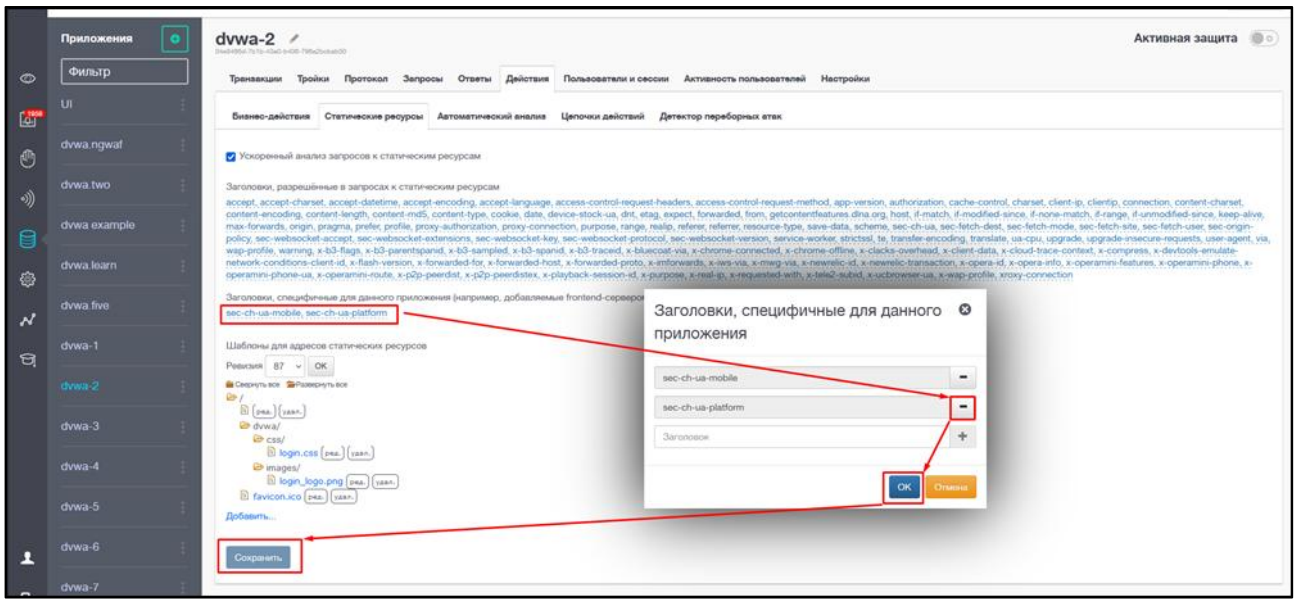

Рисунок 121 – Удаление заголовка, разрешенного в запросах к статическим ресурсам

8.5. Удаление шаблонов для адресов статических ресурсов

На WAF имеется возможность только ручного удаления шаблонов фильтрации запросов к статическим ресурсам.

Для того, чтобы удалить путь к статическому ресурсу, необходимо перейти на вкладку «Приложения» -> «Действия» -> «Статические ресурсы», нажать на кнопку «удал.» напротив шаблона, который необходимо

удалить. После удаления шаблонов фильтрации запросов к статическим ресурсам необходимо сохранить изменения на странице (см. рисунок 122).

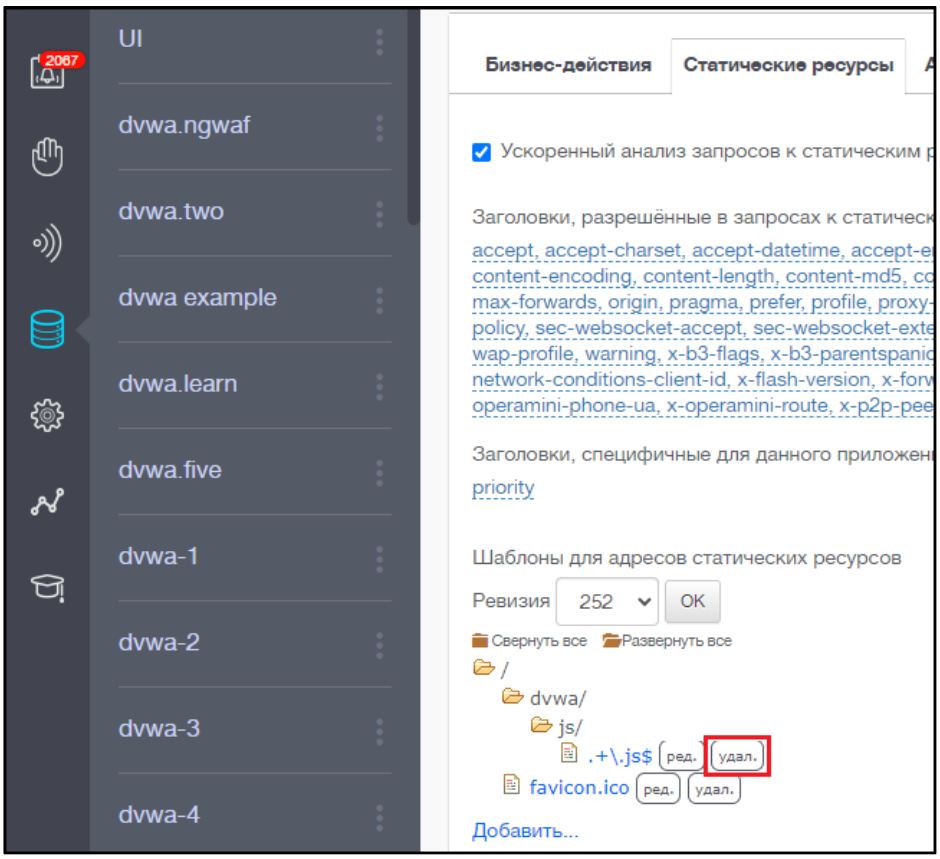

Рисунок 122 – Удаление шаблонов фильтрации запросов к статическим ресурсам

Для того, чтобы изменить путь к статическому ресурсу, необходимо перейти на вкладку «Приложения» -> «Действия» -> «Статические ресурсы», нажать на кнопку «ред.» напротив шаблона, который необходимо отредактировать. После изменения шаблонов фильтрации запросов к статическим ресурсам необходимо сохранить изменения на странице (см. Рисунок 123).

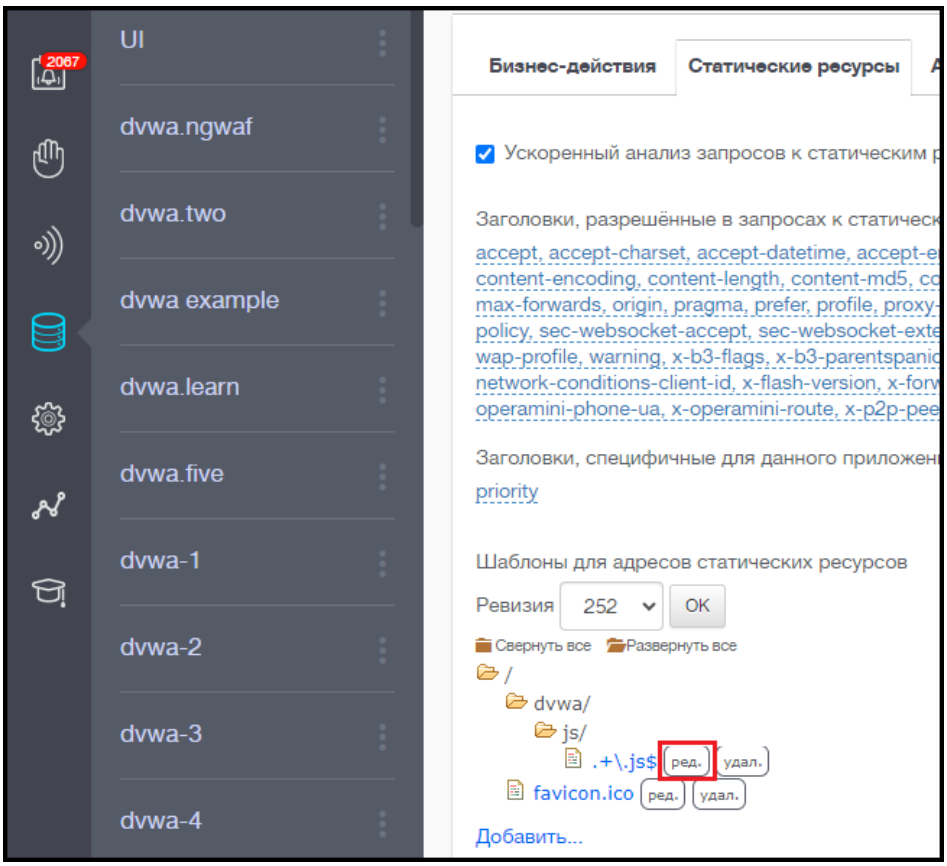

Рисунок 123 – Редактирование шаблонов фильтрации статических ресурсов

8.6. Ревизии шаблонов для адресов статических ресурсов

На WAF имеется возможность переключения между ревизиями настроек данной вкладки (настройками всех полей, таких как Заголовки, разрешённые в запросах к статическим ресурсам, Заголовки, специфичные для данного приложения, например, добавляемые frontend-сервером, Шаблоны для адресов статических ресурсов). Выбор ревизии находится в выделенной области на рисунке 124.

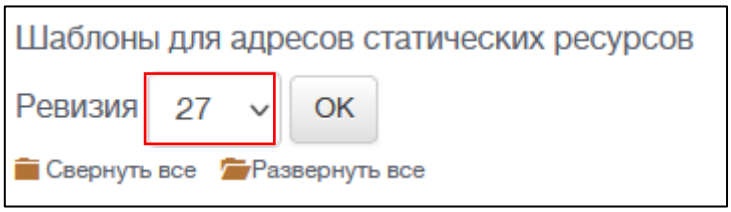

Рисунок 124 – Выбор ревизии

После выбора ревизии, отличной от актуальной, можно нажать на кнопку «ОК» для просмотра настроек данной ревизии. Для того чтобы применить выбранную ревизию, необходимо нажать на кнопку «Откатить».

9. Настройка протокольной валидации

Для того чтобы настроить протокольную валидацию необходимо перейти на вкладку «Приложения» -> «Протокол» (см. рисунок 125). Аналитику доступно изменение параметров путем заполнения выпадающих окон, изменения состояния чекбоксов и заполнения полей. Для проделанных изменений доступно три операции: сохранить изменения, просмотреть изменения и сбросить изменения. При нажатии на кнопку «Просмотреть изменения» откроется окно «Изменения», в котором все изменения представлены в виде кода.

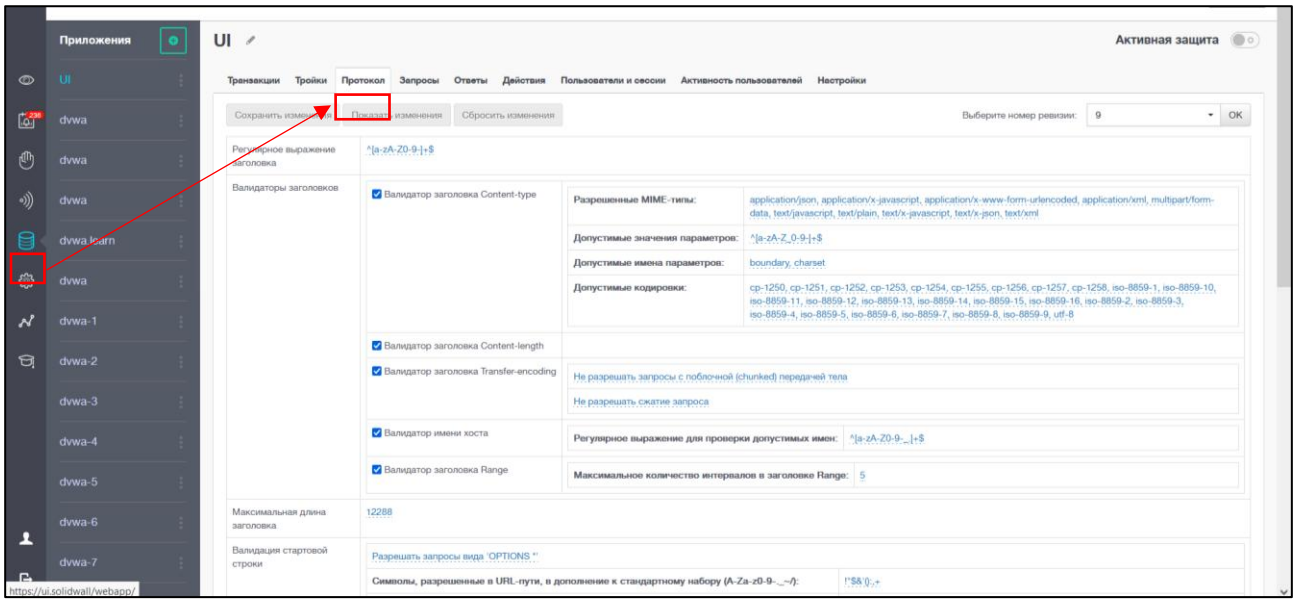

Рисунок 125 – Вкладка «Протокол»

9.1. Описание полей настроек протокольной валидации

Описание полей настроек протокольной валидации представлены в таблице 9.

Таблица 9 – Настройки протокольной валидации

Поле	Описание	Параметры	
Регулярное выражение заголовка	Регулярное выражение, которому должен соответствовать каждый заголовок транзакции	Поле ввода регулярного выражения	
Валидаторы заголовков	Проверка значений заголовков, на соответствие заданным параметрам	Чекбокс «Валидатор заголовка Content-type» включает или выключает проверку заголовка «Content-type» на соответствие заданным параметрам	Разрешенные MIME-типы – задается список разрешенных медиа типов (так же известный как Multipurpose Internet Mail Extensions или MIME тип), который описывает природу и формат документа, файла или набора байтов. MIME-типы определены в соответствии со спецификацией RFC 6838
			Допустимые значения параметров – поле ввода регулярного выражения, которому должны соответствовать значения параметров заголовка «Content-type»

Поле	Описание	Параметры	
			Допустимые имена параметров – поле ввода допустимых имен для параметров заголовка «Content-type»
			Допустимые кодировки – поле ввода допустимых кодировок заголовка «Content-type»
		Чекбокс «Валидатор заголовка Content-length» включает или выключает проверку соответствия размера заголовка «body», указанному размеру в заголовке «Content-length»	
		Чекбокс «Валидатор заголовка Transfer-encoding» включает или выключает проверку заголовка «Transfer-encoding» на соответствие заданным параметрам	Разрешать запросы с поблочной (chunked) передачей тела – при нажатии на данный текст появляется чекбокс, который включает или выключает запрет на поблочную передачу текста
			Разрешать сжатие запроса – при нажатии на данный текст появляется чекбокс, который разрешает или запрещает сжатие запроса
		Чекбокс «Валидатор имени хоста» включает или выключает проверку заголовка «host» на соответствие заданным параметрам	Регулярное выражение для проверки допустимых имен – поле ввода регулярного выражения
		Чекбокс «Валидатор заголовка Range» включает или выключает проверку заголовка «Range» на соответствие заданным параметрам	Максимальное количество интервалов в заголовке Range – поле ввода максимального количества интервалов в заголовке Range (например, если максимальное количество интервалов в заголовке Range в данном параметре задано 2, то транзакция с заголовком «Range: bytes=200-1000, 2000-6576, 19000-» будет заблокирована)
Максимальная длина заголовка	Поле для ввода максимальной длинны заголовков	Поле ввода числового значения максимальной длинны заголовков (если хотя бы один из заголовков транзакции будет длиннее заданного, тогда транзакция будет заблокирована)	
Валидация стартовой строки	Проверка значений заголовков «url» «method», на соответствие заданным параметрам	Разрешать запросы вида 'OPTIONS' – при нажатии на данный текст появляется чекбокс, который разрешает или запрещает запросы с методом «OPTIONS»	
		Символы, разрешенные в URL-пути, в дополнение к стандартному набору (A-Za-z0-9-._~/) – поле ввода символов, разрешенных для использования в заголовке «URL» в дополнение к стандартному набору	
		Максимальная длина URL-параметров (0 - без ограничения) – поле ввода числового значения максимальной длинны параметров заголовка «URL»	
		Не разрешать URL в абсолютной форме – при нажатии на данный текст появляется чекбокс, который разрешает или запрещает запросы в абсолютной форме (пример URL в абсолютной форме: scheme://server/path/resource, где scheme – схема доступа к сайту; server –	

Поле	Описание	Параметры
		имя компьютера, на котором находится ресурс; path – последовательность каталогов, ведущих к целевому объекту; resource – обычно является именем файла)
		Разрешать некорректное URL-кодирование в URL – при нажатии на данный текст появляется чекбокс, который разрешает или запрещает запросы с некорректным URL-кодированием (например, если разрешить использование некорректного URL-кодирования, транзакции, с символами не закодированными в UTF-8 будут пропущены)
		Разрешенные методы – поле ввода названий разрешенных методов
		Максимальная длина пути (0 - без ограничения) – поле ввода части path запроса
		Символы, разрешенные в URL-параметрах, в дополнение к стандартному набору (A-Za-z0-9-._~/) – поле ввода символов, которые будут разрешены к использованию в URL-параметрах в дополнение к стандартному набору (A-Za-z0-9-._~/)
Замена некоторых символов на дефисы (-) в именах заголовков	Чекбокс, который включает принудительную замену символов, введенных в поле «Символы, подлежащие замене на дефис (-) в именах заголовков» на дефис	
Символы, подлежащие замене на дефис (-) в именах заголовков	Поле ввода символов, которые необходимо заменять на дефис. Появляется только если чекбокс в пункте «Замена некоторых символов на дефисы (-) в именах заголовков» включен	
Разрешенные заголовки	Поле ввода заголовков, разрешенных для использования в запросах	
Шаблоны разрешенных заголовков	Поле ввода регулярных выражений для задания заголовков, которые разрешены для использования в запросах	
Регулярное выражение для проверки значений заголовков	Поле ввода регулярного выражения, которому должны соответствовать значения заголовков	
Разрешать дублирующиеся заголовки	Поле ввода заголовков, дублирование которых в запросах разрешено	
Максимальное количество заголовков	Поле ввода значения максимального количества заголовков в запросе	

Примечание: изменения, внесенные в протокольную валидацию, можно сохранить как для приложения, так и для всего тенанта\инсталляции, для этого необходимо выбрать соответствующий пункт в всплывающем окне, которое появляется после нажатия на кнопку «Сохранить изменения».

9.2. Ревизии настроек протокольной валидации

На WAF имеется возможность переключения между ревизиями настроек данной вкладки. Выбор ревизии находится в выделенной области на рисунке 126.

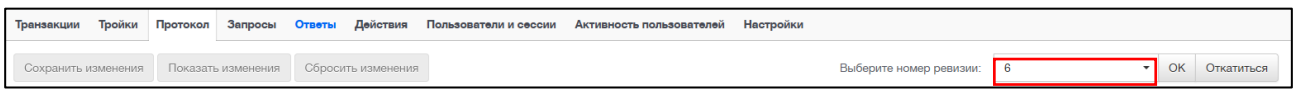

Рисунок 126 – Выбор ревизии

После выбора ревизии, отличной от актуальной, можно нажать на кнопку «ОК» для просмотра настроек данной ревизии. Для того чтобы применить выбранную ревизию, необходимо нажать на кнопку «Откатить».

10. Настройка дерева разбора

На WAF имеется возможность углубить дерево разбора запроса. Для этого необходимо перейти на вкладку «Приложения» -> «Запросы» (см. рисунок 127).

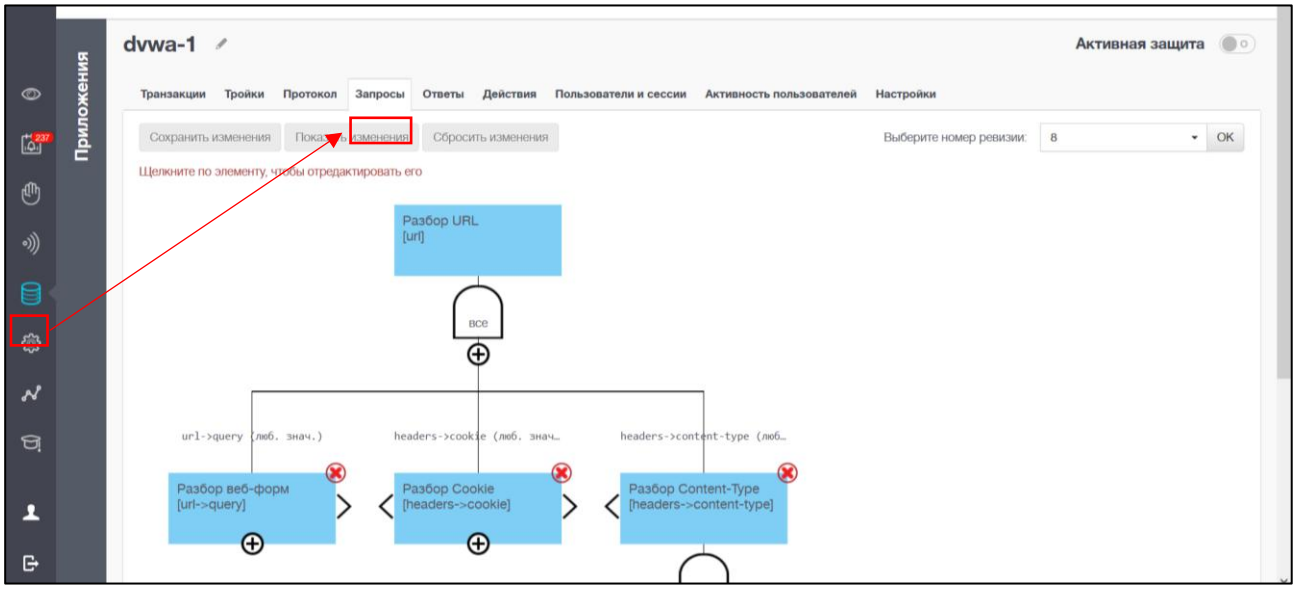

Рисунок 127 – Окно «Запросы»

10.1. Добавление и удаление блоков декодирования

Для того чтобы углубить дерево разбора необходимо нажать на иконку «⊕», в той части, где необходимо дополнить дерево разбора. После нажатия на данную иконку появляется окно создания шага разбора (см. рисунок 128).

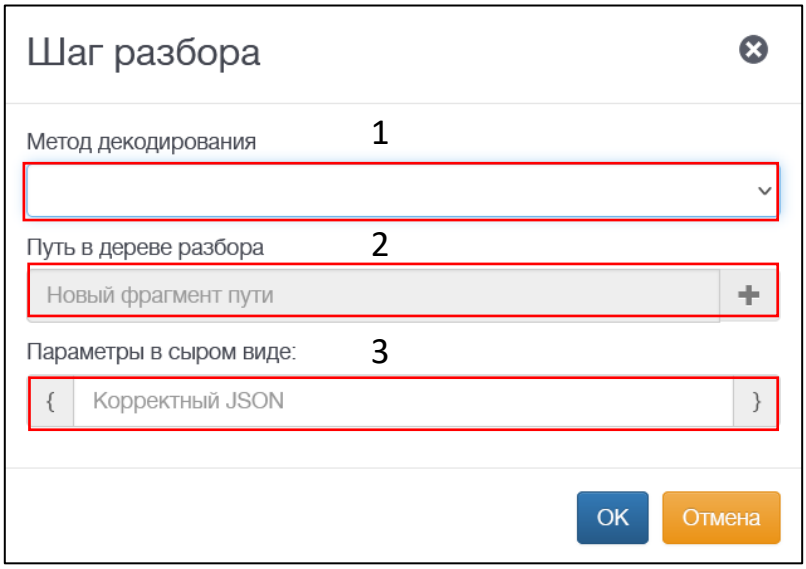

Рисунок 128 – Окно «Шаг разбора»

1. Метод декодирования – выбирается метод декодирования, с помощью которого будет разбираться значение.

Методы декодирования описаны в таблице 10.

Таблица 10 – Методы декодирования

Метод декодирования	Описание
Декомпрессия deflate	Декомпрессия данных, сжатых при помощи алгоритма сжатия deflate. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
Декомпрессия gzip	Декомпрессия данных, сжатых при помощи алгоритма сжатия GZIP. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
Метка случайного значения	Данный парсер отключает автоматическую задачу по обновлению\углублению дерева разбора для заданного в пункте 2 (см. рисунок 128) значения узла. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
Разбор веб-форм	Декодирует значения в кортежах с ключом, разделённых символом '&', с '=' между ключом и значением (content-type: application/x-www-form-urlencoded). В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
Разбор значений заголовка «Content-Type»	Разбор заголовка «Content-Type». Необходим для корректной работы модуля протокольной валидации (описана в разделе 9), а именно проверки разрешенных MIME-типов. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
Разбор значений заголовка «Cookie»	Разбирает массив кук, содержащийся в заголовке «Cookie» на отдельные элементы. Используется только для углубления дерева разбора запроса. В поле 3 (Рисунок 128) ввод дополнительных параметров не требуется
Разбор значений заголовка Set-Cookie	Разбирает массив кук, содержащийся в заголовке Set-Cookie на отдельные элементы. Используется только для углубления дерева разбора ответа. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
Разбор по заданному префиксу (prefix)	Разбирает значение, находящиеся по введенному в пункте 2 пути (см. рисунок 128), по заданному префиксу. Данный метод декодирования не будет работать, если не задать параметр в пункте 3 (см. рисунок 128). Пример параметра в сыром виде: «"prefix":""», в кавычки после знака «:» необходимо ввести значение префикса
Разбор регулярного выражения (pattern) в соответствии с именами групп (group_names)	Разбивает значение поля, заданного в пункте 2 пути (см. рисунок 128), с помощью регулярного выражения (pattern) на заданное количество групп (group_names). Количество групп в «pattern» должно совпадать с количеством имен в «group_names». Пример параметра в сыром виде: "group_names":["group1","group2"],"pattern":"(\\d+) (\\d+)"
Разбор multipart с автоопределением разделителя (применяется к дереву в целом)	Разбирает тело запроса (необходимо применять только для POST запросов) с автоматическим определением разделителя. Для корректной работы необходимо не указывать значение пути в пункте 2 (см. рисунок 128). В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется

Метод декодирования	Описание
Разбор multipart с ручной настройкой разделителя	Разделяет значение поля, заданного в пункте 2 пути (см. рисунок 128), по заданной границе (boundary). Данный метод декодирования не будет работать, если не задать параметр в пункте 3 (см. рисунок 128). Пример параметра в сыром виде: «"boundary":""», в кавычки после знака «:» необходимо ввести значение границы, по которой будет делиться значение
Разбор URL	Выполняет функцию URL декодера. Может быть использован, как и без дополнительных параметров в поле 3 (Рисунок 128), так и со следующими параметрами: default_scheme – схема, используемая в URL; normalize_path – нужно ли декодеру нормализовать путь (свернуть избыточные разделители, ссылки на более высокий уровень и т. д.); decode_path_parameters – нужно ли декодеру декодировать параметры пути. По умолчанию: «"default_scheme":"b'","normalize_path":"False", "decode_path_parameters":"False"»
Сериализованный объект PHP	Декодирование сериализованного объекта PHP. Данный метод декодирования не будет работать, если не задать параметр в пункте 3 (см. рисунок 128)
Токен, зашифрованный AES	Дешифрование токена, зашифрованного с помощью алгоритма AES. При выборе данного метода декодирования появляются дополнительные поля: Ключ – поле ввода ключа для дешифрования; Длина nonce – количество первых байт из расшифруемого значения, которые будут использованы, как вектор инициализации дешифрования; Разбор JSON – чекбокс, включающий или выключающий разбор JSON для дешифрованного сообщения. Данный метод декодирования не будет работать, если не задать данные параметры
Экранирование косой чертой (\xaf и \n и т.д.)	Убирает экранирование косой чертой по заданным параметрам: u_escape: экранирование юникода, начинающееся с обратной косой черты, строчной буквы «u» и с не более чем 4 шестнадцатеричными цифрами после; U_escape: экранирование юникода, начинающееся с обратной косой черты, заглавной буквы U и с не более чем 8 шестнадцатеричными цифрами (обратите внимание, что результирующий кодовая точка должна быть меньше MAX_UNICODE); octal_escape: обратная косая черта, за которой следуют от 1 до 3 восьмеричных цифр; hex_escape: обратная косая черта, за которой следует «x» и не более 2 шестнадцатеричных цифр. literal_escape: обратная косая черта, за которой следует символ; CSS_escape: обратная косая черта, за которой следует от 1 до 6 шестнадцатеричных цифр. Каждый из параметров может принимать только два значения «true» и «false». Пример параметра в сыром виде: "CSS_escape":"true"

Метод декодирования	Описание
Base16	Выполняет функцию Base16 декодера. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
Base32	Выполняет функцию Base32 декодера. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
Base64	Выполняет функцию Base64 декодера. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
Base64-Url	Выполняет функцию Base64-url декодера. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
CBT encrypted cookie	Дешифрование токена, зашифрованного с помощью алгоритма CBT. При выборе данного метода декодирования появляются дополнительные поля: Ключ – поле ввода ключа для дешифрования; Длина nonce – задает количество первых байт из расшифруемого значения, которые будут использованы, как вектор инициализации дешифрования. Данный метод декодирования не будет работать, если не задать данные параметры
CSV (значения, разделенные запятыми)	Деление значение формата «CSV». Может быть использован без дополнительных параметров в поле 3 (см. рисунок 128). Параметры также могут быть использованы по отдельности: Delimiter – делит значение по указанному символу; Doublequote – управляет обработкой кавычек внутри полей. При значении «True» две последовательные кавычки при чтении интерпретируются как одна, а при записи каждый символ кавычки, встроенный в данные, записывается как две кавычки; Escapechar – относится к строке из одного символа, используемой для выхода из разделителя, когда для цитирования установлено значение; Quotechar – относится к строке из одного символа, которая будет использоваться для заключения значений в кавычки, если внутри поля появятся специальные символы; Skipinitialspace – определяет, как будет интерпретироваться пробел после разделителя. Если «True», начальные пробелы будут удалены. По умолчанию оно равно «False». По умолчанию: «”delimiter”:”,”, ”doublequote”:”True”, “escapechar”:”None”, “quotechar”:”"”, “skipinitialspace”:”False”»
DSV (значения, разделенные произвольными разделителями)	Делит значение по двум заданным символам в поле 3 (см. рисунок 128). По умолчанию: «”delimiters”:”,”,”:”»
GraphQL	GraphQL парсер. Разбирает GraphQL на параметры. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
GSSC encrypted cookie	Дешифрование токена, зашифрованного с помощью алгоритма GSSC. При выборе данного метода декодирования появляются дополнительные поля: Ключ – поле ввода ключа для дешифрования; Длина nonce – задает количество первых байт из расшифруемого значения, которые будут использованы, как вектор инициализации дешифрования.

Метод декодирования	Описание
	Данный метод декодирования не будет работать, если не задать данные параметры
GWT RPC	Парсер GWT RPC. Разбирает GWT RPC. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
HTML	HTML парсер. Разбирает HTML на параметры. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
HTML-сущности	Парсер HTML-сущности. Разбирает HTML-сущность на параметры. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется.
JSON	JSON парсер. Разбирает JSON на параметры. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
JSON RPC	JSON RPC парсер. Разбирает JSON RPC на параметры. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
JSONP	JSONP парсер. Разбирает JSONP на параметры. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
Метка передачи файла определенного формата	Данный парсер отключает автоматическую задачу по обновлению\углублению дерева разбора для заданного в пункте 2 (см. рисунок 128) значения узла. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
SOAP	SOAP парсер. Разбирает SOAP на параметры. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
Url-кодирование	Выполняет функцию URL декодера. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
XML	XML парсер. Разбирает XML на параметры. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
XML RPC	XML парсер. Разбирает XML на параметры. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется
YAML	YAML парсер. Разбирает YAML на параметры. В поле 3 (см. рисунок 128) ввод дополнительных параметров не требуется

2. Путь в дереве разбора – поле задания пути к значению, которое необходимо декодировать.
3. Параметры в сыром виде – поле ввода параметров декодирования (необходимо не для всех методов декодирования).

Для удаления блока декодирования необходимо нажать на иконку «  » в правом верхнем углу того блока, который необходимо удалить.

Примечание: при удалении блока, к которому снизу присоединен еще блок (дочерний), будет удален как выбранный блок, так и дочерний. При первом сохранении дерева разбора (нулевая ревизия) – будет предложена возможность сохранить разбор по умолчанию на все приложения.

10.2. Условия для блоков декодирования

При добавлении к родительскому блоку дочернего между ними появляется условие (см. рисунок 129). Изменить условие можно в любой момент, кликнув по нему левой кнопкой мыши.

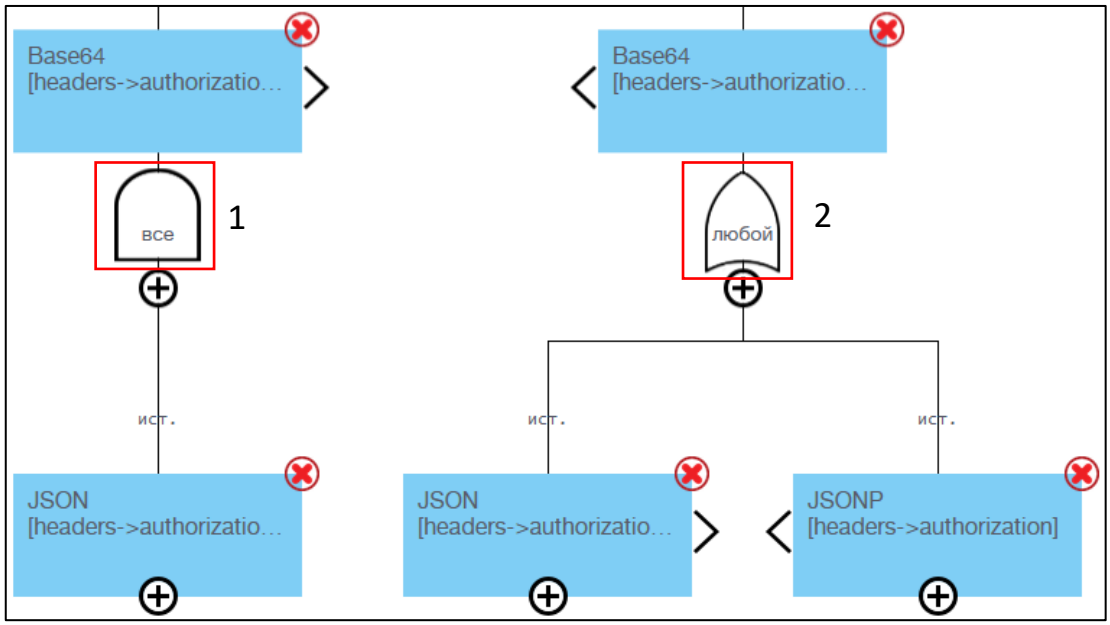

Рисунок 129 – Условие декодирования

- Все – данное условие означает, что значение должно разбираться всеми следующими за ним дочерними блоками декодирования, если хотя бы один дочерний блок не разберет значение – будет сгенерирована аномалия;
- Любой – данное условие означает, что значение должно разбираться любым следующим за ним дочерним блоком декодирования, если ни один из дочерних блоков не разберет значение – будет сгенерирована аномалия.

Над каждым блоком также присутствует его условие истинности. Задать его можно, кликнув по условию истинности (см. рисунок 130).

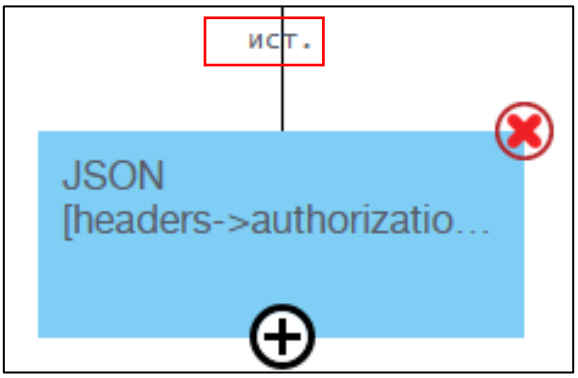

Рисунок 130 – Условие истинности

При нажатии на выбранную область появится окно задания условия истинности (см. рисунок 131).

Рисунок 131 – Окно задания условия истинности

Для изменения условия истинности необходимо кликнуть на условие. Имеется четыре варианта условий истинности:

1. По умолчанию – при выборе данного условия будет считаться, что данный блок декодирования работает всегда.
2. Регулярное выражение – при выборе данного условия необходимо ввести путь к значению и регулярное выражение, которому оно (значение) должно соответствовать. Данный блок декодирования будет работать только если выполнится заданное условие.
3. Точное значение – при выборе данного условия необходимо ввести путь к значению и его точное значение. Данный блок декодирования будет работать, только если выполнится заданное условие.
4. Наличие путей – при выборе данного условия необходимо ввести путь. Данный блок декодирования будет работать, только если в запросе\ответе (в зависимости от того, какое дерево разбора углубляется) будет присутствовать данный путь.

Примечание: условия истинности родительских блоков имеют приоритет, если они не выполняются, то и дочерние блоки тоже не работают.

10.3. Ревизии настроек дерева разбора

На WAF имеется возможность переключения между ревизиями настроек данной вкладки. Выбор ревизии находится в выделенной области на рисунке 132.

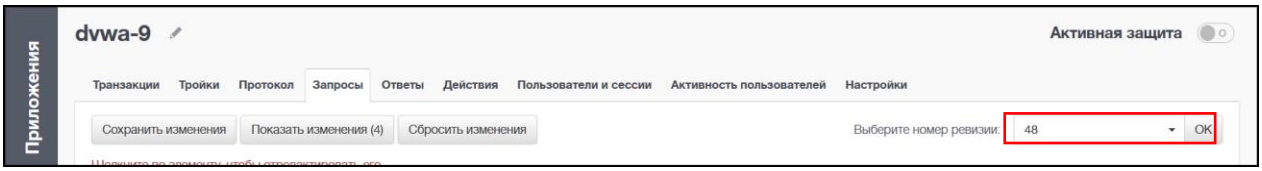

Рисунок 132 – Выбор ревизии

После выбора ревизии, отличной от актуальной, можно нажать на кнопку «ОК» для просмотра настроек данной ревизии. Для того, чтобы применить выбранную ревизию, необходимо нажать на кнопку «Откатить».

11. Маскирование

На WAF имеется возможность маскирования полей (изменяет отображение полей в веб-интерфейсе WAF).

Для настройки маскирования необходимо перейти на вкладку «Приложения» -> «Настройки» перейти вниз страницы и нажать на кнопку «+ Добавить» (см. рисунок 133).

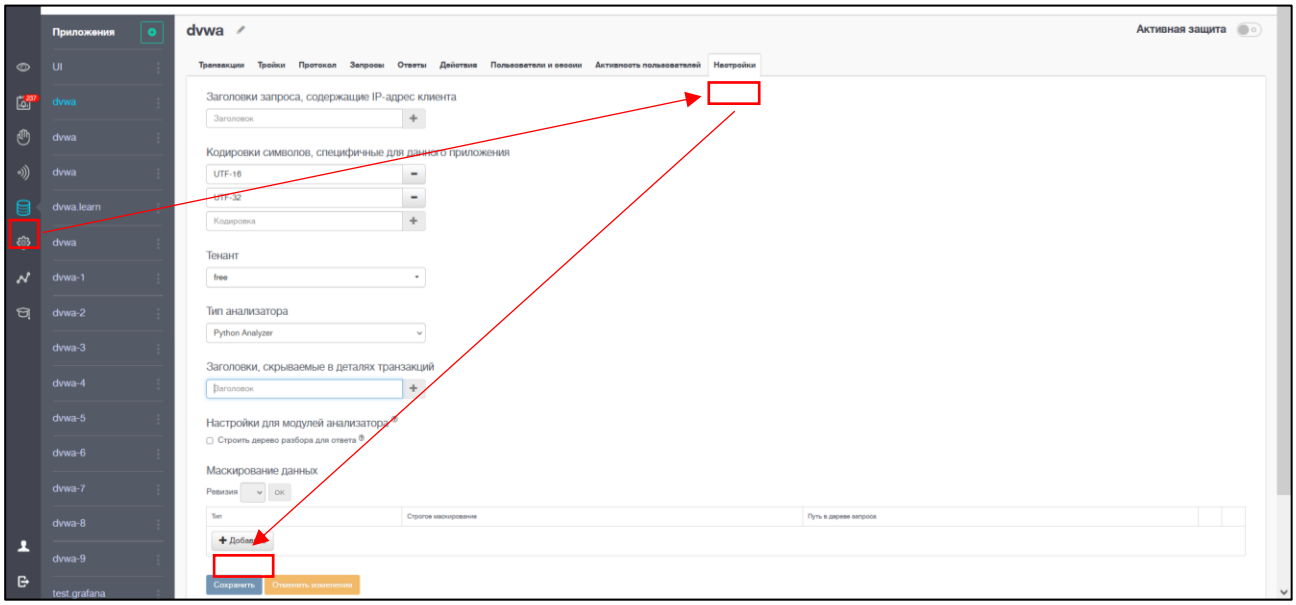

Рисунок 133 – Добавление маскирования

После нажатия на кнопку добавления появляется окно создания маскирования (см. рисунок 134).

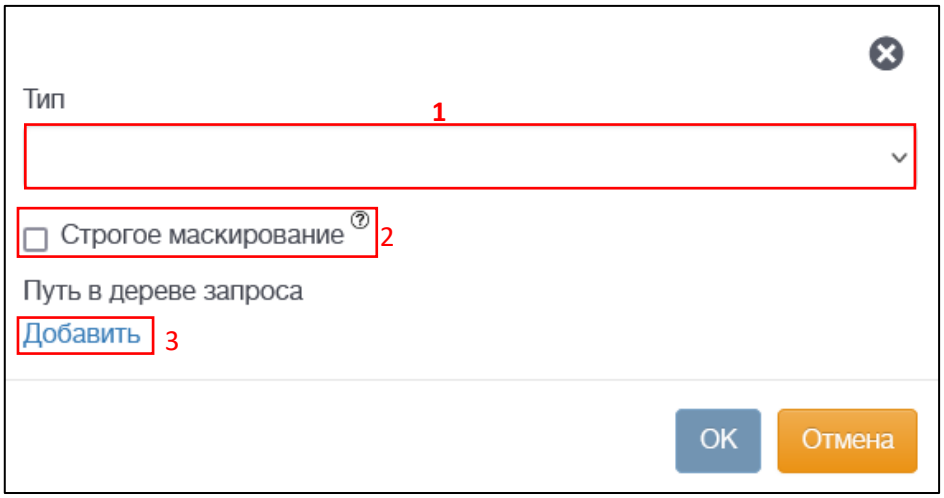

Рисунок 134 – Настройка маскирования

1. Тип – выбор типа маскирования из выпадающего списка. Описание типов изложено в таблице 11.

Таблица 11 – Описание типов маскирования

Тип	Описание
Умная замена	Сохраняет тип символа (цифры, нижний/верхний регистр ASCII), заменяя его другим случайным символом

Замена на случайные байты	Заменяет символы маскируемого элемента на случайные байты
Пароль	Заменяет символы маскируемого элемента на случайные
Число	Заменяет только числа на случайные числа
CVC	Заменяет тройки цифр на случайные символы
Номер кредитной карты	Заменяет строку, подходящую под форму номера кредитной карты на случайные цифры
Полное удаление данных поддрева	Скрывает путь дерева разбора, оставляя пустое значение на месте пути

2. Строгое маскирование – используется для замены только одним символом каждого типа (456 -> 000, word -> aaaa).
3. Путь – путь в дереве разбора до элемента, который необходимо маскировать.

Если после настройки маскирования данные в дереве разбора не маскируются, необходимо проверить, что маскирование включено в настройках анализатора (см. раздел 0).

Примечание: некорректно будет настраивать маскирование на URL или его части, это приведет к некорректному отображению транзакций в веб-интерфейсе.

11.1. SessionAnomalyCounter

Данный модуль отвечает за подсчёт количества аномалий в рамках пользовательской сессии.

Перечень настроек, которые разрешено менять пользователям представлены в таблице 12.

Таблица 12 – Перечень настроек модуля SessionAnomalyCounter

Настройки	Описание
anomaly_threshold	Размер ведра для аномалий, при переполнении которого будет сгенерирована аномалия

Примечание: остальные параметры настройки анализатора, которые не были описаны в данном документе, менять без согласования категорически не рекомендуется.

12. Работа со списками

На WAF имеется возможность создания списков, которые потом в последствии могут быть использованы в источниках.

12.1. Создание списков

Для того, чтобы создать список необходимо перейти на вкладку «Источники, списки, цели» -> «Списки» и нажать на кнопку «Добавить список» (см. рисунок 135).

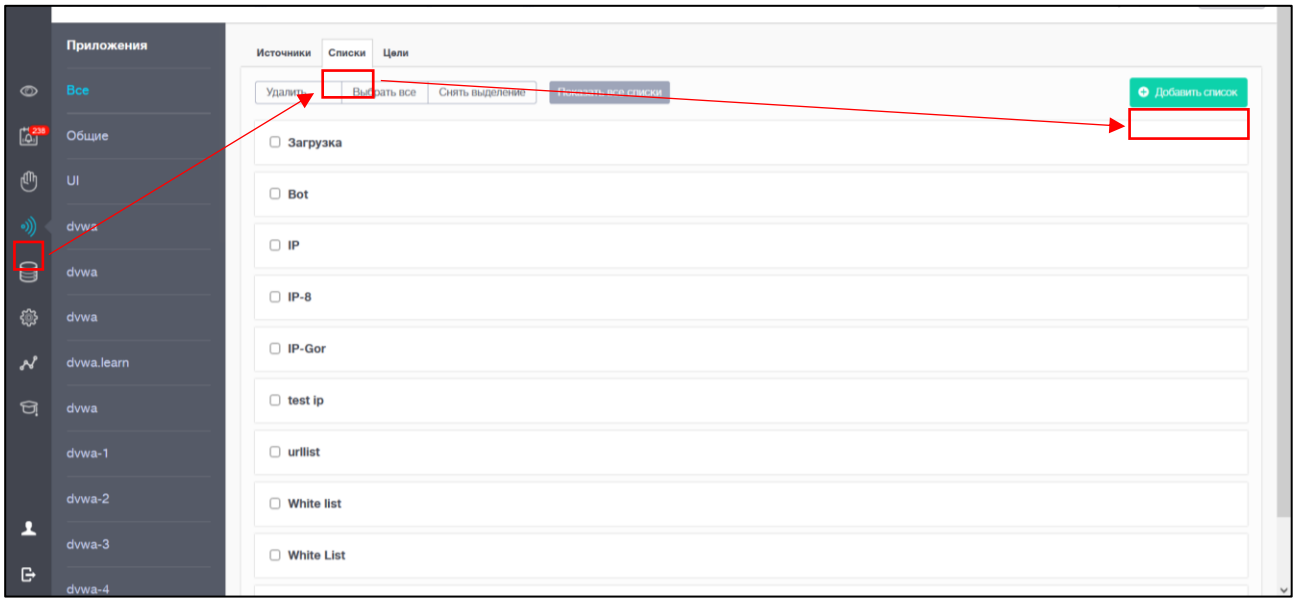

Рисунок 135 – Создание списка

После нажатия на иконку создания списка появляется окно создания нового списка (см. рисунок 136).

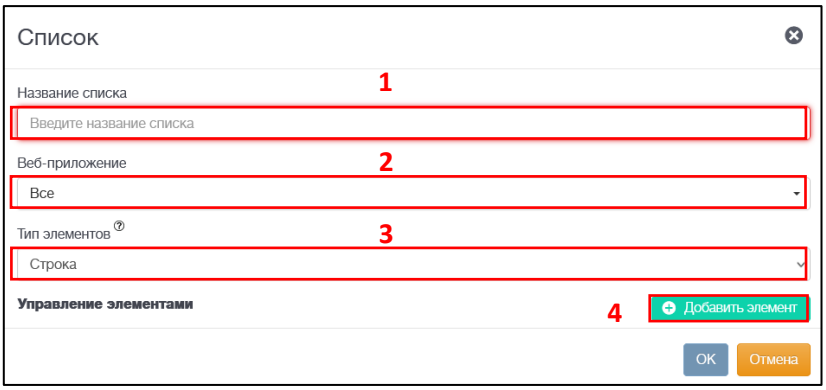

Рисунок 136 – Создание списка

1. Название списка – поле ввода название списка. Лучше давать спискам развернутые названия, так как при выборе списка в источнике будет видно только название.
2. Веб-приложение – выбор приложения из всех заведенных на тенанте или инсталляции.
3. Тип элементов – выбор расширения элементов списка. Есть три варианта: строка, целое число, IP-адрес.
4. Добавление элемента – данная кнопка открывает окно добавления элемента списка (см. рисунок 137).

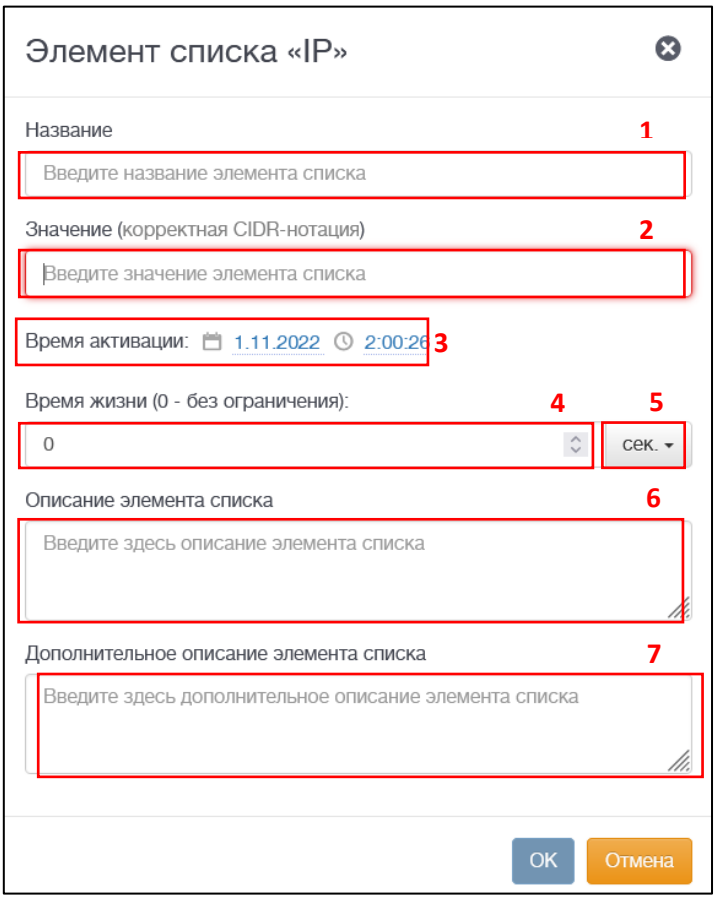

Рисунок 137 - Добавление элемента списка

Окно добавления элемента списка содержит следующие элементы:

1. Название – поле для ввода названия элемента.
2. Значение – ввод значения элемента. В данном поле присутствует проверка введенного значения на соответствие типу элемента, выбранного при создании списка.
3. Время активации – дата и время, с которого начнет работать данный элемент списка. После выбора даты открывается поле «Время жизни».
4. Время жизни – поле ввода времени жизни (имеется возможность введения дробного значения). Если в данном поле будет «0», то время жизни элемента будет без ограничений.
5. Выбор значения – имеется пять вариантов: секунды, минуты, часы, дни, недели.
6. Описание элемента списка – поле для ввода описания данного элемента списка.
7. Дополнительное описание элемента списка – дополнительное поле для ввода описания данного элемента списка.

Добавленный элемент появляется внизу окна добавления списка (см. рисунок 138). Его можно отредактировать, нажав на иконку «», или удалить, нажав на иконку «».

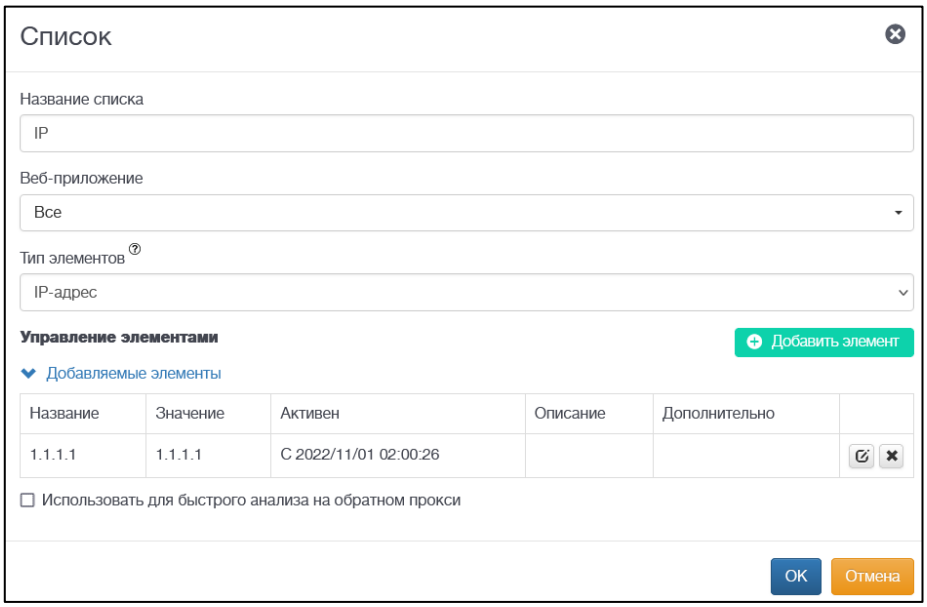

Рисунок 138 – Список, с добавленным элементом

В случае если в списке не выбрано веб-приложение, а значение поля «Тип элементов» - IP-адрес, появляется возможность использовать данный список для быстрого анализа на обратном прокси. Для этого необходимо кликнуть на квадратик возле соответствующего оповещения внизу списка (см. рисунок 139).

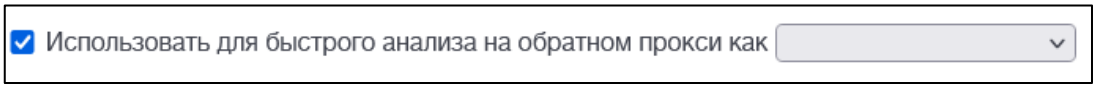

Рисунок 139 – Использование списка для быстрого анализа на обратном прокси

Есть два варианта использования списка для быстрого анализа на обратном прокси:

- Список разрешенных – транзакции, с IP-адресами, соответствующими элементам списка, будут пропускаться на обратном прокси.
- Список запрещенных – транзакции, с IP-адресами, соответствующими элементам списка, будут блокироваться на обратном прокси.

12.2. Редактирование элементов списка

Для того чтобы создать список необходимо перейти на вкладку «Источники, списки, цели» -> «Списки», открыть расширенное описание необходимого списка и нажать на кнопку «Редактировать» (см. рисунок 140). Дальнейшие действия по изменению, добавлению, удалению элементов списка идентичны описанным действиям в разделе 12.1.

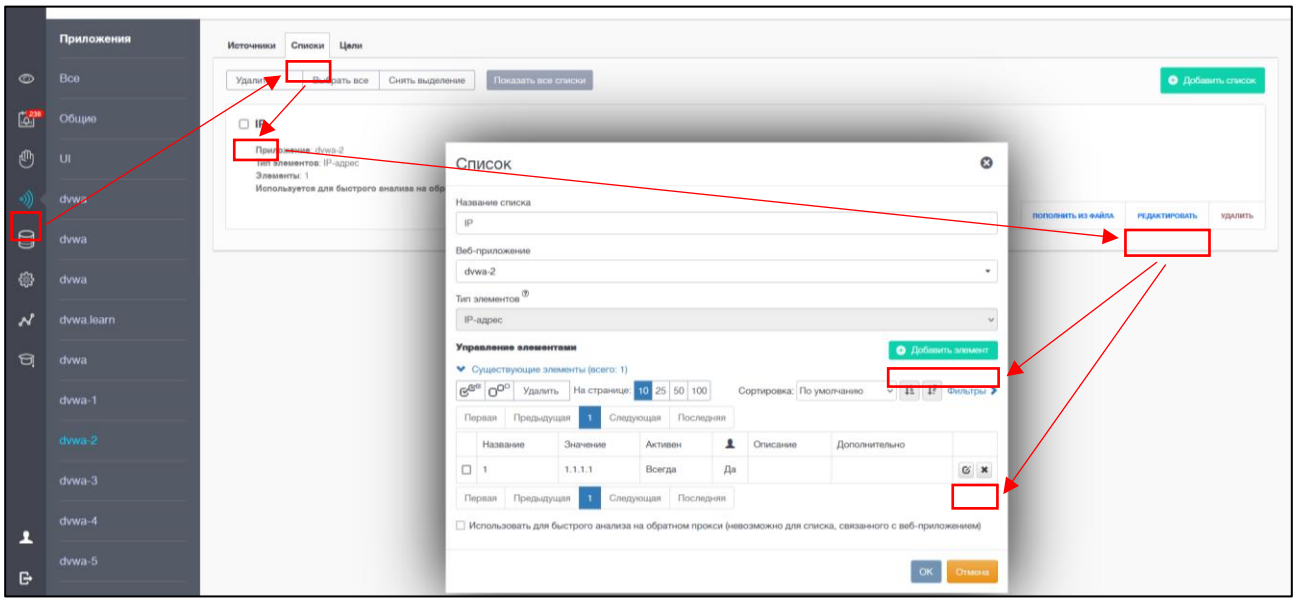

Рисунок 140 - Изменению, добавлению, удалению элементов

В уже созданный список можно добавить записи из файла в формате «CSV» (пишутся только значения элементов списка), достаточно нажать на кнопку «Загрузить из файла» и выбрать необходимый файл в появившемся окне.

13. Работа с источниками

На WAF имеется возможность использовать любой элемент дерева разбора в качестве источника. Источник может быть использован в детекторе переборных атак в качестве элемента, от которого считается количество обращений, или в правиле в качестве элемента, наличие (отсутствие) которого проверяется в поступающих транзакциях. Списки, описание работы с которыми было рассмотрено в разделе 12, могут быть использованы в источниках в качестве элемента, который реализует фильтрацию значений источника.

13.1. Создание источников

Для того чтобы создать источник необходимо перейти на вкладку «Источники, списки, цели» -> «Источники» и нажать на кнопку «Добавить источник» (см. рисунок 141).

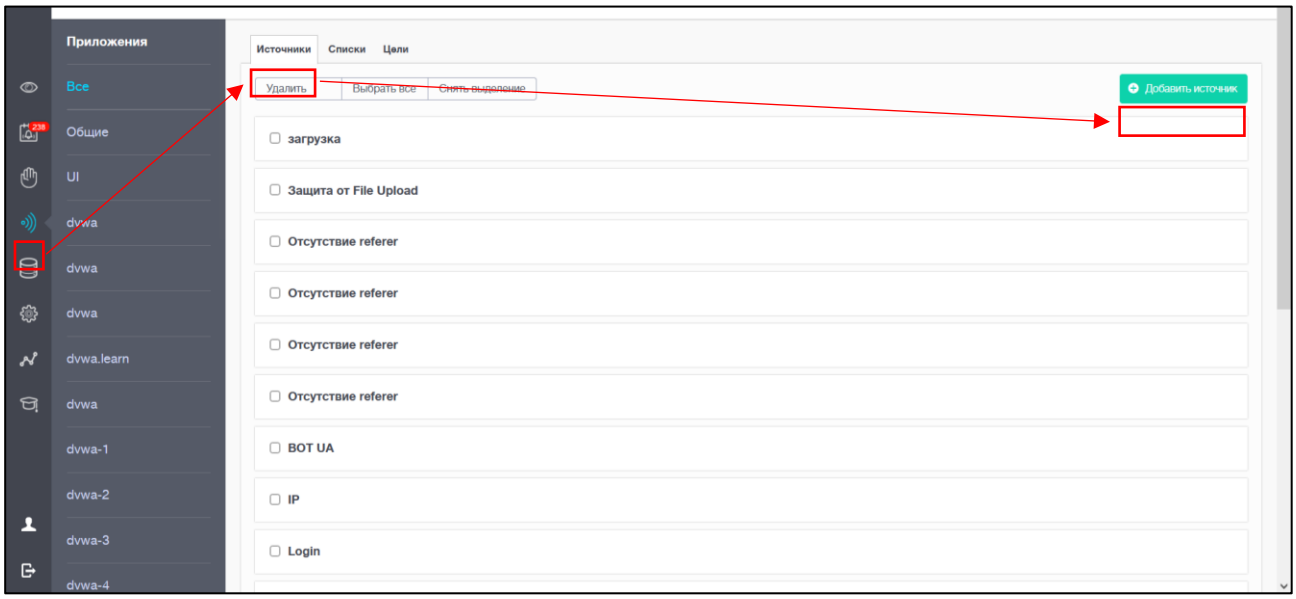

Рисунок 141 – Создание источника

После нажатия на кнопку создания источника появляется окно создания нового источника (см. рисунок 142).

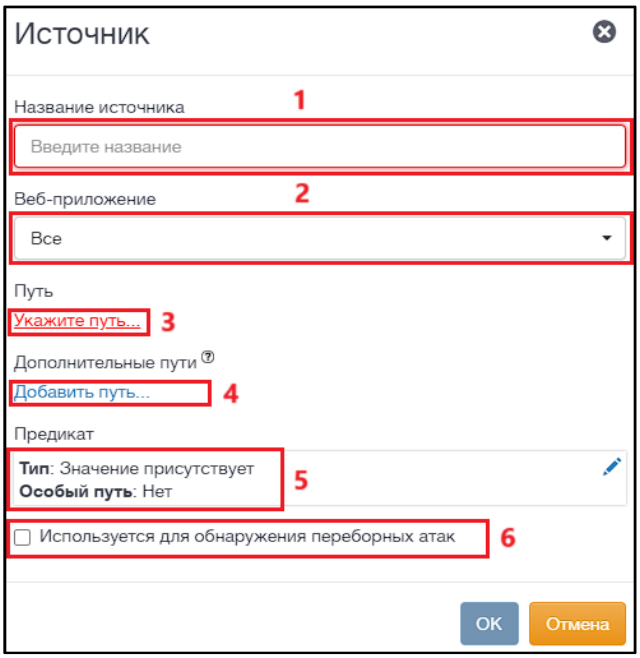

Рисунок 142 – Создание источника

Окно создания источника содержит следующие элементы:

1. Название источника – поле ввода название источника. Лучше давать источникам развернутые названия, так как при выборе источника в правиле или детекторе переборных атак будет видно только название.
2. Веб-приложение – выбор приложения из всех заведенных на тенанте или инсталляции.
3. Путь – путь в дереве разбора до элемента, выбранного в качестве источника.
4. Дополнительные пути – дополнительные пути для извлечения значения источника из дерева разбора (необходим для создания составных источников, например IP+UA). Преимущественно используются для таргетной настройки детекторов переборных атак (см. рисунок 143).

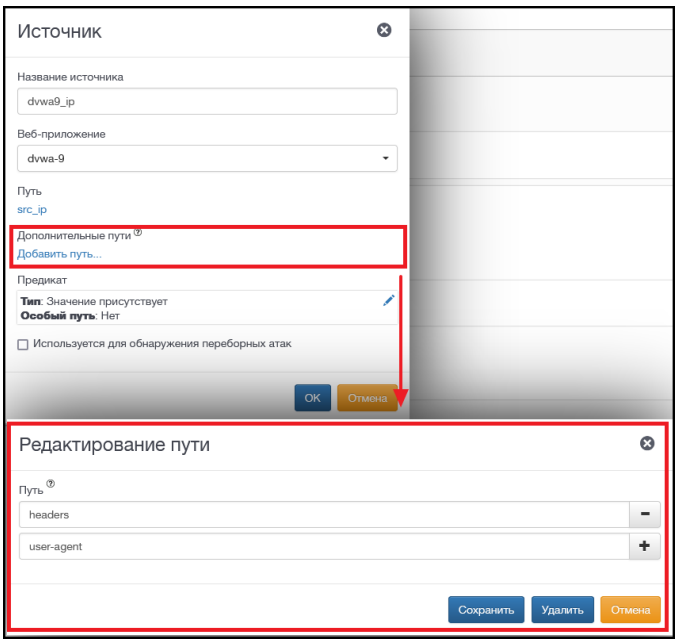

Рисунок 143 – Добавление дополнительного пути

5. Тип предиката источника – список возможных типов предикатов источника (см. рисунок 144).

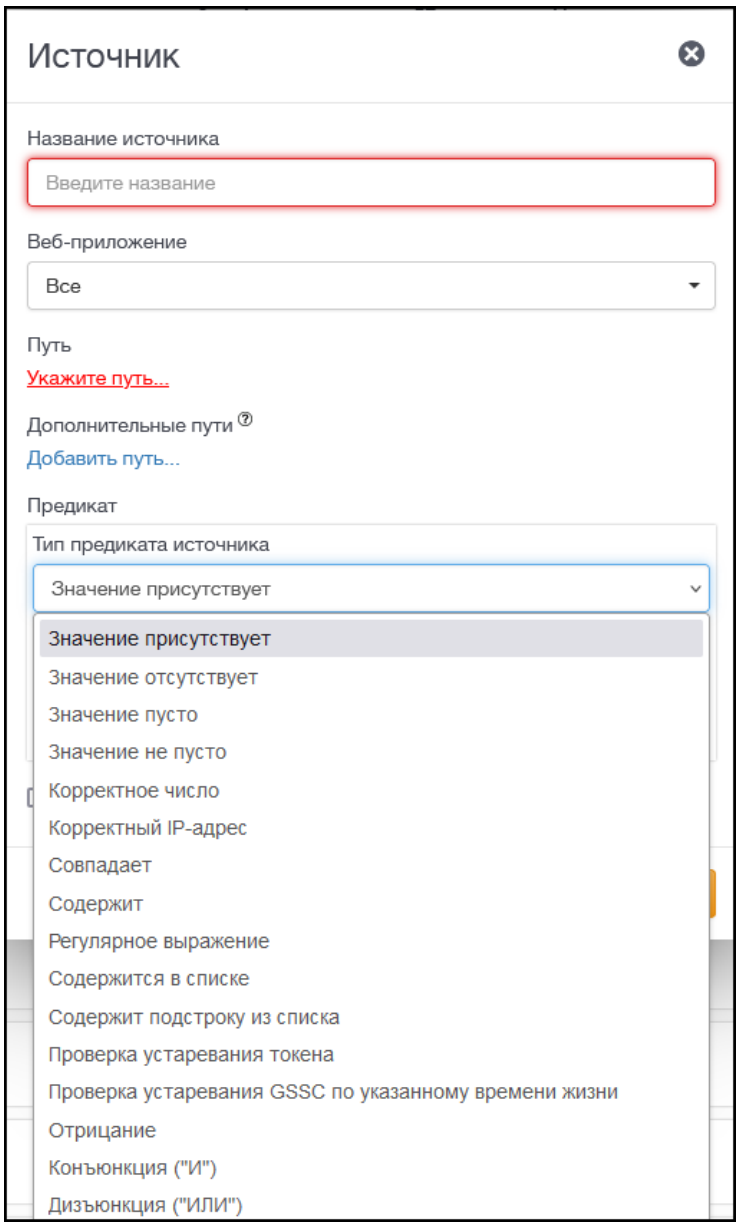

Рисунок 144 – Возможные значения предиката

Возможные значения с описанием дополнительных параметров представлены в таблице 13.

6. Используется для обнаружения переборных атак – источник появляется в меню настройки переборных атак.

Таблица 13 – Тип предиката источника

Тип предиката источника	Описание	Дополнительные параметры («–» - если их нет)
Значение присутствует	Проверяет наличие пути, заданного в 3 пункте	–
Значение отсутствует	Проверяет отсутствие пути, заданного в 3 пункте	–
Значение пусто	Проверяет отсутствие значения элемента, по заданному в 3 пункте пути	–

Тип предиката источника	Описание	Дополнительные параметры («–» - если их нет)
Значение не пусто	Проверяет наличие значения элемента по заданному в 3 пункте пути	–
Корректное число	Проверяет, что значения элемента, по заданному в 3 пункте пути, является корректным числом	–
Корректный IP-адрес	Проверяет, что значения элемента по заданному в 3 пункте пути, является корректным IP-адресом	–
Совпадает	Проверяет, что значения элемента по заданному в 3 пункте пути, совпадает с значением, указанном в дополнительном параметре «Значение»	Значение – поле для ввода значения
		Тип значения (строка, целое число, IP-адрес) – выбор типа, заданного выше значения
Содержит	Проверяет, что значения элемента по заданному в 3 пункте пути, содержит значение, указанное в дополнительном параметре «Шаблон»	Шаблон – поле ввода значения
Регулярное выражение	Проверяет, что значения элемента по заданному в 3 пункте пути, удовлетворяет регулярному выражению, заданному в дополнительном параметре «Регулярное выражение»	Регулярное выражение – поле ввода регулярного выражения
		Флаги регулярного выражения, которые можно выставить: игнорирование регистра, многострочность, сопоставление точки символам конца строки, обработка символов unicode
Содержится в списке	Проверяет, что значения элемента, по заданному в 3 пункте пути, совпадает со значением из списка, заданного в дополнительном параметре «Список»	Список – выбор списка (создание списка описано в разделе 12)
Содержит подстроку из списка	Проверяет, что значения элемента, по заданному в 3 пункте пути, содержит значение из списка, заданного в дополнительном параметре «Список»	Список – выбор списка (создание списка описано в разделе 12)
Проверка устаревания токена	Проверяет, что значения элемента по заданному в 3 пункте пути, не устарело (в соответствии с заданными значениями дополнительных параметров)	Путь-префикс – базовый путь в дереве разбора до токена. Если задан - будет префиксом для всех остальных путей, если не задан - остальные пути будут не суффиксами, а абсолютными путями в дереве разбора
		Путь к моменту устаревания токена – Путь в дереве разбора

Тип предиката источника	Описание	Дополнительные параметры («–» - если их нет)
		к временной метке или дате устаревания токена. Если задан - устаревание токена будет проверено только по данному значению, в ином случае будут проверяться время или дата создания и время жизни токена
		Путь к моменту создания токена – Путь в дереве разбора к временной метке или дате создания токена. Используется в связке с временем жизни токена, если не задан путь к временной метке или дате устаревания
		Путь к времени жизни токена – Путь в дереве разбора к времени жизни токена. Используется в паре с временной меткой или датой создания токена, если не задан путь к временной метке или дате устаревания
		Время жизни в секундах – поле, в котором задается время жизни выбранного элемента
Проверка устаревания GSSC по указанному времени жизни	Проверяет, что значения элемента по заданному в 3 пункте пути, не устарело (в соответствии с заданными значениями дополнительных параметров)	Время жизни в секундах – поле, в котором задается время жизни выбранного элемента
Отрицание	Используется как “НЕ”, например “НЕ” содержится в списке	–
Конъюнкция «И»	Означает что источник должен удовлетворять условиям логического «И» т.е должны выполняться «И одно И другое условие одновременно»	–
Дизъюнкция «ИЛИ»	Означает что источник должен удовлетворять условиям логического «ИЛИ» т.е. должны выполняться «ИЛИ одно ИЛИ другое условие»	–

13.2. Редактирование источников

Созданные в разделе 13.1 источники можно в любой момент отредактировать, перейдя на вкладку «Источники, списки, цели» -> «Источники», затем открыть на обзор источник, который необходимо отредактировать, и нажать кнопку «Редактировать» (см. рисунок 145). При нажатии кнопки «Редактировать» откроется меню изменения источника (см. рисунок 146).

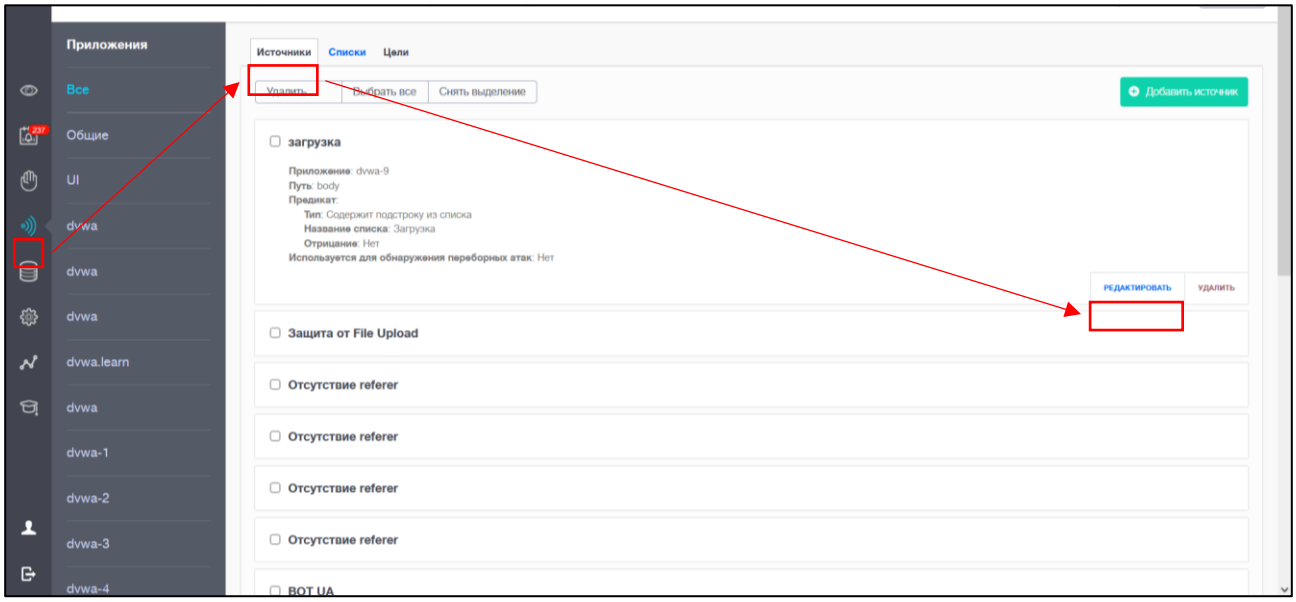

Рисунок 145 – Редактирование источника

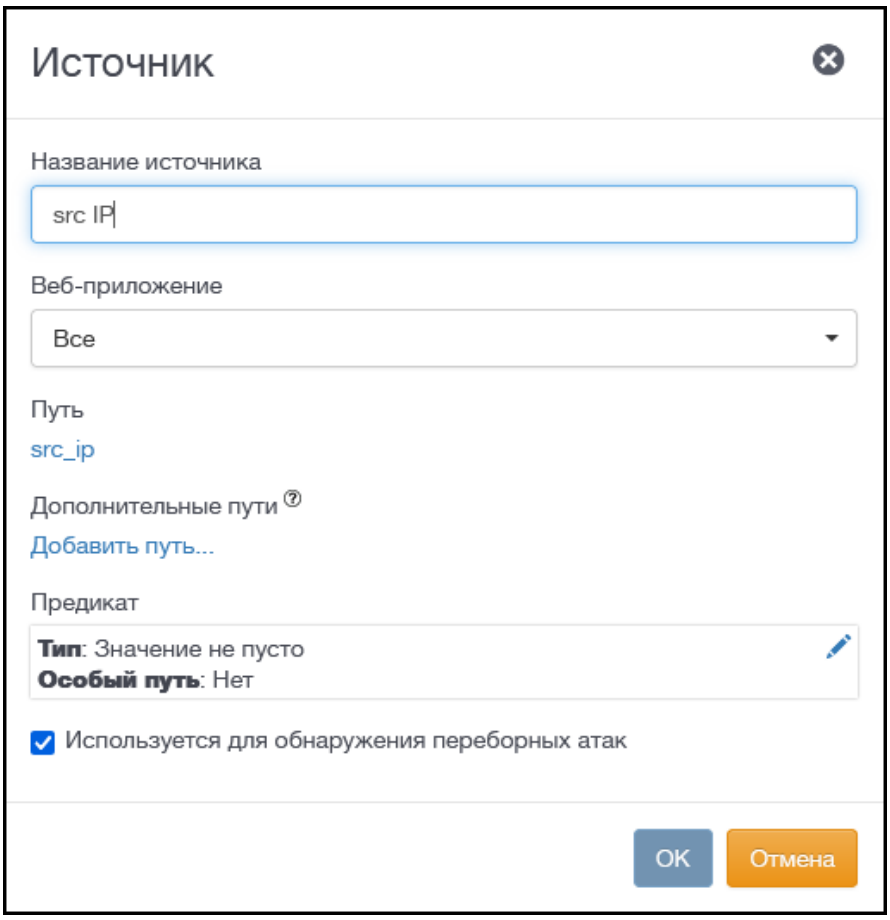

Рисунок 146 **– Редактирование источника**

14. Создание целей

На WAF имеется возможность использовать любой элемент дерева разбора в качестве цели. Источник может быть использован в детекторе переборных атак и в правиле.

14.1. Создание целей

Для того чтобы создать цель необходимо перейти на вкладку «Источники, списки, цели» -> «Цели» и нажать на кнопку «Добавить цель» (см. рисунок 147).

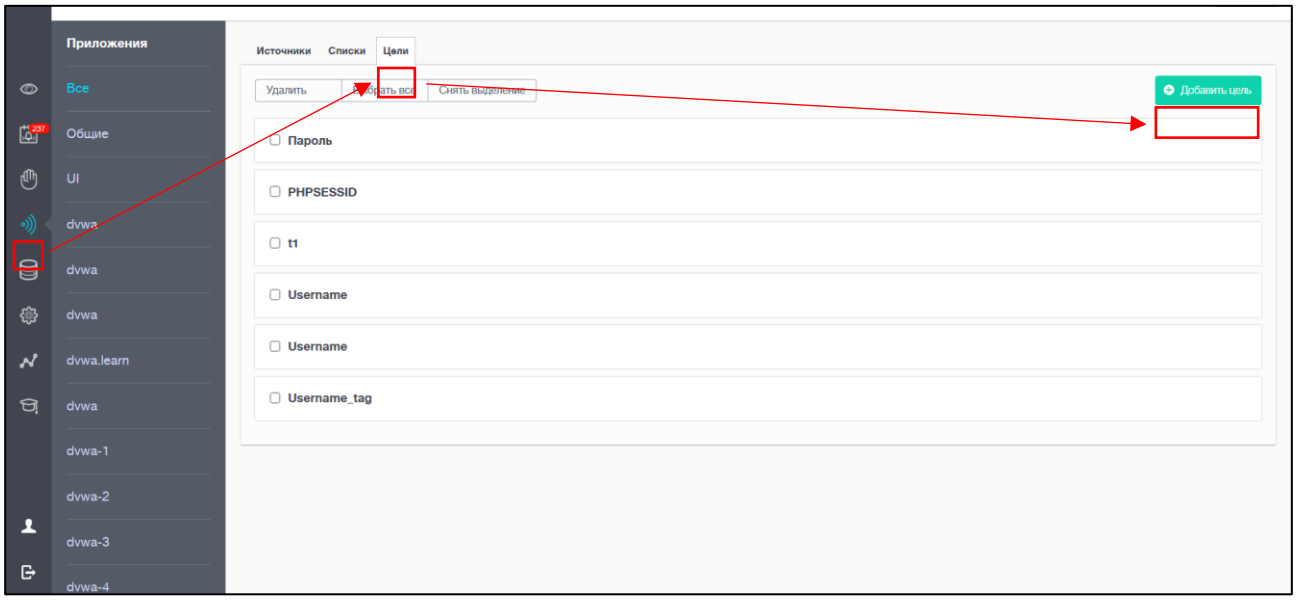

Рисунок 147 – Добавление цели

После нажатия на кнопку создания цели появляется окно создания новой цели (см. рисунок 148).

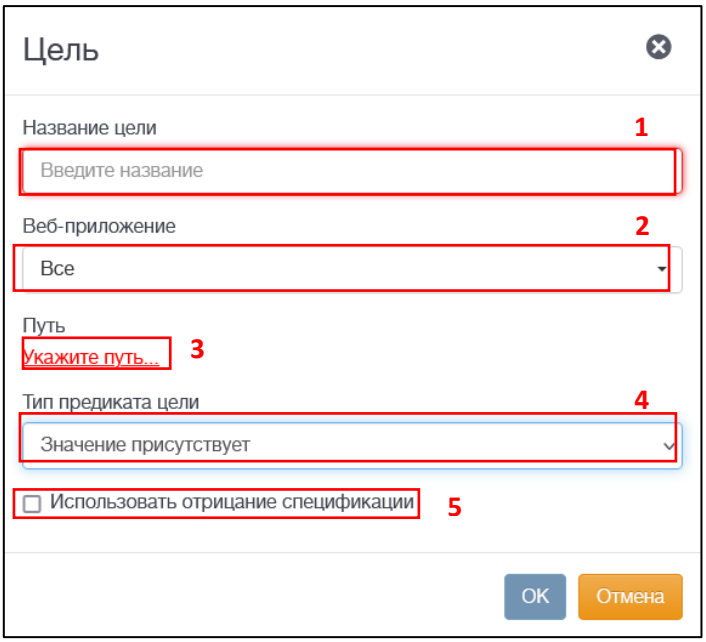

Рисунок 148 - Создание цели

Окно создания цели включает в себя следующие элементы:

1. Название цели – поле ввода название цели. Лучше давать целям развернутые названия, так как при выборе цели в правиле или детекторе переборных атак будет видно только название.
2. Веб-приложение – выбор приложения из всех заведенных на тенанте или инсталляции.
3. Путь – путь в дереве разбора до элемента, выбранного в качестве источника.
4. Тип предиката источника – список возможных типов предиката источника. Возможны два варианта значений данного поля: значение присутствует и значение не пусто.
5. Использовать отрицание спецификации – бинарное поле, которое может принимать значения «Да» или «Нет» («☑», «☐» соответственно). Данное поле отвечает за отрицание значения, выбранного в источнике.

14.2. Редактирование целей

Созданные в разделе 14.1 цели можно в любой момент отредактировать, перейдя на вкладку «Источники, списки, цели» -> «Цели», где открыть на обзор цель, которую необходимо отредактировать, и нажать кнопку «Редактировать» (см. рисунок 149).

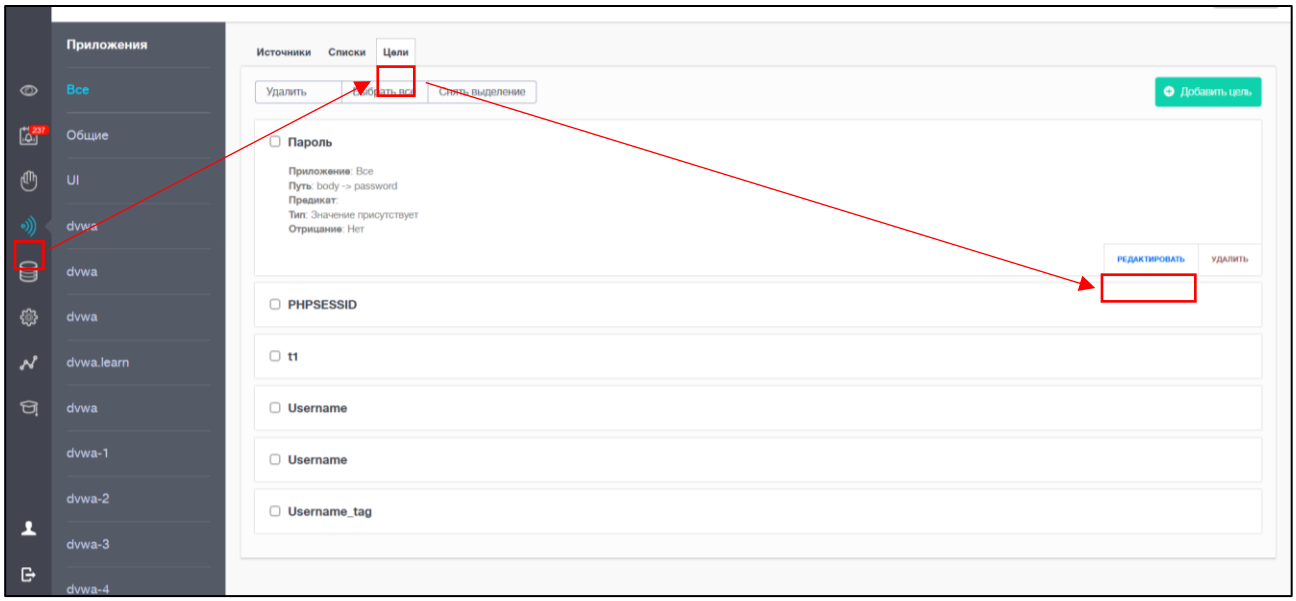

Рисунок 149 – Редактирование цели

15. Работа с действиями

На WAF имеется такая сущность, как действия. Действия – это сопоставление операций клиентов на веб-приложении с логикой работы приложения. При создании действия можно добавлять не только URL, но и другие параметры запроса, отправляемого клиентом.

Созданные действия могут быть использованы для точечного подавления аномалий в качестве параметра в правиле, в качестве параметра при настройке детектора переборных атак, в качестве параметров при настройке сессионной модели, а также других смежных с ней модулей.

По аналогии с настройкой фильтрации запросов к статическим ресурсам, на WAF действия создаются тремя способами, которые описаны в пунктах 15.1 – 15.3.

15.1. Ручное создание действий

Чтобы создать действие, необходимо перейти на вкладку «Приложения» -> «Действия» -> «Бизнес-действия» и нажать на поле «Добавить действие» (см. рисунок 150).

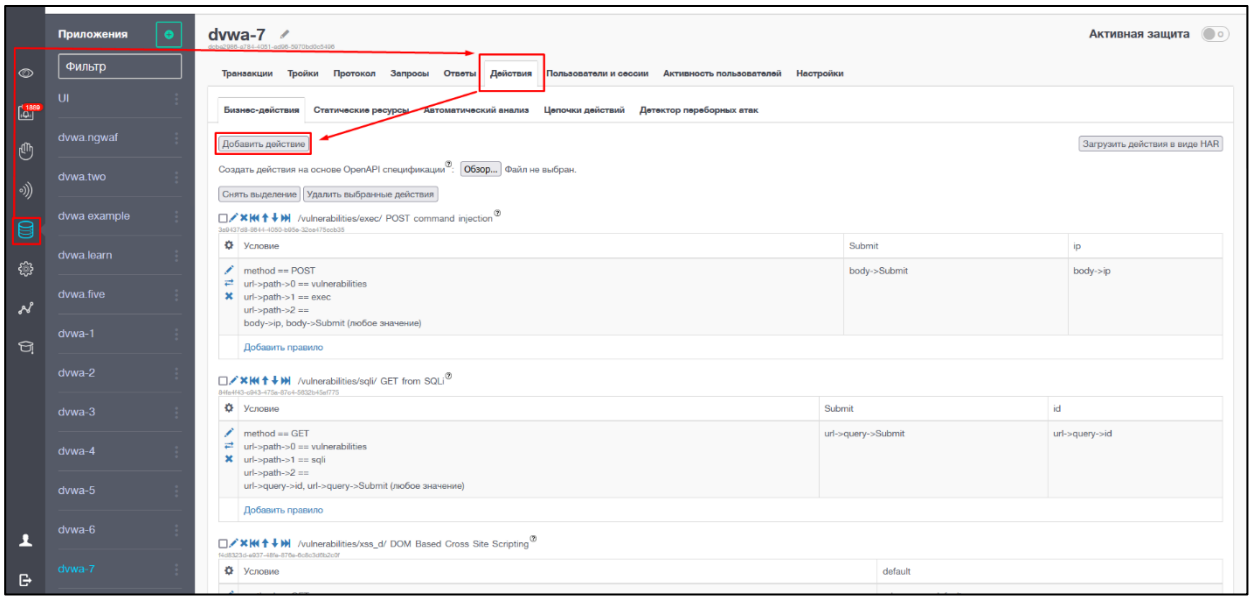

Рисунок 150 – Создание действия

При нажатии на данное поле открывается окно «Модель действия» (см. рисунок 151).

Рисунок 151 – Окно «Модель действия»

Окно «Модель действия» содержит следующие элементы:

1. Название действия – поле для ввода названия действия.
2. Название – поле для ввода параметра действия. В качестве параметра действия можно выбрать один или несколько элементов дерева разбора, которые критичны в рамках данного действия.
3. Обязательный – бинарное поле, которое может принимать значения «Да» или «Нет» («☑» или «☐» соответственно). Данное поле отвечает за обязательность наличия параметра для действия.
4. Массив – бинарное поле, которое может принимать значения «Да» или «Нет» («☑» или «☐» соответственно). Данное поле отвечает за характеристику параметра, как массива данных.
5. Модель – при нажатии выделенной иконки, открывает окно «Редактирование модели параметра» (см. рисунок 152).

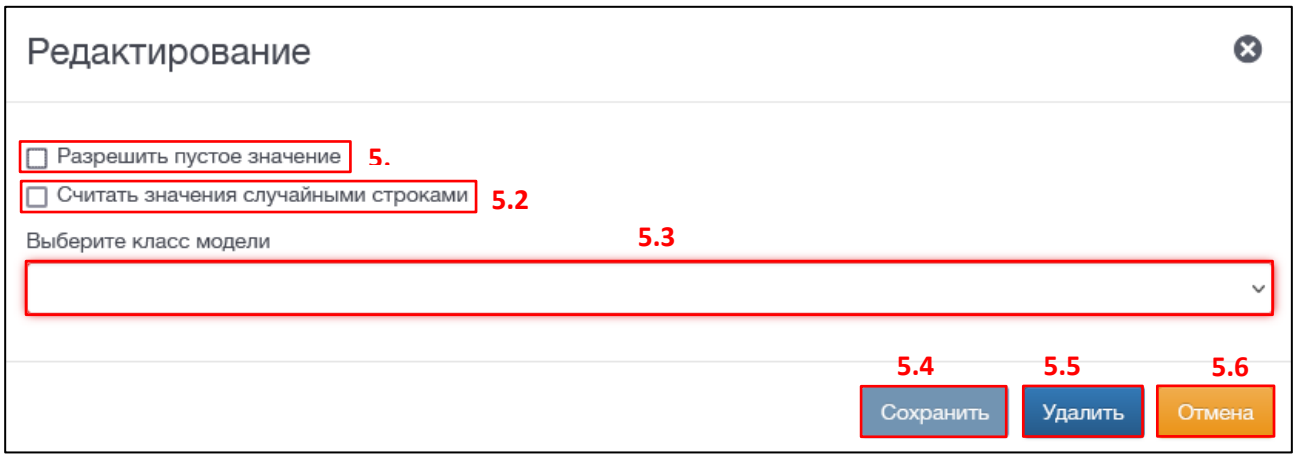

Рисунок 152 – Окно «Редактирование»

5.1. Разрешить пустое значение - бинарное поле, которое может принимать значения «Да» или «Нет» («☑», «☐» соответственно). Данное поле разрешает или запрещает пустое значение выбранного параметра модели.

5.2. Считать значения случайными строками - бинарное поле, которое может принимать значения «Да» или «Нет» («☑», «☐» соответственно). Данное поле разрешает или запрещает интерпретировать выбранный параметр модели действия, как случайную строку.

5.3. Выбор класса модели – выбор из списка возможных классов параметра модели действия. Список с описаниями представлен в таблице 14.

Таблица 14 – Классы модели действия

Класс	Описание	Параметры
Диапазон длин	Неизменяемая последовательность целых чисел	Длина между – выбор значений, между которыми будет рассматриваться длина
Шаблон	Позволяет задавать с помощью регулярного выражения, значения параметра модели действия	Регулярное выражение – поле ввода регулярного выражения значения параметра модели действия
		Допустимые варианты – поле ввода строго заданных допустимых значений для параметра модели действия
Перечисление	Перечисление допустимых вариантов значения параметра модели действия	Допустимые варианты – поле ввода строго заданных допустимых значений для параметра модели действия
E-mail	Проверка значения параметра модели действия на соответствие его стандартному виду адреса электронной почты	Допустимые варианты – поле ввода строго заданных допустимых значений для параметра модели действия
Дата и время	Проверка значения параметра модели действия на соответствие его формату даты и время	Формат – поле ввода формата даты и время
		Допустимые значения – ограничение значений даты и время заданным периодом (по умолчанию ограничений нет)
		Допустимые варианты – поле ввода строго заданных допустимых значений для параметра модели действия
Число	Проверяет значение параметра модели действия на использование в нем исключительно чисел	Разрешить числа с плавающей точкой – поле, разрешающие использование в качестве значения параметра модели действия числа с плавающей точкой
		От…До – диапазон, который могут принимать значения параметра модели действия
		Допустимые варианты – поле ввода строго заданных допустимых

Класс	Описание	Параметры
		значений для параметра модели действия
URL	Проверяет значение параметра модели действия на соответствие его идентификатору ресурса единого формата	Разрешить абсолютные URL – разрешает использование абсолютных URL в качестве значения параметра модели действия
		Разрешить относительные URL - разрешает использование относительных URL в качестве значения параметра модели действия
		Разрешить URL с параметрами – разрешает использование URL с параметрами в качестве значения параметра модели действия
		Разрешенные схемы URL – ввод разрешенных схем URL (HTTP, HTTPS) в значении параметра модели действия
		Допустимые варианты – поле ввода строго заданных допустимых значений для параметра модели действия
Строка	Проверяет значение параметра модели действия на соответствие его строке (string)	
Имя файла	Проверяет, что в качестве значения параметра модели действия передаётся файл	Допустимые расширения – допустимые значения расширения файла, который передается в качестве значения параметра модели действия
		Допустимые варианты – поле ввода строго заданных допустимых значений для параметра модели действия
Номер банковской карты	Проверяет значение параметра модели действия на соответствие его стандартному виду номера банковской карты	Допустимые варианты – поле ввода строго заданных допустимых значений для параметра модели действия
Строка из шестнадцатеричных цифр	Проверяет значение параметра модели действия на соответствие его строке из шестнадцатеричных цифр	Допустимые варианты – поле ввода строго заданных допустимых значений для параметра модели действия
Структура	Проверяет, что в качестве значения параметра модели действия	Некорректная модель, необходимо пересмотреть - выключает

Класс	Описание	Параметры
	передается структура (json, xml, query)	существующую модель и обучает ее заново при следующем запуске задания
		Типы структур – возможные значения json, xml, query
		Допустимые варианты – поле ввода строго заданных допустимых значений для параметра модели действия
Токен	Проверяет, что в качестве значения параметра модели действия передается токен с заданной длинной	Максимальная длина токена – поле для ввода максимальной длинны значения параметра модели действия
		Допустимые варианты – поле ввода строго заданных допустимых значений для параметра модели действия
GUID	Проверяет, что в качестве значения параметра модели действия передается статистически уникальный 128-битный идентификатор	Допустимые варианты – поле ввода строго заданных допустимых значений для параметра модели действия
Универсальная текстовая модель	Проверяет, что в качестве значения параметра модели действия передается универсальная текстовая модель. Универсальную модель нельзя создать вручную (Может быть создана только автоматически)	Некорректная модель, необходимо пересмотреть - Выключает существующую модель и обучает ее заново при следующем запуске задания
		Допустимые варианты – поле ввода строго заданных допустимых значений для параметра модели действия
Математическое ожидание длины	Проверяет, что в качестве значения параметра модели действия передается среднее (взвешенное по вероятностям возможных значений) значение случайной величины	Математическое ожидание длины
		Среднеквадратичное отклонение - значение параметра, длина которого отличается от математического ожидания длины более, чем на 3 среднеквадратичных отклонения, будет считаться аномальным
Одномерное распределение Гаусса	Проверяет, что в качестве значения параметра модели действия передается значение, попадающее под заданную модель	Модель в формате JSON
Многомерное распределение Гаусса	Проверяет, что в качестве значения параметра модели действия	Модель в формате JSON

Класс	Описание	Параметры
	передается значение, попадающее под заданную модель	

5.4. Сохранить – сохраняет внесенные изменения в модель параметра действия.
5.5. Удалить – удаляет модель параметра действия.
5.6. Отменить – отменяет внесенные изменения в модель параметра действия.

6. В выделенной области находится иконка, при нажатии на которую добавляется еще одна строка ввода параметра модели.
7. Добавить условие успешности – открывает окно «Редактирование условия успешности» (см. рисунок 153).

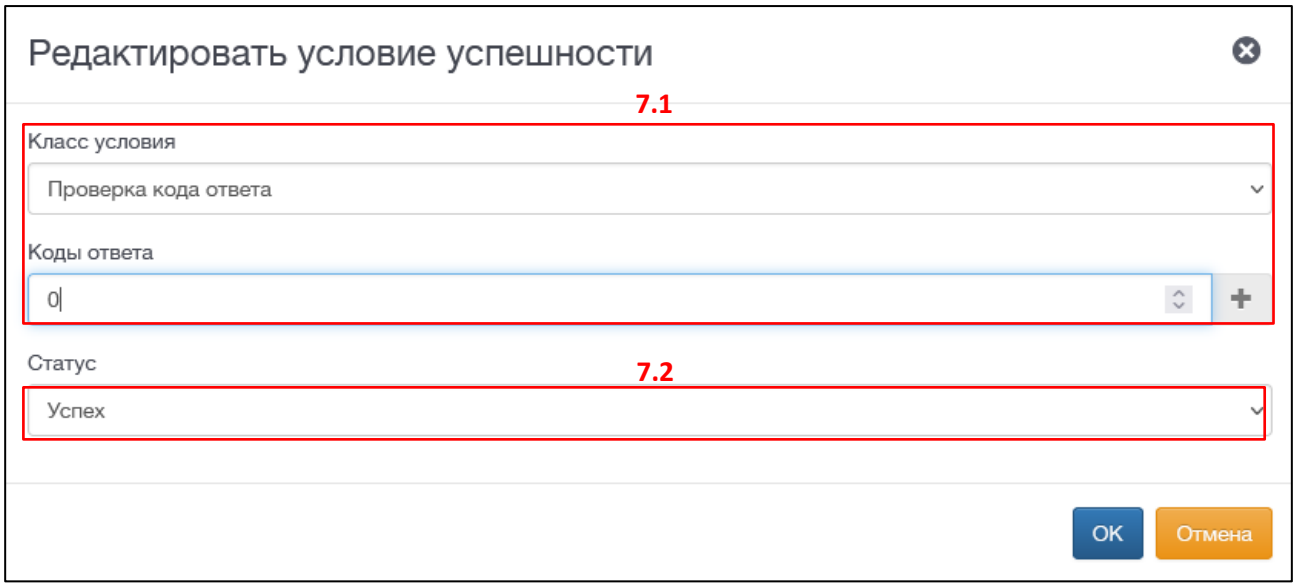

Рисунок 153 – Окно «Редактирование условия успешности»

7.1. Класс условия – выбор из заданного списка классов условий. В зависимости от выбранного класса условия, меняется параметр, с помощью которого данный класс задается (см. таблицу 15).

Таблица 15 – Классы условий

Класс условия	Описание	Параметр
Проверка кода ответа	Проверяет значение кода ответа на соответствие заданному в параметре, в случае совпадения транзакции выдается статус успешности, выбранный в пункте 7.2	Код ответа – поле, в котором можно ввести значение кода ответа. Имеется возможность добавления дополнительных полей ввода нажатием на иконку «»
Проверка соответствия тела ответа регулярному выражению	Проверяет значение тела ответа на соответствие заданному в параметре регулярному выражению, в случае соответствия транзакции выдается статус успешности, выбранный в пункте 7.2	Регулярное выражение – поле, в которое можно ввести регулярное выражение

Класс условия	Описание	Параметр
Определение состояния по дереву разбора	Проверяет значения заданных путей дерева разбора ответа на соответствие заданным параметрам, в случае соответствия транзакции выдается статус успешности, выбранный в пункте 7.2	Можно добавить параметры со следующими классами условий: регулярное выражение – проверка соответствия значения в заданной ветке дерева разбора ответа регулярному выражению; точное значение - проверка соответствия значения в заданной ветке дерева разбора ответа введенному значению; наличие путей – проверка наличия заданной ветки дерева разбора ответа

7.2. Статус – поле выбора одного из трех вариантов: успех, ошибка валидации, ошибка логики.

8. Сохранить действие в базу данных, если оно найдено в транзакции - бинарное поле, которое может принимать значения «Да» или «Нет» («☑» или «☐» соответственно). Данное поле отвечает за сохранение действия в базу данных, если оно найдено в транзакции.
9. Требует разбор ответа - бинарное поле, которое может принимать значения «Да» или «Нет» («☑» или «☐» соответственно). В случае если в действии используется условие успешности, данное поле необходимо включать в обязательном порядке.
10. Сохранить – сохраняет внесенные изменения.
11. Отменить – отменяет внесённые изменения.

После сохранения изменений действие появится на вкладке «Бизнес-действия» с заданным названием. Отредактировать его условия можно, нажав на поле «Добавить правило» (если по действию уже есть условия, для редактирования условий необходимо нажать на иконку «✎» в левой части поля «Условия»), в результате чего откроется конструктор условий, в котором путем нажатия на «Добавить условие», можно добавлять условия (см. рисунок 154).

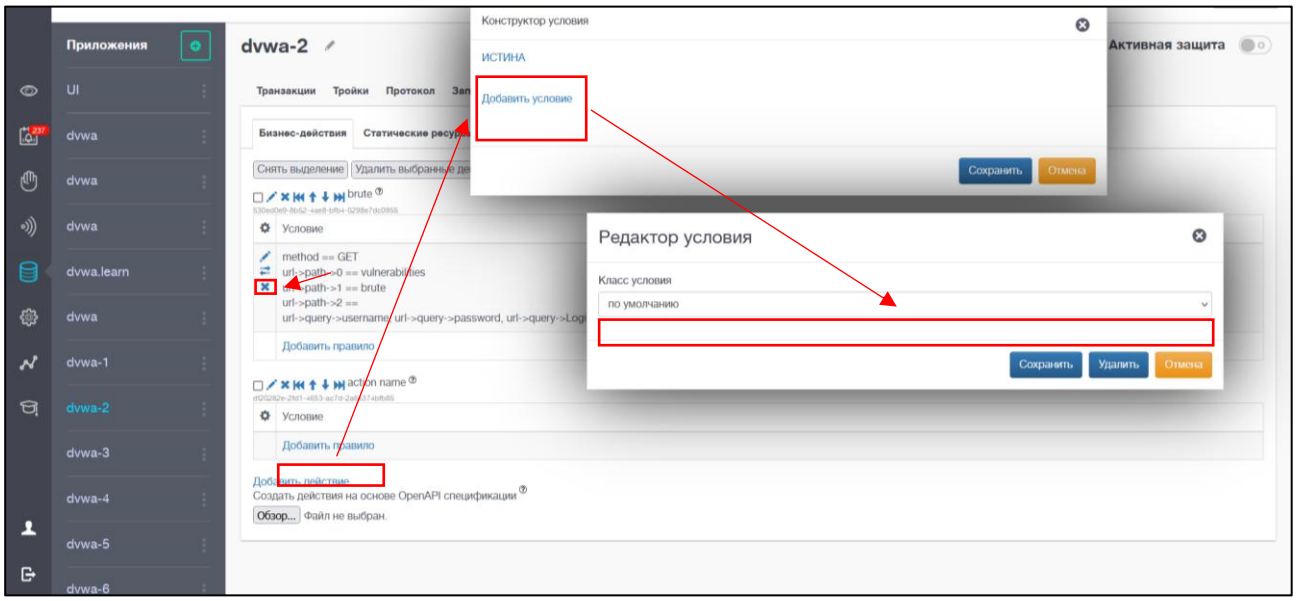

Рисунок 154 – Добавление условий

В открывшемся окне нужно задать один из трёх значений поля «Класс условия»:

- регулярное выражение – проверка соответствия значения в заданной ветке дерева разбора регулярному выражению;
- точное значение - проверка соответствия значения в заданной ветке дерева разбора введенному значению;
- наличие путей – проверка наличия заданной ветки дерева разбора ответа.

15.2. Полуавтоматическое создание действий

На WAF имеется возможность создания действий на основе транзакций. Для того чтобы создать действие таким образом, необходимо перейти на вкладку «Приложения» -> «Транзакции» и открыть окно обзора транзакции, по которой необходимо создать действие, а затем перейти на вкладку «Действия» и нажать на кнопку «Создать действие на основе этой транзакции» (см. рисунок 155).

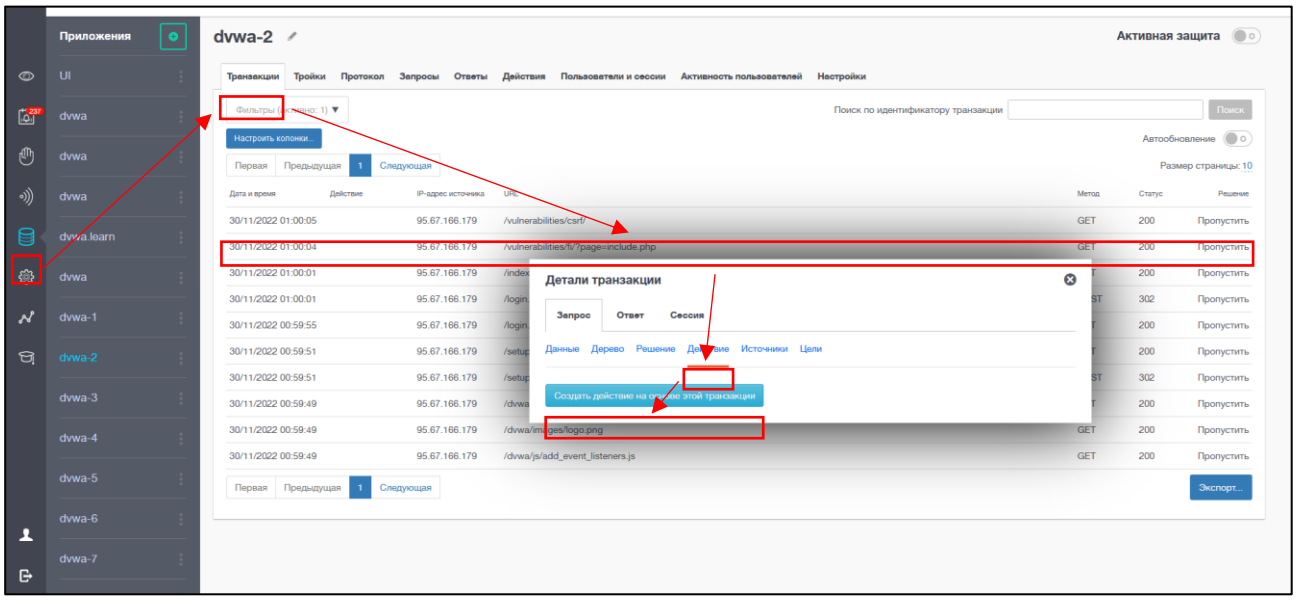

Рисунок 155 – Создание действия из окна «Транзакции»

После нажатия на данную кнопку, появится информационное окно с идентификатором созданного действия, который используется для обозначения данного действия в базах данных (см. рисунок 156).

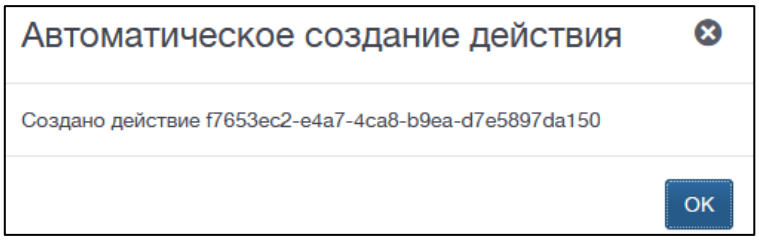

Рисунок 156 – Информационное окно с идентификатором созданного действия

Созданное действие можно найти на вкладке «Приложения» -> «Действия» -> «Бизнес-действия» в самом низу (см. рисунок 157).

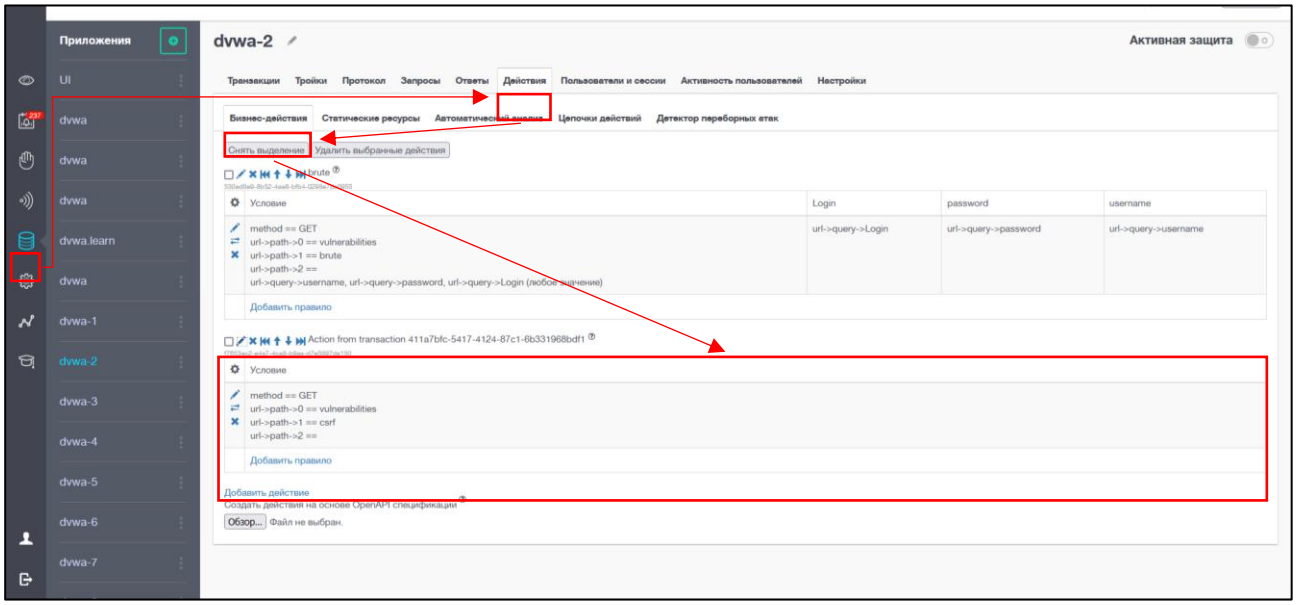

Рисунок 157 – Местонахождение созданного действия

Редактирование действия описано в разделе 15.1.

15.3. Автоматическое создание действий

На WAF имеется возможность автоматического добавления действий на основе машинного обучения. Данный модуль включен по умолчанию и его дополнительно можно настроить из веб-интерфейса WAF. Для этого необходимо перейти на вкладку «Приложения» -> «Действия» -> «Автоматический анализ» и отредактировать задание «Разметка действий приложения» (см. рисунок 158), нажав на иконку с изображением карандаша.

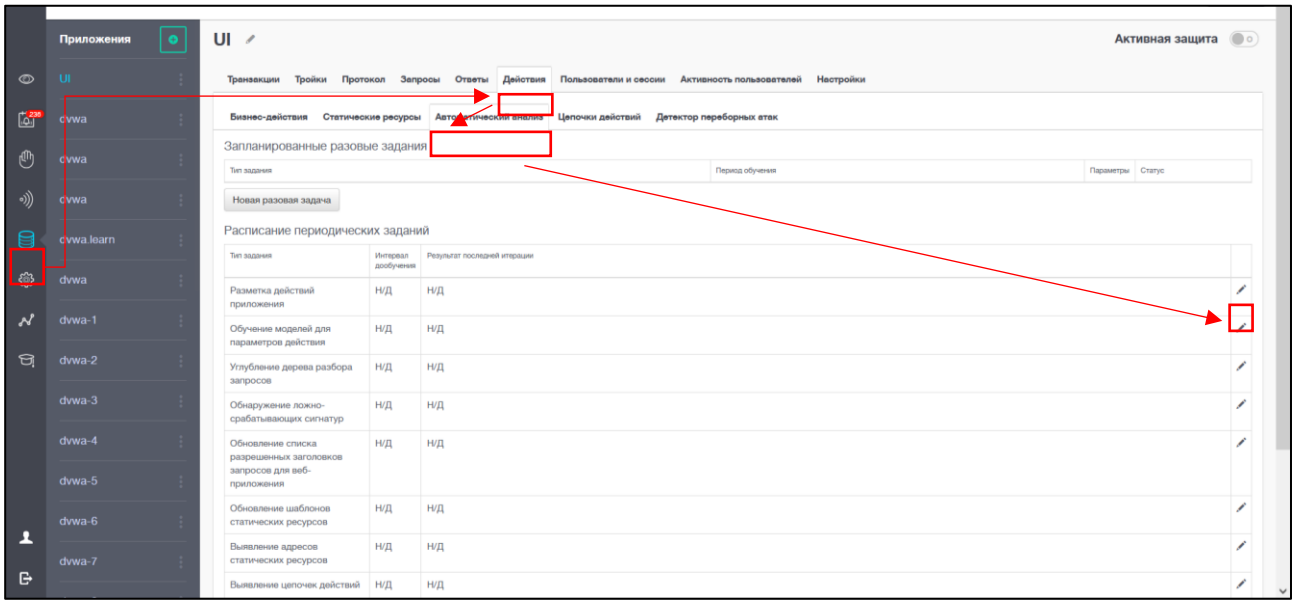

Рисунок 158 – Автоматический анализ

При нажатии на выделенную иконку (см. рисунок 158) открывается окно «Параметры обучения» (см. рисунок 159).

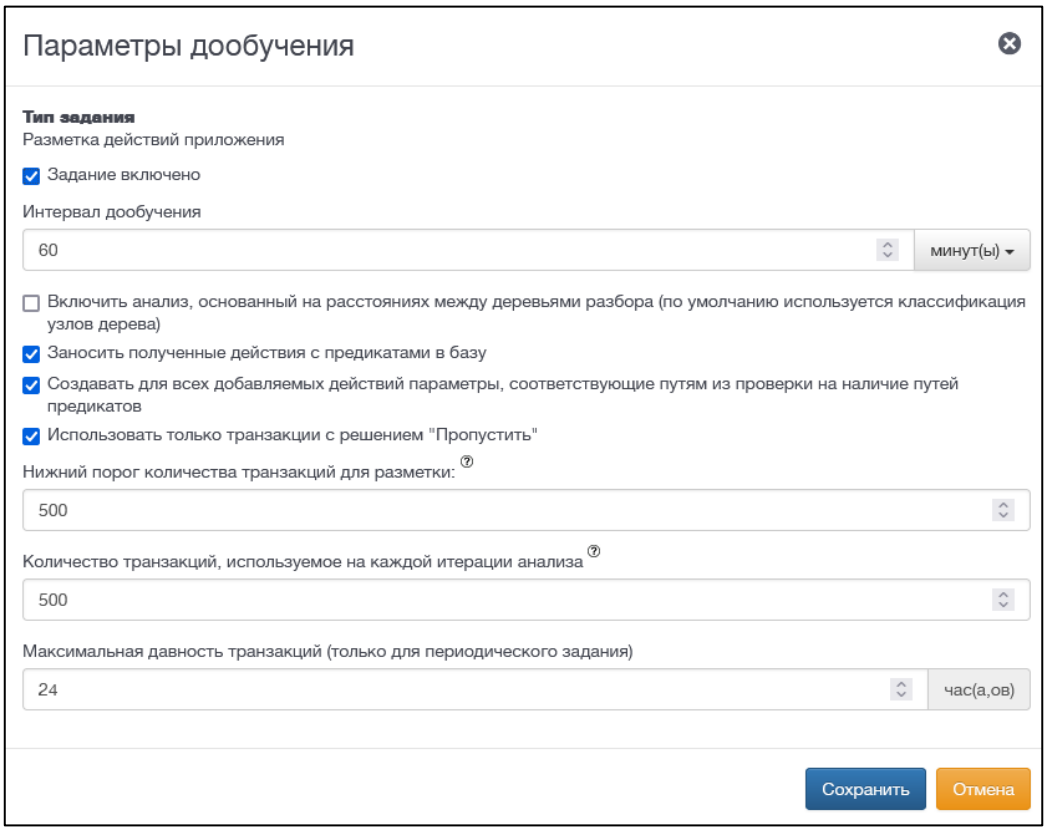

Рисунок 159 – Окно «Параметры обучения»

Описание полей данного окна представлено в таблице 16.

Таблица 16 – Описание полей

Поле	Описание
Интервал обучения	Интервал запуска задачи
Включить анализ, основанный на расстояниях между деревьями разбора	В настоящий момент не используется. Оставлять значение по умолчанию: классификация узлов дерева
Заносить полученные действия с предикатами в базу	Заносит действие в базу для предотвращения появления одинаковых действий
Создавать для всех добавляемых действий параметры, соответствующие путям из проверки на наличие путей предикатов	Создает модель действия
Использовать только транзакции с решением «Пропустить»	Игнорирует все транзакции со статусом отличным статусу «Пропустить»
Нижний порог количества транзакций для разметки	Задается нижний порог количества транзакций от различных источников с одинаковой структурой, при достижении которого будет создано действие. Не более 10000
Количество транзакций, используемое на каждой итерации анализа	Задается порог анализируемых транзакций на каждой итерации анализа. Не более 10000

Максимальная давность транзакций	Задается глубина анализа транзакций. Только для периодического задания

15.4. Создание действие с помощью Open API

Open API - популярный стандарт для написания REST API в формате JSON/XML.

Благодаря поддержке этой спецификации можно быстро и массово загружать действия на WAF, экономя много времени на этапах начального обучения приложений, если ML по какой-то причине не работает/не успевает отработать.

Алгоритм загрузки действий на WAF:

1. **Получить** любым удобным способом (ELK, Postgres, Burp, ручной анализ, что-то ещё) **данные о ручках и методах в формате (URL METHOD)**:

```
/local/templates/helpheart/include_areas/articles_interesting.php POST
/local/templates/helpheart/include_areas/cookie-notice.php POST
/arterialnoe-davlenie/lechenie/kak-bystro-snizit/ GET
/infarkt/ob-infarkte-miokarda/skolko-zhivut-posle-infarkta/ GET
/ GET
/ POST
/arterialnoe-davlenie/riski-prichiny-i-posledstviya/pochemu-posle-edy-menyaetsya-davlenie-i-kak-eto-predotvratit/ GET
/arterialnoe-davlenie/riski-prichiny-i-posledstviya/arterialnoe-davlenie-pri-stresse/ GET
/povyshennyy-kholesterin/o-kholesterine/povyshennyy-kholesterin-u-zhenshchin/ GET
/arterialnoe-davlenie/ob-arterialnom-davlenii/shum-v-ushah/ GET
/arterialnoe-davlenie/riski-prichiny-i-posledstviya/golovokruzhenie-u-zhenschin/ GET
```

Рисунок 160 – Формат данных о ручках

2. **Отсортировать действия по убыванию**, чтобы менее точные пути были внизу списка.
3. **Подготовить действия к загрузке**, срезая лишние пути, удаляя корневые и другие действия.
4. **«Обернуть» действия в валидный JSON**, используя шаблон выше любым удобным образом, и сохраняем их в файл (см. рисунок 161).


```
{
 "openapi": "3.0.3", "info": {"title": "", "version": ""}, "paths": {
 "/raschet-riska/": {"get": {"operationId": "/raschet-riska/ GET","responses": {"200": {"description": "some_litter"}}}},
 "/povyshennyy-kholesterin/": {"get": {"operationId": "/povyshennyy-kholesterin/ GET","responses": {"200": {"description": "some_litter"}}}},
 "/ofitsialnoe-uvedomlenie/": {"get": {"operationId": "/ofitsialnoe-uvedomlenie/ GET","responses": {"200": {"description": "some_litter"}}}},
 "/obratnaya-svyaz/": {"get": {"operationId": "/obratnaya-svyaz/ GET","responses": {"200": {"description": "some_litter"}}}},
 "/local/templates/helpheart/include_areas/cookie-notice.php": {"post": {"operationId": "/local/templates/helpheart/include_areas/cookie-notic
 "/local/templates/helpheart/include_areas/articles_interesting.php": {"post": {"operationId": "/local/templates/helpheart/include_areas/artic
 "/infarkt/": {"get": {"operationId": "/infarkt/ GET","responses": {"200": {"description": "some_litter"}}}},
 "/consultation/": {"get": {"operationId": "/consultation/ GET","responses": {"200": {"description": "some_litter"}}}},
 "/arterialnoe-davlenie/riski-prichiny-i-posledstviya/": {"get": {"operationId": "/arterialnoe-davlenie/riski-prichiny-i-posledstviya/ GET","r
 "/arterialnoe-davlenie/ob-arterialnom-davlenii/": {"get": {"operationId": "/arterialnoe-davlenie/ob-arterialnom-davlenii/ GET","responses": {
 "/arterialnoe-davlenie/lechenie/": {"get": {"operationId": "/arterialnoe-davlenie/lechenie/ GET","responses": {"200": {"description": "some_l
 "/arterialnoe-davlenie/": {"get": {"operationId": "/arterialnoe-davlenie/ GET","responses": {"200": {"description": "some_litter"}}}},
 "/actuator/health": {"get": {"operationId": "/actuator/health GET","responses": {"200": {"description": "some_litter"}}}}
 }
}
```


Рисунок 161 – Валидный JSON

5. Перейти на вкладку «Приложения» -> «Действия» -> «Бизнес-действия» и нажать на поле «Обзор». Далее необходимо указать путь к файлу в формате JSON/XML, содержащий необходимые действия (см. рисунок 162).

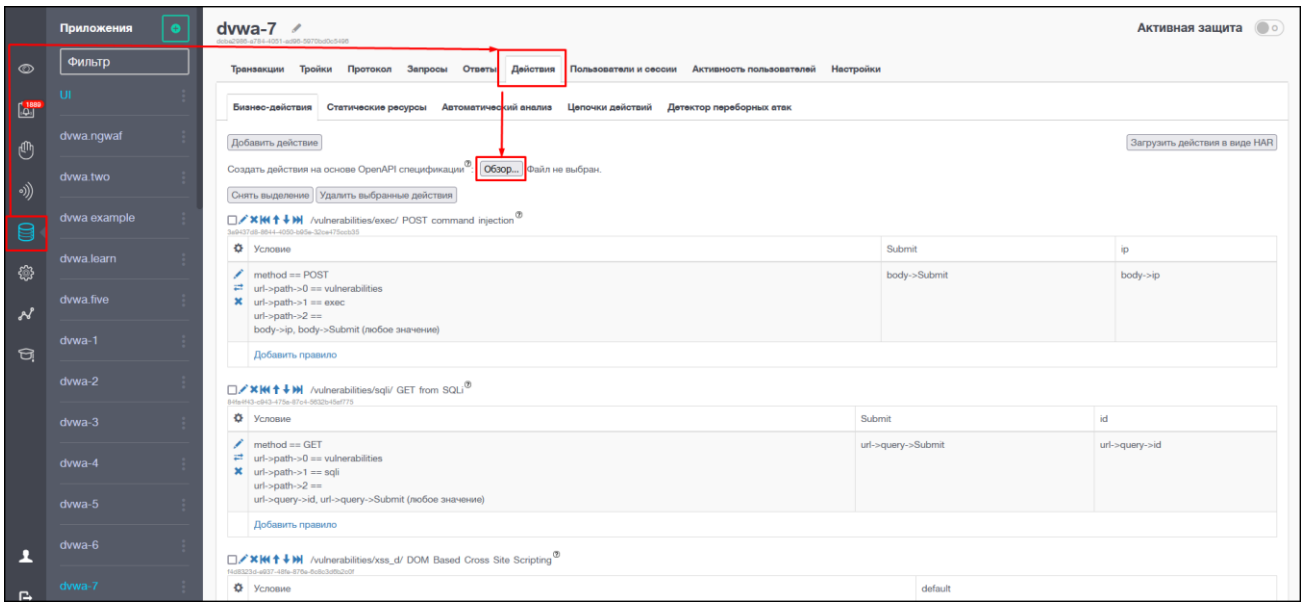

Рисунок 162 **– Создание действий с помощью Open API**

16. Детектор переборных атак

Детектор переборных атак способен обнаруживать слишком частые обращения к отдельным действиям веб-приложения (переборные атаки). Для этого Детектор переборных атак реализует алгоритм макетного ведра, обеспечивая таким образом ограничение допустимого числа запросов к веб-приложению за единицу времени (rate limiting). Субъектами, для которых вводятся ограничения на число запросов в единицу времени, являются источники.

16.1. Детектор переборных атак «Действие\Источник»

Данный детектор переборных атак работает следующим образом: все запросы для разных пар «источник - действие веб-приложения» обрабатываются Детектором переборных атак отдельно друг от друга. Иными словами, для каждого отдельного источника запросов и каждого отдельного действия веб-приложения имеется собственное ведро с маркерами, состояние которого мониторит частоту обращения от конкретного источника к конкретному действию веб-приложения. Таким образом возможно настроить, например, максимальное число запросов в единицу времени с каждого отдельного IP-адреса, или ввести для каждого отдельного пользователя ограничения на количество попыток входа в веб-приложение. Вкладка «Детектор переборных атак» список действий, настроенных на вкладке «Действия» в представлении «Бизнес-действия» (см. рисунок 163).

Рисунок 163 – Вкладка «Детектор переборных атак»

Статус детектора переборных атак для действия может принимать три значения:

- «✔» - детектор переборных атак для действия включен, а настройки параметров детектора установлены по умолчанию для модуля и доступны к просмотру в секции «BruteforceDetector» конфигурации модулей анализаторов;
- «✔✎» - детектор включен, для пары «Источник – Действие» заводится индивидуальное маркерное ведро с установленными параметрами;
- «⊘» - детектор выключен.
- Для изменения состояния детектора необходимо щелкнуть мышкой по соответствующей ячейке (см. рисунок 164).

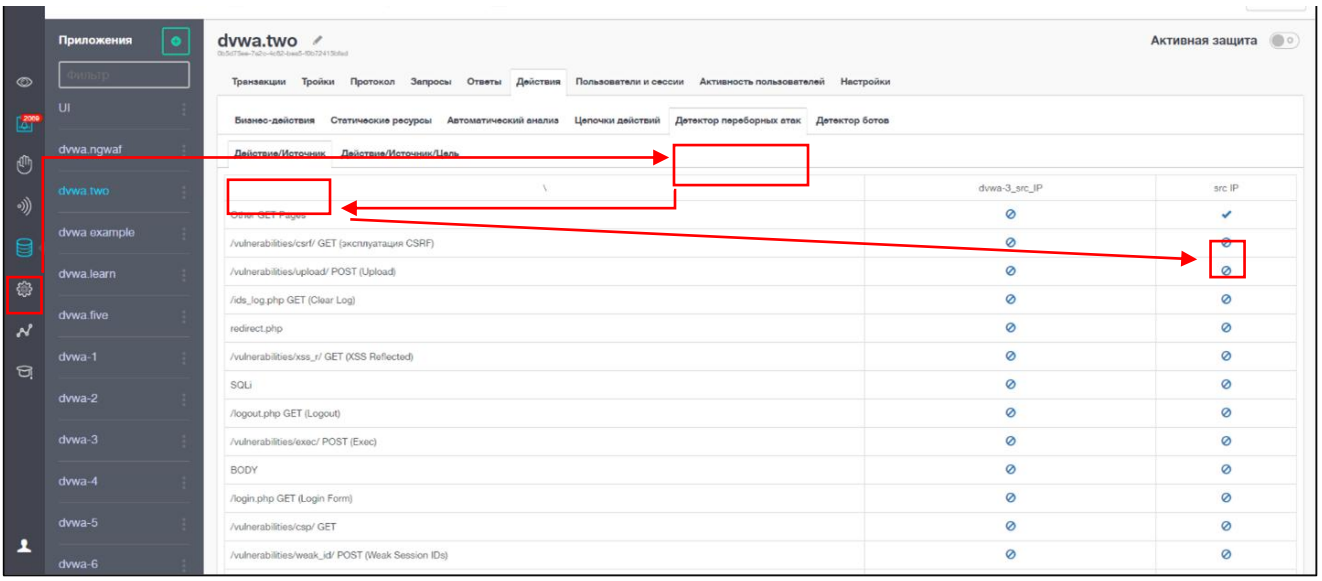

Рисунок 164 – Открытие параметров детектора переборных атак Действие\Источник

В результате откроется окно для тонкой настройки параметров детектора переборных атак (см. рисунок 165).

Рисунок 165 – Параметры детектора переборных атак

Настройка детектора переборных атак для пар «Действие\Источник» содержит следующие поля:

1. Включить – чекбокс включения детектора переборных атак.
2. Интерпретация источника – есть два варианта интерпретации источника:

- Сущность – для каждого нового значения источника создается новая корзина;
- Набор значений – создается одна корзина для всех значений источника.

3. Использовать индивидуальные настройки – чекбокс включения индивидуальных настроек.
4. Размер текущего ведра с маркерами – сколько маркеров может содержаться в ведре. При очередном запросе, если в ведре накопилось больше маркеров, чем заданное число - будет сгенерирована аномалия.
5. Собирать статистику для значений наполнения текущего ведра – если будет включена задача «Расчет ограничений размера текущего ведра», то по переборникам с активным чекбоксом будут

подбираться пороговые значения переборников, исходя из собранной статистики и заданных настроек задачи.

6. Скорость истечения маркеров из ведра - сколько маркеров вытекает из ведра каждую секунду. Характеристика определяет время, за которое полное ведро опустеет.
7. Число маркеров, добавляемое в ведро при каждом запросе - каждый запрос вначале добавляет данное число маркеров в ведро. После этого проверяется, не переполнилось ли ведро. В зависимости от этого либо создается аномалия, либо запрос благополучно проходит.
8. Включить режим блокировки по таймеру - если эта опция включена, то при переполнении ведра на все последующие запросы от этого источника будут некоторое установленное время генерироваться аномалии вне зависимости от состояния ведра. По истечению данного таймаута - ведро принудительно опустошается.
9. Время блокировки запросов в режиме блокировки по таймеру - управляет таймаутом, который включает предыдущая опция.
10. Новые запросы переустанавливают таймер - если включено, то последующие запросы в режиме блокировки по таймеру взводят таймер заново. В ином случае, таймаут не переустанавливается.
11. Количество маркеров, добавляемых в ведро в случае ответа с кодом 404 – Запрос обрабатывается по текущему состоянию ведра. При получении ответа веб-приложения анализируется код ответа. Если он равен 404, то в ведро будет добавлено указанное количество маркеров. Эта опция полезна, если требуется обнаруживать попытки forceful browsing веб-приложения - угадывания прямых URL, вместо перехода по ссылкам.
12. Количество маркеров, добавляемых в ведро для неуспешных действий – Запрос обрабатывается по текущему состоянию ведра. При получении ответа веб-приложения анализируется успешность действия. Если действие не успешное - в ведро будет добавлено указанное количество маркеров. Полезность использования данной опции будет проиллюстрирована далее.

16.2. Детектор переборных атак «Действие\Источник\Цель»

Если предыдущий детектор переборных атак (Действие\источник) считал количество обращений от источника к действию, то детектор переборных атак Действие\Источник\Цель считает количество обращений к цели от источника в рамках конкретного действия. Т.е. данный вид детектора переборных атак хорошо подходит при переборе значений отдельных полей, будь то поле ввода логина, пароля, промокодов или что-то иное.

Чтобы добавить настройку детектора переборных атак «Действие\Источник\Цель» необходимо перейти на вкладку «Приложения» -> «Действия» -> «Детектор переборных атак» -> «Действие\Источник\Цель» и нажать на кнопку «Добавить настройку», появится окно «Настройка параметров для детектора переборных атак» (см. рисунок 166).

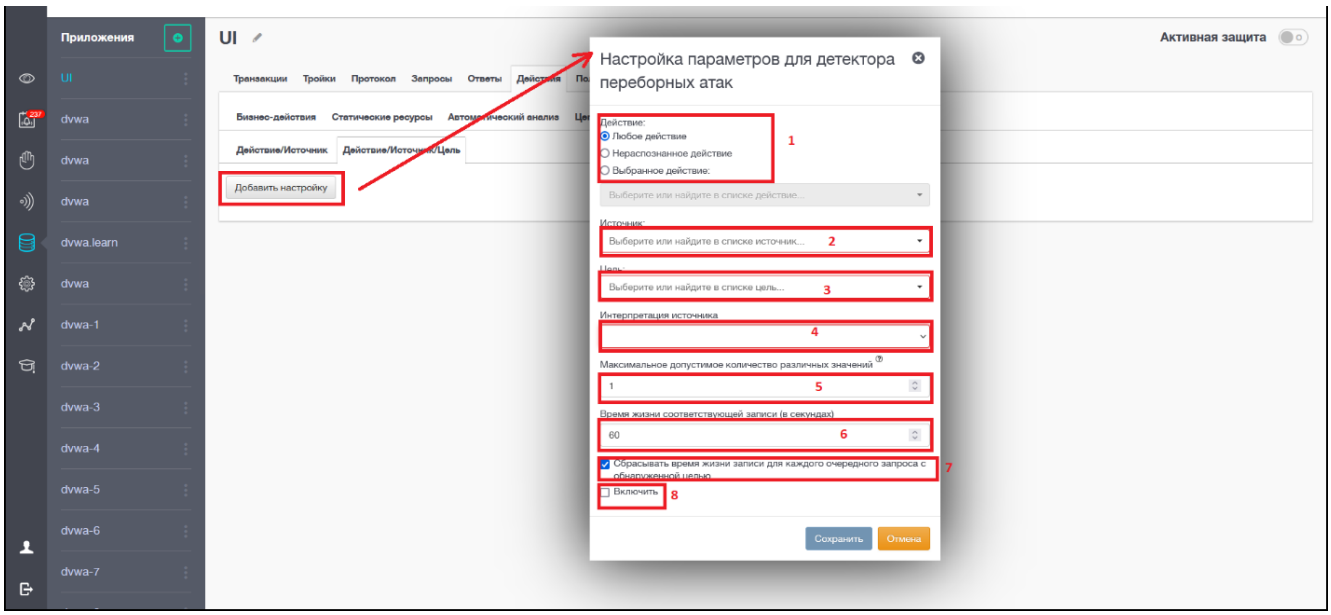

Рисунок 166 – Окно «Настройка параметров для детектора переборных атак»

Окно «Настройка параметров для детектора переборных атак» содержит следующие элементы:

1. Действие – выбор действия, для которого будет настроен детектор переборных атак. Есть три варианта выбора действия:

- Любое действие – все действия на данном приложении, включая нераспознанные;
- Нераспознанное действие – под данное действие попадают те транзакции, которые не попали ни под одно из настроенных действий;
- Выбранное действие – выбор одного действия из списка действий, настроенных на данном приложении.

2. Источник – выбор источника из настроенных на приложении.
3. Цель – выбор перебираемого элемента из настроенных на приложении.
4. Интерпретация источника – есть два варианта интерпретации источника:

- Сущность – для каждого нового значения источника создается новая корзина;
- Набор значений – создается одна корзина для всех значений источника.

5. Максимально допустимое количество различных значений – указывает максимальное количество разных значений, которые может принимать один объект веб-приложения до начала генерации аномалий.
6. Время жизни соответствующей записи (в секундах) – время, которое живет генерируемая детектором переборных атак запись.
7. Сбрасывать время жизни записи для каждого очередного запроса с обнаруженной целью – обновляет заданный в пункте 6 таймер, при получении записи, которая идентична уже созданной.
8. Включить – чекбокс включения детектора переборных атак.

17. Настройка модулей

Ряд модулей имеет общие параметры, которые перечислены в таблице 17.

Таблица 17 – Общие настройки

Параметр	Описание
group_name	Параметр для выбора очереди обмена сообщениями с ZeroMQ. Значение по умолчанию - local. BrokerQueue (broker) - работа только с брокером ZeroMQ, без передачи сообщений внутри процесса; LocalQueue (local) - локальная очередь, осуществляющая передачу данных в только рамках одного процесса; CombinedQueue (combined) - прием и отправка сообщений как с использованием ZeroMQ, так и внутри процесса
max_cache_size	Размер общего кеша между модулем записи транзакций и модулем записи действий
num_instances	Количество используемых процессов для модуля. По умолчанию равно 4. Количество процессов (pipeline) должно быть равно: «Число ядер ЦПУ» - 2 - на узле с выделенным анализатором; «Число ядер ЦПУ» * 0.5 - для standalone инсталляции
python_implementation	Тип интерпретатора Python для анализатора. Интерпретатор по умолчанию - Cpython, данное значение менять не стоит
use_redis_mgmt	Использование общего Redis между анализаторами для централизованного хранения параметров. Данную настройку не стоит использовать вместе с указанием отдельного адреса централизованного Redis в рамках одного модуля: false - не использовать указанный во вкладке redis_mgmt настроек анализатора общий адрес для централизованного Redis (По умолчанию); true – использовать общий адрес для централизованного Redis, который указан во вкладке redis_mgmt настроек анализатора
redis -> url	Адрес централизованного Redis для хранения вёдер детектора переборных атак, если таковой используется. Данную настройку не стоит использовать вместе с use_redis_mgmt, так как в ней задаётся отдельный адрес централизованного Redis, а не используется общий Redis, указанный во вкладке redis_mgmt настроек анализатора. В случае отсутствия централизованного Redis используется локальный на каждой из НОД

17.1. BruteforceDetector

Данный модуль отвечает за работу детектора переборных атак.

Перечень настроек, которые разрешено менять пользователям представлены в таблице 18.

Таблица 18 – BruteforceDetector

Параметр	Описание
bucket_size	Размер ведра для действия со значением детектора переборных атак по умолчанию
leak_rate	Количество «вытекаемых» из ведра токенов за секунду по умолчанию
relieve_on_timeout	Включение режима блокировки по таймеру при наполнении ведра, в секундах: false - выключено (по умолчанию); true - включено
relieve_timeout	Время блокировки запросов в режиме блокировки по таймеру, в секундах
timeout_reset	Переустановка таймера с каждым новым запросом: false - выключено (по умолчанию); true - включено
tokens_per_action	Количество токенов, добавляемых в ведро при запросе
tokens_per_failed_action	Количество токенов, добавляемых в ведро при запросе с нарушением успешности действия
tokens_per_response_404	Количество токенов, добавляемых в ведро при запросе с нарушением успешности действия
unrecognized_action	Параметры детектора исключительно для неизвестного действия, описание параметров совпадает с вышеперечисленными

17.2. DecisionMakerModule

Данный модуль отвечает за принятие решения о пропуске или блокировке транзакции на основе результата анализа других модулей анализатора.

Перечень настроек, которые разрешено менять пользователям представлены в таблице 19.

Таблица 19 – DecisionMakerModule

Параметр	Описание
debug_timeline	Лог описания момента принятия решения DecisionMaker. Добавляет информацию в таблицу аномалий. Информация оттуда отображается в нижней части вкладки «Решение» при просмотре транзакции. Нужен только для отладки. false - выключено (по умолчанию); true - включено
processing_timeout	Время на сбор аномалий перед принятием конечного решения DecisionMaker. При наличии «тяжелых» запросов на приложениях инсталляции можно увеличивать значение данного параметра. Хорошей практикой считается изменять его вместе со значением decision_timeout настроек модуля NginxZmqAdapter по следующей формуле:

Параметр	Описание
	`processing_timeout + 0.1 = = decision_timeout` Это позволит выделить время на отправку данных модулем NginxZmqAdapter после принятия решения модулем DecisionMaker и избежать ошибок, связанных с таймаутом

17.3. DecisionTreeResponseParser

Данный модуль отвечает за разбор дерева ответа на запрос. Выключен на большей части инсталляций, так как требует большого количества ресурсов.

Перечень настроек, которые разрешено менять пользователям представлены в таблице 20.

Таблица 20 – DecisionTreeResponseParser

Параметр	Описание
parse_unrecognized_action	Параметр, отвечающий за разбор ответа при нераспознанном WAF действии: false - выключено (по умолчанию); true - включено
use_webapp_control	Настройка для управления параметром разбора ответов для каждого приложения отдельно: false - выключено (по умолчанию); true - включено (в этом случае настройка выполняется во вкладке «Настройки» каждого приложения на инсталляции. Параметр, отвечающий за это, называется «Строить дерево разбора для ответа»

17.4. DumperBatchModule

Данный модуль отвечает за запись транзакций в базу данных (Postgres, MongoDB).

Перечень настроек, которые разрешено менять пользователям представлены в таблице 21.

Таблица 21 – DumperBatchModule

Параметр	Описание
mask	Параметр, включающий возможность маскирования данных: false - выключено (по умолчанию); true - включено
max_batch_size	Размер пачки транзакций, которая будет записываться в базу
max_watched_action_num	Размер буфера для действий
max_watched_tx_num	Размер буфера для транзакций
normal_tx_sample_rate	Параметр, указывающий коэффициент семплирования (частичной записи в базу) для пропущенных транзакций с целью экономии места на диске

Параметр	Описание
store_all_actions	Параметр, включающий сохранение всех действий в отдельной таблице в Postgres. Используется для интеграции со внешними приложениями, например, с SIEM. Значения: false - выключено (по умолчанию); true - включено
store_normal_anomalies	Параметр, указывающий сохранять ли в базу подавленные аномалии (ложные сработки): false - выключено (по умолчанию); true – включено
store_normal_txns	Параметр, указывающий сохранять ли обычные транзакции без сработок на WAF: false – выключено; true - включено (по умолчанию)
store_unknown	Параметр, указывающий хранить ли транзакции с неизвестными для WAF действиями: false – выключено; true - включено (по умолчанию)
tx_data_wait_timeout	Время ожидания данных транзакции, после которого идёт принудительная запись в базу, в секундах
wait_for_all_data	Ожидание всех данных перед записью, чтобы снизить количество запросов на изменение в базу данных, так как UPDATE считается ресурсоёмким запросом: false – выключено; true - включено (по умолчанию)

17.5. IcapClient

Данный модуль используется для отправки данных во внешние системы через протокол ICAP.

Перечень настроек, которые разрешено менять пользователям представлены в таблице 22.

Таблица 22 – IcapClient

Параметры	Описание
icap_server_address	IP-адрес ICAP-сервера
port	Порт ICAP-сервера
service	Адрес AV-сервера, которому передаются данные для проверки
socket_timeout	Время ожидания ответа в секундах

17.6. LWSessionTracker

Данный модуль отвечает за работу легковесного отслеживания пользовательских сессий на основе указанных значений сессионных атрибутов.

Перечень настроек, которые разрешено менять пользователям представлены в таблице 23.

Таблица 23 – LWSessionTracker

Параметр	Описание
max_users_allowed	Максимальное количество изменений идентификатора сессии. Как правило, имени пользователя
session_lifetime	Время жизни сессии между запросами в секундах

17.7. ModsecurityAnalyzer

Данный модуль отвечает за работу с оптимизированным сигнатурным анализатором на основе Modsecurity.

Перечень настроек, которые разрешено менять пользователям представлены в таблице 24.

Таблица 24 – ModsecurityAnalyzer

Параметры	Описание
config_file	Путь хранения конфигурации Modsecurity
config_name	Название файла конфигурации Modsecurity

17.8. NginxDecisionDumper

Данный модуль Nginx отвечает за запись данных о решении Decision Maker’а в базу Postgres.

Перечень настроек, которые разрешено менять пользователям представлены в таблице 25.

Таблица 25 – NginxDecisionDumper

Параметры	Описание
dumper -> max_watched_tx_num	Размер кеша для транзакций
store_normal_anomalies	Параметр, определяющий сохранять ли в базу подавленные аномалии (ложные сработки): false – выключено (по умолчанию); true – включено
wait_for_all_data	Ожидание всех данных перед записью, чтобы снизить количество запросов на изменение в базу данных, так как UPDATE считается ресурсоёмким запросом. Имеет следующие значения: false – выключено; true - включено (по умолчанию)

17.9. NginxZmqAdapter

Данный адаптер Nginx для быстрой асинхронной поставки данных в анализатор с использованием оптимизированной библиотеки для обмена сообщениями ZeroMQ.

Перечень настроек, которые разрешено менять пользователям представлены в таблице 26.

Таблица 26 – NginxZmqAdapter

Параметр	Описание
decision_timeout	Время ожидания решения от модулей анализатора, после истечения которого будет принято решение по умолчанию. При наличии «тяжелых» запросов на приложениях инсталляции можно увеличивать значение данного параметра. Хорошей практикой считается изменять его вместе со значением processing_timeout настроек модуля DecisionMakerModule по следующей формуле: processing_timeout + 0.1 = = decision_timeout Это позволит выделить время на отправку данных модулем NginxZmqAdapter после принятия решение модулем DecisionMaker и избежать ошибок, связанных с таймаутами
default_decision_for_ unknown_webapp	Решение по умолчанию для транзакций от неизвестного приложения. Неизвестным приложением считается приложение, трафик которого попал на Nginx, но не определился к какому-либо приложению на WAF через тройки. Может принимать следующие значения: PASS, пропустить (по умолчанию для всех версий именно iBatyr-nginx); BLOCK, заблокировать

17.10. SequenceAnomalyDetector

Данный модуль отвечает за работу цепочек действий пользователя.

Перечень настроек, которые разрешено менять пользователям представлены в таблице 27.

Таблица 27 – SequenceAnomalyDetector

Параметр	Описание
anomaly_threshold	Размер ведра для аномалий, при переполнении которого будет сгенерирована аномалия
deep_pattern_violation_score	Количество токенов, добавляемых в ведро при нарушении цепочки плоского типа (после действия всегда одно другое, нет ветвления)
max_trace_length	Максимальная длина цепочки
sequence_ttl	Время актуальности действий в рамках цепочки
session_lifetime	Время жизни сессии пользователя
short_pattern_violation_score	Количество токенов, добавляемых в ведро при нарушении цепочки древовидного типа (после действия есть несколько вариантов ветвления)

17.11. SessionAnomalyCounter

Данный модуль отвечает за подсчёт количества аномалий в рамках пользовательской сессии.

Перечень настроек, которые разрешено менять пользователям представлены в таблице 28.

Таблица 28 – SessionAnomalyCounter

Параметр	Описание
anomaly_threshold	Размер ведра для аномалий, при переполнении которого будет сгенерирована аномалия

Примечание: Остальные параметры настройки анализатора, которые не были описаны в данном документе, менять без согласования категорически не рекомендуется.

18. Настройка сессионной модели

Сессия – это механизм, позволяющий отличать запросы одного пользователя от запросов другого. В связи с тем, что в протоколе HTTP нет такого понятия как механизм отслеживания сессий, для реализации этой задачи принято использовать cookie. Классический вариант решения выглядит следующим образом: когда клиент переходит в приложение, то ему выдается cookie уникально его идентифицирующая; после чего с каждым запросом данного клиента отправляется выданная ему cookie. Для подобного рода cookie может быть установлено время жизни.

Сессионная модель – это механизм, позволяющий на WAF привязаться к сессиям, описанным выше.

18.1. Создание сессионных атрибутов

На основе сессионных атрибутов WAF генерирует ID сессии. Формат ID сессии не специфицирован, реализуется как hash-функция от набора значений сессионных атрибутов и различается для разных сессий. Используется только внутри WAF.

Создавать сессионные атрибуты можно как на вкладке «Пользователи и сессии» окна «Приложения», тогда сессионный атрибут будет использоваться для выбранного приложения, так и на вкладке «Отслеживание сессий» окна «Настройки», тогда будет возможность выбрать, будет ли использован данный сессионный атрибут для всех приложений инсталляции или только для какого-то определенного приложения.

Окно создания сессионного атрибута представлено на рисунке 167.

Для того чтобы сессионная модель заработала необходимо убедится, что модуль легковесного отслеживания сессий (LWSessionTracker) включен в настройках анализатора. Если необходим функционал отслеживания предварительного выставления сессионной cookie – необходимо включить модуль разбора запросов (DecisionTreeResponseParser). Подробнее о настройках модулей анализатора написано в разделе 17.

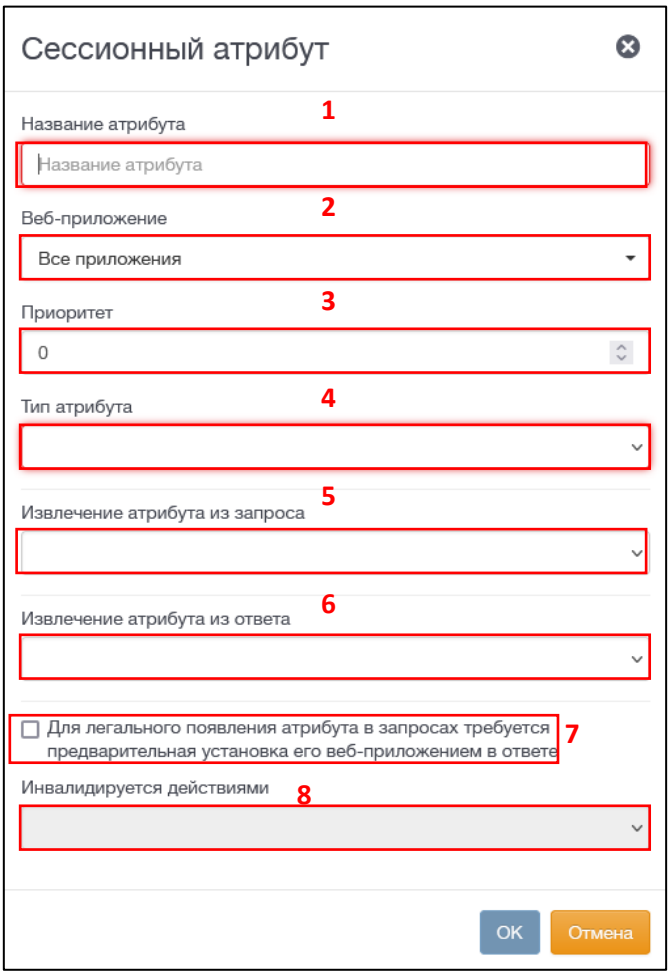

Рисунок 167 – Окно «Сессионный атрибут»

Настройки сессионного атрибута содержат следующие элементы:

1. Название атрибута – поле ввода названия сессионного атрибута.
2. Веб-приложение – поле выбора приложения из заведенных на инсталляции.
3. Приоритет – поле ввода приоритета сессионного атрибута. Чем меньше число, выставленное в приоритете, тем важнее для WAF этот атрибут.
4. Тип атрибута – выбор типа атрибута из трех предложенных:

- Идентификатора сессии – сессионный атрибут, который уникально идентифицирует сессию;
- Идентификатора последовательности – необходим для того, чтобы сделать переход от неавторизированной сессии к авторизированной, в тех случаях, когда сессионный атрибут изменяется при авторизации (например, PHPSESSIONID);
- Идентификатора пользователя – извлечение имени пользователя дает возможность отслеживать активность пользователя в рамках сессии.

5. Извлечение атрибута из запроса – выбор места запроса, откуда будет извлекаться сессионный атрибут. В некоторых вариантах необходимо указать путь в дереве разбора запроса к элементу, который будет использоваться в качестве сессионного атрибута.
6. Извлечение атрибута из ответа – выбор места ответа, откуда будет извлекаться сессионный атрибут. В некоторых вариантах необходимо указать путь в дереве разбора ответа к элементу, который будет использоваться в качестве сессионного атрибута.

7. Для легального появления атрибута в запросах требуется предварительная установка его веб-приложением в ответе – в случае использования данного чекбокса, если в транзакции будет использоваться сессионный атрибут, который до этого не был установлен в ответе – транзакция будет заблокирована.
8. Инвалидируется действием – выбор действия из заведенных на приложении (доступен, если в пункте 2 выбрано приложение), в качестве инвалидирующего сессионного атрибута.

18.2. Аномалии, генерируемые сессионной моделью

Модуль LWSessionTracker генерирует аномалии RequestAnomaly следующих видов:

- для атрибутов в запросе, которые требовали установки в ответе, но не были установлены:
  - reason — Session with these attributes is unknown;
  - topics — MODEL, DEFAULT_SESSION, CORRELATION;
  - дополнительно — список с uuid, типами, названиями и значениями атрибутов-нарушителей и хинт о том, что ситуация может быть из-за того, что отключен разбор ответов;
- при превышении предельного числа пользователей на одну sequence_id:
  - reason — Multiple user ids in the same action sequence;
  - topics — AUTOMATION, SESSION, CORRELATION;
  - дополнительно — текущее число наблюдавшихся для последовательности разных пользователей;
- для ошибок валидации кастомных атрибутов:
  - reason — Custom attribute validation error;
  - topics — MODEL, CORRELATION, INVALID_CUSTOM_ATTRIBUTE;
  - дополнительно — списком ошибки от каждого из кастомных валидаторов (их конкретный формат и содержимое зависит от сработавших валидаторов).

18.3. Создание цепочек действий

Во время работы с веб-приложением предполагается, что у пользователей должны быть устойчивые паттерны в действиях, в первую очередь обусловленные веб-интерфейсом приложения.

Классический пример: легитимный пользователь не может отправить форму без предварительной ее загрузки. Следовательно, на WAF сперва будет виден GET-запрос загрузки формы авторизации, а после этого должен идти POST-запрос отправки данных. Очень часто бот-системы игнорируют действие загрузки формы и отправляют сразу POST-запросы с данными для авторизации, тем самым нарушая нормальную последовательность работы с веб-приложением.

Именно на этих отличиях и строится работа модуля «Последовательности действий». Важно понимать, что цепочки действий работают поверх сессионной модели.

Для настройки цепочки действий необходимо перейти на вкладку «Приложения» -> «Действия» -> «Цепочки действий» и нажать на кнопку «Добавить новую цепочку действий» (см. рисунок 168).

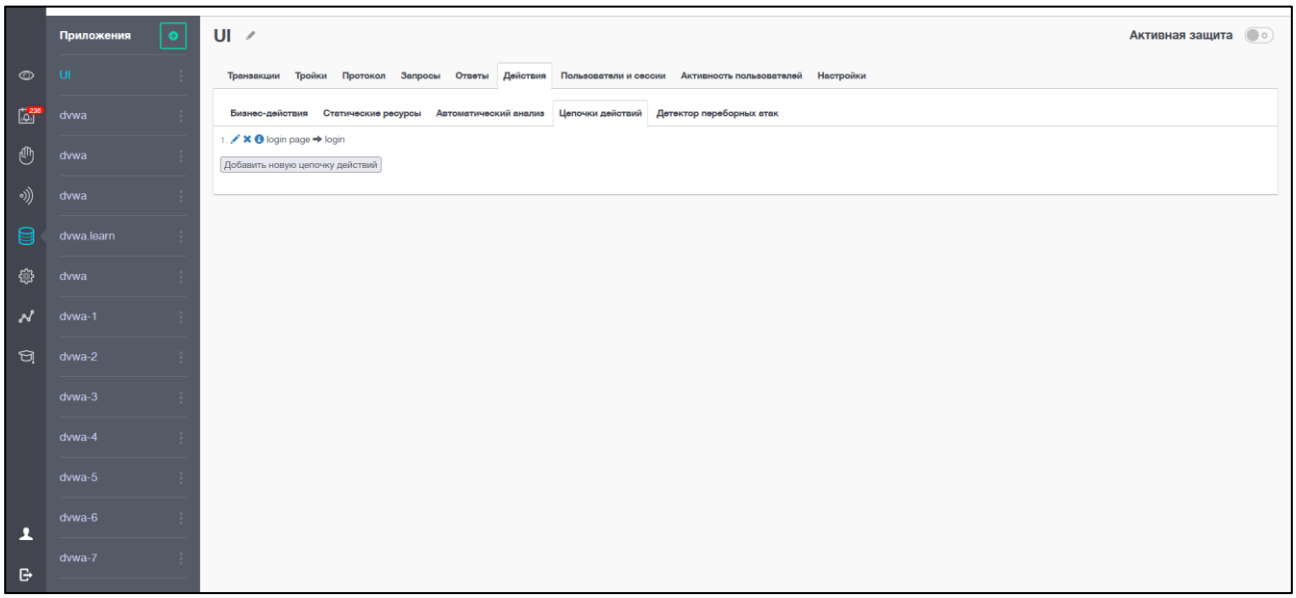

Рисунок 168 – Цепочки действий

Откроется окно «Цепочка действий», в котором можно создать новую цепочку действий (см. рисунок 169).

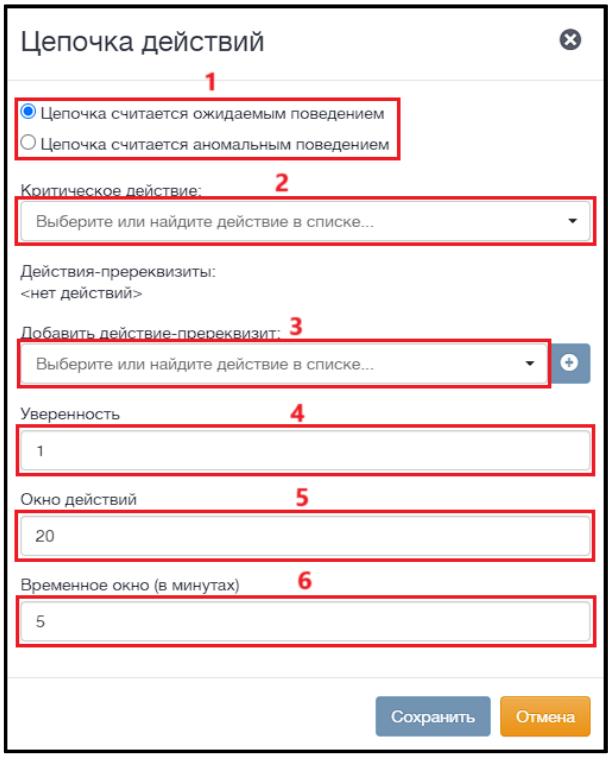

Рисунок 169 – Окно «Цепочка действий»

Окно «Цепочка действий» содержит следующие элементы:

1. Выбор цепочки действий - выбор цепочки, которая будет считаться либо аномальной (негативная модель), либо ожидаемой (позитивная модель).
2. Критическое действие – выбор действий из заведенных на приложении в качестве действия, которым должна закончиться цепочка действий.

3. Действие-пререквизит – выбор действия из заведенных на приложении в качестве действия, которым должна начинаться цепочка действий. Имеется возможность выбора нескольких действий-пререквизитов.
4. Уверенность – дробное значение от 0 до 1. Степень достоверности цепочки. Чем чаще действия внутри цепочки будут идти одновременно и в одинаковом порядке относительно друг друга, тем выше будет значение уверенности для цепочки при ее генерации инструментами машинного обучения. Этот параметр используется для модуля выявления аномальности сессии при нарушении цепочек. Так как при создании цепочек вручную мы достоверно знаем какое действие-предикат должно быть перед критичным действием данное значение выставляется в 1.
5. Окно действий – целое число больше 0. При появлении транзакции с критическим действием формируется трасса, состоящая из последних n транзакций, где n - окно действий для цепочки с этим критическим действием. То есть окно действий это n- транзакций до критического действия, среди которых должно быть действие предикат.
6. Временное окно – целое число больше 0. Величина в минутах. В рамках временного окна рассматривается окно действий, то есть трасса формируется из n-транзакций (где n есть величина окна действий), которые были сделаны за последние m-минут (где m есть величина временного окна) до критического действия. Транзакции, выходящие за рамки временного окна, не учитываются.

Для корректной работы модуля требуется его настройка в анализаторе (см. раздел 0).

19. Настройка отслеживания открытого перенаправления (Open redirect)

На WAF имеется возможность закрытия уязвимости открытого перенаправления (Open redirect), которая позволяет незаметно направить пользователя на любой сайт с доверенного домена. Данная уязвимость может использоваться, например:

- для кражи учетных данных, путём подмены страницы авторизации на фишинговую;
- для понижения рейтинга поисковой выдачи сайта, с которого происходит открытое перенаправление.

Для работы данного модуля достаточно включить в анализаторе модули OpenRedirectDetector и DecisionTreeResponseParser (подробнее можно прочитать в разделе 15) и включить преднастроенное правило «Открытое перенаправление» (см. рисунок 170).

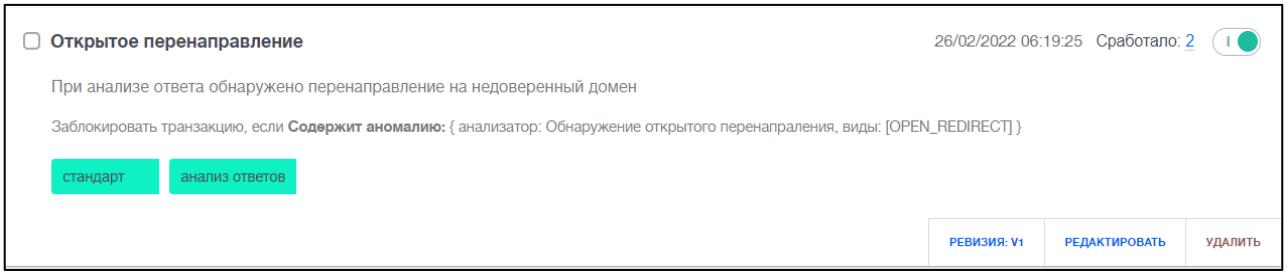

Рисунок 170 – Правило «Открытое перенаправление»

Данный модуль работает на основе анализа ответа. Детектор смотрит значение заголовков location и refresh в ответе и блокирует запросы, в которых значения данных заголовков отличны от значения заголовка host в запросе.

В настройках приложения (см. п. 3.5.8) так же можно задать доверенные домены для модуля Open redirect (см. Рисунок 171).

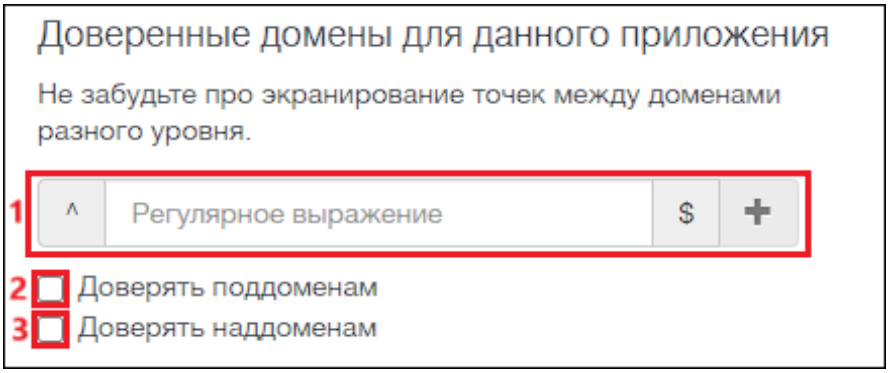

Рисунок 171 – Доверенные домены для данного приложения

Доверенные домены для данного приложения содержит следующие элементы:

1. Поле ввода домена, после ввода домена нужно нажать кнопку « + ».
2. Доверять поддоменам – после активации чекбокса « ☑ » в белый список попадут все поддомены. Для домена ex.example, ex является поддоменом.
3. Доверять наддоменам – после активации чекбокса « ☑ » в белый список попадут все наддомены. Для домена ex.example, example является наддоменом.

20. Настройка CSRF детектора

На WAF имеется возможность закрытия уязвимости межсайтовой подделки запросов (CSRF), которая позволяет злоумышленнику действовать на сайте от имени другого зарегистрированного посетителя.

Для работы данного модуля достаточно включить в анализаторе модуль CsrfDetector и включить преднастроенное правило «CSRF-атака» (см. рисунок 172).

Рисунок 172 – Правило «CSRF-атака»

Данный модуль блокирует POST-запросы, в которых домен в заголовке referer не совпадает с доменом в заголовке host.

В настройках приложения пункт 4.5.8 так же можно задать доверенные домены для модуля CSRF (см.).

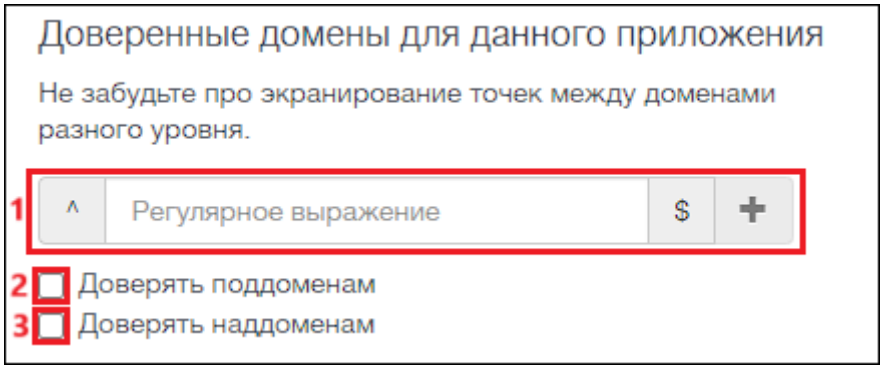

Рисунок 173 – Доверенные домены для данного приложения

Доверенные домены для данного приложения содержит следующие элементы:

1. Поле ввода домена, после ввода домена нужно нажать кнопку « + ».
2. Доверять поддоменам – после активации чекбокса « ☑ » в белый список попадут все поддомены. Для домена ex.example, ex является поддоменом.
3. Доверять наддоменам – после активации чекбокса « ☑ » в белый список попадут все наддомены. Для домена ex.example, example является наддоменом.

21. Создание правил

Для того чтобы создать правило необходимо перейти на вкладку «Правила» и нажать на кнопку «Добавить правило» (см. рисунок 174).

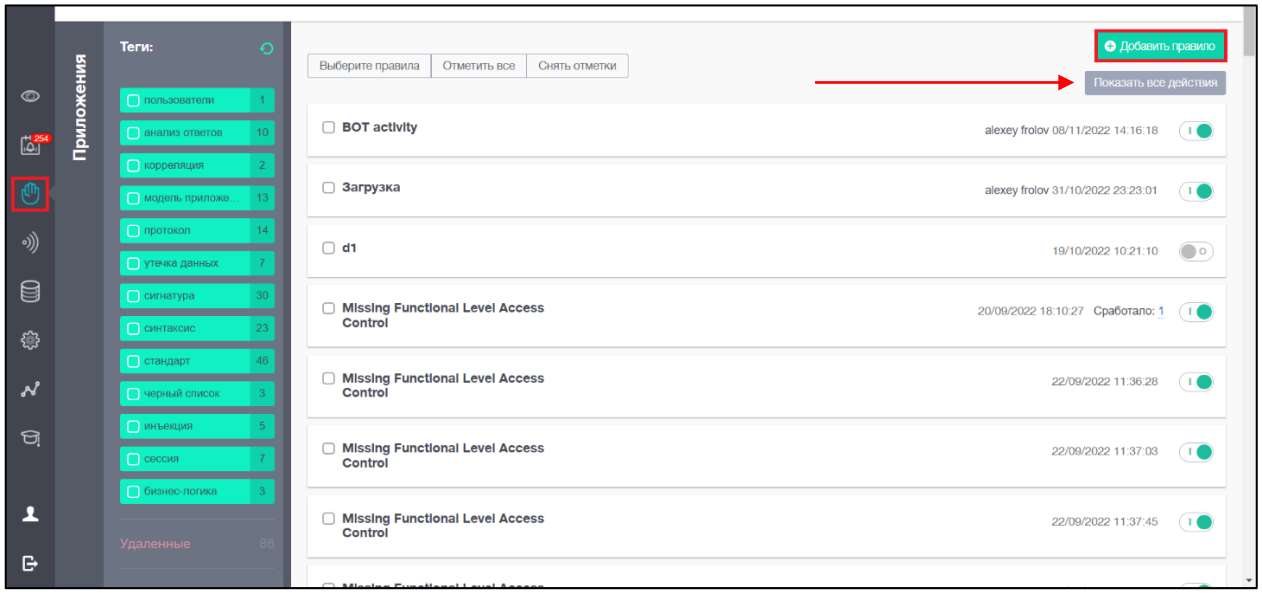

Рисунок 174 – Создание правила

После нажатия на кнопку «Добавить правило» появляется окно создания нового правила (см. рисунок 175).

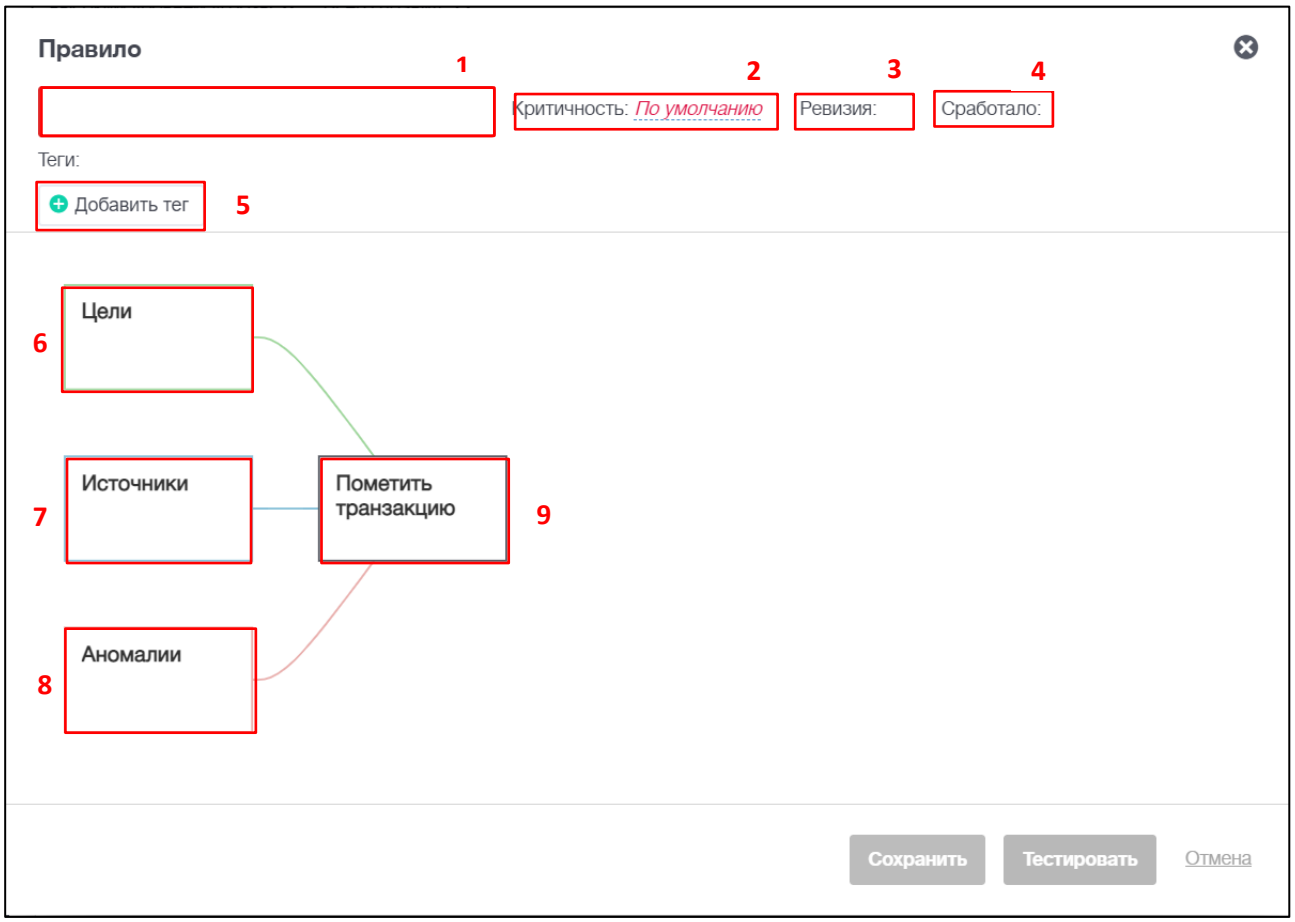

Рисунок 175 – Окно создания правила

Окно создания правила содержит следующие элементы:

1. Название правила – поле ввода названия правила.
2. Критичность – в данном окне задаётся критичность правила из предложенного списка (см. рисунок 176). Критичность правила проставляется для дополнительной информации пользователю и не влияет на очередность срабатывания правил.

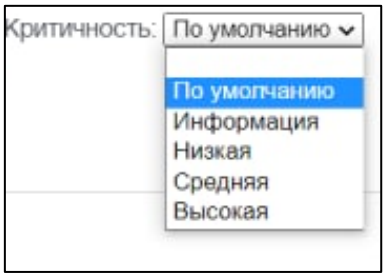

Рисунок 176 – Меню выбора критичности правила

3. Ревизия – окно выбора версионности правила с возможностью переключения на более старую версию.
4. В данном окне указывается количество срабатываний данного правила.
5. Добавление тега – в данном окне можно добавить теги из существующих (см. рисунок 177) или создать новые. Данный функционал позволяет пользователя фильтровать правила по категориям.

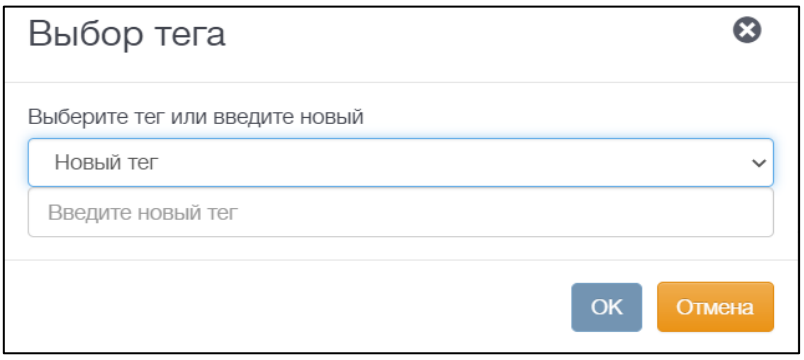

Рисунок 177 – Выбор существующего тега или создание нового

Примечание: при выборе тега появляется выпадающее меню с уже созданными тегами (см. рисунок 178). Меню содержит только те теги, на которые были созданы общие правила. Тег, использующийся только для правил на конкретное приложение, предлагаться не будет. Однако, при необходимости, его можно ввести в строку ввода тега вручную.

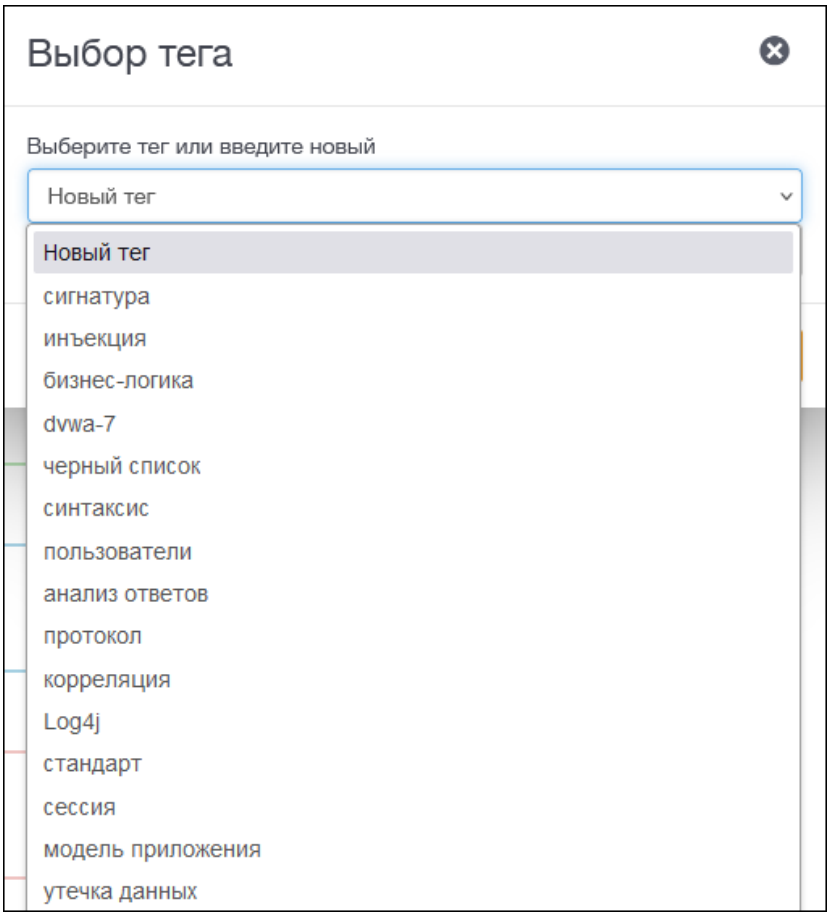

Рисунок 178 – Меню выбора тегов

6. Цели – в данном разделе выбирается цель из предложенного списка (см. рисунок 179). Также имеется возможность выбора отрицания выбранного условия (см. рисунок 180). Доступные цели при создании правила описаны в таблице 29.

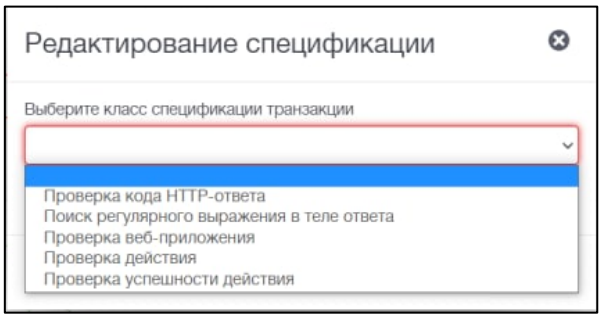

Рисунок 179 – Выбор цели

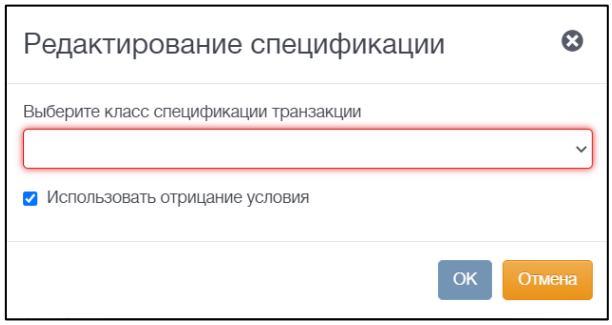

Рисунок 180 – Возможность использования отрицания условия

Таблица 29 – Выбор цели при создании правила

Возможные классы спецификации транзакции	Возможные параметры	Примечание
Проверка кода HTTP-ответа	Укажите коды ответов	Правило работает только для перечисленных кодов ответов
	Использовать отрицание условия	Правило работает для всех кодов ответов, кроме перечисленных
Поиск регулярного выражения в теле ответа	Регулярное выражение	Правило работает для ответов, содержащих указанное регулярное выражение
	Использовать отрицание условия	Правило работает для всех ответов, которые не содержат регулярное выражение
Проверка веб-приложения	Выберите приложение	Правило будет распространяться только на трафик приложения
	Использовать отрицание условия	Правило будет распространяться на трафик всех приложений, кроме указанного
Проверка действия	Выберите действие	Может использоваться только после блока «Проверка веб-приложения». Правило распространяется только на трафик приложения, который

Возможные классы спецификации транзакции	Возможные параметры	Примечание
		соответствует выбранному действию
	Использовать отрицание условия	Может использоваться только после блока «Проверка веб-приложения». Правило распространяется на весь трафик приложения кроме того, который соответствует выбранному действию
Проверка успешности действия	Выберите статус успешность действия	Правило будет распространяться только на выбранный статус успешности действия
	Использовать отрицание условия	Правило будет распространяться на трафик всех статусов успешности, кроме указанного

7. Источники – в данном разделе выбирается источник из предложенного списка (см. рисунок 181). Также имеется возможность выбора отрицания выбранного условия. Доступные источники при создании правила описаны в таблице 30.

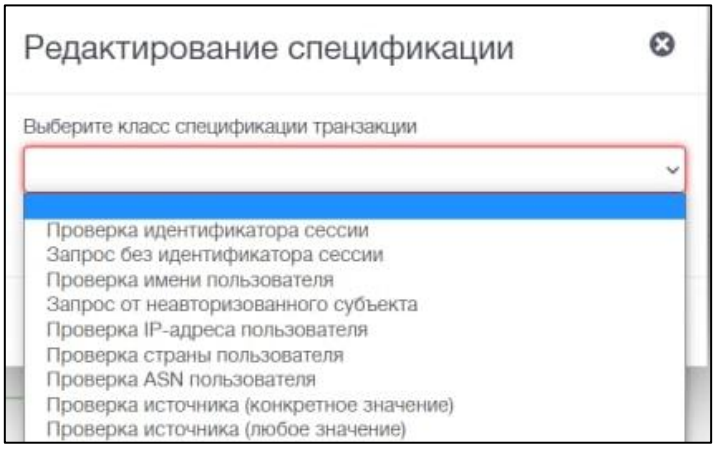

Рисунок 181 – Выбор источника

Таблица 30 – Выбор источника при создании правила

Возможные классы спецификации транзакции	Возможные параметры	Примечание
Проверка идентификатора сессии	Укажите идентификатор сессии	Правило работает для всех запросов, идентификатор сессии которых соответствует заданному
	Использовать отрицание условия	Правило работает для всех запросов, идентификатор сессии

Возможные классы спецификации транзакции	Возможные параметры	Примечание
		которых не соответствует заданному
Запрос без идентификатора сессии	-	Правило работает для всех запросов без идентификатора сессии
	Использовать отрицание условия	Правило не работает для всех запросов без идентификатора сессии
Проверка имени пользователя	Укажите имя пользователя	Правило работает для запросов, относящихся к указанному пользователю
	Использовать отрицание условия	Правило работает для запросов, относящихся ко всем пользователям кроме указанного
Запрос от неавторизованного субъекта	-	Правило работает для запросов неавторизованных пользователей
	Использовать отрицание условия	Правило работает для всех запросов, кроме запросов неавторизованных пользователей
Проверка IP-адреса пользователя	Укажите IP-адрес	Правило работает для запросов, поступающих с указанного IP-адреса с указанной маской подсети
	Маска подсети	
	Использовать отрицание условия	Правило работает для всех запросов кроме запросов, поступающих с указанного IP-адреса с указанной маской подсети
Проверка страны пользователя	Укажите страну	Правило работает для всех запросов, поступающих с IP-адресов, относящихся к определённой стране
	Использовать отрицание условия	Правило работает для всех запросов кроме запросов, поступающих с IP-адресов, относящихся к определённой стране
Проверка ASN пользователя	Укажите ASN	Правило работает для запросов, поступающих с указанного ASN

Возможные классы спецификации транзакции	Возможные параметры	Примечание
	Использовать отрицание условия	Правило работает для запросов кроме запросов, поступающих с указанного ASN
Проверка источника (конкретное значение)	Укажите источник	Правило работает для запросов, поступающих с указанного источника и с указанным значением для поиска совпадений с этим источником
	Укажите значение для поиска совпадения	
	Использовать отрицание условия	Правило работает для запросов кроме запросов, поступающих с указанного источника и с указанным значением для поиска совпадений с этим источником
Проверка источника (любое значение)	Укажите источник	Правило работает для запросов, поступающих с указанного источника
	Использовать отрицание условия	Правило работает для запросов кроме запросов, поступающих с указанного источника

8. Аномалии – в данном разделе выбирается аномалия из предложенного списка (см. рисунок 182). Также имеется возможность выбора отрицания выбранного условия. Доступные аномалии при создании правила описаны в таблице 31.

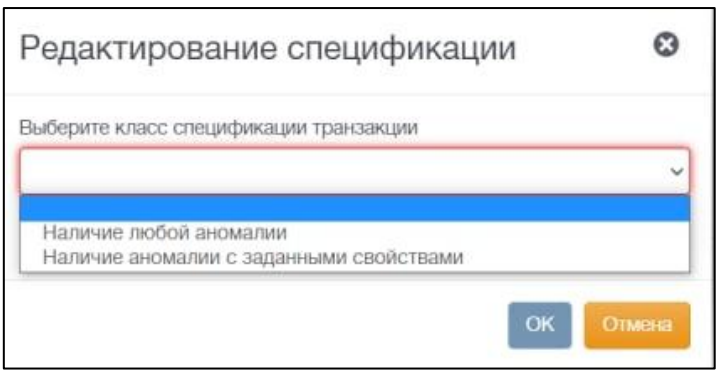

Рисунок 182 – Выбор аномалии

Таблица 31 – Выбор аномалии при создании правила

Возможные классы спецификации транзакции	Возможные параметры	Примечание
Наличие любой аномалии	–	Правило работает для любой транзакции с выявленной аномалией

Возможные классы спецификации транзакции	Возможные параметры	Примечание
	Использовать отрицание условия	Правило работает для всего трафика, в котором не выявлены аномалии
Наличие аномалии с заданными свойствами	Выберите модуль анализа (Обнаружение аномалий в последовательностях действий; Детектор CSFR-атак; Обнаружение переборных атак; Разбор ответа; Модуль обратного прокси; Отслеживание пользователей; Подсчёт аномальности сессии; Проверка синтаксиса параметров действий; Разбор запроса; Сигнатурный анализ; Обнаружение SQL- инъекций; Выделение действий; Отслеживание сессий)	Правило работает для транзакции с выявленной выбранным модулем аномалией. Обязательное поле
	Задайте виды аномалий	Правило работает для транзакции с выявленными выбранным модулем заданными аномалиями
	Выберите тип расположения аномалий: не проверять; HTTP- сообщение в целом; первая строка HTTP- сообщения в целом; Заголовок; тело в целом; параметр в теле запроса; URL в целом; параметр URL; cookie; элемент дерева разбора; сессионные данные; источник (подробное описание детектора переборных атак – Действие/Источник находится в разделе 16.1); цель/объект веб-приложения (Подробное описание детектора переборных атак – Действие/Источник/Цель находится в разделе 16.2)	Правило работает для транзакции с выявленной выбранным модулем аномалией, с указанным расположением
	Выберите имя расположения аномалии	Правило работает для транзакции с выявленной выбранным модулем

Возможные классы спецификации транзакции	Возможные параметры	Примечание
		аномалией, с указанным расположением и указанным именем расположения аномалии
	Использовать отрицание условия	Правило работает для всех транзакций кроме транзакций, соответствующих указанным параметрам

9. В данном разделе выбирается действие из предложенного списка (см. рисунок 183) для созданного правила. Доступные действия при создании правила описаны в таблице 32.

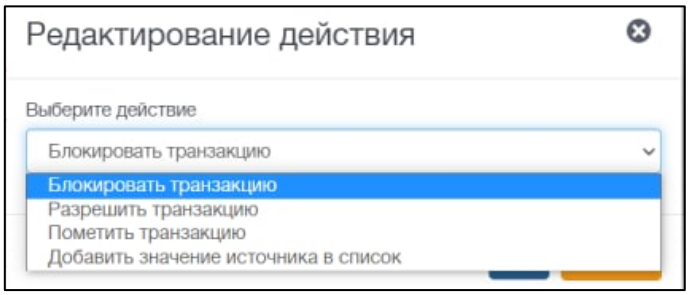

Рисунок 183 – Выбор действия

Таблица 32 – Выбор действия при создании правила

Действие	Возможные параметры	Примечание
Пометить транзакцию	–	Транзакция, соответствующая заданным в спецификациях «Цели», «Источники» и «Аномалии», помечается для дальнейшего анализа. Используется как действие по умолчанию
Разрешить транзакцию	–	Транзакция, соответствующая заданным в спецификациях «Цели», «Источники» и «Аномалии», пропускается как легитимная
Блокировать транзакцию	–	Транзакция, соответствующая заданным в спецификациях «Цели», «Источники» и «Аномалии», блокируется
Добавить значение источника в список	Прервать цепочку применения правил	При срабатывании правила цепочка применения правил прерывается
	Решение для транзакции	При срабатывании правила устанавливается выбранное решение

Действие	Возможные параметры	Примечание
	Источник	При срабатывании правила значение указанного источника добавляется в список
	Список	При срабатывании правила значение источника добавляется в указанный список
	Описание добавляемого в список элемента	Дополнительная информация о добавляемом значении источника
	Время жизни добавляемого элемента (в секундах)	Значение источника будет добавлено на указанное время в список

После заполнения всех необходимых полей необходимо нажать кнопку «Сохранить», в результате чего созданное правило появится в списке всех доступных правил.

Примечание: после создания правило находится в выключенном режиме, не забудьте включить правило, если это необходимо.

21.1. Особый шаблон ответа

Для настройки выдачи JavaScript-верификации с редиректом вместо блокировки в панели управления необходимо выбрать специальный шаблон ответа *redirect.response.json* (см. рисунок 184).

Рисунок 184 – Редирект вместо блокировки

Стандартная конфигурация /etc/ibatyr-nginx/templates/redirect.response.json выглядит так:

```
{
  "$apply": "challenge",
  "type": "redirect",
  "valid_for": 300
}
```

Параметры:

1. Параметр valid_for отвечает за время в секундах, в течение которого действительна уже пройденная ранее валидация.

Если задано значение null, то валидация имеет бесконечный срок действия. Срок действия проверяется каждый запрос, к которому применяется мягкая реакция, так что если конфигурация меняется, то сразу используются новые настройки.

2. Недокументированный параметр obfuscation отвечает за настройки способа обфускации JavaScript-кода и имеет разумные умолчания, подобранные эмпирически.

Шаблон страницы при желании можно кастомизировать, отредактировав файл **/etc/ibatyr-nginx/templates/redirect.html**.

При блокировке с использованием этой мягкой реакции происходит следующее:

1. Проверяется, не проходил ли пользователь ранее эту валидацию.
2. Если старая валидация все еще действительна и IP-адрес пользователя не менялся, то запрос пропускается.

В журнале iBatyr Nginx это решение отображается как «Pass: challenge passed: redirect».

3. В противном случае в ответ отдается блокировка с обфусцированным JavaScript-кодом, который делает следующее:

   3.1. В случае наличия признаков использования управляемого браузера, валидация считается неуспешной.

   3.2. В случае успешной валидации:

   – Выполняется установка зашифрованного JWE-токена в cookie, имя которой определяется настройкой SESSIONS_COOKIE_NAME (по умолчанию — __sw). Результат валидации привязывается к IP-адресу пользователя.
   – Происходит перенаправление (GET-запрос) на изначально запрошенный URL.

22. Работа с Modsecurity

Вкладка конфигурации модулей находится по пути «Настройки» -> «Конфигурации модулей» (см. рисунок 185).

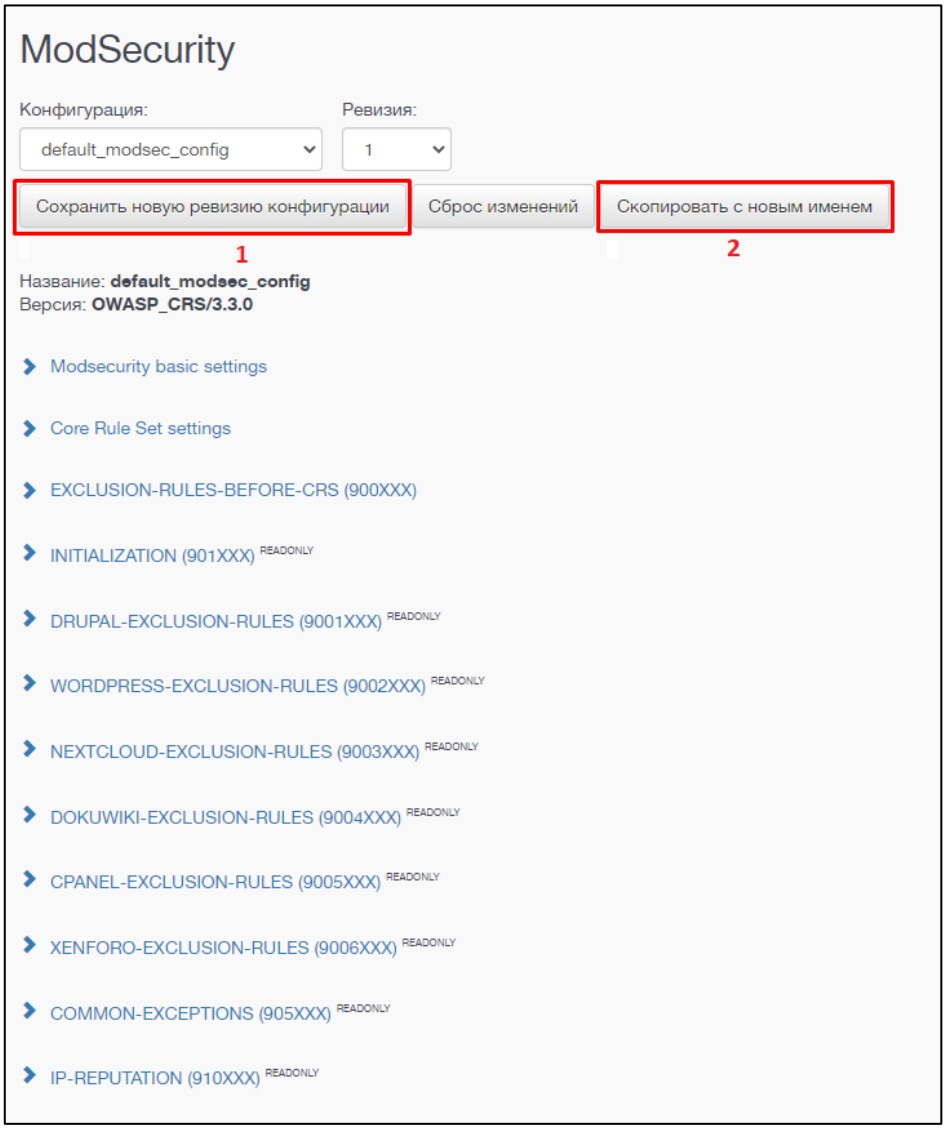

Рисунок 185 – Вкладка «Конфигурации модулей»

Вкладка «Конфигурация модулей» содержит следующие элементы:

1. Сохранить новую ревизию конфигурации – сохранить изменения в новой ревизии.
2. Скопировать с новым именем – скопировать выбранную конфигурацию в новую с новым именем.

На данной вкладке находятся сигнатуры для сигнатурного анализатора Modsecurity, расположенные по соответствующим группам.

22.1. Общий вид сигнатуры для ModSecurity

В упрощенном виде сигнатура для ModSecurity выглядит следующим образом:

```
[Директива] [Переменная] [Оператор] [Номер правила] [Решение] [Тег правила]
```

```
SecRule REQUEST_COOKIES "@rx %2f" "id:999000, phase:2, block,
tag:'castom_teg'"
```

В выше записанной сигнатуре:

1. SecRule – директива, отвечающая за создание правила.
2. REQUEST_COOKIES – переменная, которая указывает на место, анализируемое правилом.
3. @rx – оператор, определяющий способ ввода шаблона значения.
4. id:999000 – идентификационный номер правила.
5. phase:2 – фаза, на которой работает правило.
6. block – решение по правилу (в случае работы ModSecurity в связке с WAF, не имеет силы. Блокировки на WAF происходят, исходя из правил безопасности. Но данный параметр должен присутствовать в сигнатуре, во избежание ошибки синтаксиса).
7. tag:'castom_teg' – тег правила, по нему в разрезе правил WAF осуществляется блокировка.

22.1.1. Директивы ModSecurity

Директива в ModSecurity выполняет роль выбора «режима» работы сигнатуры ModSecurity. Директивы, корректно, работающие на WAF представлены в таблице 33.

Таблица 33 – Директивы ModSecurity

Директивы	Описание	Пример
SecRule	Создает правило, которое будет анализировать выбранные переменные с помощью выбранного оператора	`SecRule ARGS "@rx attack" "phase:1,log,deny,id:1"`
SecAction	Обрабатывает список действий, который получает в качестве параметра	`SecAction "action1,action2,action3,..."`
SecRuleUpdateActionById	Обновляет список действий указанного правила. Эта директива перезапишет список действий указанного правила. У него есть два ограничения: его нельзя использовать для изменения тега или параметра правила. Перезаписываются только действия, которые могут появиться только один раз. Действия, которым разрешено появляться в списке несколько раз, будут добавлены в конец списка.	`SecRuleUpdateActionById 954100 "tag:'LEAKAGE',tag:'ERRORS_IIS'"`
SecRuleRemoveById	Удаляет правила сопоставления из текущего контекста конфигурации. Эта директива поддерживает несколько параметров, каждый из которых может быть идентификатором правила или диапазоном. Параметры, содержащие пробелы, должны быть разделены двойными кавычками.	`SecRuleRemoveById 942420`

Директивы	Описание	Пример
SecRuleUpdateTargetByTag	Обновляет целевой список (переменных) указанного правила по тегу правила. Эта директива добавит (или заменит) переменные в текущий список целей указанного правила целями, указанными во втором параметре	`SecRuleUpdateTargetByTag TEXT TARGET1[,TARGET2,TARGET3] REPLACED_TARGET`
SecMarker	Добавляет фиксированный маркер правила, который можно использовать в качестве цели в действии SkipAfter. Директива SecMarker по сути создает правило, которое ничего не делает и единственной целью которого является перенос данного идентификатора.	

22.1.2. Переменные ModSecurity

Переменная в сигнатуре служит указателем на место, подвергающееся анализу. Переменные ModSecurity представлены в таблице 34.

Таблица 34 – Переменные ModSecurity

Переменные	Описание	Пример
REQUEST_LINE	Эта переменная содержит полную строку запроса, отправленную на сервер (включая метод запроса и информацию о версии HTTP)	`SecRule REQUEST_LINE "!(^((?:(?:POS|GE)T|HEAD))|HTTP/(0\.9|1\.0|1\.1)$)" "phase:1,id:49,log,block,t:none"`
ARGS	ARGS — эта переменная, которую можно использовать отдельно (означает все аргументы, включая полезную нагрузку POST), со статическим параметром (сопоставляет аргументы с этим именем) или с регулярным выражением (сопоставляет все аргументы с именем, соответствующим регулярному выражению). Чтобы просмотреть только строку запроса или аргументы тела, см. директивы ARGS_GET и ARGS_POST	`SecRule ARGS dirty "id:7"`
ARGS_NAMES	Содержит все имена параметров запроса. Вы можете искать конкретные имена параметров, которые хотите проверить. В положительном сценарии политики вы также можете внести в белый список (используя перевернутое	`SecRule ARGS_NAMES "!^(p|a)$" "id:13"`

Переменные	Описание	Пример
	правило с восклицательным знаком) только имена авторизованных аргументов. В этом примере правила допускается только два имени аргумента: p и a	
ARGS_GET	ARGS_GET аналогичен ARGS, но содержит только параметры строки запроса	`SecRule ARGS_GET dirty "id:7"`
ARGS_POST	ARGS_POST аналогичен ARGS, но содержит только аргументы из тела POST	`SecRule ARGS_POST dirty "id:7"`
REQUEST_COOKIES	Эта переменная представляет собой коллекцию всех файлов cookie запроса (только значения). Пример: в следующем примере используется специальный оператор «Амперсанд» для подсчета количества переменных в коллекции. В этом правиле оно сработает, если запрос не содержит заголовков файлов cookie	`SecRule &REQUEST_COOKIES "@eq 0" "id:44"`
REQUEST_BODY	Содержит необработанное тело запроса. Эта переменная доступна только в том случае, если использовался обработчик тела запроса URLENCODED, что происходит по умолчанию при обнаружении типа контента application/x-www-form-urlencoded, или если использование анализатора тела запроса URLENCODED было принудительно	`SecRule REQUEST_BODY "^username=\w{25,}\&password=\w{25,}\&Submit\=login$" "id:43"`
REQUEST_COOKIES_NAMES	Эта переменная представляет собой набор имен всех файлов cookie запроса. Например, следующее правило сработает, если файл cookie JSESSIONID отсутствует	`SecRule &REQUEST_COOKIES_NAMES:JSESSIONID "@eq 0" "id:45"`
REQUEST_HEADERS	Эту переменную можно использовать либо как коллекцию всех заголовков запроса, либо для проверки выбранных заголовков (с использованием синтаксиса REQUEST_HEADERS:Header-Name)	`SecRule REQUEST_HEADERS:Host "^[\d\.]+$" "deny,id:47,log,status:400,msg:'Host header is a numeric IP address'"`
REQUEST_HEADERS_NAMES	Эта переменная представляет собой набор имен всех заголовков запроса	`SecRule REQUEST_HEADERS_NAMES "^x-forwarded-for" "log,deny,id:48,status:403,t:lowercase,msg:'Proxy Server Used'"`

Переменные	Описание	Пример
XML	Специальная коллекция, используемая для взаимодействия с парсером XML. Его можно использовать отдельно в качестве цели для операторов validateDTD и validateSchema. В противном случае оно должно содержать допустимое выражение XPath, которое затем будет сравниваться с ранее проанализированным деревом XML DOM	`SecRule REQUEST_HEADERS:Content-Type ^text/xml$ "phase:1,id:87,t:нижний регистр,nolog,pass,ctl:requestBodyProcessor=XML"` `SecRule REQBODY_PROCESSOR "!^XML$" SkipAfter:12345,id:88`
validateSchema	Проверяет дерево XML DOM на соответствие предоставленной схеме XML. Дерево DOM должно быть предварительно построено с использованием процессора тела запроса XML. Этот оператор сигнализирует, когда проверка не удалась	`SecRule REQUEST_HEADERS:Content-Type ^text/xml$ "phase:1,id:190,nolog,pass,t:нижний регистр,ctl:requestBodyProcessor=XML"`
validateDTD	Проверяет дерево XML DOM на соответствие предоставленному DTD. Дерево DOM должно быть предварительно построено с использованием процессора тела запроса XML. Этот оператор сигнализирует, когда проверка не удалась	`SecRule XML "@validateDTD /path/to/xml.dtd" "phase:2,id:181,deny,msg:'Ошибка проверки DTD'"`
REMOTE_ADDR	Выполняет быстрое сопоставление ipv4 или ipv6 переменной REMOTE_ADDR, загружая данные из файла. Может обрабатывать следующие форматы: Полный IPv4-адрес — 192.168.1.100. Адрес сетевого блока/CIDR — 192.168.1.0/24 Полный адрес IPv6 — 2001:db8:85a3:8d3:1319:8a2e:370:7348 Адрес сетевого блока/CIDR — 2001:db8:85a3:8d3:1319:8a2e:370:0/24	`SecRule REMOTE_ADDR "@ipMatchFromFile ips.txt" "id:163"`
REQUEST_URI	проверяет REQUEST_URI, содержащий данные, защищенные механизмом хеширования	`SecRule REQUEST_URI "@validatehash "product_info|product_list" "phase:1,deny,id:123456"`
AUTH_TYPE	Эта переменная содержит метод аутентификации, используемый для проверки пользователя, если используется какой-либо из методов, встроенных в HTTP. При развертывании	`SecRule AUTH_TYPE "Basic" "id:14"`

Переменные	Описание	Пример
	обратного прокси-сервера эта информация не будет доступна, если аутентификация выполняется на внутреннем веб-сервере.	
FILES	Содержит коллекцию исходных имен файлов (как они назывались в файловой системе удаленного пользователя). Доступно только для проверенных запросов multipart/form-data	`SecRule FILES "@rx \.conf$" "id:17"`
FILES_NAMES	Содержит список полей формы, которые использовались для загрузки файлов. Доступно только для проверенных запросов multipart/form-data	`SecRule FILES_NAMES "^upfile$" "id:19"`
FULL_REQUEST	Содержит полный запрос: строку запроса, заголовки запроса и тело запроса (если есть). Последний доступен только в том случае, если для параметра SecRequestBodyAccess установлено значение «Вкл.». Обратите внимание, что здесь будут учитываться все свойства SecRequestBodyAccess, например: SecRequestBodyLimit	`SecRule FULL_REQUEST "User-Agent: ModSecurity Regression Tests" "id:21"`
FILES_TMPNAMES	Содержит список имен временных файлов на диске. Полезно при использовании вместе с @inspectFile. Доступно только для проверенных запросов multipart/form-data	`SecRule FILES_TMPNAMES "@inspectFile /path/to/inspect_script.pl" "id:21"`
PATH_INFO	Содержит дополнительную информацию URI запроса, также известную как информация о пути. (Например, в URI /index.php/123 /123 — это информация о пути.) Доступно только во встроенных развертываниях	`SecRule PATH_INFO "^/(bin|etc|sbin|opt|usr)" "id:33"`
REMOTE_PORT	Эта переменная содержит информацию об исходном порте, который клиент использовал при инициировании соединения с нашим веб-сервером. В следующем примере мы оцениваем, меньше ли REMOTE_PORT 1024, что указывает на то, что пользователь является привилегированным пользователем	`SecRule REMOTE_PORT "@lt 1024" "id:37"`
REQUEST_FILENAME	Эта переменная содержит относительный URL-адрес запроса без части строки запроса (например, /index.php)	`SecRule REQUEST_FILENAME "^/cgi-bin/login\.php$" phase:2,id:46,t:none,t:normalizePath`

Переменные	Описание	Пример
REQUEST_METHOD	Эта переменная содержит метод запроса, используемый в транзакции	`SecRule REQUEST_METHOD "^(?:CONNECT|TRACE)$" "id:50,t:none"`
REQUEST_PROTOCOL	Эта переменная содержит информацию о версии протокола запроса	`SecRule REQUEST_PROTOCOL "!^HTTP/(0\.9|1\.0|1\.1)$" "id:51"`
REQUEST_BASENAME	Эта переменная содержит только часть имени файла REQUEST_FILENAME (например, index.php)	`SecRule REQUEST_BASENAME "^login\.php$" phase:2,id:42,t:none,t:lowercase`

22.1.3. Операторы ModSecurity

Операторы определяют методы и данные для сравнения. Операторы ModSecurity представлены в таблице 35.

Таблица 35 – Операторы ModSecurity

Операторы	Описание
@rx	Строка, следующая за оператором, будет интерпретироваться как регулярное выражение
@eq	Оператор считает количество символов в выбранном поле, и сравнивает с заданным после оператора числом
@inspectFile	Оператор изначально был разработан для проверки файлов (отсюда и название), но его также можно использовать в любой ситуации, требующей принятия решений с использованием внешней логики
@ipMatch	Оператор выполняет быстрое сопоставление ipv4 или ipv6 переменных данных REMOTE_ADDR
@ipMatchFromFile	Оператор выполняет быстрое сопоставление ipv4 или ipv6 переменной REMOTE_ADDR, загружая данные из файла
@le	Оператор выполняет числовое сравнение и возвращает true, если входное значение меньше или равно параметру оператора
@lt	Оператор выполняет числовое сравнение и возвращает true, если входное значение меньше параметра оператора
@pm	Оператор выполняет сопоставление предоставленных фраз без учета регистра с желаемым входным значением. Оператор использует алгоритм сопоставления на основе множеств (Aho-Corasick), что означает, что он будет параллельно сопоставлять любое количество ключевых слов. Когда требуется сопоставление большого количества ключевых слов, этот оператор работает намного лучше, чем регулярное выражение
@pmFromFile	Выполняет без учета регистра сопоставление предоставленных фраз с желаемым входным значением. Оператор использует алгоритм сопоставления на основе множеств (Aho-Corasick), что означает, что

	он будет параллельно сопоставлять любое количество ключевых слов. Когда требуется сопоставление большого количества ключевых слов, этот оператор работает намного лучше, чем регулярное выражение. Этот оператор аналогичен @pm, за исключением того, что в качестве аргументов он принимает список файлов. Оно будет соответствовать любой фразе, указанной в файле(ах) в любом месте целевого значения
@rb	Оператор ищет входное значение в RBL (списке блоков реального времени), заданном в качестве параметра. Параметром может быть IPv4-адрес или имя хоста
@streq	Оператор выполняет сравнение строк и возвращает true, если строка параметра идентична входной строке. Расширение макроса выполняется для строки параметра перед сравнением
@strmatch	Оператор выполняет сопоставление строки предоставленного слова с желаемым входным значением. Оператор использует алгоритм сопоставления с образцом Бойера-Мура-Хорспула, что означает, что это одиночный оператор сопоставления с образцом. Этот оператор работает намного лучше, чем регулярное выражение
@within	Оператор возвращает значение true, если входное значение находится в любом месте параметра @within

22.1.4. Функции преобразования ModSecurity

Функции преобразования применяются для изменения входных данных перед их использованием при сопоставлении (т. е. выполнении оператора). На самом деле, входные данные никогда не изменяются — всякий раз, когда запрашивается использование функции преобразования, ModSecurity создаст копию данных, преобразует её, а затем запустит оператор для результата. В случае если данные не могут быть преобразованы функцией преобразования, ModSecurity анализирует исходные данные. Можно использовать несколько функций преобразования в рамках одной сигнатуры.

Функции преобразования ModSecurity представлены в таблице 36.

Таблица 36 – Функции преобразования ModSecurity

Функции преобразования	Описание
t:base64Decode	Декодирует строку в кодировке Base64
t:sqlHexDecode	Декодирует шестнадцатеричные данные SQL. Например, (0x414243) будет декодирован в (ABC)
t:base64DecodeExt	Декодирует строку в кодировке Base64. В отличие от base64Decode, в этой версии используется щадящая реализация, игнорирующая недопустимые символы
t:cmdLine	В Windows и Unix команды могут экранироваться разными способами, например: * c^команда /c ...; * "команда" /c...;

	* команда,/c.... * обратная косая черта в середине команды Unix Функция преобразования cmdLine позволяет избежать этой проблемы, манипулируя переменной contend следующими способами: * удаление всех обратных косых черт [\]; * удаление всех двойных кавычек ["]; * удаление всех одинарных кавычек [']; * удаление всех кареток [^]; * удаление пробелов перед косой чертой /; * удаление пробелов перед открывающей скобкой [(]; * замена всех запятых [,] и точки с запятой [;] на пробел; * замена всех нескольких пробелов (включая табуляцию, новую строку и т. д.) в один пробел; * преобразовать все символы в нижний регистр
t:hexDecode	Декодирует строку, закодированную с использованием замены каждого байта входной последовательности двумя шестнадцатеричными символами
t:none	Не фактическая функция преобразования, а инструкция ModSecurity. Удаляет все функции преобразования, связанные с текущим правилом
t:urlDecode	Декодирует входную строку в кодировке URL. Недопустимые кодировки (т. е. те, которые используют нешестнадцатеричные символы или те, которые находятся в конце строки и в которых отсутствует один или два байта) не преобразуются, но ошибка не возникает. Чтобы обнаружить недопустимые кодировки, сначала используйте оператор @validateUrlEncoding для входных данных. Функцию преобразования не следует использовать для переменных, которые уже были декодированы с помощью URL-адреса (например, параметров запроса), если только вы не намерены выполнять декодирование URL-адреса дважды!
t:urlDecodeUni	Подобно urlDecode, но с поддержкой кодировки %u, специфичной для Microsoft. Если код находится в диапазоне FF01–FF5E (полноширинные коды ASCII), то старший байт используется для обнаружения и корректировки младшего байта. В противном случае будет использоваться только младший байт, а старший байт обнуляется

22.2. Просмотр правила блокировки

Для того чтобы просмотреть правило Modsecurity, ставшее причиной блокировки транзакции, необходимо открыть детали транзакции, перейти на вкладку «Аномалии», найти аномалию от модуля ModsecurityAnalyzer и нажать на {…} для открытия дополнительной информации (см. рисунок 186).

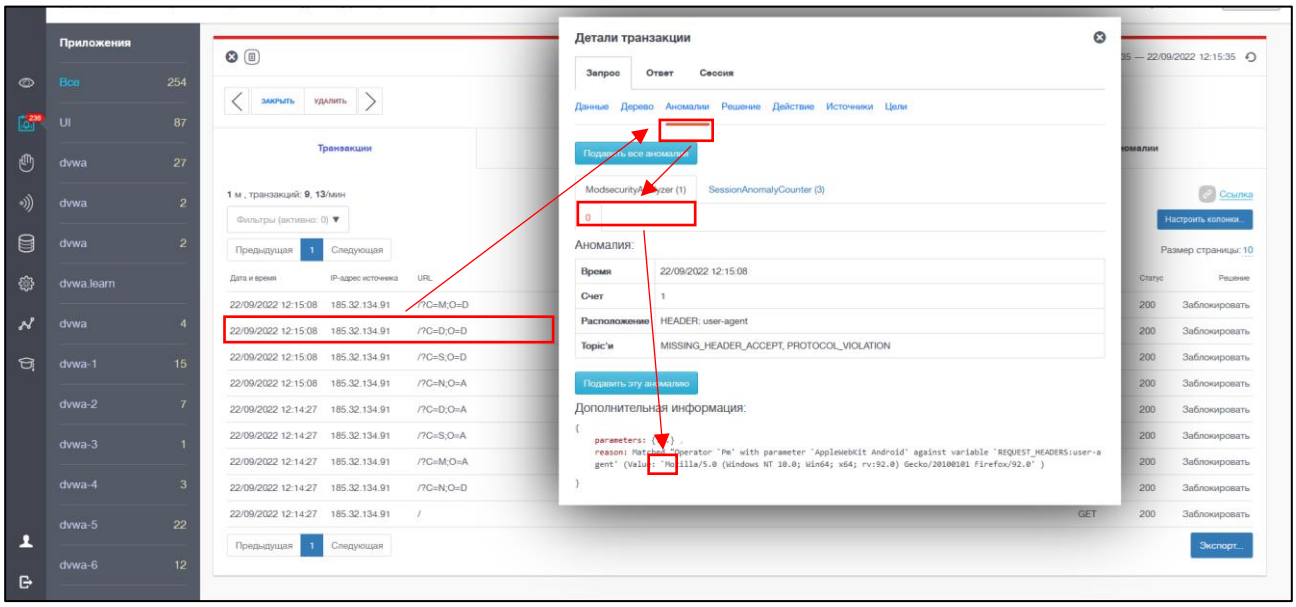

Рисунок 186 - Аномалия ModSecurity

В открывшемся блоке с дополнительной информацией будет поле «id» (см. рисунок 187), которое указывает на номер сигнатуры Modsecurity.

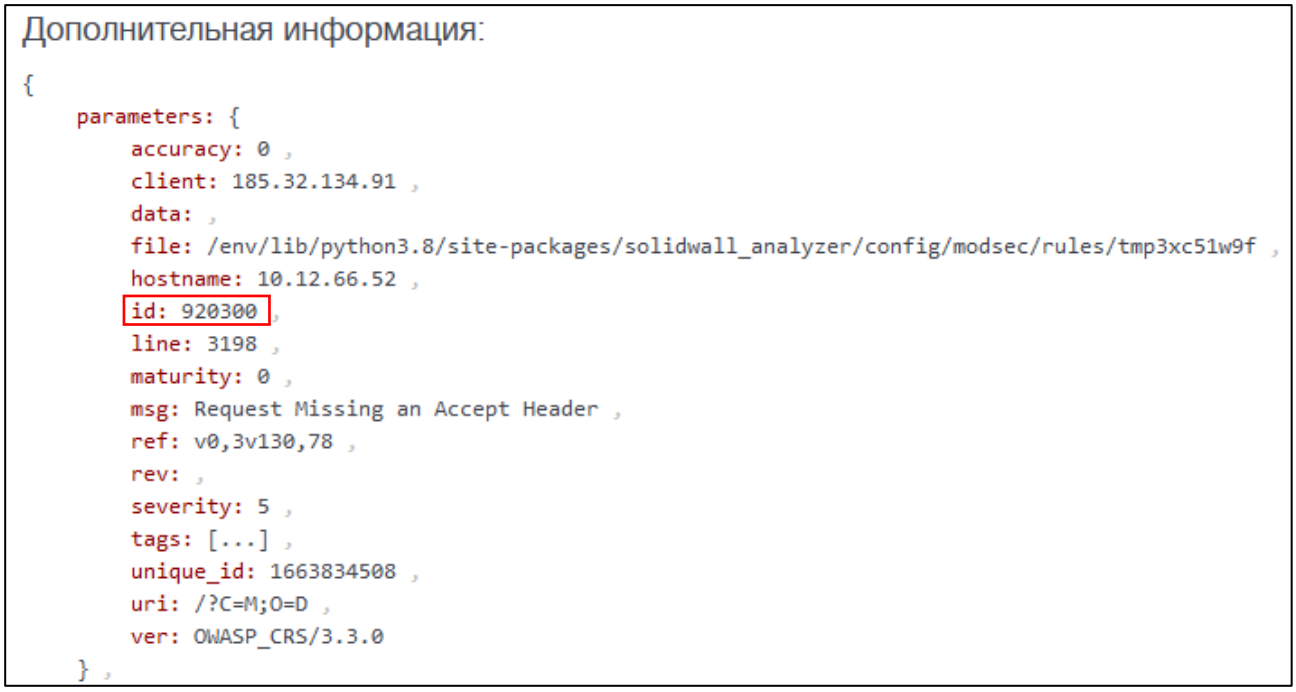

Рисунок 187 – Дополнительная информация

Чтобы найти правило по идентификатору нужно перейти на вкладку «Конфигурации модулей» окна «Настройки», где в сгруппированном виде находятся все сигнатуры ModSecurity. Для удобства поиска после названия группы в скобках указаны номера попадающих под них сигнатур, где «X» это любое число (см. рисунок 188).

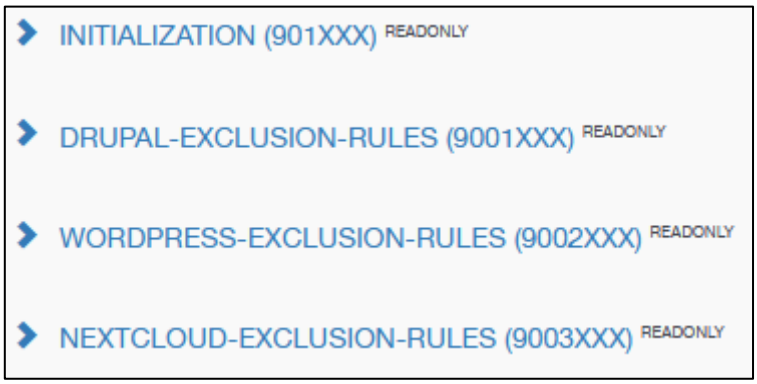

Рисунок 188 – Сгруппированные правила ModSecurity

В данном списке необходимо найти группу, в которую попадает наша сигнатура, раскрыть ее, щелкнув левой кнопкой мыши по названию, и найти интересующую нас сигнатуру по ее id (для удобства можно использовать поиск через «Ctrl+F»). Сигнатура из примера представлена на рисунке 189.

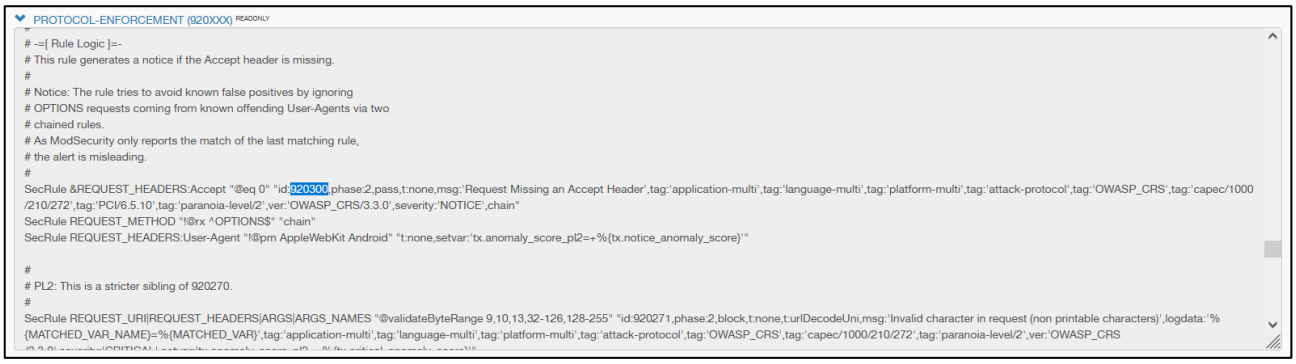

Рисунок 189 – Сигнатура ModSecurity

22.3. Выключение сигнатуры для всей инсталляции

На вкладке «Конфигурации модулей» окна «Настройки» необходимо открыть группу сигнатур «EXCLUSION-RULES-AFTER-CRS (999XXX)», пролистать ее в самый низ и добавить запись «SecRuleRemoveById ID», где ID это номер отключаемой сигнатуры (см. рисунок 190). После этого необходимо сохранить изменения, нажав на кнопку «Сохранить новую ревизию конфигурации» в самом верху данной вкладки.

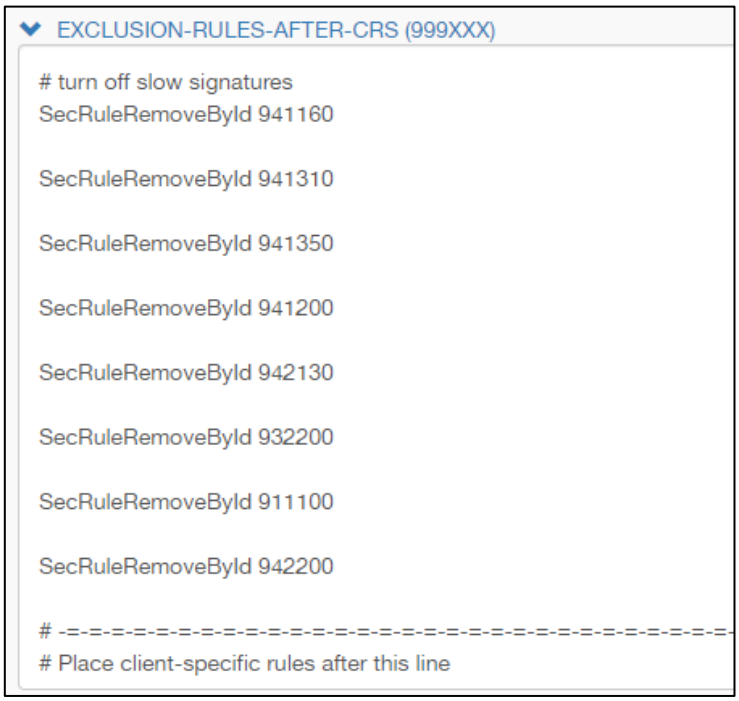

Рисунок 190 – Пример отключения сигнатур Modsecurity

22.4. Добавление сигнатуры для всей инсталляции

На вкладке «Конфигурации модулей» окна «Настройки» необходимо открыть группу сигнатур «EXCLUSION-RULES-AFTER-CRS (999XXX)», пролистать её в самый низ и добавить сигнатуру в соответствии с синтаксисом Modsecurity (см. рисунок 191). После этого необходимо сохранить изменения, нажав на кнопку «Сохранить новую ревизию конфигурации» в самом верху данной вкладки.

Рисунок 191 – Пример добавленной сигнатуры для поиска попытки эксплуатации Log4j

22.5. Откат к предыдущей ревизии

Для того чтобы откатиться к предыдущей ревизии Modsecurity необходимо перейти на вкладку «Конфигурации модулей» окна «Настройки» (см. рисунок 192).

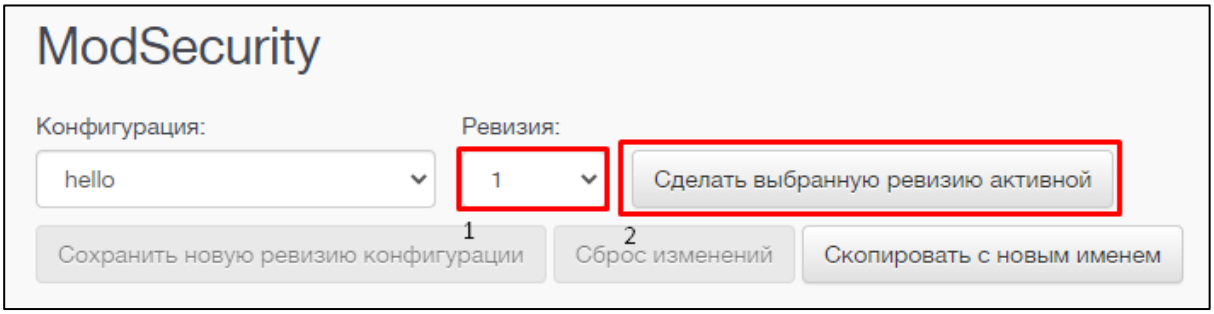

Рисунок 192 – Откат к предыдущей версии ревизии

В области 1, отмеченной на рисунке 192, необходимо выбрать номер интересующей нас ревизии и нажать на кнопку «Сделать выбранную ревизию активной» (область 2).

23. Подавление аномалий

Для подавления аномалий необходимо перейти в раздел «Настройки» -> «Подавление аномалий».

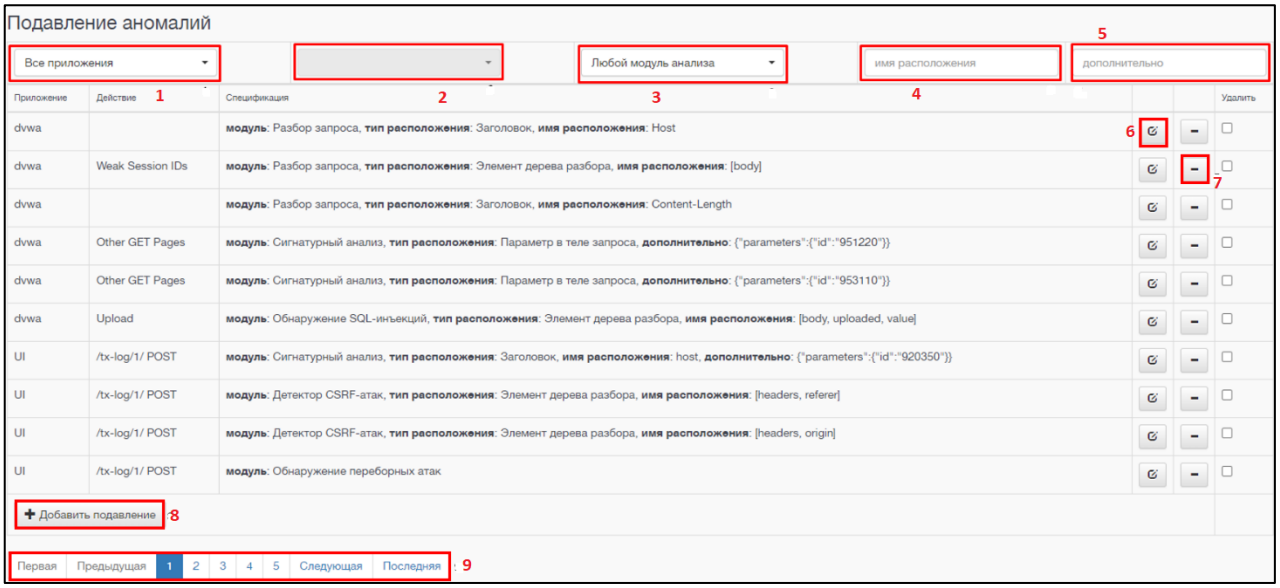

Рисунок 193 – Вкладка "Подавления аномалии"

В данном разделе можно анализировать подавленные аномалии на инсталляции, а также фильтровать их по следующим параметрам:

1. По приложению.
2. По действию (становится активным только после выбора целевого приложения).
3. По модулю анализа.
4. По имени расположения.
5. По значению дополнительных данных, записанных в базу в случае сработки Modsecurity, или введённых при подавлении аномалии в поле пункта «Дополнительные параметры».

Также в данном меню можно:

6. Изменять уже подавленные аномалии, нажав на кнопку редактирования справа.
7. Удалять подавления аномалий, нажав на кнопку удаления. В данном случае присутствует возможность выбора нескольких аномалий для группового удаления.
8. Создать новое подавление, нажав на кнопку добавления подавления и выбрав соответствующие параметры для подавления.
9. Также есть возможность перехода по страницам с подавленными аномалиями в нужном направлении.

Подробнее о кнопках управления можно прочитать в разделе 23.

При нажатии на кнопки, помеченные 6 и 8, открывается окно «Подавление» (см. рисунок 194), в котором можно настроить подавление аномалий.

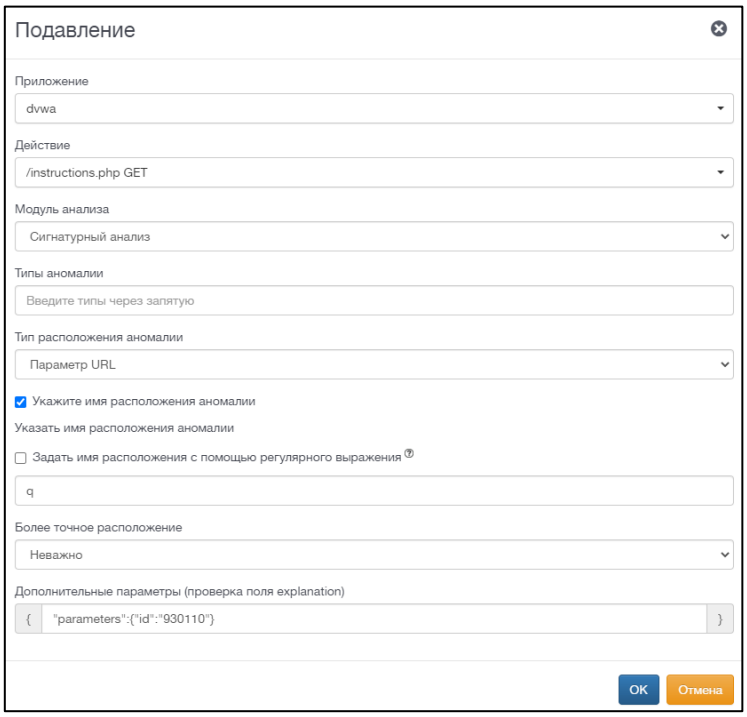

Рисунок 194 – Окно «Подавление»

Данное окно также можно увидеть при нажатии на кнопку «Подавления аномалии» в окне «Детали транзакции» на вкладке «Аномалии» (см. рисунок 194).

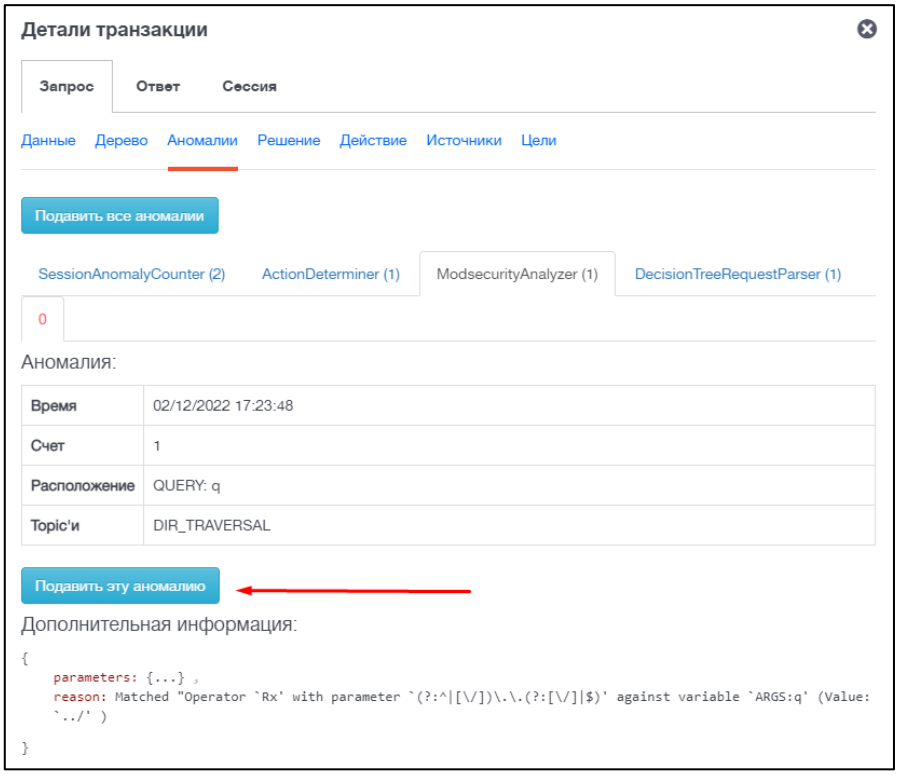

Рисунок 195 – Окно «Детали транзакции» вкладка «Аномалии»

На данном окне имеются следующие поля, представленные в таблице 37.

Таблица 37 – Поля окна «Подавление аномалий»

Поле	Описание
Приложение	Выбор приложения на WAF, для которого нужно подавить сработку
Действие	Выбор действия на WAF, для которого нужно подавить сработку
Модуль анализа	Выбор модуля анализа, сработки для которого нужно подавить
Типы аномалии	Указание группы сработок (тегов), для которой нужно применить подавление
Тип расположения аномалии	Указание более точного пути, для которого нужно применить подавление аномалии
Укажите имя расположения аномалии	Чекбокс, отвечающий за включение анализа указанного ниже имени расположения аномалии, или более точного пути, по которому находится аномалия. Возможные варианты типов расположения с их описанием даны в таблице 38
Задать имя расположения с помощью регулярного выражения	Чекбокс, отвечающий за включение анализа имени расположения аномалии как регулярного выражения. Регулярное выражение не должно содержать группы (обозначаемые круглыми скобками) и должно описывать имя расположения целиком, а не только его часть
Более точное расположение	Параметр, отвечающий за выбор, где именно по указанному выше пути находится аномалия: в значении заголовка или же – только в его названии
Дополнительные параметры (проверка поля explanation)	Структура в JSON, в которую при необходимости может быть записана какая-то важная информация. При сработке сигнатурного анализатора Modsecurity там указывается идентификатор сработавшей аномалии

Стандартные типы аномалий:

- PROTOCOL_VIOLATION;
- PROTOCOL_VIOLATION;
- XSS;
- PHP_INJECTION;
- SQL_INJECTION;
- FILE_INJECTION;
- COMMAND_INJECTION;
- DIR_TRAVERSAL;
- SESSION_FIXATION;
- RFI;
- ERRORS_IIS;
- ERRORS_PHP;

- ERRORS_SQL;
- ERRORS_JAVA;
- INFO_DIRECTORY_LISTING;
- SOURCE_CODE_JAVA;
- SOURCE_CODE_PHP;
- ENCODING_NOT_ALLOWED;
- PROTOCOL_NOT_ALLOWED;
- INVALID_HREQ;
- HEADER_RESTRICTED;
- MISSING_HEADER_HOST;
- METHOD_NOT_ALLOWED;
- REQUEST_SMUGGLING;
- EXT_RESTRICTED;
- SIZE_LIMIT;
- IP_HOST;
- CRAWLER;
- SCRIPTING;
- EVASION;
- SECURITY_SCANNER.

Возможные варианты типов расположения аномалий с описанием представлены в таблице 38.

Таблица 38 – Расположение аномалий

Тип расположения	Описание
Не проверять	Не проверять расположение аномалии
HTTP-сообщение в целом	Аномалия может быть в любом месте сообщения
Первая строка HTTP-сообщения в целом	Аномалия может быть в первой строке сообщения
Заголовок	Аномалия может быть в заголовке
Тело в целом	Аномалия может быть во всем теле до декомпрессии и распаковки
Параметр в теле запроса	Аномалия может быть во всем неразобранном теле после декомпрессии и распаковки
URL в целом	Аномалия может быть где-то в URL без привязки к конкретному параметру
Параметр URL	Аномалия может быть где-то в части запроса URL, но не в каком-то конкретном параметре
Cookie	Аномалия может быть в файле cookie с именем, указанным идентификатором, если таковой указан
Элемент дерева разбора	Указание пути до конкретного целевого параметра с аномалией

Тип расположения	Описание
Сессионные данные	Указание сессионных данных для подавления (обычно не используется)
Источник	Указание определённого источника для подавления (обычно не используется)
Цель/Объект веб-приложения	Указание определённой цели для подавления (обычно не используется)

23.1. Подавление ложноположительных срабатываний

Ложноположительное срабатывание (False positive) - это срабатывание WAF на запрос, который является легитимным, однако WAF обнаружил в нем признаки атаки.

В таблице 39 представлены модули анализатора, от которых могут возникать аномалии, и их описание.

Таблица 39 – Модули анализатора

Модуль	Описание
Сигнатурный анализ	Данный модуль генерирует аномалии от встроенных сигнатур ModSecurity
Обнаружение инъекций	Данный модуль генерирует аномалии от встроенного модуля Libinjection
Проверка синтаксиса параметров действий	Аномалии от данного модуля возникают, если значение параметра действия не соответствует его модели или обязательный параметр действия не был передан
Выделение действий	Аномалия от данного модуля возникает, если данный запрос не описан в бизнес-действиях
Обнаружение открытого перенаправления	Аномалия от данного модуля возникает, если домен в заголовке «Host» запроса не соответствует домену в заголовках «Location», или «Refresh» в ответе
Протокольная валидация	Аномалии от данного модуля возникают, если запрос не соответствует протоколу
Разбор запроса	Аномалии возникают, если в процессе применения дерева разбора к данному запросу возникли ошибки
Разбор ответа	Аномалии возникают, если в процессе применения дерева разбора к данному ответу возникли ошибки
Детектор CSRF-атак	Аномалии возникают, если в запросе отсутствует заголовок «Referer», или «Origin», а также если значение заголовка «Referer» не совпадает со значением в заголовке «Host»
Обнаружение переборных атак	Аномалии возникают, когда запрос попадает под условия переборных атак. Например, с одного IP было отправлено больше запросов, чем положено
Упрощенное/легковесное отслеживание сессий	Аномалия возникает, если пользователь пытается использовать неизвестный системе, т.е. не выданный ранее самим приложением

Модуль	Описание
	идентификатор сессии (сессионный атрибут), а также, если в запросе отсутствует необходимый согласно модели сессионный атрибут
Обнаружение аномалий в последовательности действий	Аномалии возникают, если поведение пользователя не совпадает с настроенной цепочкой действий
Интеграция с сигнатурным анализом на ICAP-сервере	Аномалия возникает, если в POST-запросе или мультипарт-ответе вызвали срабатывание антивируса на ICAP-сервере
Модуль обратного прокси	Аномалии возникают при множественном значении IP адреса в заголовках. Например, если задублирован заголовок X-Forwarded-For
Внутренняя ошибка анализатора	Аномалия возникает при неработоспособности одного из модулей, участвующих в анализе
Обнаружение ботов по временным характеристикам трафика	Аномалия возникает при отклонении на заданное значение от высчитанной медианы задержек

23.2. Общий вид аномалии

Вывод аномалий на WAF стандартизирован, несмотря на наличие множества модулей. В данном разделе будет рассмотрена вкладка «Аномалии» с точки зрения анализа сработки. Подробнее о функциональных особенностях данной вкладки можно прочитать в разделе 23.

Пример аномалии показан на рисунке 196.

Рисунок 196 – Пример аномалии

1. В выделенной области находятся модули, аномалии от которых присутствуют в выбранной транзакции. Цифра в круглых скобках говорит о количестве аномалий от модуля для выбранной транзакции.
2. В выделенной области находятся вкладки с аномалиями от выбранного в области 1 модуля. Аномалий может быть несколько, нумерация начинается с 0.
3. В данной области находятся общие сведения об аномалии, такие как:

   3.1. Время – показывает время, в которое аномалия сработала на данную транзакцию (ввиду того, что анализ транзакции происходит за сотые секунды, время, в которое аномалия сработала, совпадает с временем получения транзакции WAF).

   3.2. Счет – показывает значение отличное от 1, в случае наличия двух одинаковых аномалий от одного модуля.

   3.3. Расположение – в общем виде показывает расположение аномалии. В зависимости от модуля может выдавать как путь в дереве разбора, так и ссылку на верхнеуровневую модель запроса.

   3.4. Topic'и – показывают общие теги аномалий. Используются в правилах для более точечной настройки агрегации транзакций.

4. В области с дополнительной информацией находятся общие сведения о причине возникновения выбранной аномалии. Для того, чтобы подробнее ознакомиться с причиной возникновения аномалии, необходимо нажать на символы «{…}».

23.3. Особенности подавления аномалий от модулей

Если выявленная аномалия является ложноположительным срабатыванием, то в зависимости от того, к какому типу модуля относится детектор, обнаруживший данную аномалию, выполняется подавление ложного срабатывания или корректировка модели:

1. Сигнатурный анализ.

У данного модуля есть сразу несколько особенностей при подавлении аномалий:

- ввиду того, что данный модуль самостоятельно разбирает запросы, при его подавлении могут использоваться регулярные выражения на путь;
- подавление отдельно взятых сигнатур данного модуля происходит через «Дополнительные параметры» в окне «Подавление» (если оставить поле «Дополнительные параметры» пустым, модуль будет подавлен полностью).

   1.1. Аномалии в Cookie.

При работе с аномалиями от сигнатурного детектора часто встречаются аномалии в cookie (см. рисунок 197). Такие аномалии корректнее подавлять на всё приложение. В некоторых случаях можно подавить не конкретную сигнатуру, а модуль целиком.

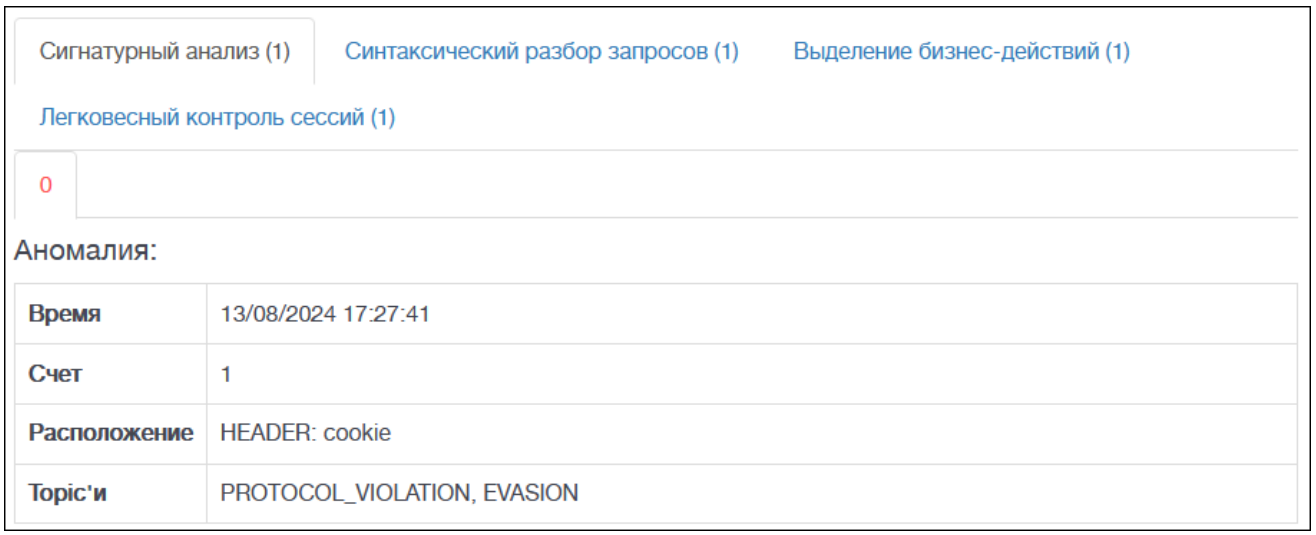

Рисунок 197 – Аномалия в Cookie

1.2. Аномалии в стандартных для приложения\браузера заголовках.

Подавление аномалий в стандартных заголовках запросов (см. рисунок 198), которые могут появиться в транзакциях к любому действию приложения, следует производить на приложение в целом.

Рисунок 198 – Аномалия на заголовок «sec-ch-ua»

1.3. Аномалия открытого перенаправления.

Среди правил реагирования данного детектора имеется сигнатура с номером 931130, которая работает на поиск открытого перенаправления (см. рисунок 199). Несмотря на то, что для детектирования такого рода аномалий есть отдельный модуль, данная сигнатура не выключается ввиду того, что она работает в запросе, в отличие от модуля «Обнаружение открытого перенаправления», который работает на ответ.

При работе с сигнатурой присутствует дополнительное ограничение: отсутствие возможности добавления исключений, поэтому данную аномалию так же часто подавляют на всё приложение.

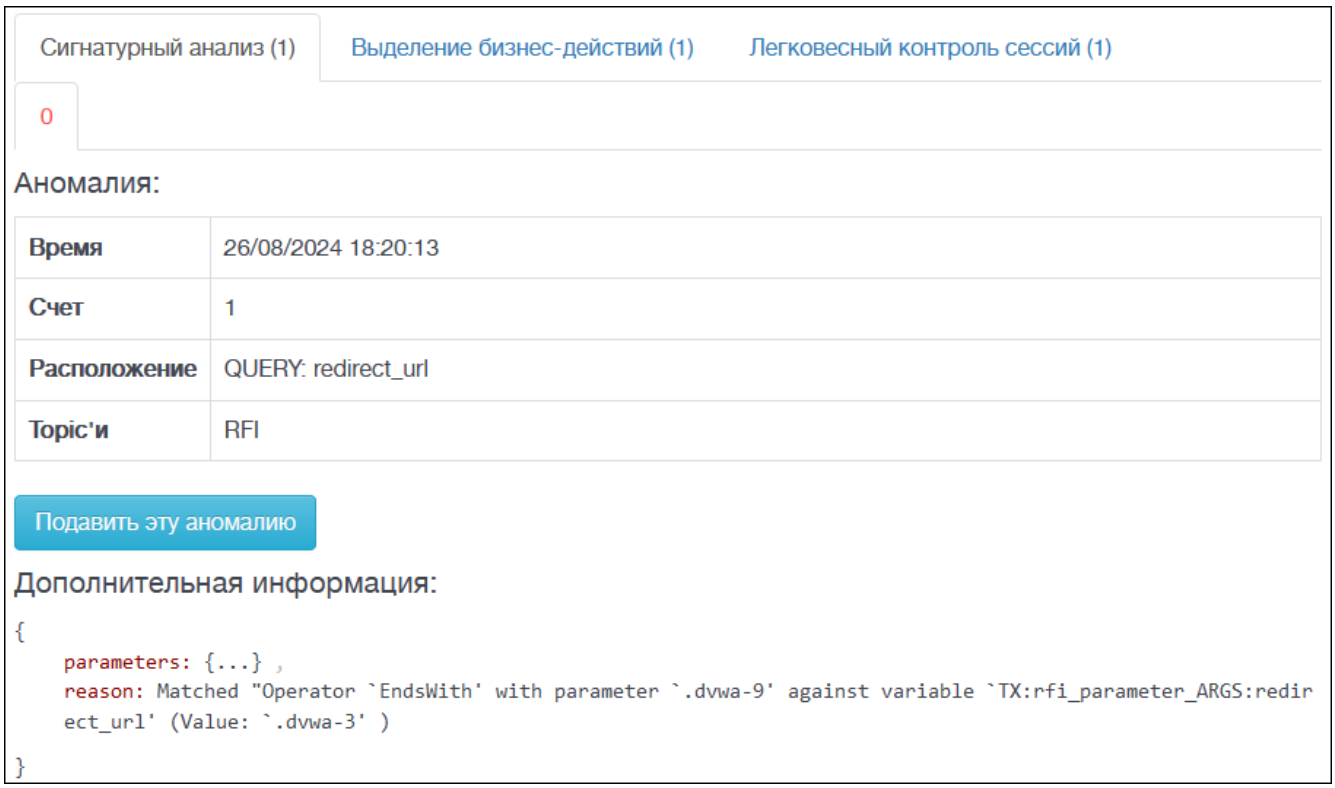

Рисунок 199 – Аномалия открытого перенаправления

1.4. Аномалия на обращение к приложению по IP

Периодически встречаются аномалии на обращение к приложению по IP (см. рисунок 200). В зависимости от приложения, это может быть как нормальным поведением, так и легитимной блокировкой нестандартного трафика. В случае если обращение по IP является нормой для ресурса – данную аномалию необходимо подавить на всё приложение.

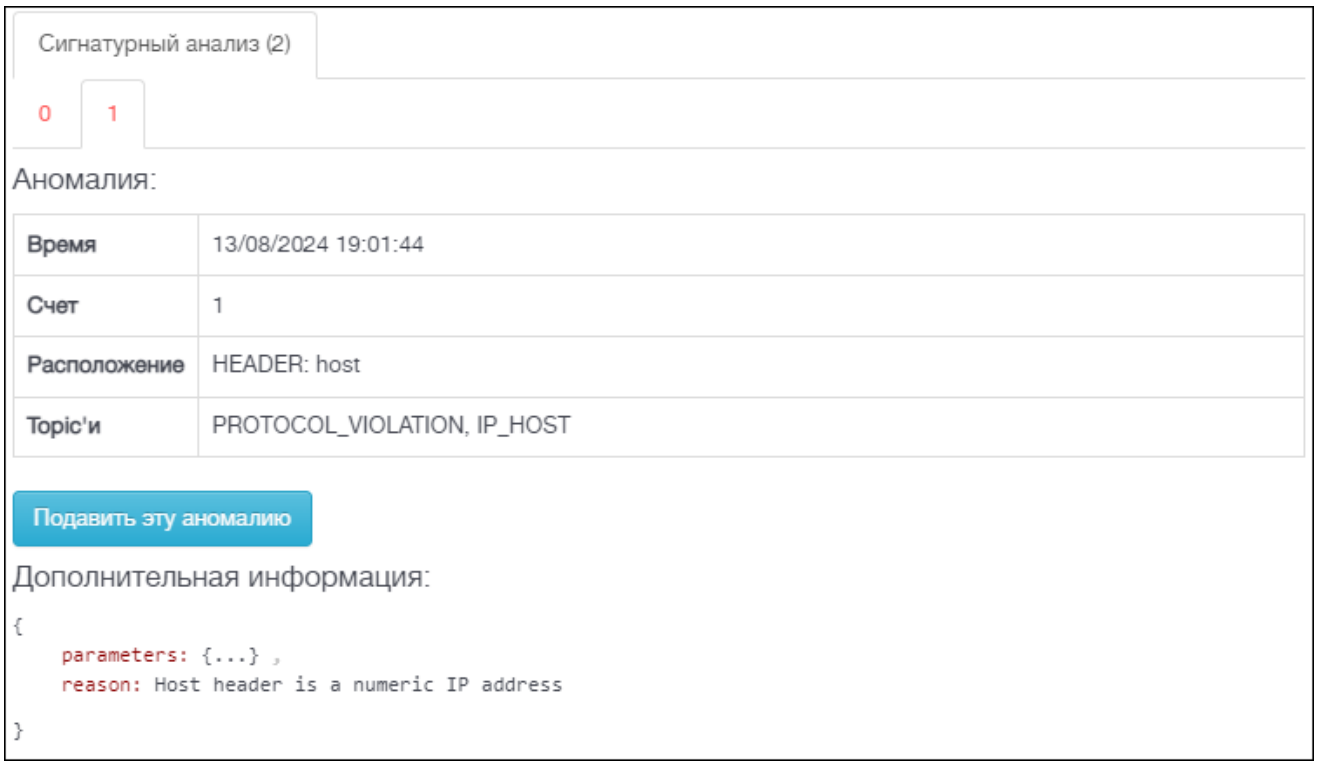

Рисунок 200 – Аномалия на IP адрес в заголовке «Host»

1.5. Аномалия на пароль пользователя

В запросах на авторизацию и\или смену пароля часто встречаются ложно-позитивные сработки от сигнатурного детектора на поле, в котором передается пароль. В таком случае следует анализировать возможность атаки через данное поле. В зависимости от результатов анализа, можно подавить как частную сигнатуру, так и весь модуль целиком. В случае с паролем корректнее будет сделать модель параметра действия, в котором передается пароль.

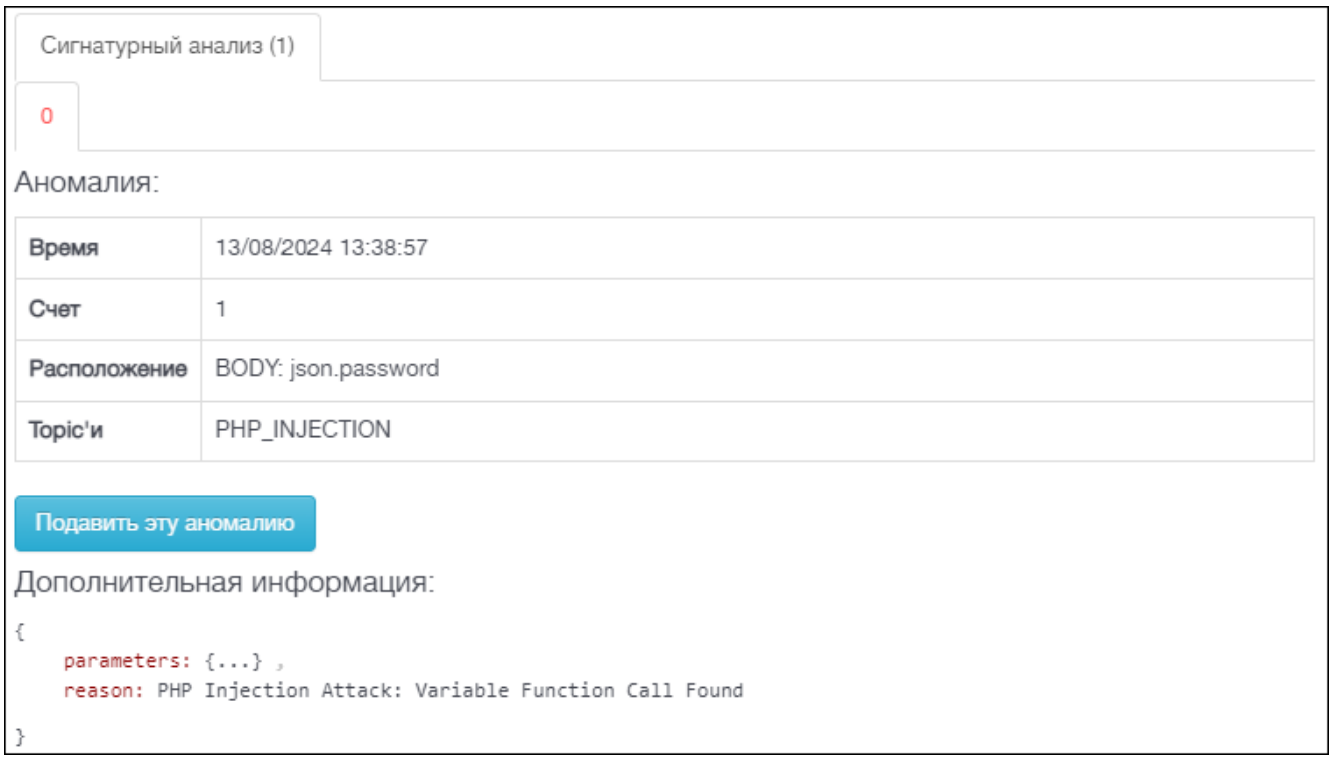

Рисунок 201 – Аномалия на пароль пользователя

1.6. Аномалия на некорректное составление запроса

Часто при обращении к веб-приложению встречаются запросы, не соответствующие нормальной модели. Например, в случае с GET запросами, могут встречаться транзакции с заголовком «content-type» и\или «transfer-encoding», что считается некорректным (см. рисунок 202). В случае малого количества подобных транзакций, это может говорить о попытке использования средств автоматизации при формировании запросов, и в таком случае данную аномалию подавлять не стоит. В случае защиты API – данное поведение считается нормальным, следует подавить данные сработки на всё приложение.

Зеркальные примеры такого поведения встречаются с POST-запросами. Заголовок «content-type» и\или «transfer-encoding» могут отсутствовать. В данном случае следует анализировать поведение приложения, но запросы, в которых отсутствует заголовок «content-type», крайне редко являются легитимными.

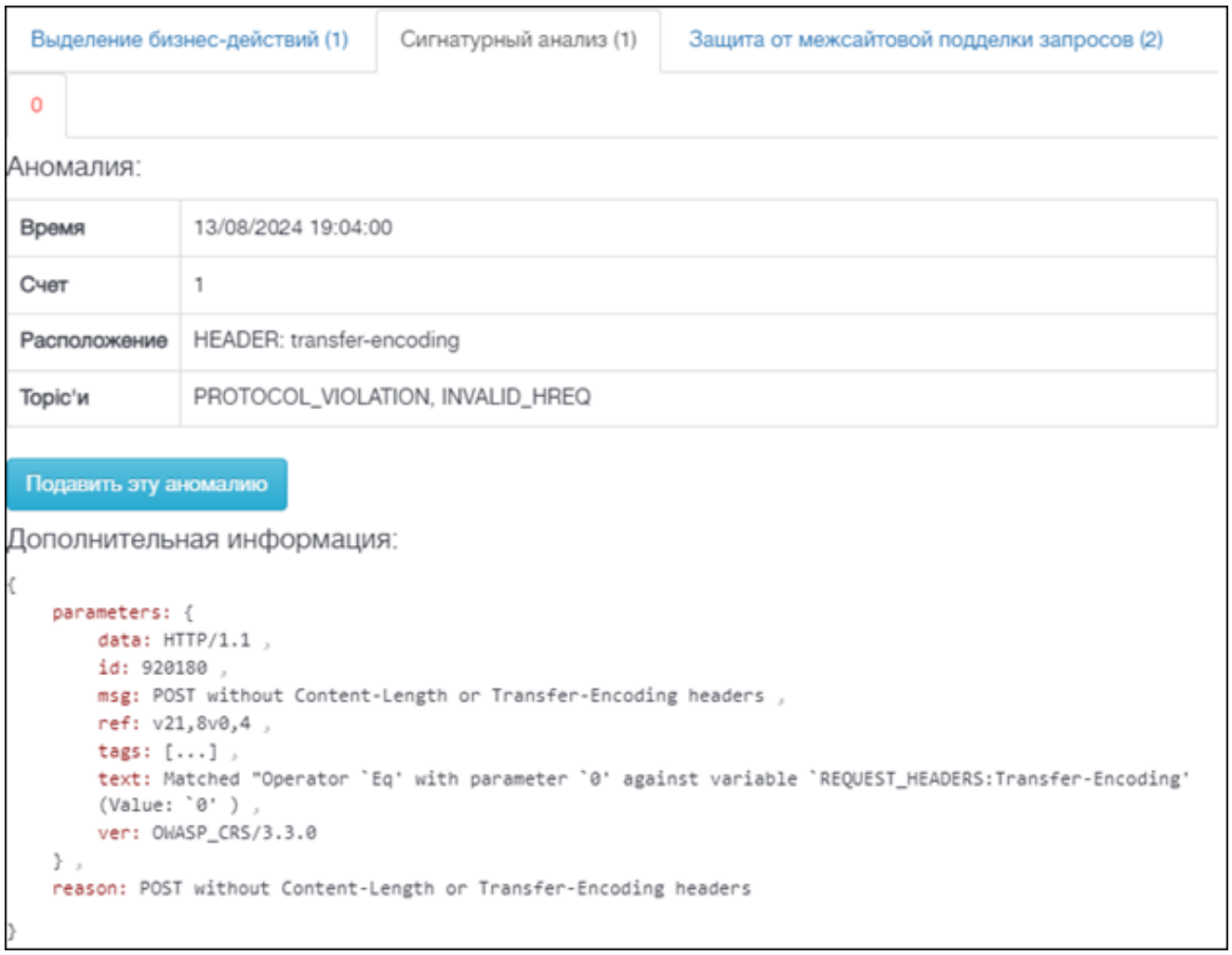

Рисунок 202 – Заголовок «transfer-encoding» в GET запросе

2. Обнаружение инъекций

Подавление аномалий данного модуля обладает следующими особенностями:

- при подавлении аномалий происходит подавление всего модуля;
- при подавлении аномалий не работают регулярные выражения на путь.

Пример аномалии показан на рисунке 203.

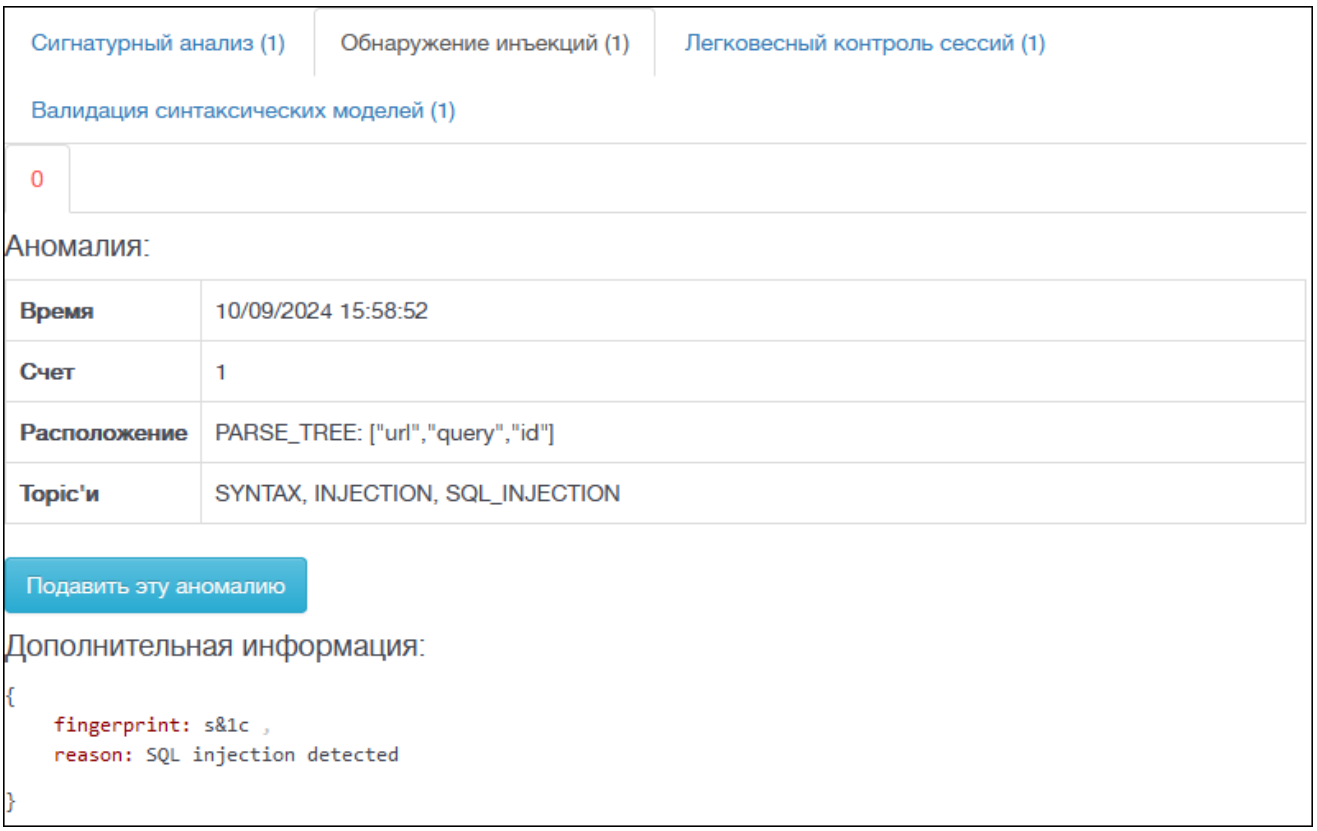

Рисунок 203 – Аномалия от модуля «Обнаружение инъекций»

3. Проверка синтаксиса параметров действий

Аномалии от данного модуля не следует продавлять, лучше отредактировать модель действия, в котором возникла данная аномалия.

Пример аномалии показан на рисунке 204.

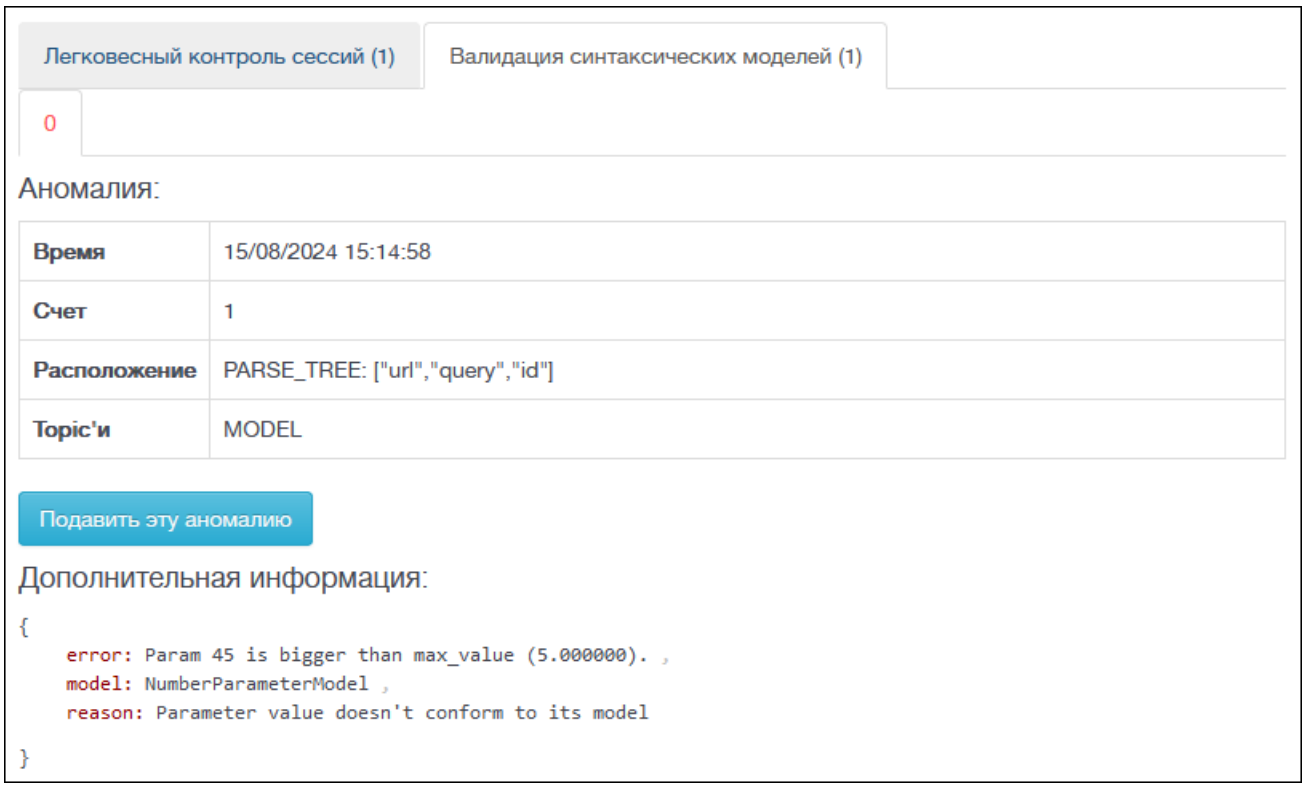

Рисунок 204 – Аномалия модуля «Валидация синтаксической модели»

В данном случае аномалия возникает на параметр, который находится по пути «url -> query -> id». Как видно из описания аномалии, по данному пути находится параметр со значением «45», что больше максимально разрешенного «5».

Для того, чтобы корректно обработать данную аномалию, необходимо выполнить следующие шаги.

3.1. Перейти на вкладку «Действие» данной транзакции и запомнить, или скопировать название действия, которым матчится (сопоставляется) данная транзакция (см. рисунок 205).

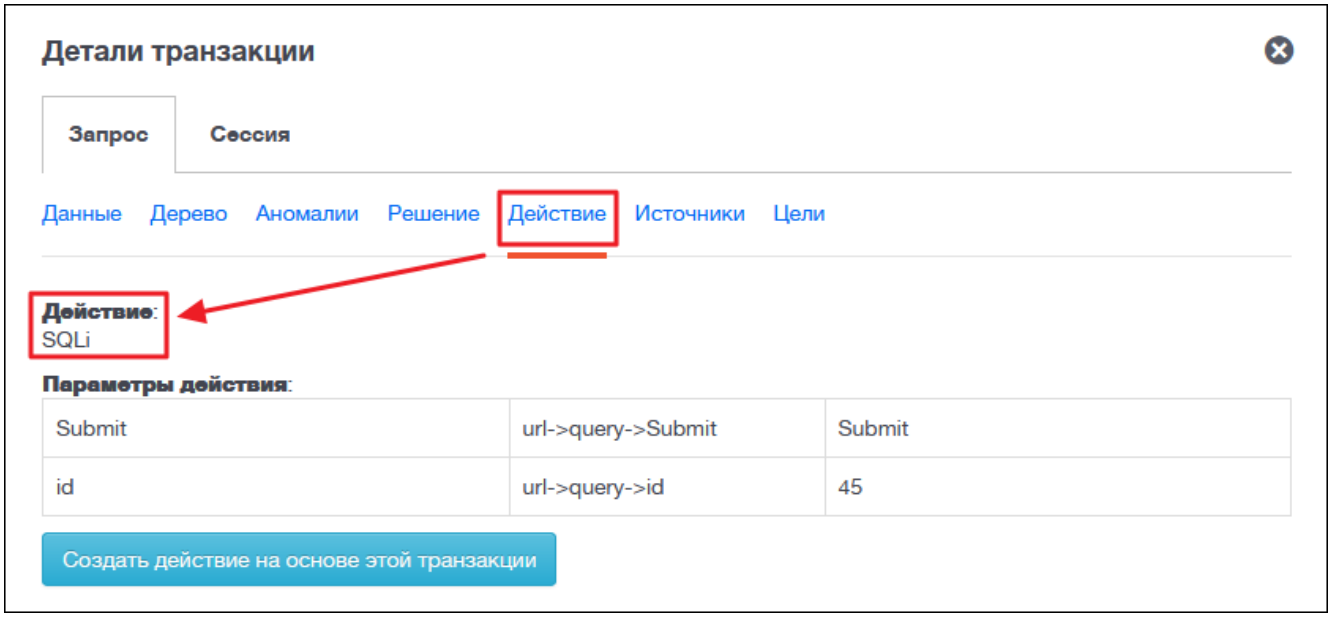

Рисунок 205 – Вкладка «Действие»

3.2. Закрыть просмотр транзакции, перейти в раздел «Действия», найти соответствующее действие и нажать на иконку редактирование модели действия (см. рисунок 206).

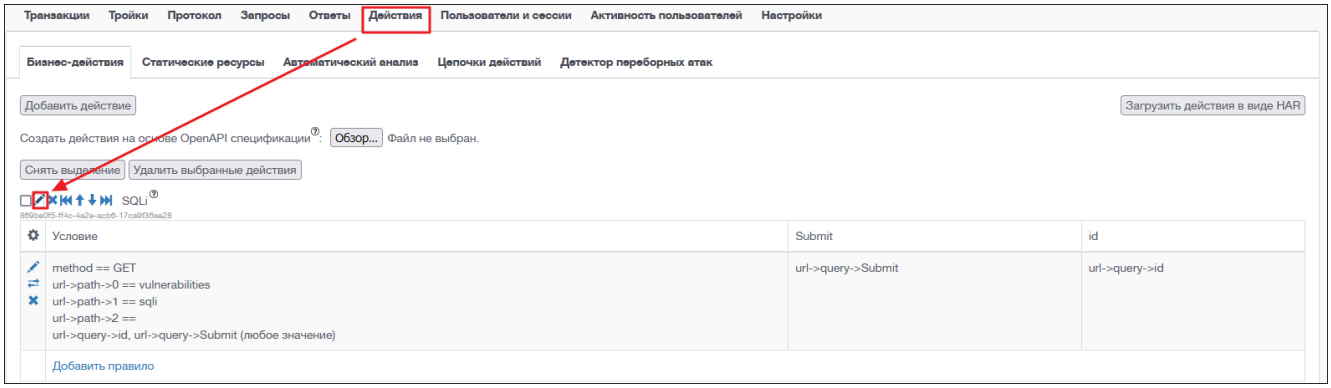

Рисунок 206 – Редактирование действия

3.3. В появившемся диалоговом окне отредактировать соответствующую модель параметра (см. рисунок 207).

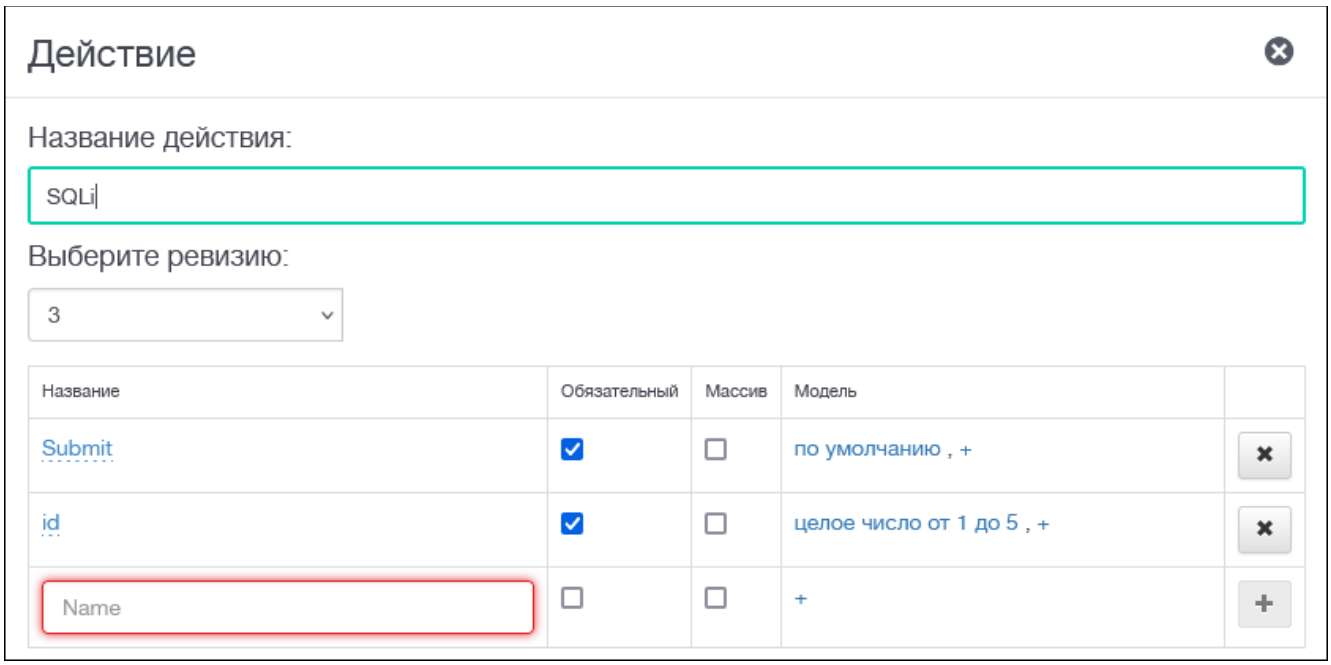

Рисунок 207 – Модель параметра действия

4. Выделение бизнес-действий

Аномалии от данного модуля подавлять нежелательно. Возникновение в транзакции данной аномалии говорит о том, что данная транзакция не матчится с действием в разрезе WAF (не создано или не попадает под условие уже созданных действий). Для того чтобы данная аномалия пропала из транзакции, необходимо создать действие, соответствующее данной транзакции (подробнее о создании действий описано в разделе 15). В крайне редких случаях, если события по правилу «Неизвестное действие» сильно переполняет базу, продуктивнее будет отключить данное правило, чем подавлять аномалию от данного модуля.

Примечание: данное правило также используется для противодействия dirbusting (перебора каталога и файлов). После полного описания всех возможных действий на приложении, данное правило включается в блокировку и режет весь трафик к неизвестным URL.

Пример аномалии показан на рисунке 208.

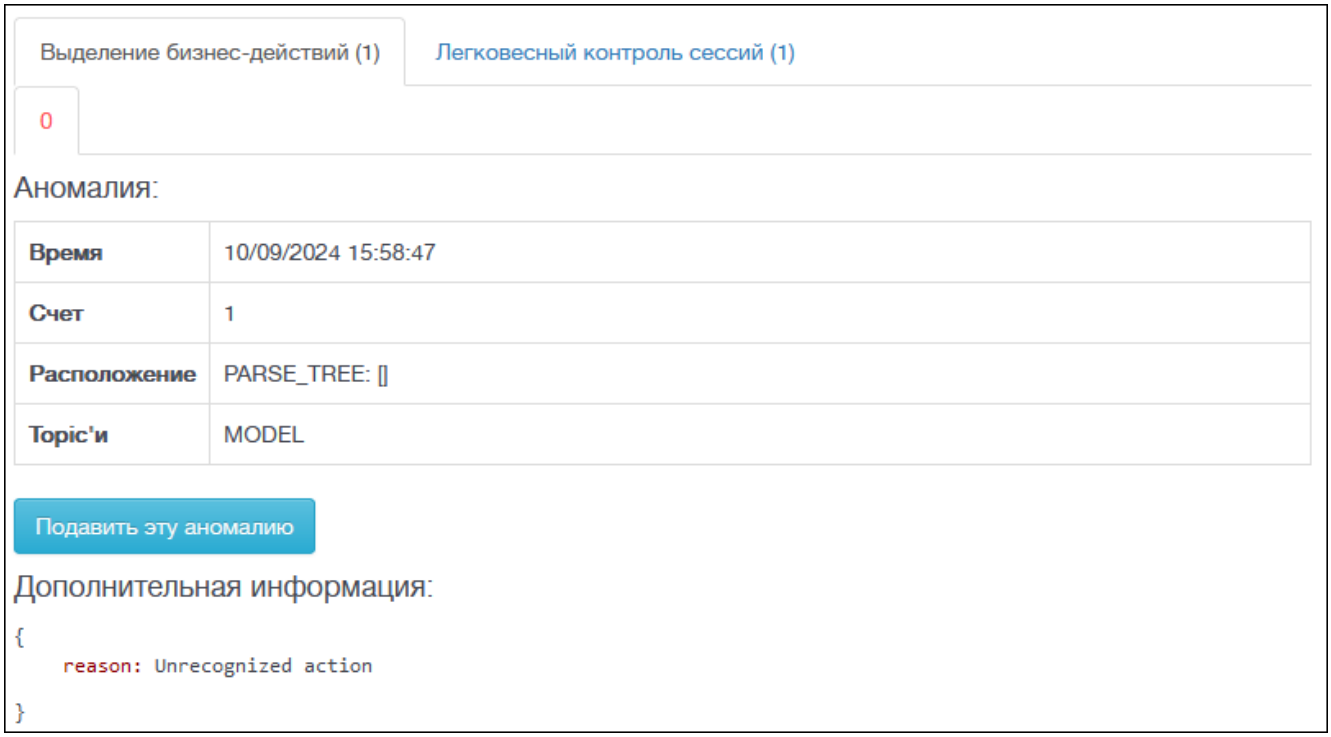

Рисунок 208 – Аномалия модуля «Выделение бизнес-действий»

Особенностью данной аномалии является то, что это одна из немногих аномалий, которая срабатывает на транзакцию целиком, о чём свидетельствует отсутствие конкретного расположения аномалии.

5. Обнаружение открытого перенаправления

Подавление аномалий от данного модуля обладает следующими особенностями:

- аномалия возникает не в запросе, а в ответе;
- данные аномалии лучше не подавлять, а редактировать разрешённые домены в настройках приложения (подробнее см. в разделе 19). Подавление данной аномалии приведёт к отключению модуля в разрезе выбранных параметров (приложения и\или действия).

Пример аномалии показан на рисунке 209.

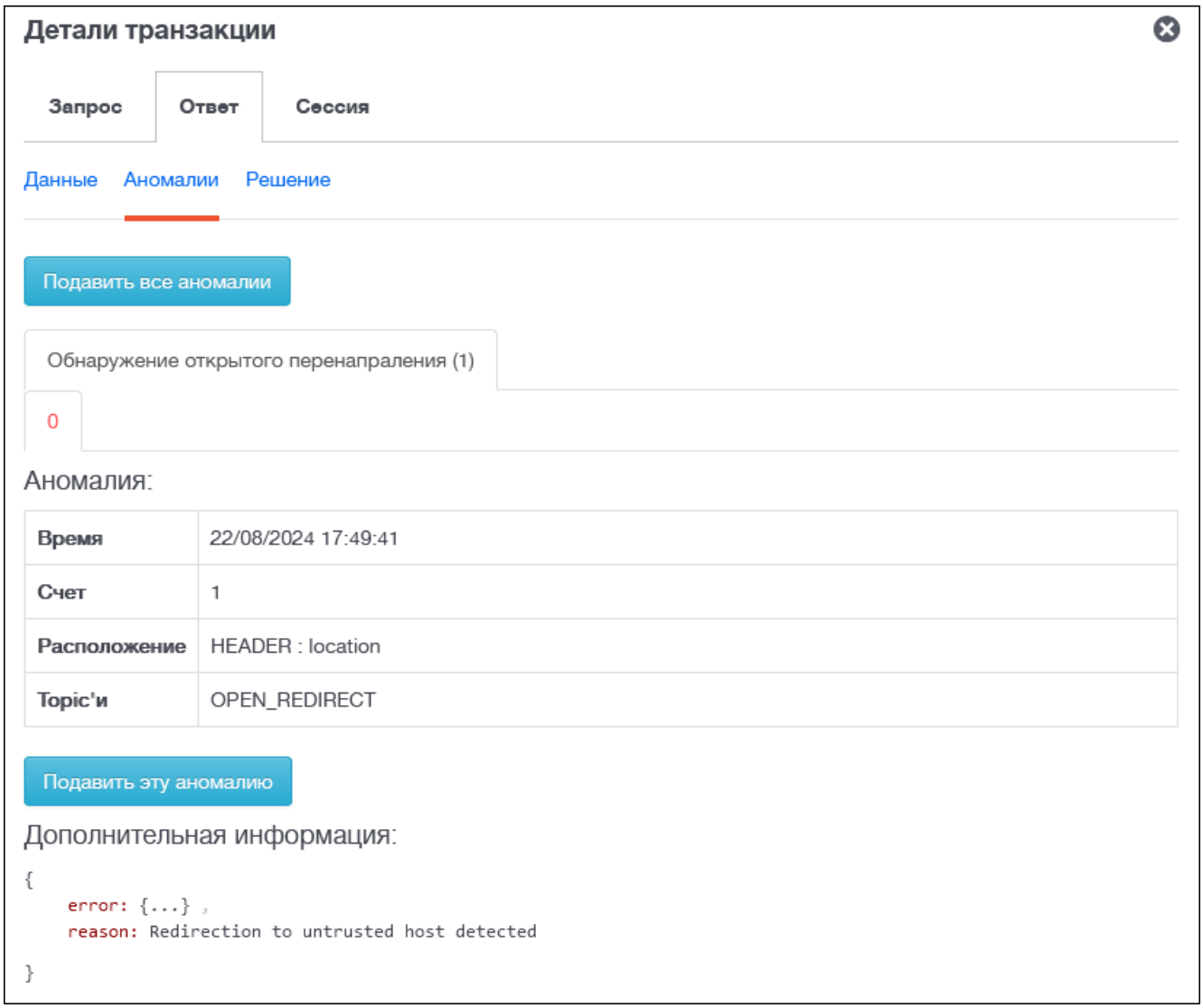

Рисунок 209 - Аномалия от модуля «Обнаружение открытого перенаправления»

Как уже было сказано выше, аномалии от модуля «Обнаружение открытого перенаправления» следует искать не в запросе, а ответе. О наличии такой аномалии говорит в первую очередь решение «Переписать», так же такого рода транзакции помечаются не красным, а жёлтым цветом. Стоит так же отметить, что транзакции с решением «Переписать» доходят до бекэнда, в них блокируется не запрос, а именно ответ от сервера.

6. Протокольная валидация

Аномалии от данного модуля подавлять нежелательно, корректнее изменить настройки протокольной валидации в разрезе данного приложения (подробнее см. в разделе 9). Подавление данного модуля приведет к отключению его части в разрезе выбранных параметров (приложения и\или действия).

6.1. Несоответствие названий заголовков регулярному выражению (HEADER_INVALID_CHARACTER).

Аномалия возникает при наличии в транзакции заголовка или параметра с наименованием, не соответствующим регулярному выражению, заданному в протоколе (см. рисунок 210).

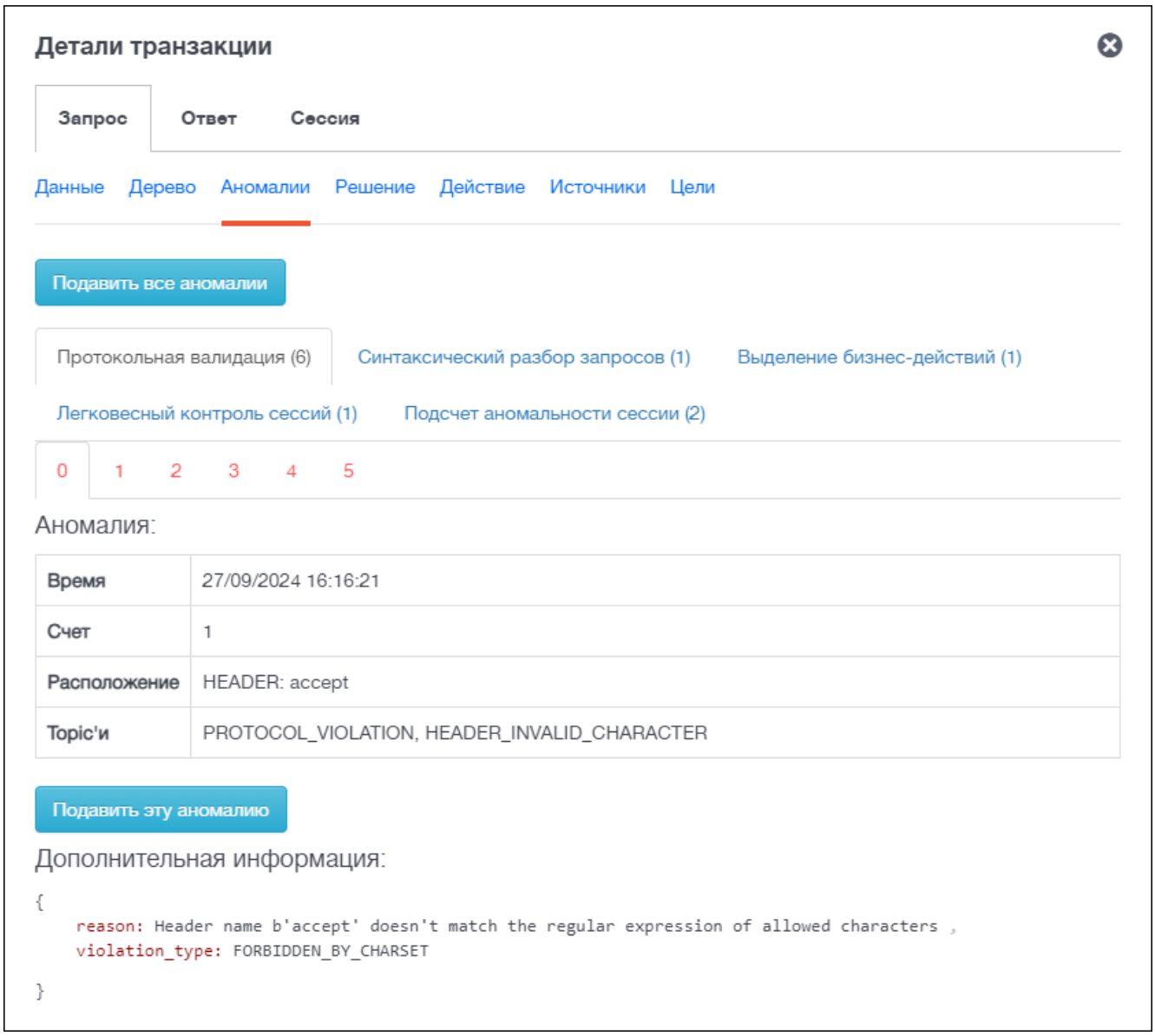

Рисунок 210 – Аномалия имени заголовка

Чтобы данная аномалия больше не возникала, необходимо внести изменение в «Регулярное выражение заголовка» на вкладке «Приложение» – «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.2. Аномалия запрещенного MIME-типа (FORBIDDEN_MEDIA_TYPE).

Аномалия возникает при наличии в параметре content-type MIME-типа, не прописанный в протоколе. MIME-типы определены в соответствии со спецификацией RFC 6838 (см. рисунок 211).

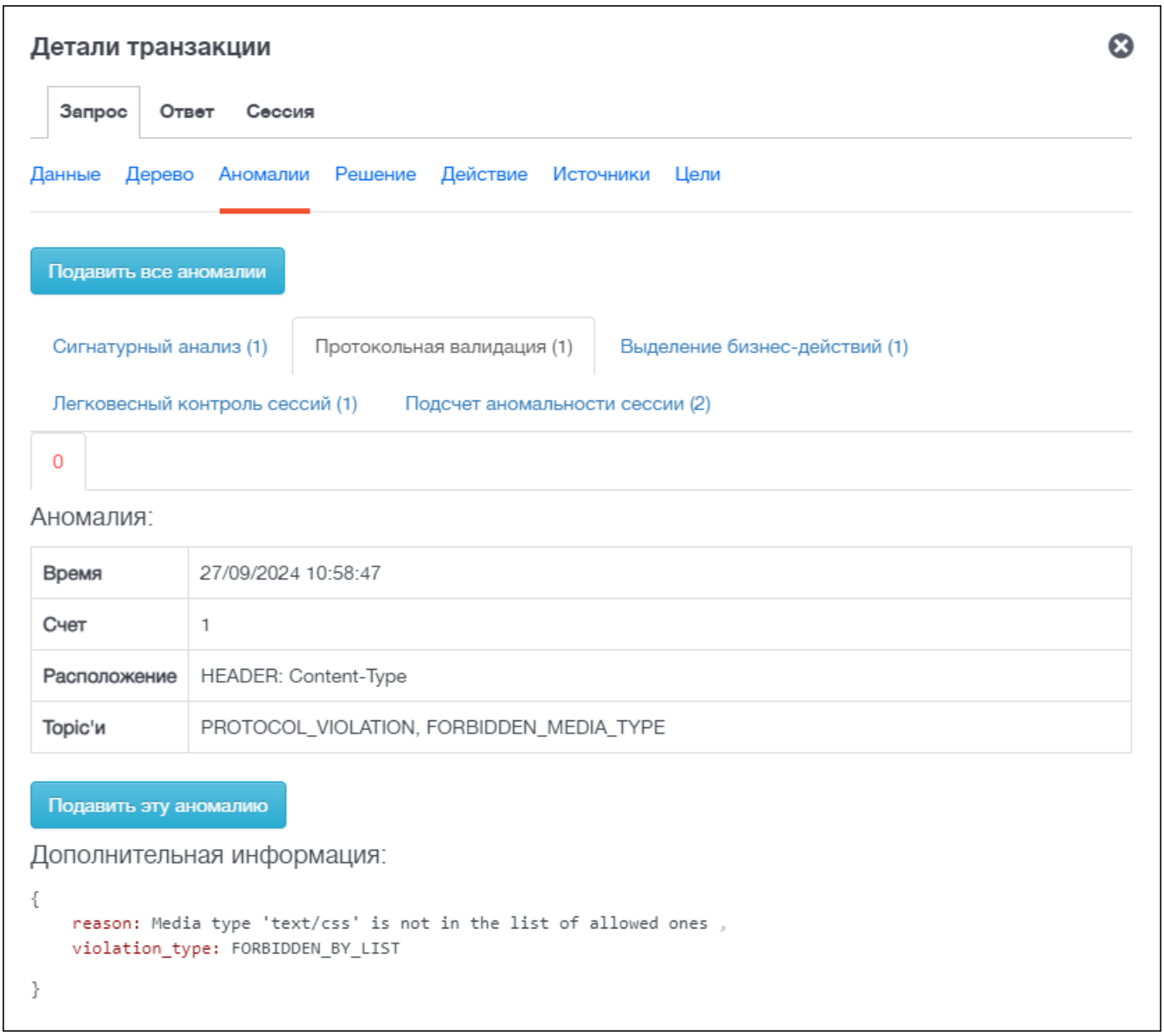

Рисунок 211 – Аномалия запрещенного MIME-типа

Чтобы данная аномалия больше не возникала, необходимо внести MIME-тип в список разрешенных на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.3. Недопустимые имена параметров в заголовке «Content-type» (CONTENT_TYPE).

Допустимые имена параметров – поле ввода допустимых имен для параметров заголовка «Content-type». Аномалия возникает, когда имена параметров «Content-type» не соответствуют протоколу (см. рисунок 212).

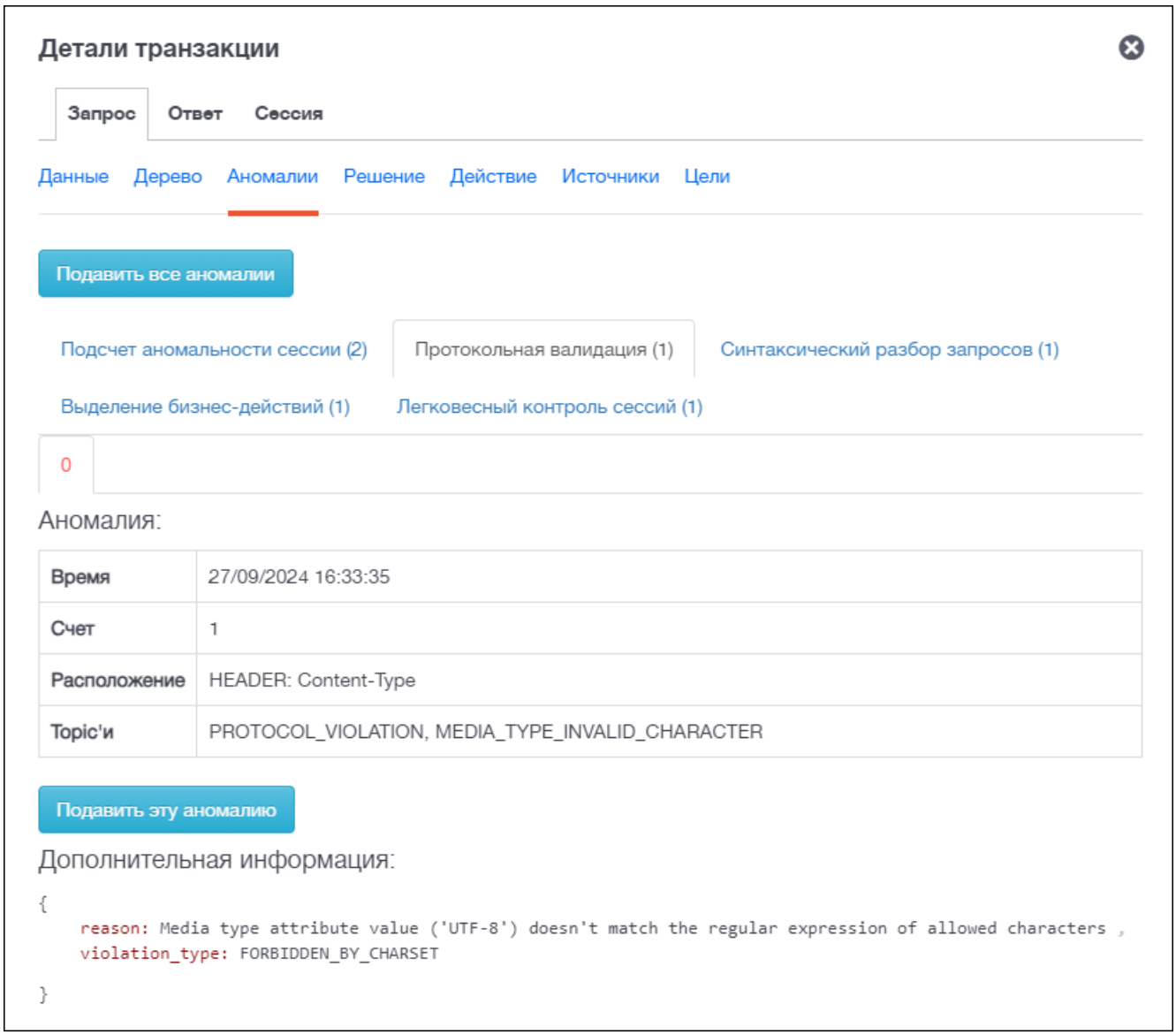

Рисунок 212 – Аномалия недопустимых значений параметра «Content-Type»

Чтобы данная аномалия больше не возникала, необходимо внести MIME-тип в список разрешенных на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.4. Недопустимые имена параметров в заголовке «Content-type» (CONTENT_TYPE).

Допустимые имена параметров – поле ввода допустимых имен для параметров заголовка «Content-type». Аномалия возникает, когда имена параметров «Content-type» не соответствуют протоколу (см. рисунок 213).

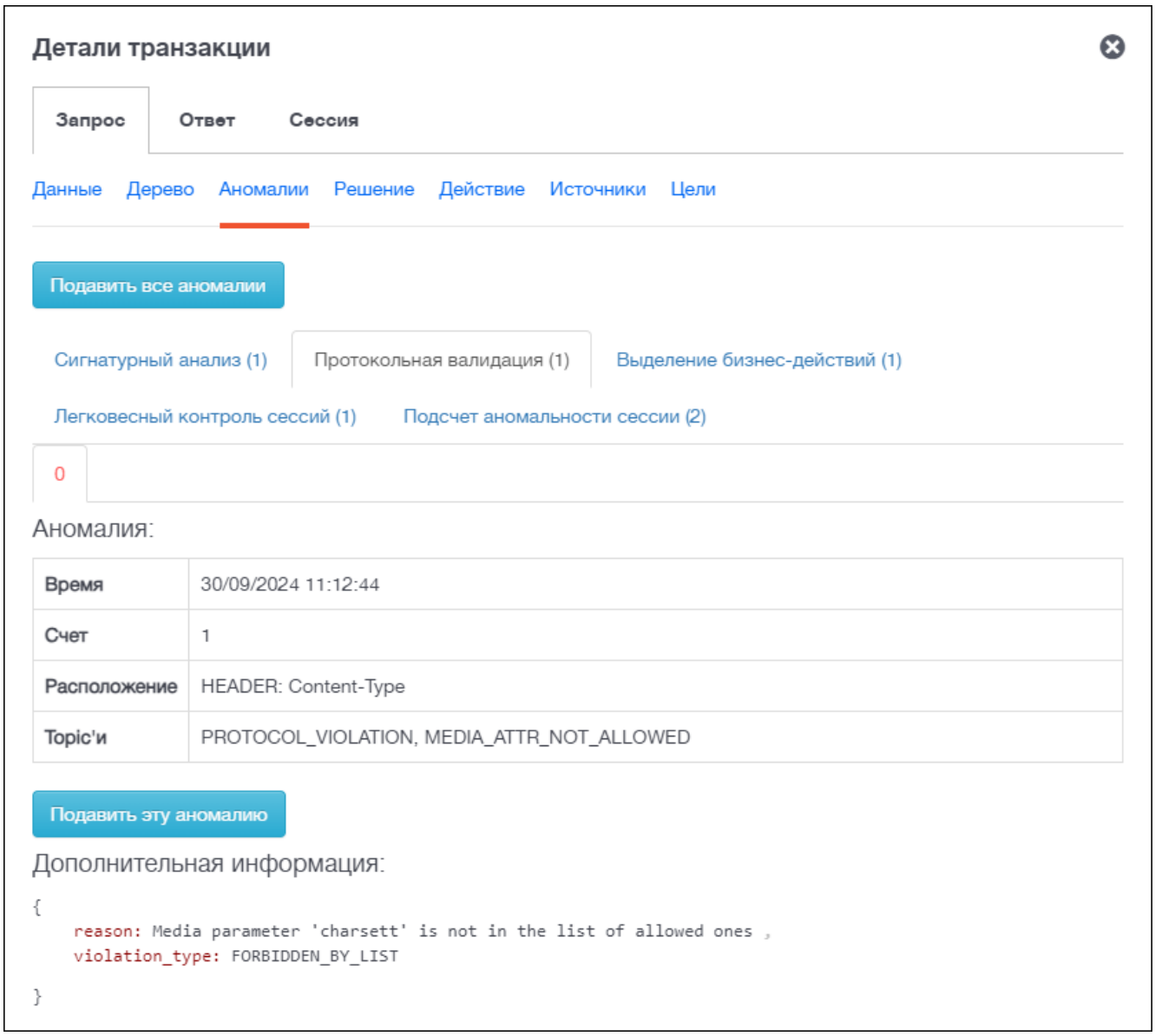

Рисунок 213 – Аномалия недопустимых имен параметра «Content-Type»

Чтобы данная аномалия больше не возникала, необходимо внести MIME-тип в список разрешенных на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.5. Недопустимые кодировки (MEDIA_TYPE_FORBIDDEN_ENCODING).

Аномалия возникает, если в параметрах Content-type передается кодировка, неуказанная в протоколе (см. рисунок 214).

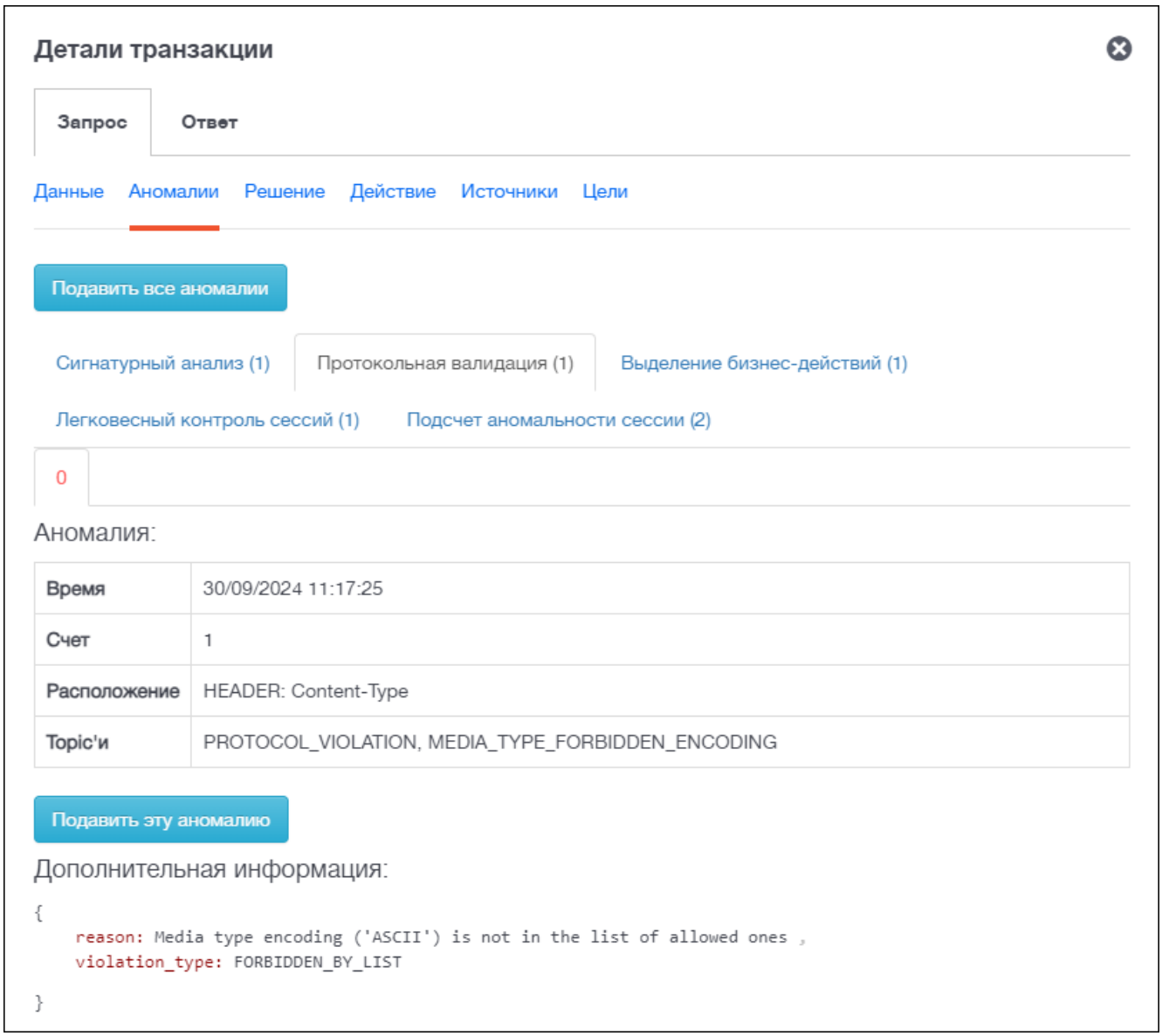

Рисунок 214 – Аномалия недопустимых кодировок

Чтобы данная аномалия больше не возникала, необходимо внести MIME-тип в список разрешенных на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.6. Некорректная валидация заголовка «Content-Length» (PROTOCOL_VIOLATION).

Аномалия возникает при несоответствии размера тела запроса со значением, указанным в заголовке «Content-Lenght» (см. рисунок 215).

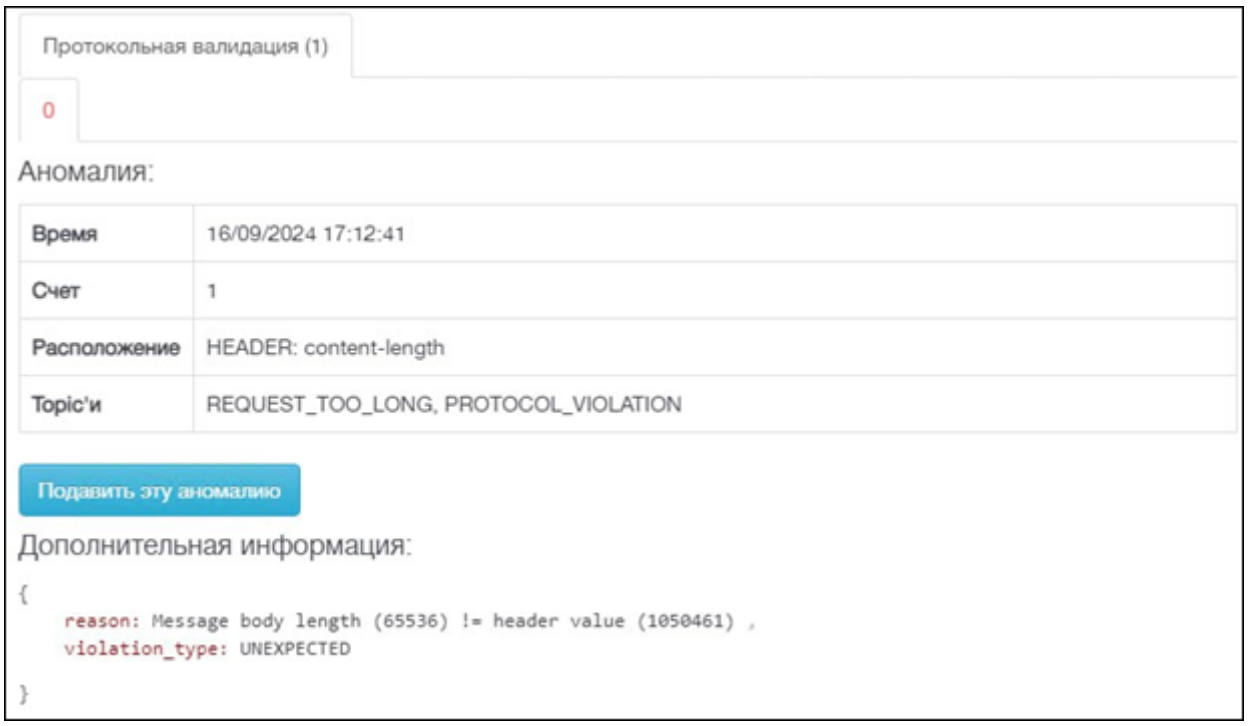

Рисунок 215 – Аномалия валидации заголовка «Content-Length»

На вкладке «Приложение» - «Протокол» можно отключить валидацию заголовка «Content-Length». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.7. Ошибка валидатора имени хоста (VALUE_INVALID_CHARACTER).

Аномалия возникает при несоответствии значения заголовка «Host» регулярному значению в заголовке протокола (см. рисунок 216).

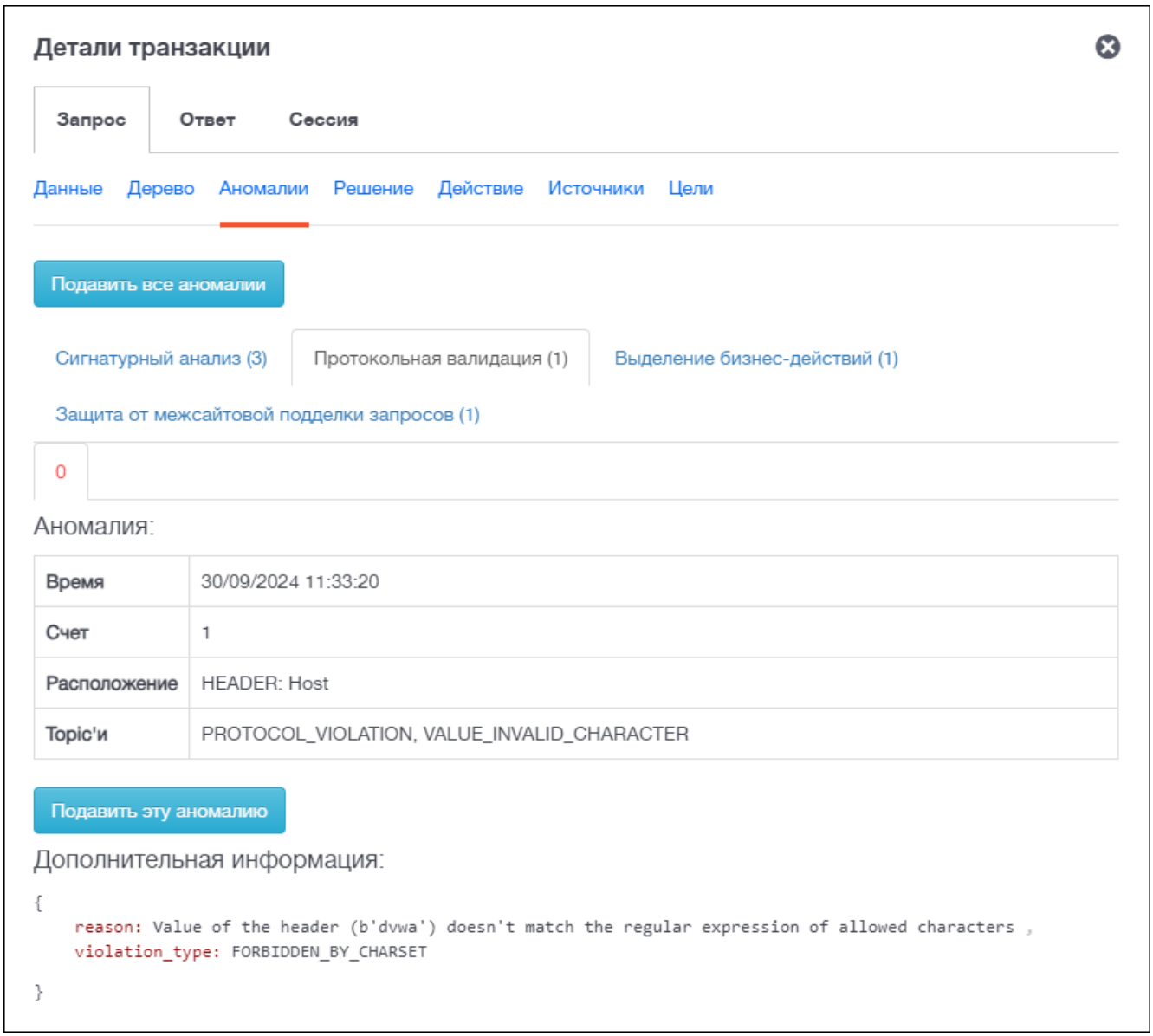

Рисунок 216 – Аномалия валидации имени хоста

Чтобы данная аномалия больше не возникала, необходимо внести изменение в регулярное выражение для проверки допустимых имен, на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.8. Превышение количества интервалов заголовка Range (INTERVAL_RANGE_EXCEEDED).

Аномалия возникает при превышении допустимого количества интервалов в заголовке «Range» (см. рисунок 217). Количество допустимых интервалов устанавливается в протоколе.

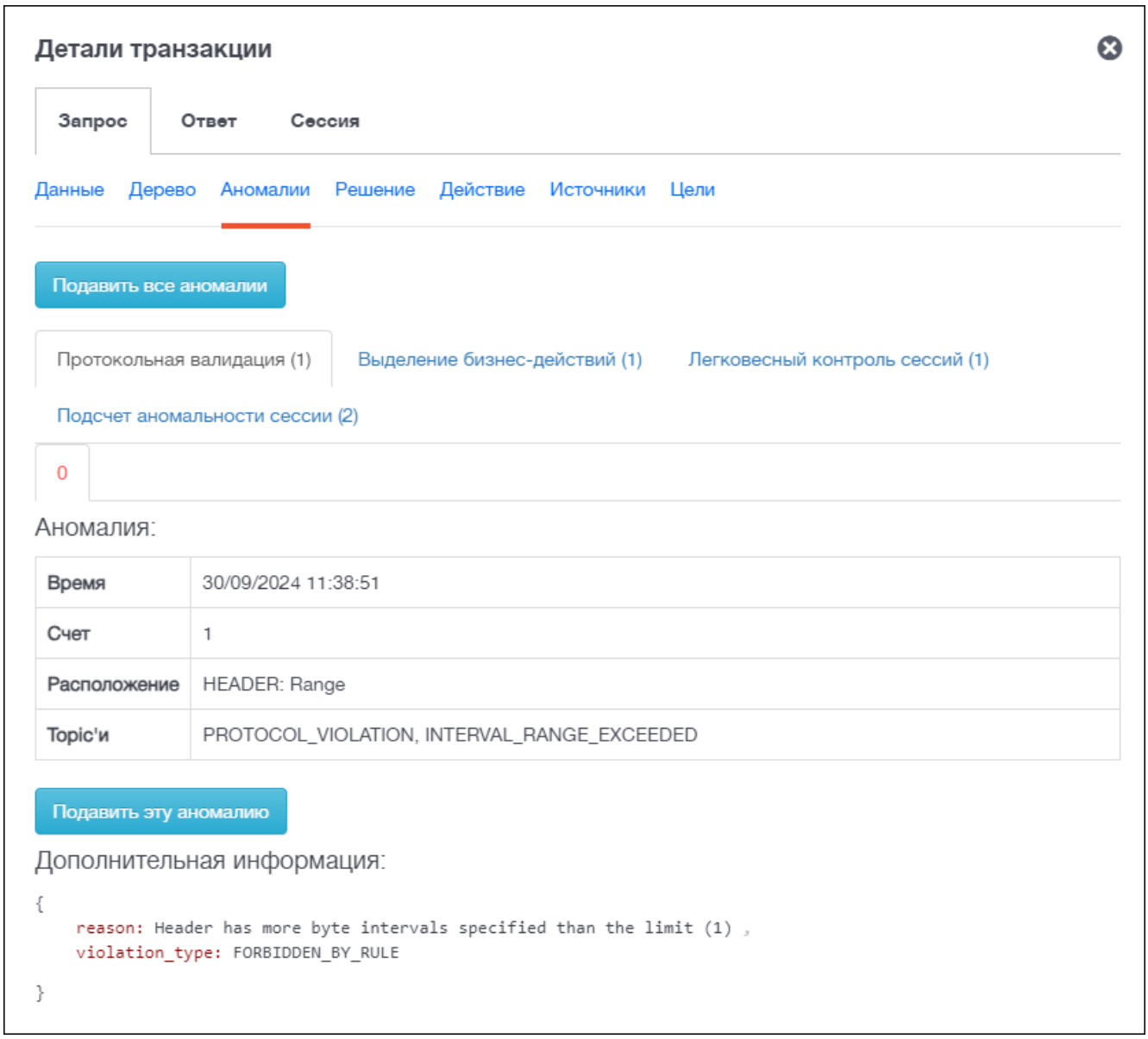

Рисунок 217 – Аномалия количества интервалов заголовка «Range»

Чтобы данная аномалия больше не возникала, необходимо внести изменение в поле максимальное количество интервалов в заголовке Range на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.9. Превышена максимальная длина заголовка (HEADER_VALUE_TOO_LONG).

Данная аномалия возникает при превышении допустимой длины заголовка header (см. рисунок 218). Допустимая максимальная длина заголовка указывается в протоколе.

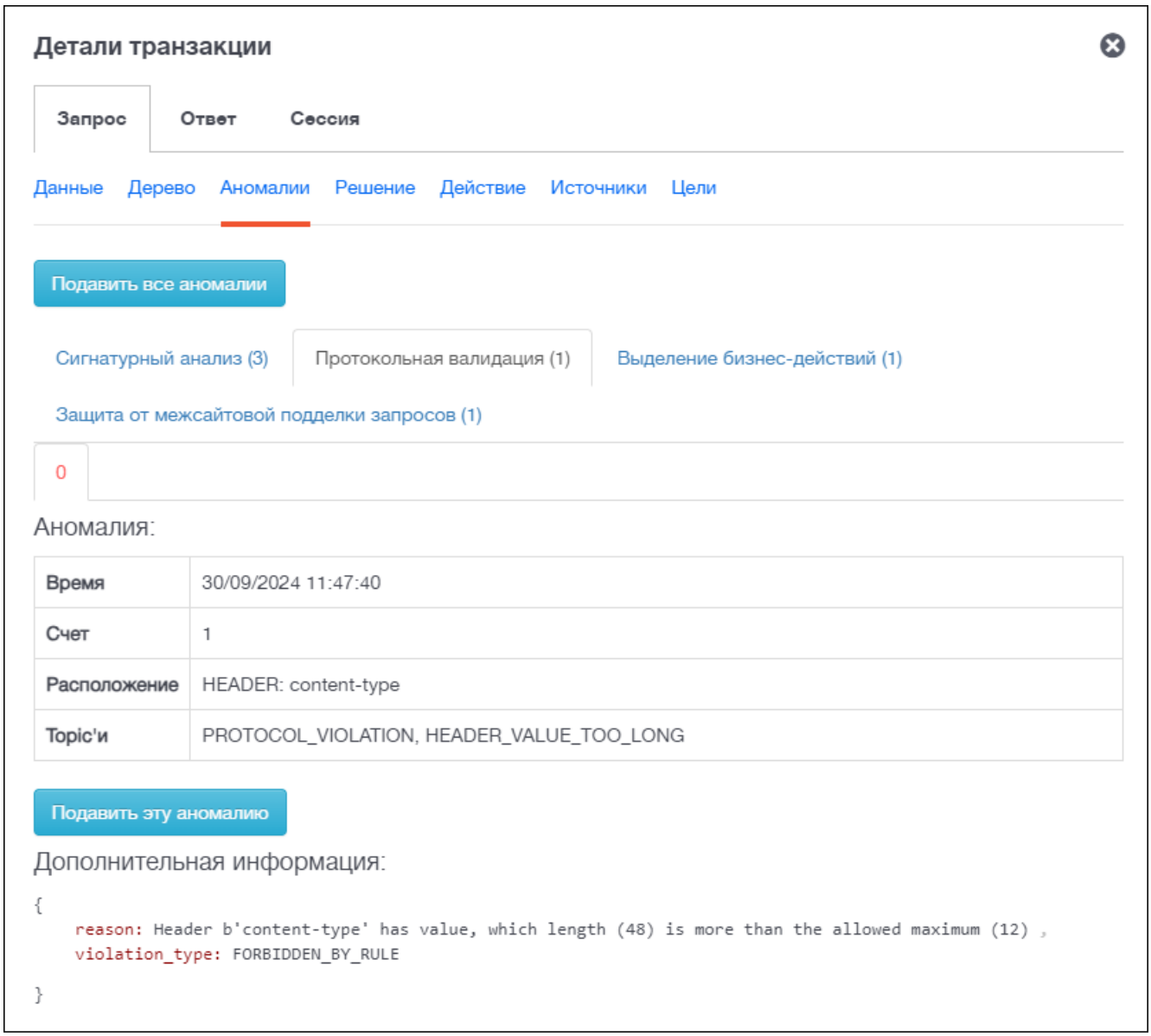

Рисунок 218 – Аномалия длины заголовка

Чтобы данная аномалия больше не возникала, необходимо внести изменения в значения параметра «Максимальная длина заголовка» на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.10. Запрещенные символы в URL-пути (VALUE_INVALID_CHARACTER).

Аномалия возникает при наличии в URL-пути символов, отличных от указанных в протоколе (см. рисунок 219).

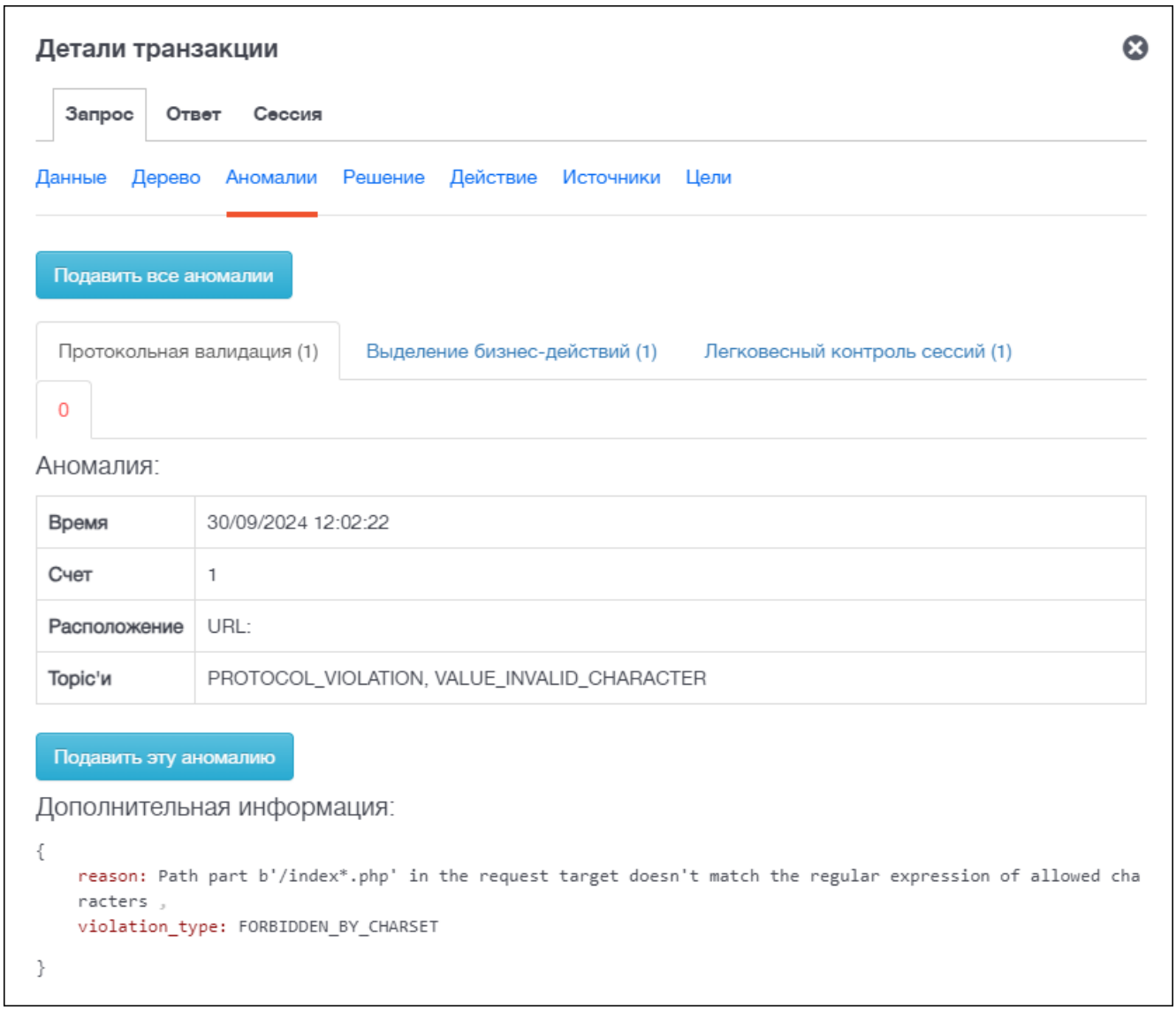

Рисунок 219 – Аномалия некорректного URL

Чтобы данная аномалия больше не возникала, необходимо откорректировать поле «Символы, разрешенные в URL-пути, в дополнение к стандартному набору (A-Za-z0-9-._~/):» на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.11. Недопустимый метод (FORBIDDEN_METHOD).

Аномалия возникает при недопустимом методе HTTP запроса (см. рисунок 220).

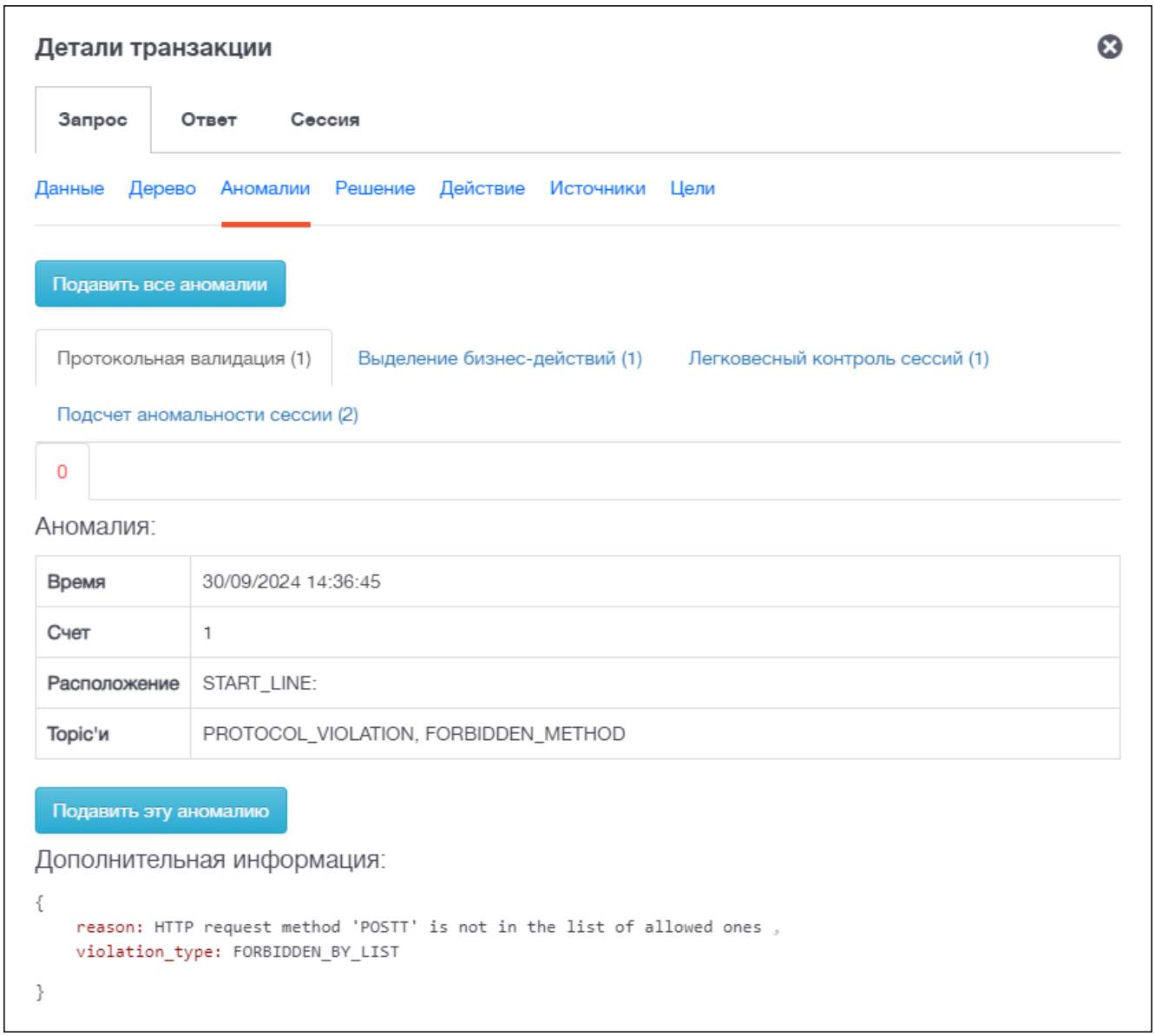

Рисунок 220 – Аномалия недопустимого метода

Чтобы данная аномалия больше не возникала, необходимо откорректировать поле «Разрешенные методы» на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.12. Недопустимая длина Url-пути.

Аномалия возникает, если длина Url-пути превышает максимально допустимое значение (см. рисунок 221). Максимальное значение длины пути определяется протоколом.

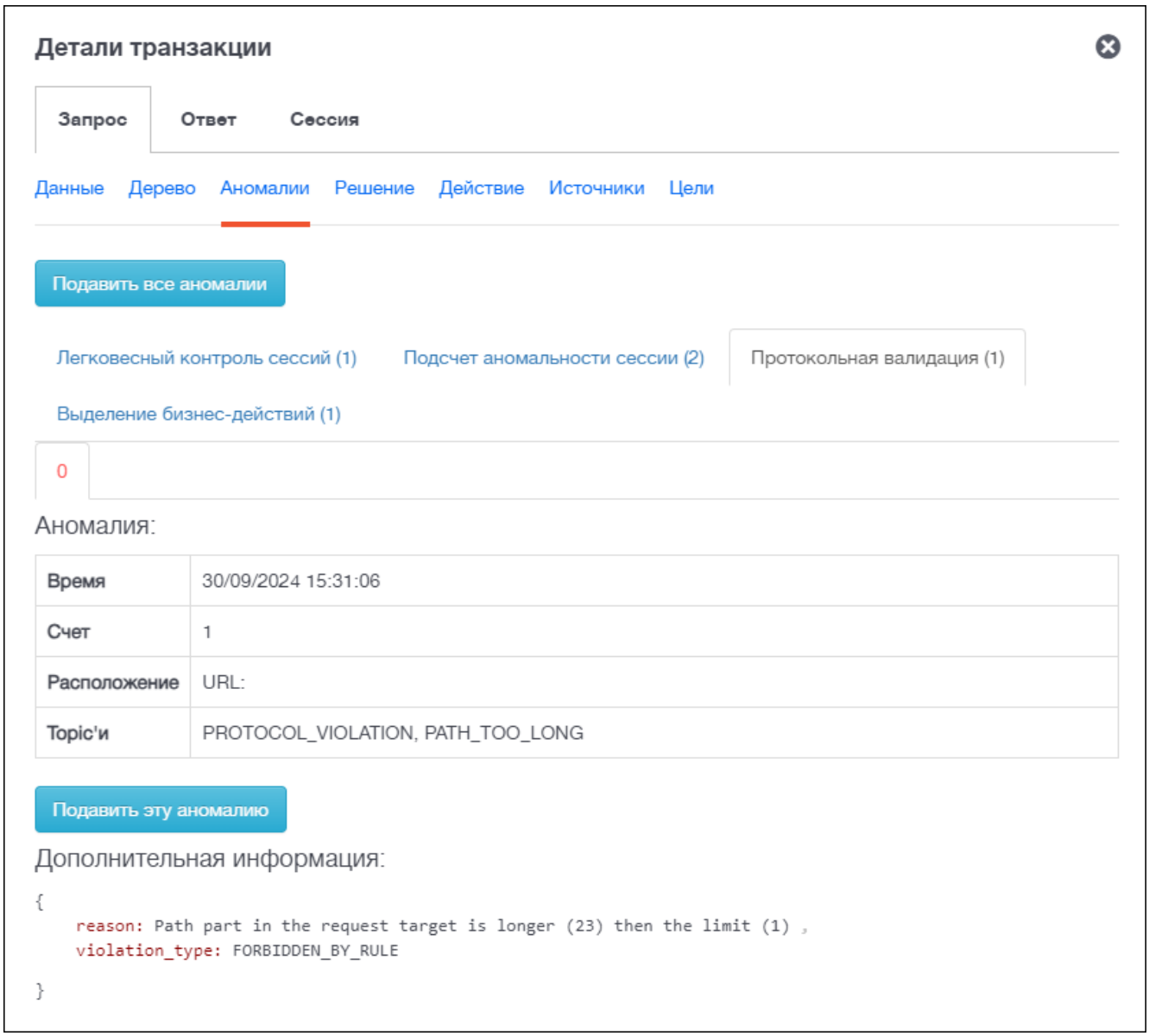

Рисунок 221 – Аномалия недопустимой длины URL-пути

Чтобы данная аномалия больше не возникала, необходимо изменить значение поля «Максимальная длина пути» на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.13. Ошибка в имени URL-параметров (INVALID_QUERY).

Аномалия возникает при несоответствии имен параметров URL протоколу (см. рисунок 222).

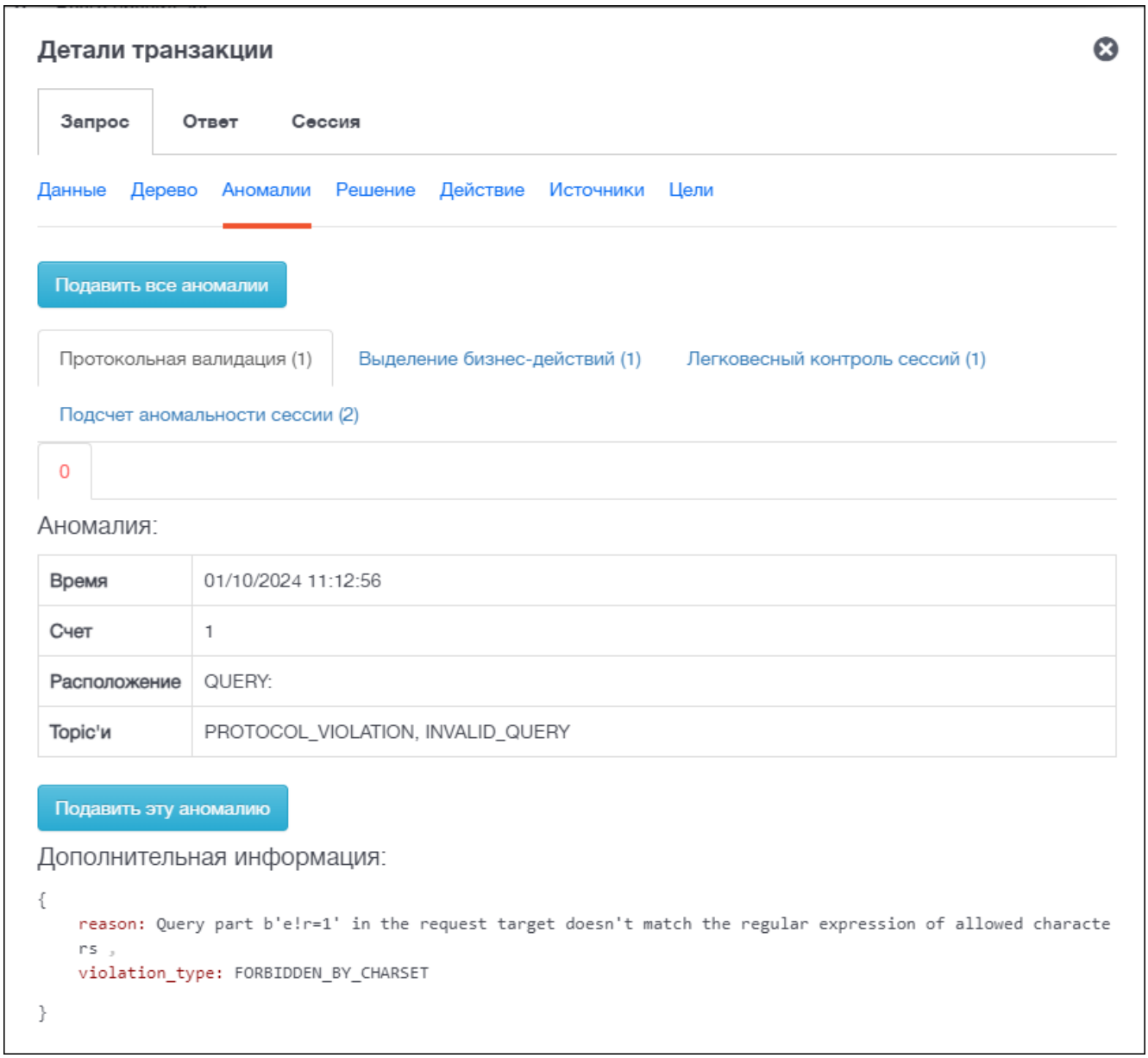

Рисунок 222 – Аномалия некорректного имени URL-параметра

Чтобы данная аномалия больше не возникала, необходимо изменить значение поля «Символы, разрешенные в URL-параметрах, в дополнение к стандартному набору (A-Za-z0-9-._~/):» на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.14. Запрещенный заголовок (FORBIDDEN_HEADER).

Аномалия возникает при отсутствии заголовка в списке разрешенных заголовков (см. рисунок 223). Разрешенные заголовки указываются в протоколе.

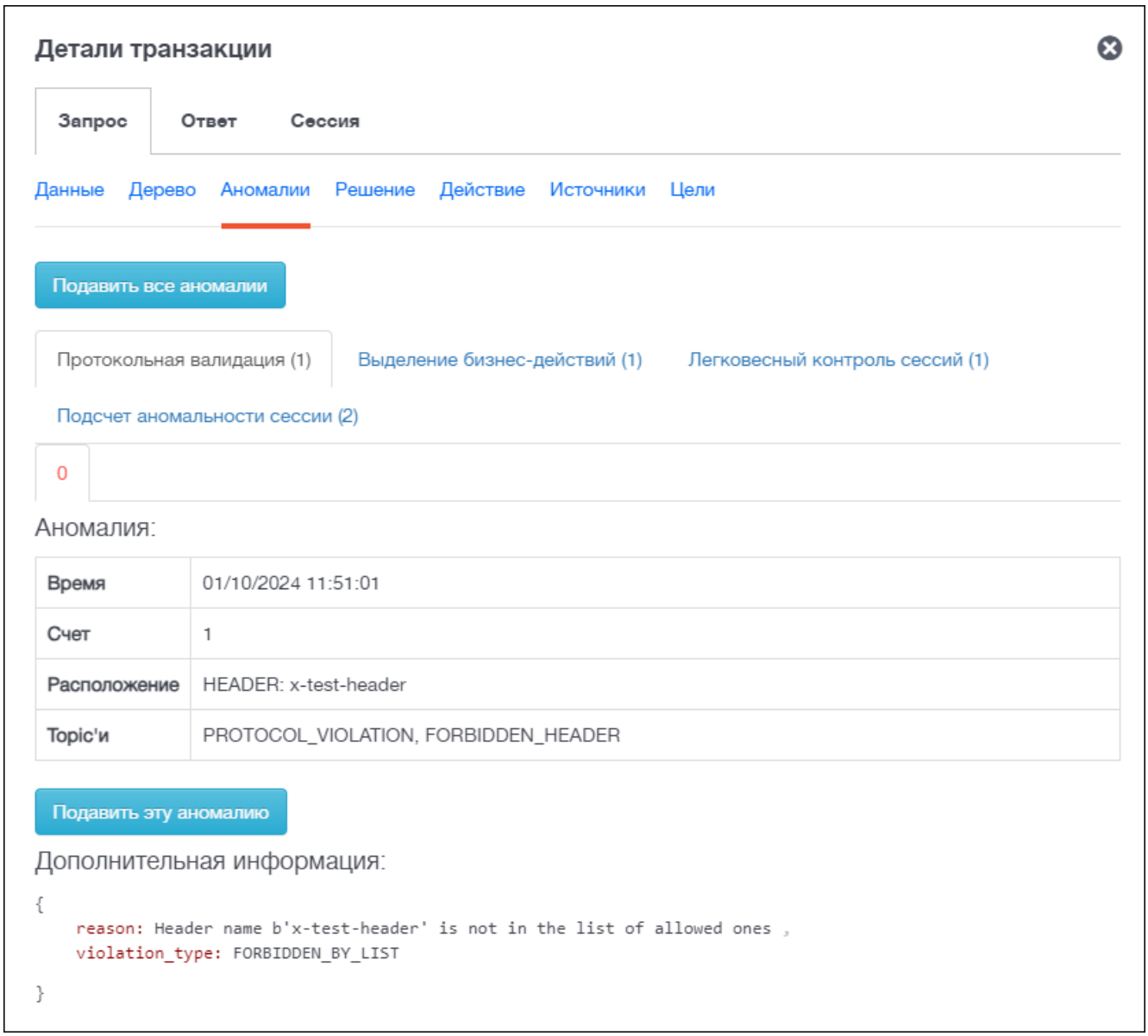

Рисунок 223 – Аномалия запрещенного заголовка

Чтобы данная аномалия больше не возникала, необходимо изменить значение поля «Разрешенные заголовки» или добавить регулярное выражение в поле «Шаблоны разрешенных заголовков» на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.15. Дублирование заголовков (DUPLICATE_HEADER).

Аномалия возникает при наличии в транзакции двух и более одинаковых заголовков (см. рисунок 224). При этом заголовки не внесены в перечень дублируемых в протоколе.

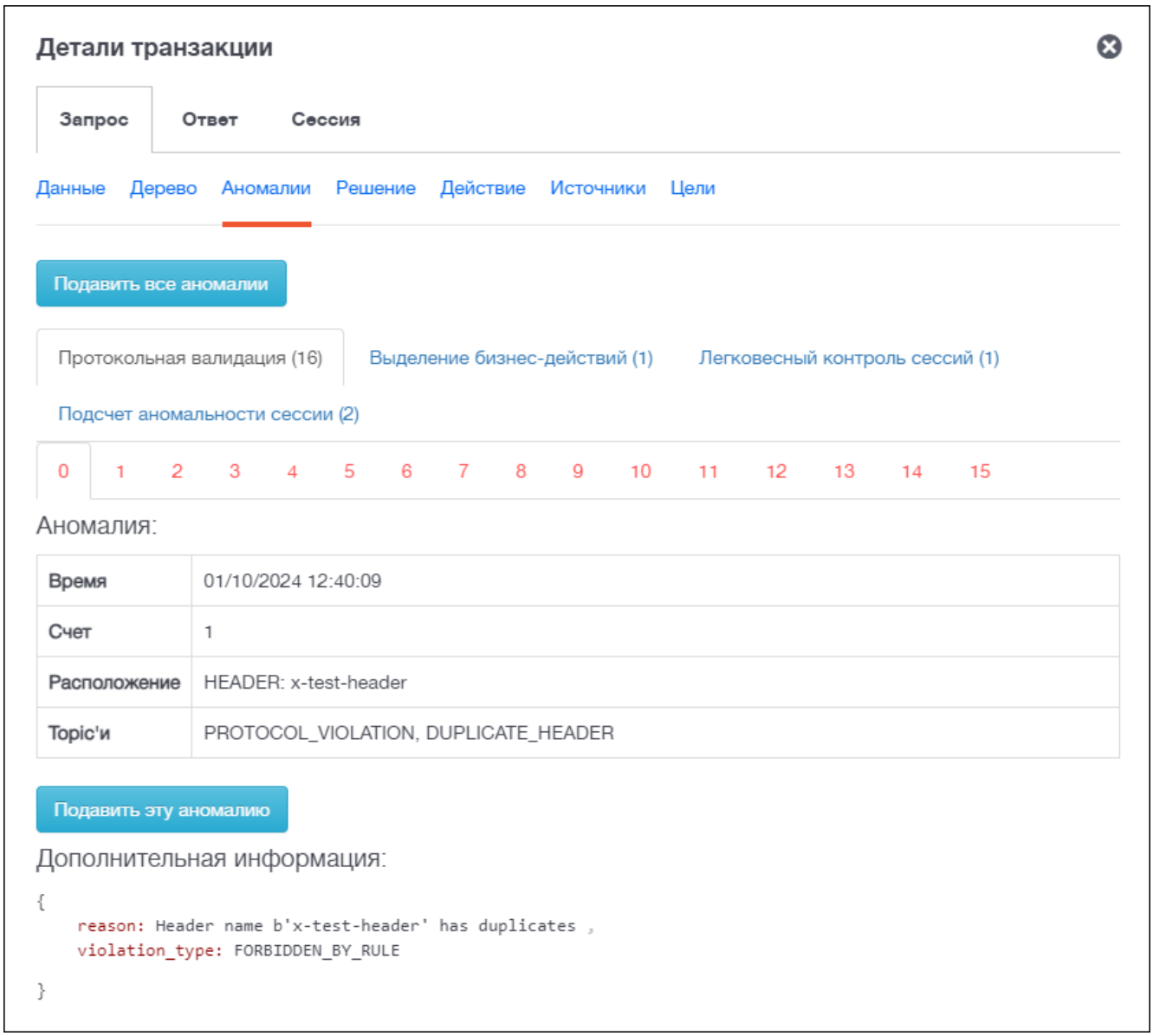

Рисунок 224 – Аномалия дублирования заголовков

Чтобы данная аномалия больше не возникала, необходимо изменить значение поля «Разрешать дублирующиеся заголовки» на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.16. Ошибка значений заголовков (VALUE_INVALID_CHARACTER).

Аномалия возникает при несоответствии значений заголовков регулярному выражению заголовков протокола (см. рисунок 225).

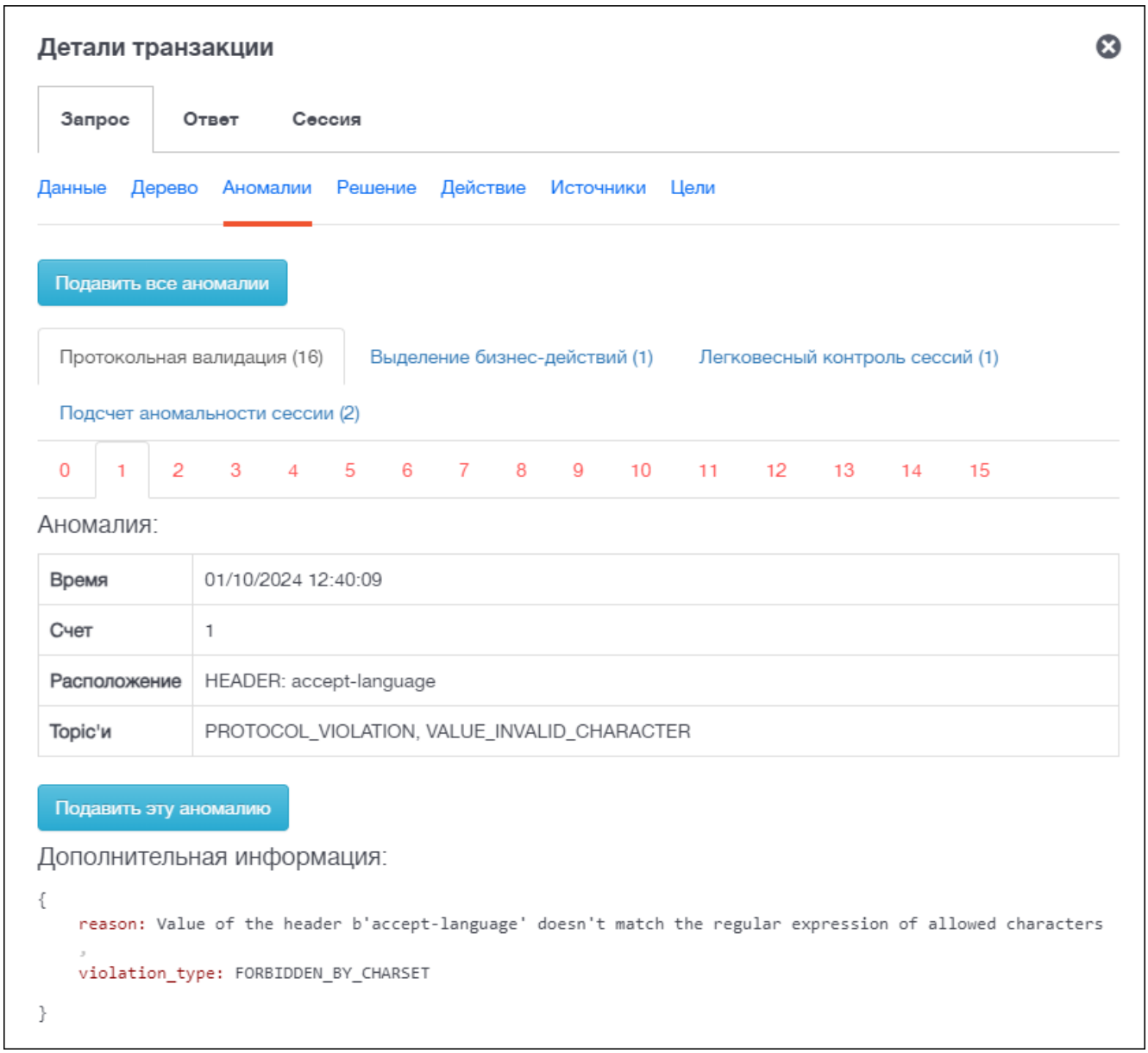

Рисунок 225 – Аномалия некорректного значения заголовка

Чтобы данная аномалия больше не возникала, необходимо изменить значение поля «Регулярное выражение для проверки значений заголовков» на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

6.17. Превышение количества разрешенных заголовков (TOO_MANY_HEADERS).

Аномалия возникает при превышении допустимого числа заголовков, определенных протоколом (см. рисунок 226).

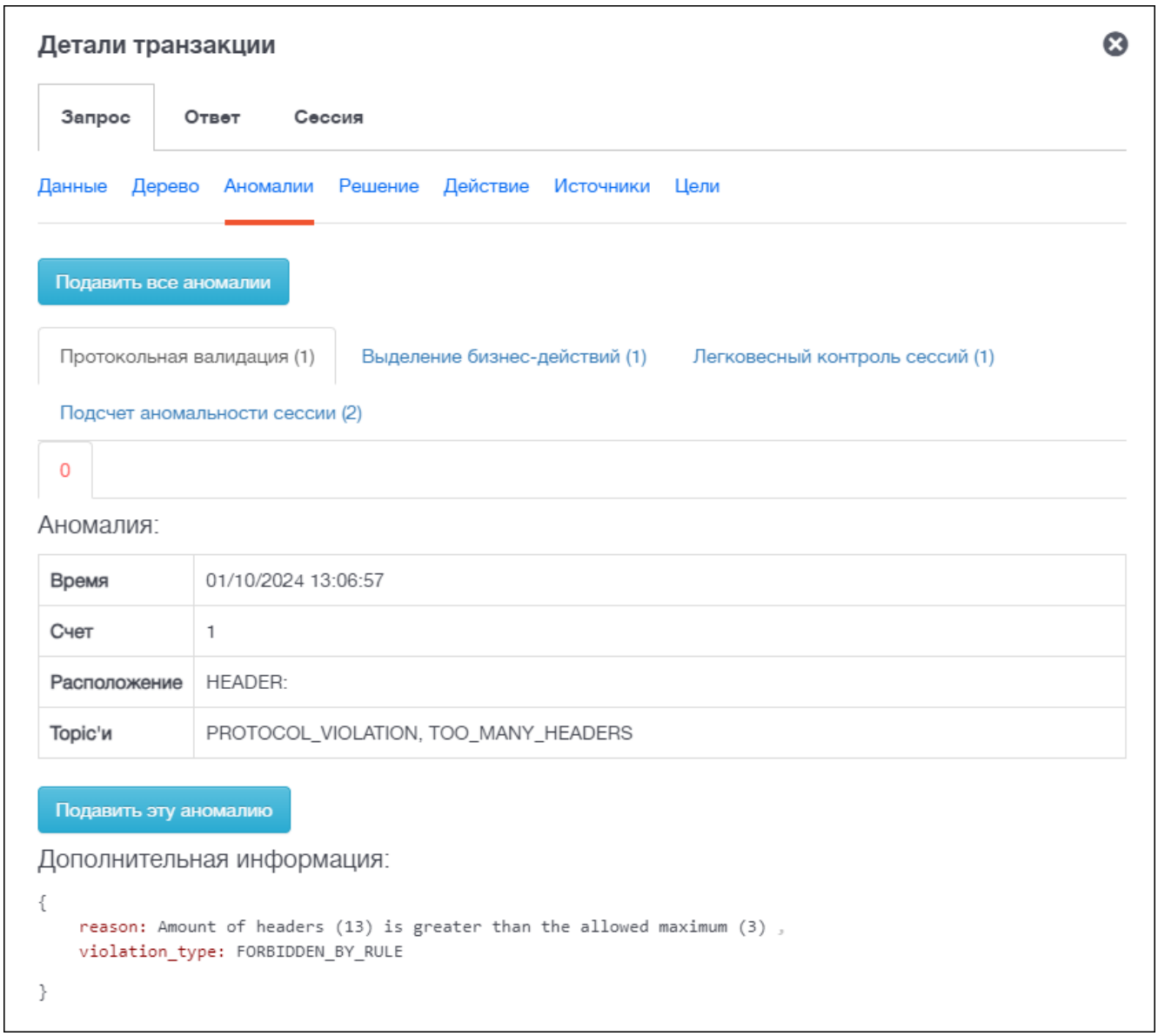

Рисунок 226 – Аномалия недопустимого количества заголовков

Чтобы данная аномалия больше не возникала, необходимо изменить значение поля «Максимальное количество заголовков» на вкладке «Приложение» - «Протокол». Подробное описание вкладки «Протокол» можно найти в разделе 3.5.3.

7. Синтаксический разбор запросов.

Аномалии от данного модуля подавлять нежелательно, корректнее изменить настройки разбора запроса в разрезе данного приложения (подробнее см. в разделе 10). Подавление данного модуля приведет к отключению его части в разрезе выбранных параметров (приложения и\или действия).

Ввиду того, что данный модуль проверяет как наличие разбираемого заголовка, если задать условия истинности над блоком разбора, так и корректность разбираемых данных, аномалии от данного модуля можно разделить на два вида:

7.1. Отсутствие заданного в условии истинности пути.

Данная аномалия появляется, если WAF не может найти данные для разбора по причине их отсутствия.

На примере из рисунка 227, можно наблюдать ошибку отсутствия обязательного (исходя из настроек) заголовка Authorization. В данном случае, если погрузиться в логику работы приложения, заголовок Authorization не появляется у неавторизованных пользователей, соответственно, настройка, в которой данный заголовок обязательный, является некорректной. Следует поставить условие, которое будет применять разбор заголовка только при его наличии (подробнее о том, как это сделать можно прочитать в разделе 10).

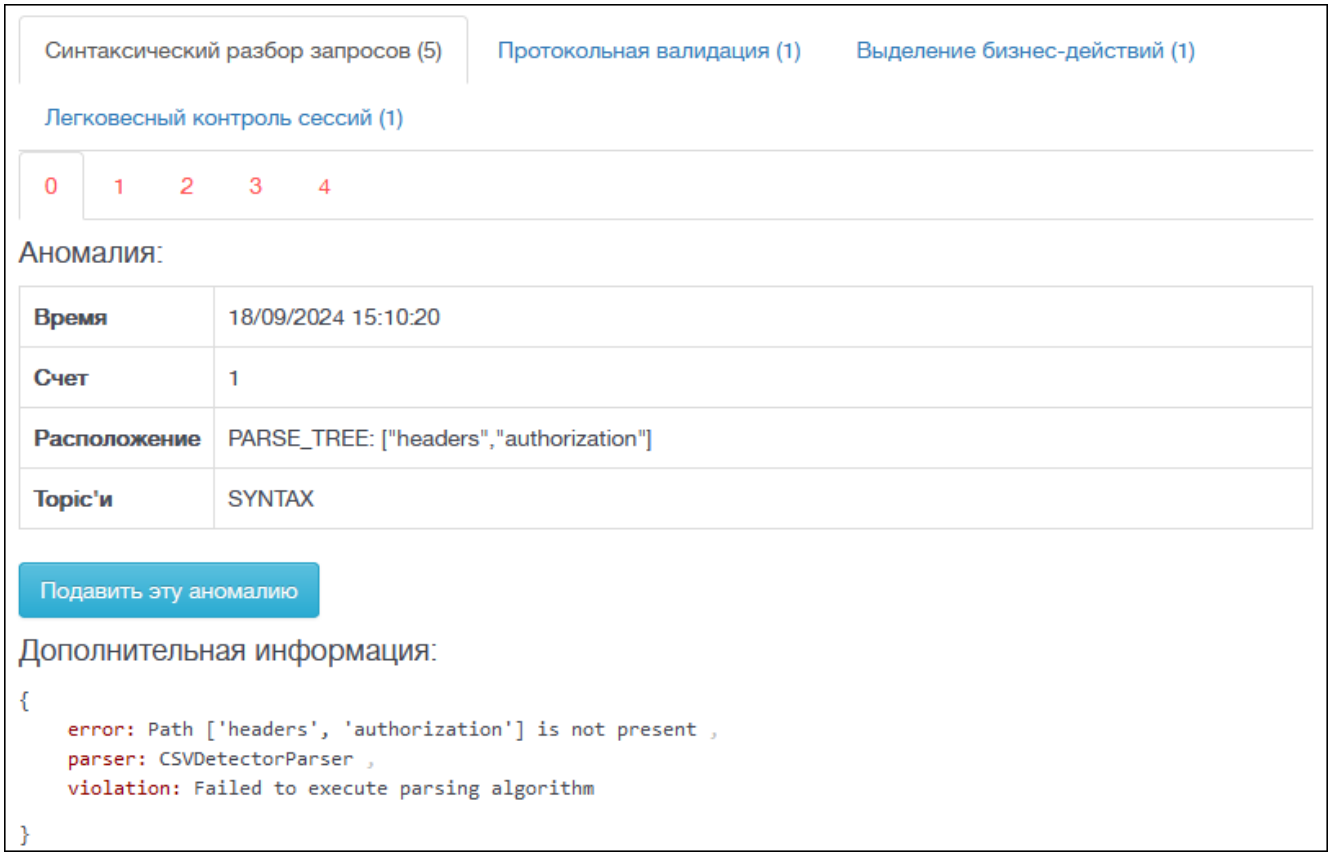

Рисунок 227 – Ошибка при разборе запроса

7.2. Ошибка разбора данных.

При формировании дерева разбора WAF проверяет валидность разбираемых данных. Существует несколько причин, по которым WAF не может корректно разобрать содержимое заголовка:

- В запросе передаются невалидные данные. Например, на рисунке 228 показана ошибка при валидации JSON в заголовке «body». В случае если в данном заголовке используется специфичная структура JSON, которая не проходит валидацию, то данную аномалию следует подавить.
- Ошибка разбора данных в заголовке «body», вызванная обрезанием тела запроса (обычно так делают для уменьшения объема логов). До версии анализатора 2.15 данная аномалия сопровождалась следующей аномалией от модуля «Протокольная валидация». В таких случаях существует два варианта:
  - подавить аномалию, если устраивает оптимизация хранимых данных;
  - увеличить максимальный размер тела запроса, если в приоритете защита приложения.

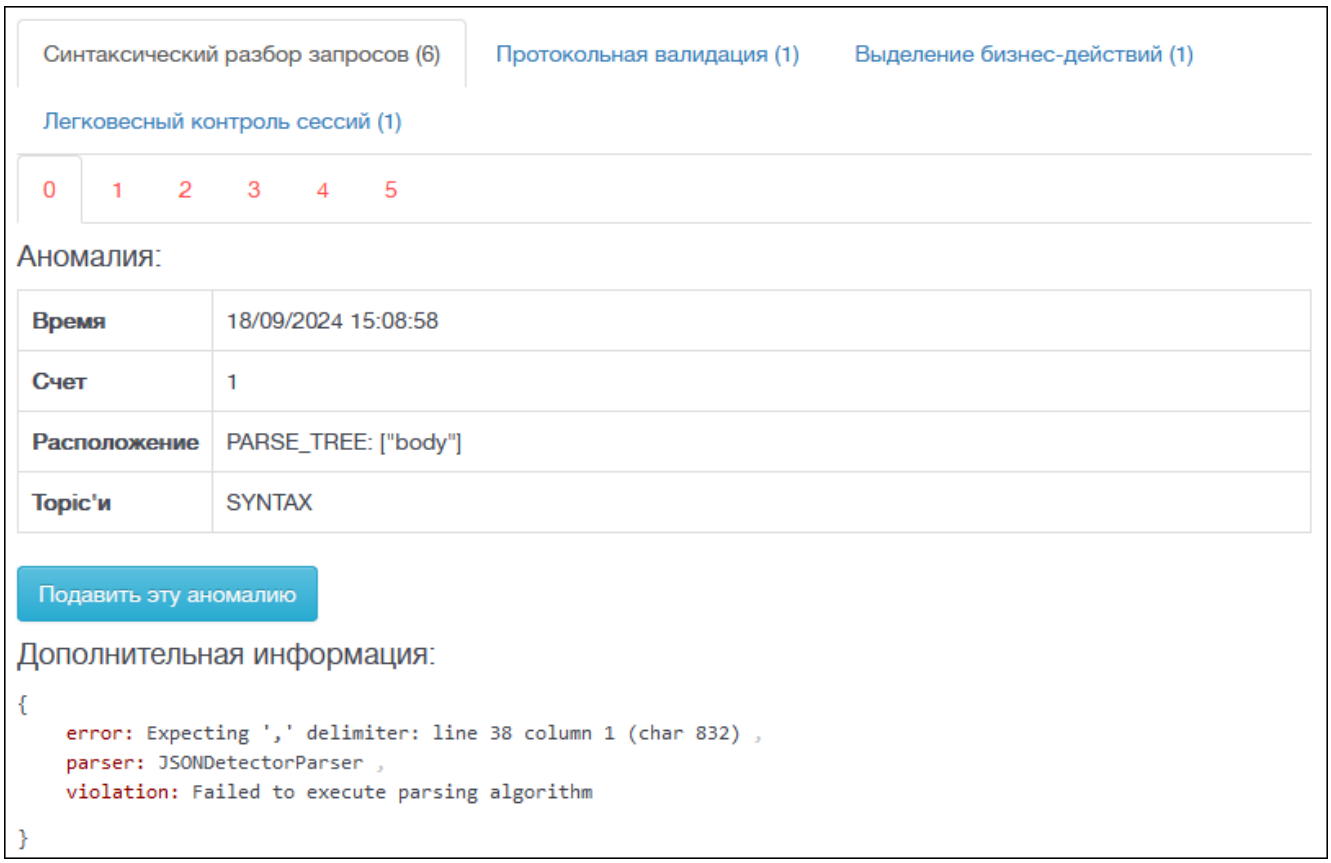

Рисунок 228 – Ошибка разбора данных

8. Синтаксический разбор ответов.

Аномалии от данного модуля подавлять нежелательно, корректнее изменить настройки разбора ответа в разрезе данного приложения. Подавление данного модуля приведет к отключению его части в разрезе выбранных параметров (приложения и\или действия).

Аномалии от модуля «Синтаксический разбор ответов» идентичны аномалиям от модуля «Синтаксический разбор запросов». Различие данных модулей только в области действия. Как можно понять из названия, первый работает на разбор запросов, а второй на разбор ответов.

9. Детектор CSRF-атак.

Аномалии от данного модуля лучше не подавлять, а редактировать разрешенные домены в настройках приложения (подробнее см. в разделе 3.6). Подавление данной аномалии приведет к отключению модуля в разрезе выбранных параметров (приложения и\или действия).

Так как суть данного детектора в проверке заголовков «Origin» и «Referer запроса, аномалии данного детектора привязаны к этим заголовкам и их состояниям.

9.1. Несовпадение домена в заголовке «Referer» с доменом в заголовке «Host».

О том, что данная аномалия вызвана именно несовпадением домена в заголовке «Referer» с доменом в заголовке «Host», говорит расположение аномалии, которое указывает на путь в дереве разбора до заголовка «Referer» (см. рисунок 229).

Такое часто бывает, когда авторизация проходит на другом приложении. В таких случаях необходимо добавлять домен в разрешенные. Подробнее о добавлении домена можно прочитать в разделе 20.

Рисунок 229 – Несовпадение домена в заголовке «Referer» с доменом в заголовке «Host»

9.2. Несовпадение домена в заголовке «Origin» с доменом в заголовке «Host».

О том, что данная аномалия вызвана именно несовпадением домена в заголовке «Origin» с доменом в заголовке «Host», говорит расположение аномалии, которое указывает на путь в дереве разбора до заголовка «Origin» (см. рисунок 230).

Как и в случае несовпадения значения домена в заголовках «Referer» и «Host», такое часто бывает, когда авторизация проходит на другом приложении. В таких случаях необходимо добавлять домен в разрешенные. Подробнее о добавлении домена можно прочитать в разделе 20.

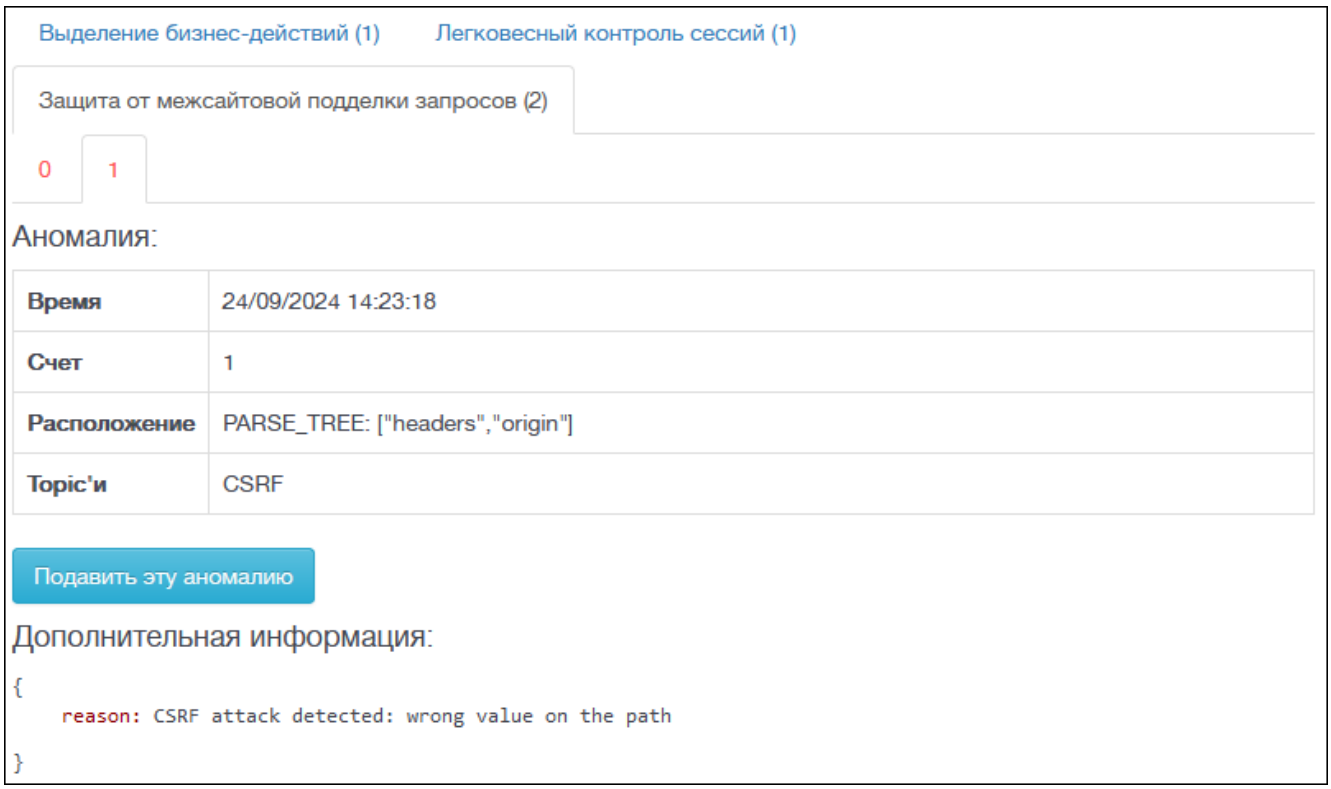

Рисунок 230 – Несовпадение домена в заголовке «Origin» с доменом в заголовке «Host»

9.3. Отсутствие заголовка «Referer» в запросе.

О том, что данная аномалия вызвана именно отсутствием заголовка «Referer», говорит расположение аномалии, которое указывает на путь в дереве разбора до заголовка «Referer» и дополнительная информация (см. рисунок 231).

Такая аномалия типична, если в качестве защищаемого приложения выступает API. В таких случаях следует отключать модуль «Защита от межсайтовой подделки запросов» для данного приложения, и корректнее это будет сделать через исключение в правиле «CSRF-атака». Подробнее о добавлении исключений в правила можно прочитать в разделе 21.

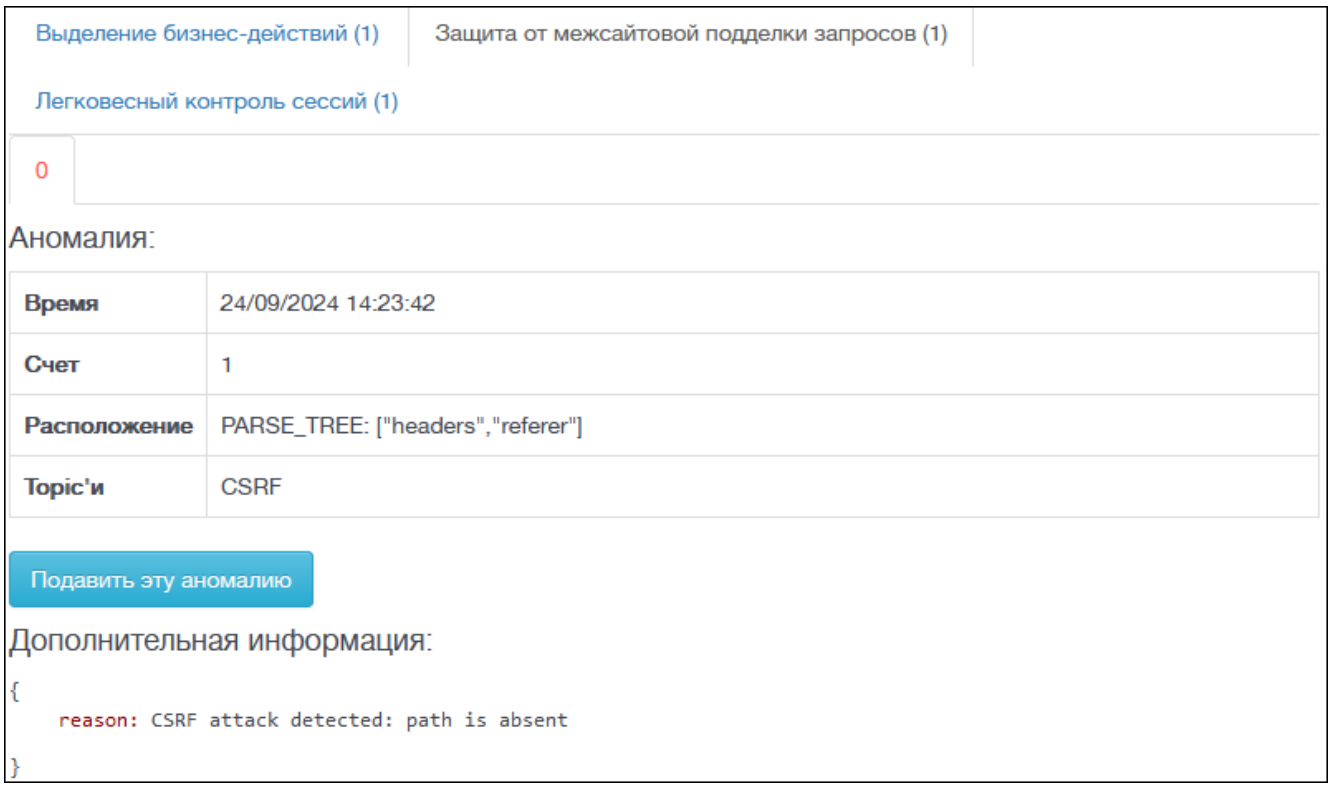

Рисунок 231 – Отсутствие заголовка «Referer» в запросе

10. Обнаружение переборных атак.

Аномалии от данного модуля подавлять не следует, необходимо редактировать параметры настроенных детекторов переборных атак (подробнее см. в разделе 16). Подавление данной аномалии приведет к отключению модуля в разрезе источника\цели по приложению и\или действию.

У данного модуля есть два вида аномалий, по количеству видов детекторов переборных атак.

10.1. Аномалия детектора переборных атак Действие/Источник.

Для данного вида аномалии характерно расположение аномалии на источник, который используется в рамках настройки детектора переборных атак (см. рисунок 232). Данного рода атаки подавлять не следует, корректнее поменять настройки детектора переборных атак.

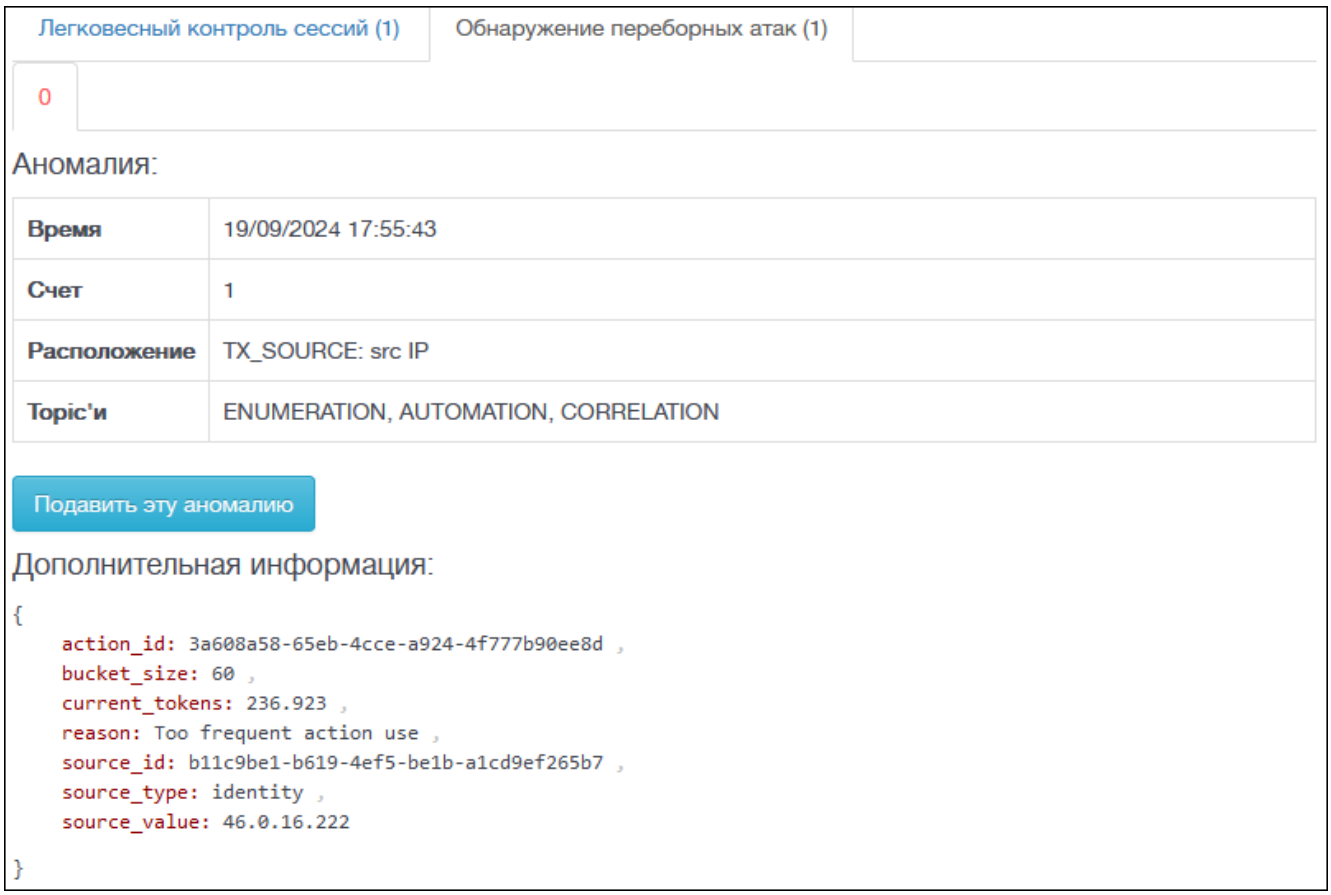

Рисунок 232 – Аномалия детектора переборных атак Действие/Источник

10.2. Аномалия детектора переборных атак Действие/Источник/Цель.

Для данного вида аномалии характерно расположение аномалии на цель (таргет), которая используется в рамках настройки детектора переборных ватак (см. рисунок 233).

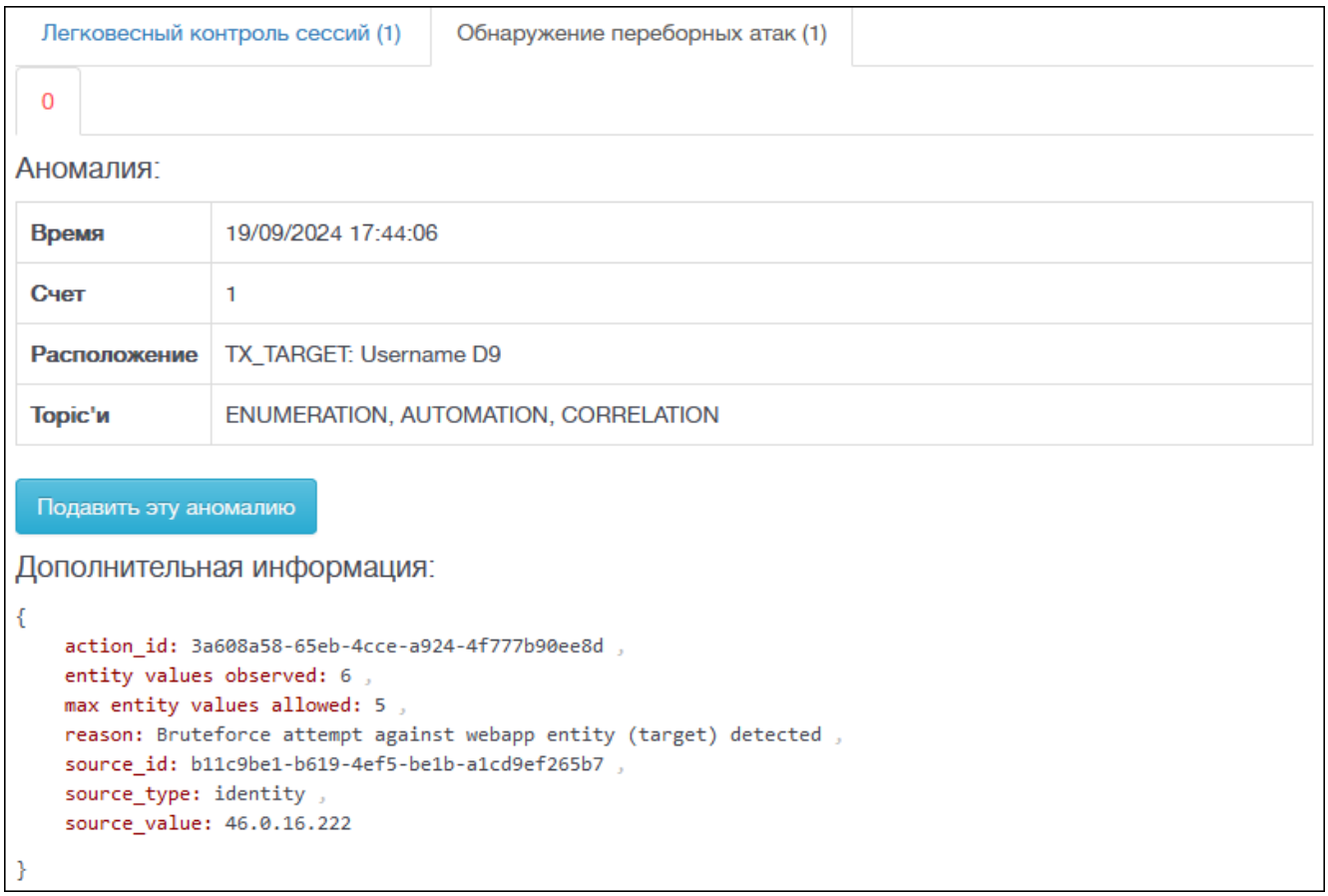

Рисунок 233 – Аномалия детектора переборных атак Действие/Источник/Цель

11. Упрощенное/легковесное отслеживание сессий.

Аномалии от данного модуля подавлять не следует, необходимо редактировать соответствующие настройки.

11.1. Аномалия использования cookie без предварительной её установки в ответе.

Данная аномалия возникает, если в запросе к приложению используются cookie, которые не были направлены пользователю в ответе, в разрезе данной сессии, или время жизни сессии в разрезе WAF истекло (см. рисунок 234). Данную аномалию подавлять не следует, корректнее будет воспользоваться одним из следующих вариантов:

- увеличить время сессии в разрезе WAF;
- отключить проверку выдачи cookie сервером.

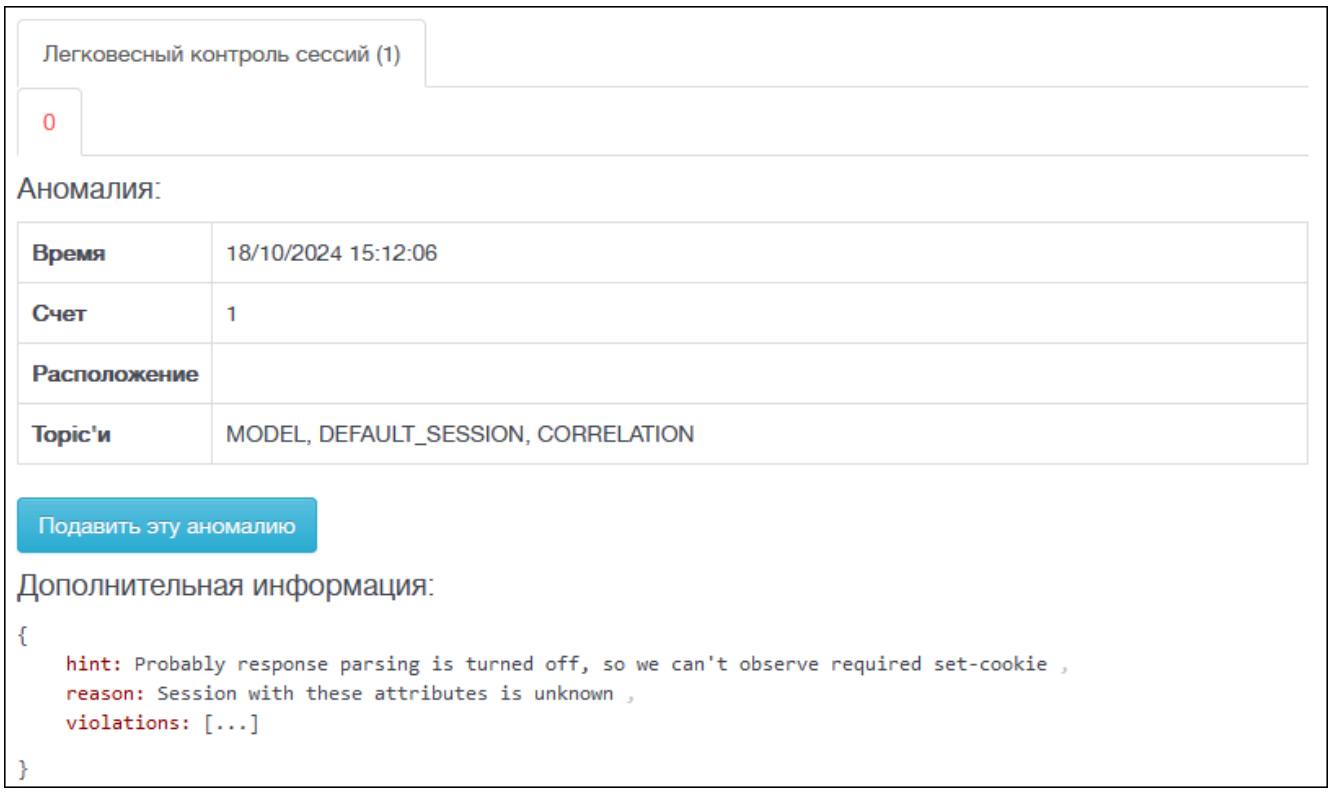

Рисунок 234 – Аномалия использования Cookie без предварительной их установки в ответе

12. Обнаружение аномалий в последовательности действий.

Аномалии от данного модуля подавлять не следует, необходимо редактировать соответствующие настройки.

У данного модуля есть два вида аномалий:

12.1. Аномалия нарушения цепочки действия с ожидаемым поведением.

Данная аномалия возникает в случае нарушения цепочки действий, которая задана на WAF как цепочка с ожидаемым поведением. Данную аномалию подавлять не стоит, корректнее будет отредактировать критерии, которым не соответствует данная цепочка (подробнее см. в разделе 18.3), или удалить данную цепочку действий.

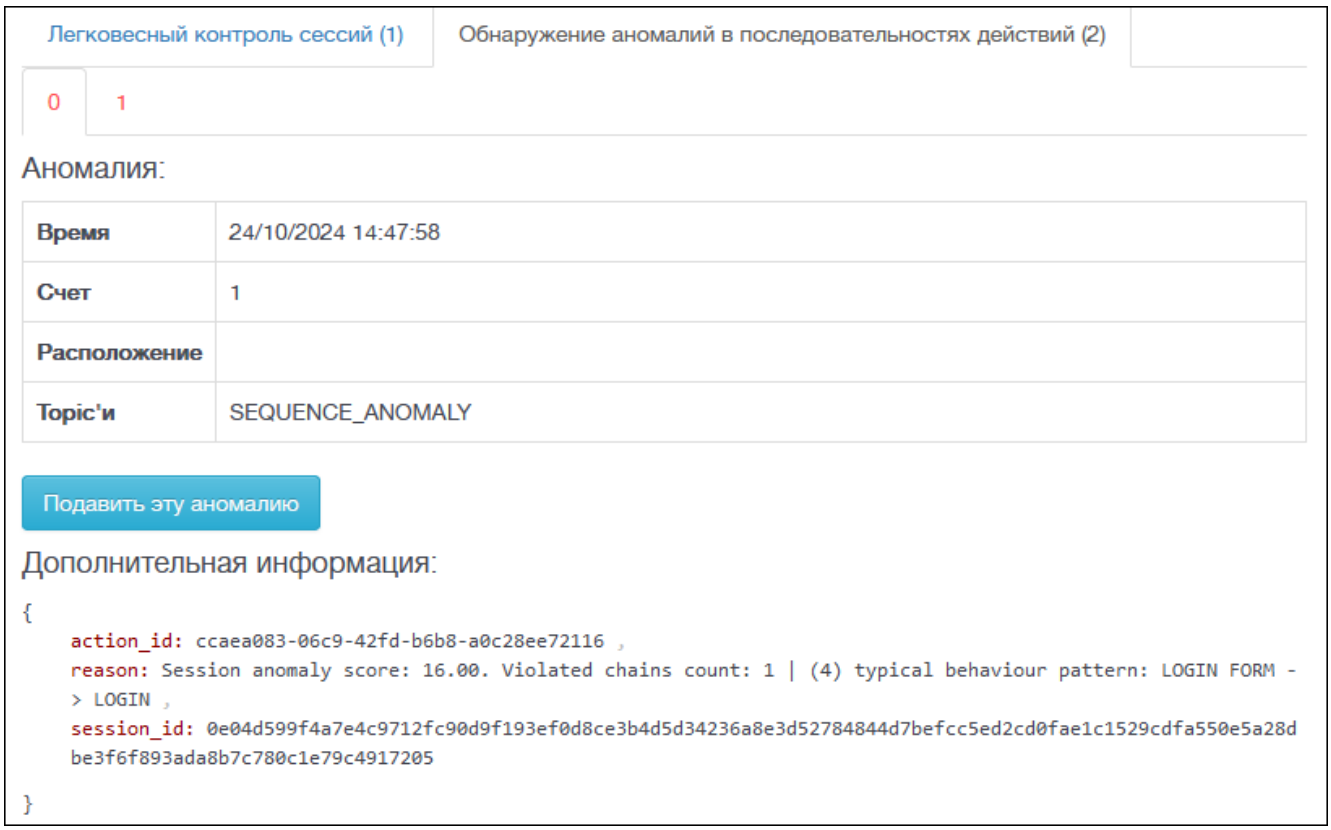

Рисунок 235 – Аномалия нарушения цепочки действия с ожидаемым поведением

12.2. Аномалия обнаружения цепочки действия с аномальным поведением.

Вид данной аномалии идентичен аномалии нарушения цепочки действия с ожидаемым поведением, но возникает в случае нарушения цепочки действий, которая задана на WAF как цепочка с аномальным поведением. Данную аномалию подавлять не стоит, корректнее будет отредактировать критерии, которым не соответствует данная цепочка (подробнее см. в разделе 18.3), или удалить данную цепочку действий.

13. Интеграция с сигнатурным анализом на ICAP-сервере.

Аномалии от данного модуля подавлять не следует, необходимо редактировать настройки реагирования на стороне ICAP-сервера. Подавление данной аномалии приведет к отключению модуля в разрезе приложения и\или действия.

14. Модуль обратного прокси.

Подавление данного модуля, в случае его ложно-позитивной сработки, необходимо осуществлять на всё приложение.

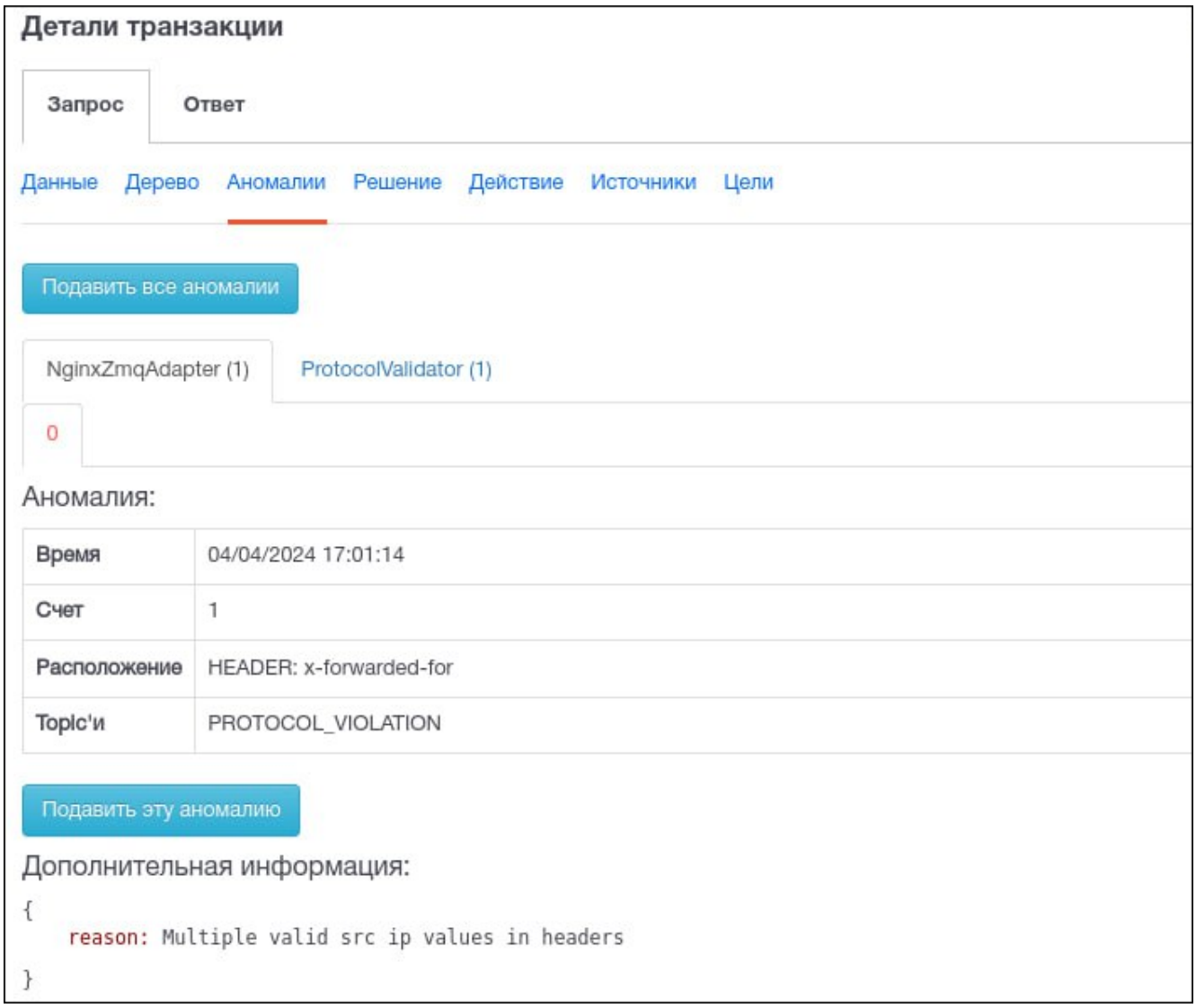

Рисунок 236 – Модуль обратного прокси

15. Внутренняя ошибка анализатора.

Внутренняя ошибка анализатора может происходить по следующим причинам:

- отключен один из модулей, которые участвуют в анализе запроса;
- некорректно прописан путь до БД;
- некорректно прописаны сигнатуры.

Подавить данные аномалии не получится. Необходимо корректировать настройки на вкладке «Настройки анализатора» (подробнее можно прочитать в разделе 17).

15.1. Пример аномалии № 1.

Данный вид аномалий сигнализирует о некорректности работы одного из модулей. В данном случае аномалия говорит о некорректной работе правила «Перебор login», которое, как видно из названия, работает благодаря модулю «Обнаружение переборных атак». Данная аномалия возникала из-за некорректности настроек данного модуля в анализаторе, а именно ошибке в пути к БД (в данном случае было написано «redis://redis.127.0.0.1:1234», когда корректно «redis://127.0.0.1:1234»).

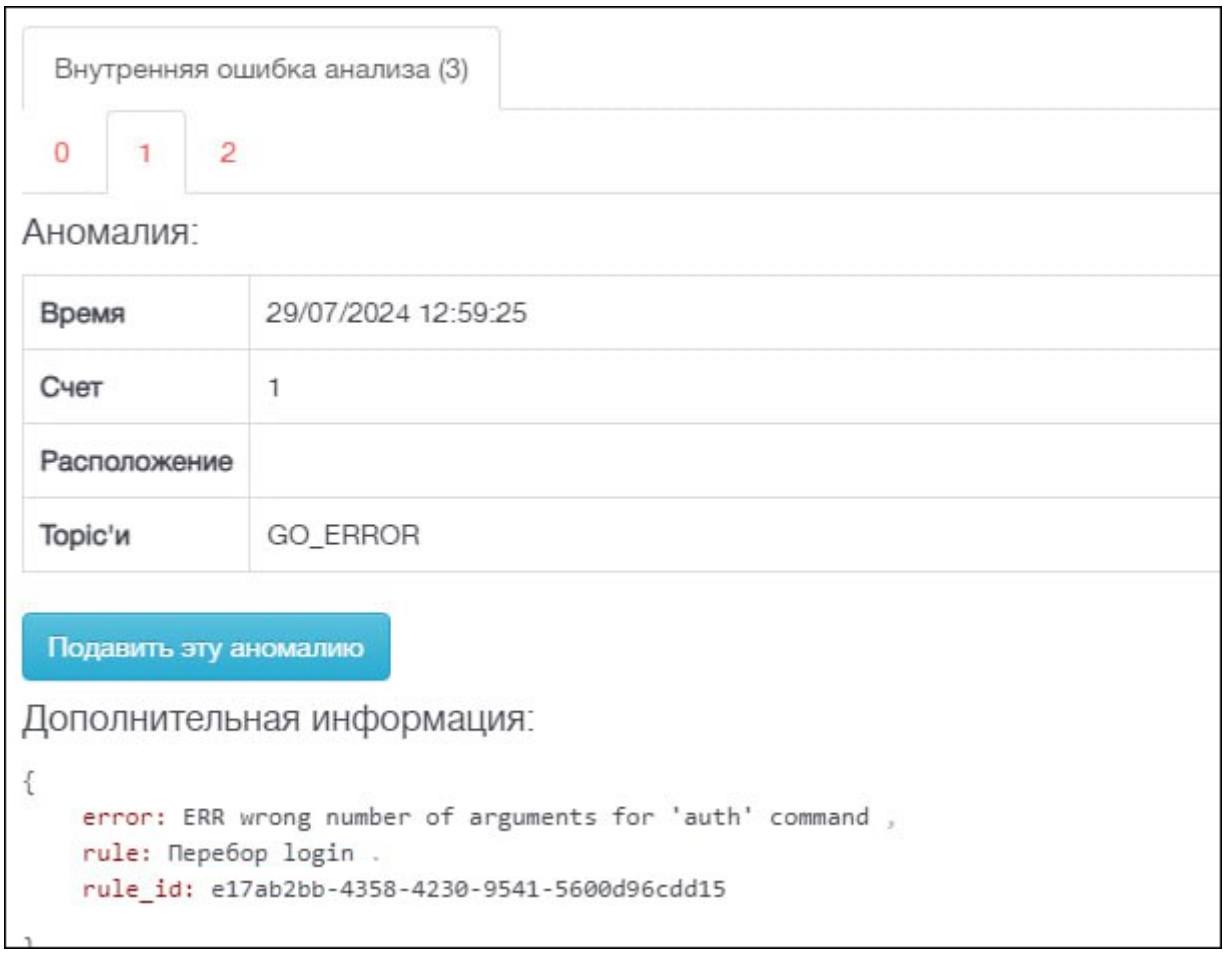

Рисунок 237 – Аномалия внутренней ошибки анализатора № 1

15.2. Пример аномалии № 2.

Ещё один пример внутренней ошибки анализатора. Данная ошибка говорит о том, что список ASN и GeoIP не загружен или работает некорректно.

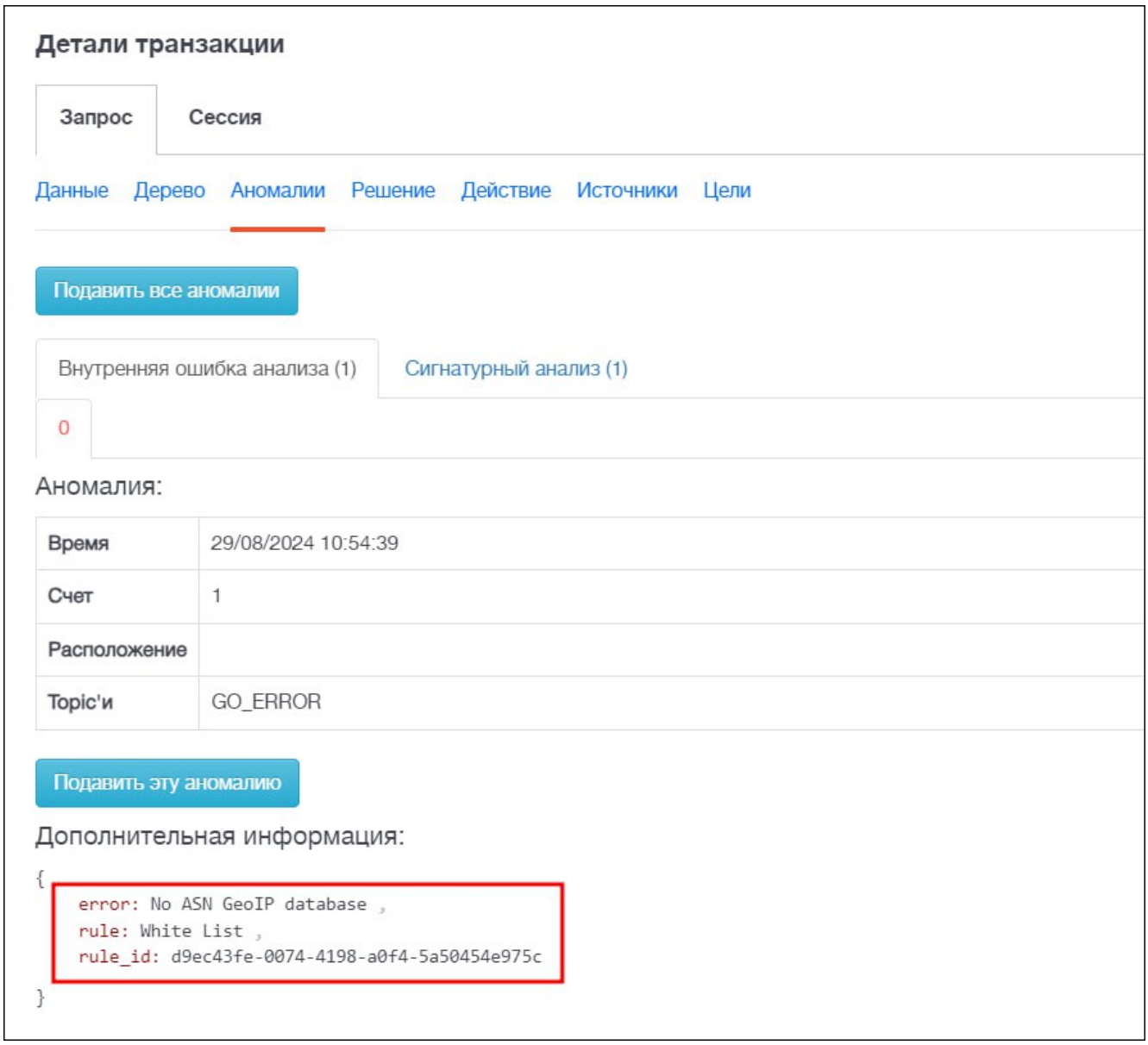

Рисунок 238 – Аномалия внутренней ошибки анализатора № 2

16. Обнаружение ботов по временным характеристикам трафика.

Аномалии от данного модуля подавлять не следует, необходимо редактировать настройки реагирования данного модуля (подробнее см. в разделе 17). Подавление данной аномалии приведет к отключению модуля в разрезе приложения и\или действия.

У данного модуля имеется всего два вида аномалий, которые отличаются местом сработки.

16.1. Обнаружение ботов в разрезе выбранного действия.

Данная аномалия возникает при настройке детектора ботов на конкретное действие. О том, что данная аномалия именно на действие, будет говорить дополнительная информация.

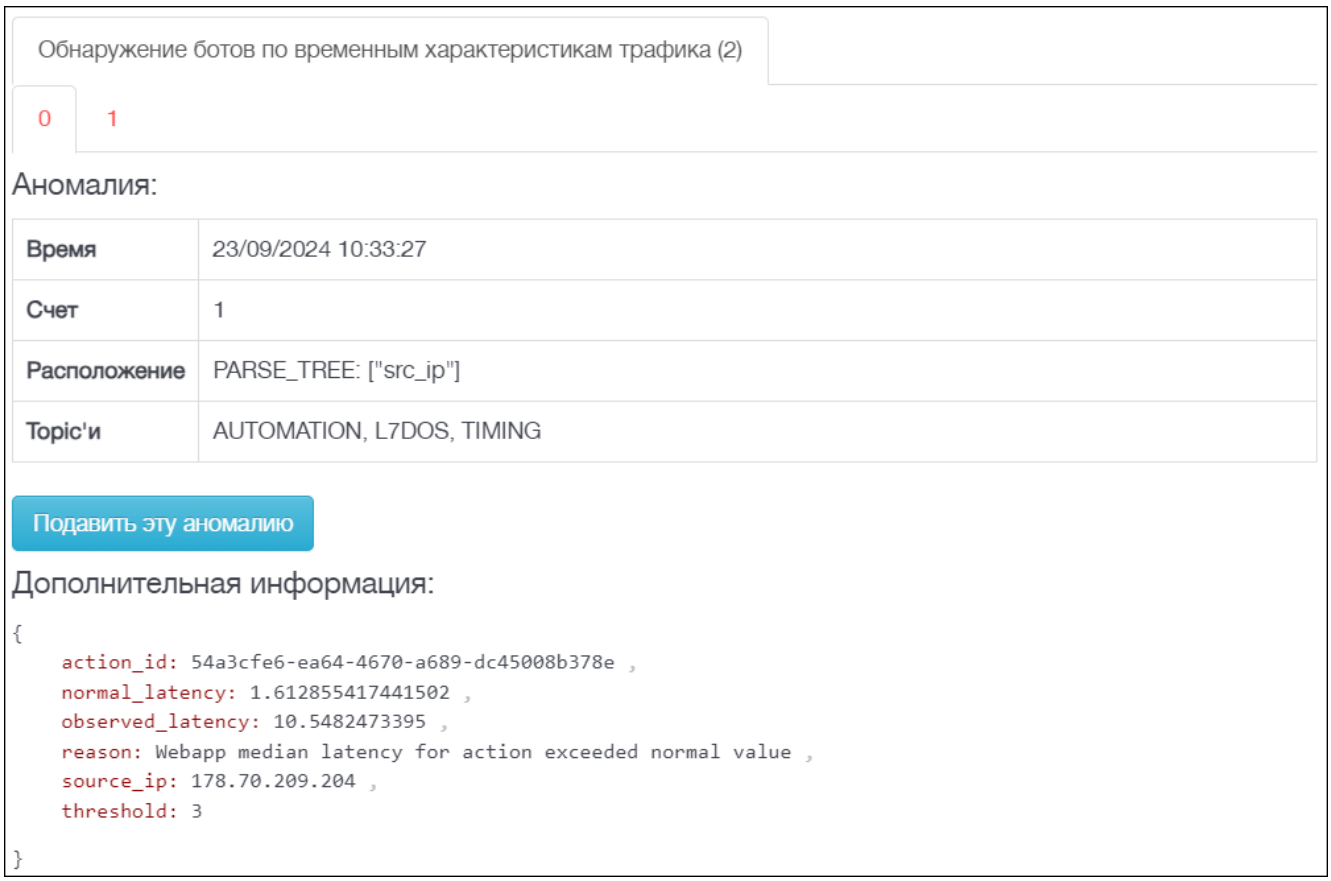

Рисунок 239 – Аномалия обнаружения ботов на выбранное действие

16.2. Обнаружение ботов в разрезе всего приложения.

Данная аномалия возникает при настройке детектора ботов на все приложение. О том, что данная аномалия именно на все приложение будет говорить дополнительная информация.

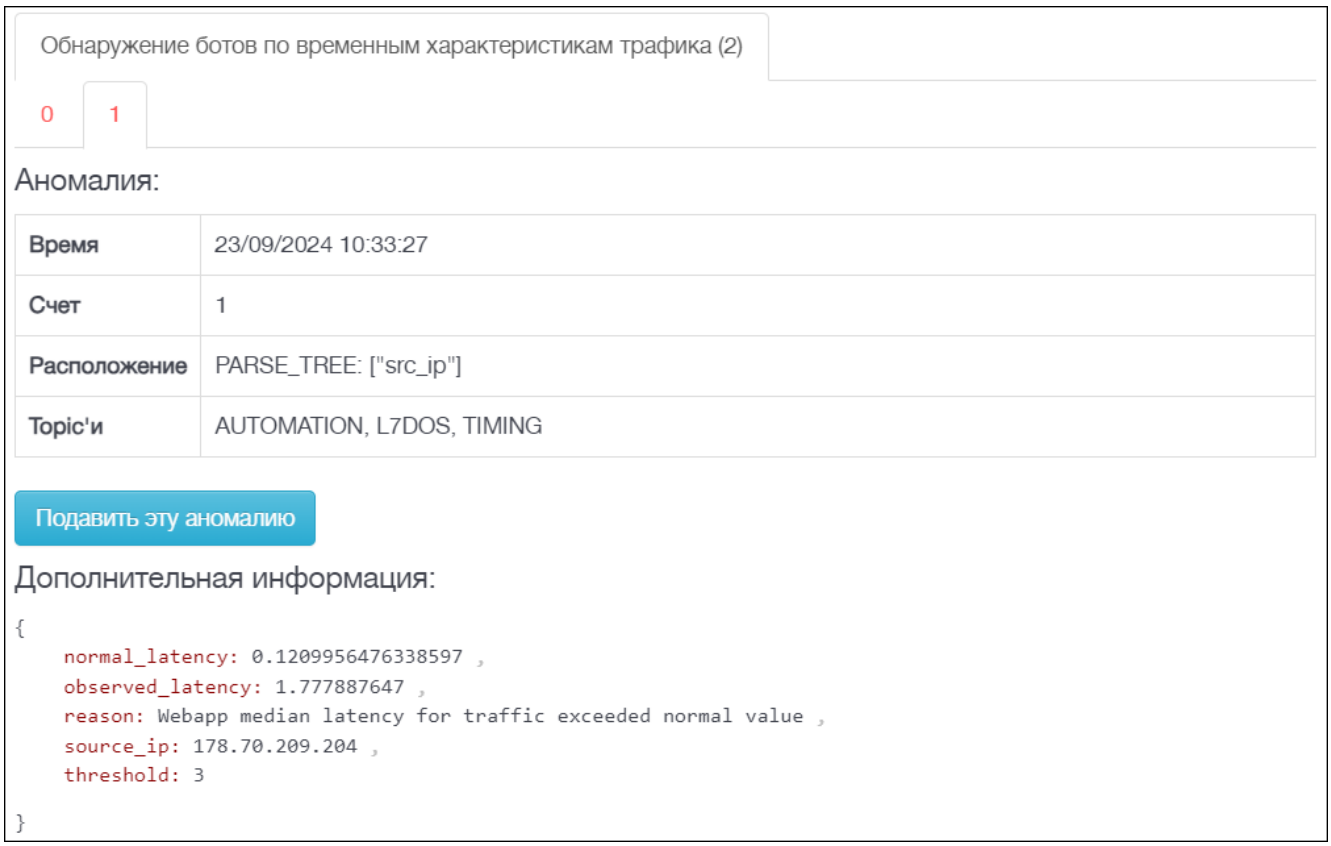

Рисунок 240 – Аномалия обнаружения ботов на всё приложение

24. Журнал

Журнал позволяет отслеживать действия пользователей WAF в веб-интерфейсе (см. рисунок 241).

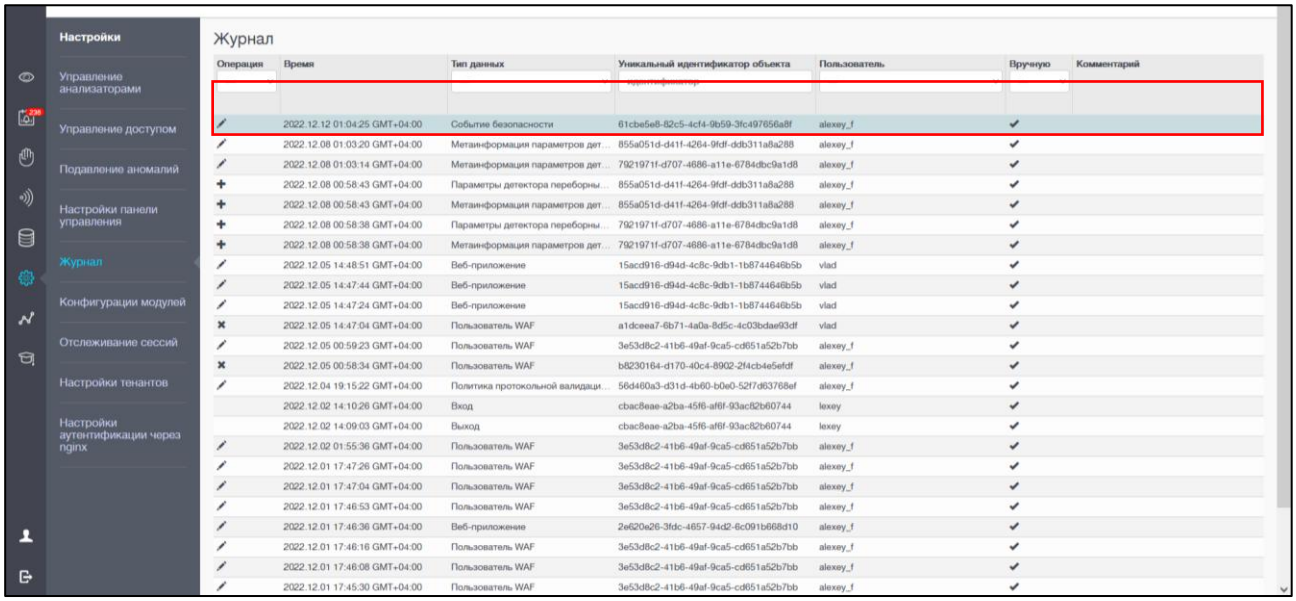

Рисунок 241 – Вкладка «Журнал»

В верхней части окна расположено поле фильтров. Описание фильтров представлено в таблице 40.

Таблица 40 – Фильтры

Фильтр	Описание
Операция	Выбор из трех возможных операций: создание, модификация, удаление
Тип данных	Выбор из предложенных типов данных, с которыми производились операции
Уникальный идентификатор объекта	У каждого объекта на WAF имеется свой уникальный идентификатор (будь то источник, список, действие и т.д.). Данное поле позволяет отфильтровать операции для просмотра операций по объекту с указанным идентификатором
Пользователь	Ввод имени пользователя, который производил операции в системе
Вручную	Операция производилась вручную пользователем или автоматически WAF

Каждую запись в журнале можно открыть, кликнув на нее левой кнопкой мыши для того, чтобы просмотреть внесенные изменения данной операцией (см. рисунок 242).

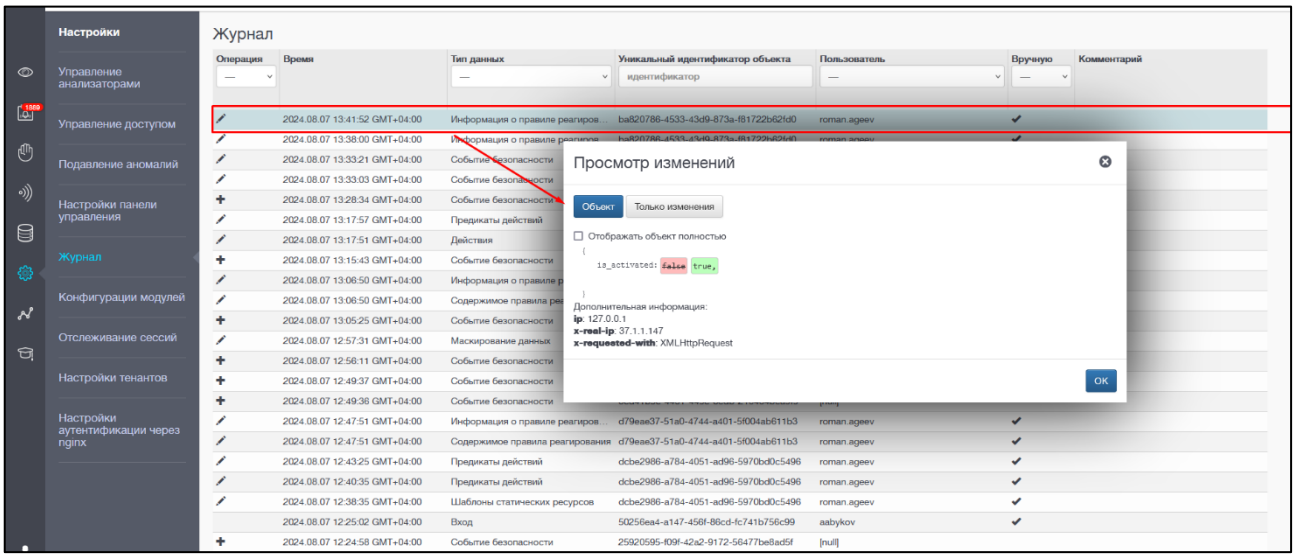

Рисунок 242 – Просмотр изменений

Изменение можно просмотреть полностью для этого необходимо нажать левой кнопкой мыши на квадрат возле текста «Отображать объект полностью».

25. Примеры работы

25.1. Настройка детекторов переборных атак

Разберём настройку детекторов переборных атак на примере настройки правила, которое ограничивает число попыток ввода учетных данных для формы ввода логина\пароля на приложении (см. рисунок 243).

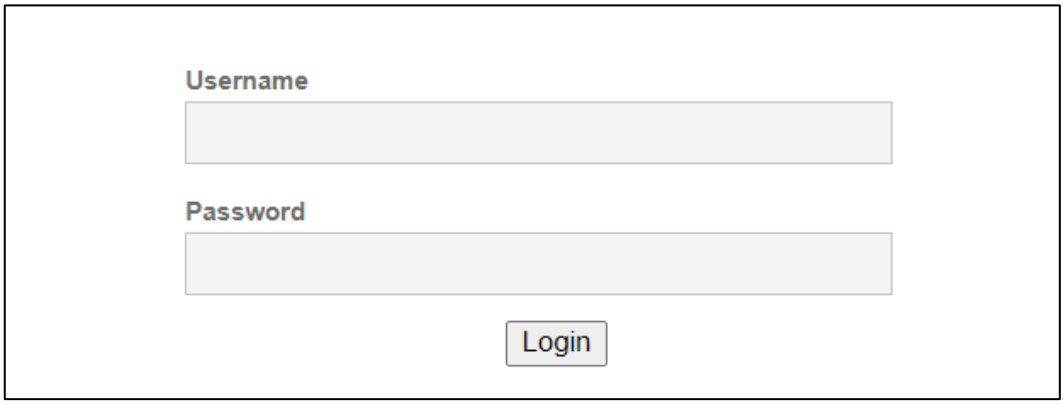

Рисунок 243 – Форма ввода логина/пароля

Для этого нужно:

1. Создать действие на форму ввода логина/пароля (создание действий описано в разделе 15). Пример созданного действия для формы ввода пароля (см. рисунок 243) показан на рисунке 244.

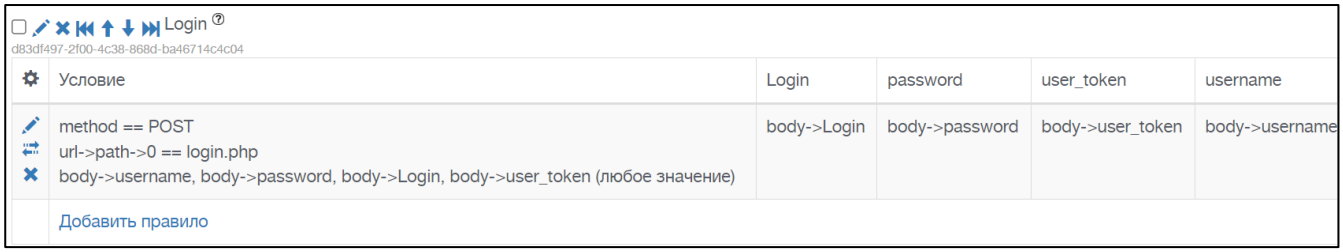

Рисунок 244 – Созданное действие для формы ввода логина/пароля

2. Создать источник, в рамках которого будет считаться перебор значений (создание источника описано в разделе 13). При настройке данного детектора переборных атак будет использован коробочный источник «src_ip», т.е. мы будем считать количество обращений от отдельных элементов источника к выбранному действию. В качестве источника в детекторе переборных атак может быть использован любой элемент дерева разбора запроса.
3. Настроить детектор переборных атак «Действие\Источник» (Создание детектора переборных атак Действие\Источник описано в разделе 16.1). При настройке детектора переборных атак «Действие\Источник» стоит учитывать его особенность, а именно возможность задать скорость истечения маркеров из ведра. Если провести аналогию настройки детектора переборных атак с задачей выше, то получается при равномерном распределении запросов во времени верно следующее выражение:

$$\text{Количество маркеров в секунду} = \text{Приток} - \text{Отток}$$

Где:

- Количество маркеров в секунду – количество маркеров, которое кладется в ведро в секунду;

- Приток – число маркеров, добавляемых в ведро при каждом запросе, умноженное на количество запросов в секунду (RPS атаки);
- Отток – скорость истечения маркеров из ведра, единиц в секунду.

Тогда получается, чтобы посчитать на какой секунде будет заблокирована транзакция (наступит время блокировки) можно воспользоваться следующим выражением:

$$\text{Время блокировки} = \frac{60}{\text{Количество маркеров в секунду}}$$

Например, если необходимо настроить детектор переборных атак на 20 RPM (20 запросов за минуту), т.е. если пользователь отправит более 20 запросов на авторизацию, то следующий подобный запрос будет заблокирован детектором переборных атак. Для того чтобы рассчитать количество маркеров в секунду для этих показателей - разделим 60 на желаемое время блокировки в секундах (60 сек). Получим, что количество маркеров, которое кладется в ведро в секунду для данного случая должно равняться 1. Тогда из формулы для расчета количества маркеров в секунду мы получим, что «Приток – Отток» у нас должны равняться 1. Дальше стоит учитывать, что чем больше отток, тем меньше вероятность затронуть легитимный трафик. Например, на рисунках 245 и 246 представлены графики зависимости количества маркеров в ведре от времени для разбираемого примера. Красным на графике показана заполняемость ведра при атаке в 0,34 RPS (приблизительно 20 RPM), а зеленым показана заполняемость ведра при обычном трафике в 0,3 RPS (18 RPM), описанные данные действительны для обоих рисунков. Для рисунка 245 скорость истечения маркеров из ведра равна 1, а число маркеров, добавляемых в ведро при каждом запросе равно 6. При такой настройке атакующий будет заблокирован на 60 секунде, а легитимный пользователь на 79.

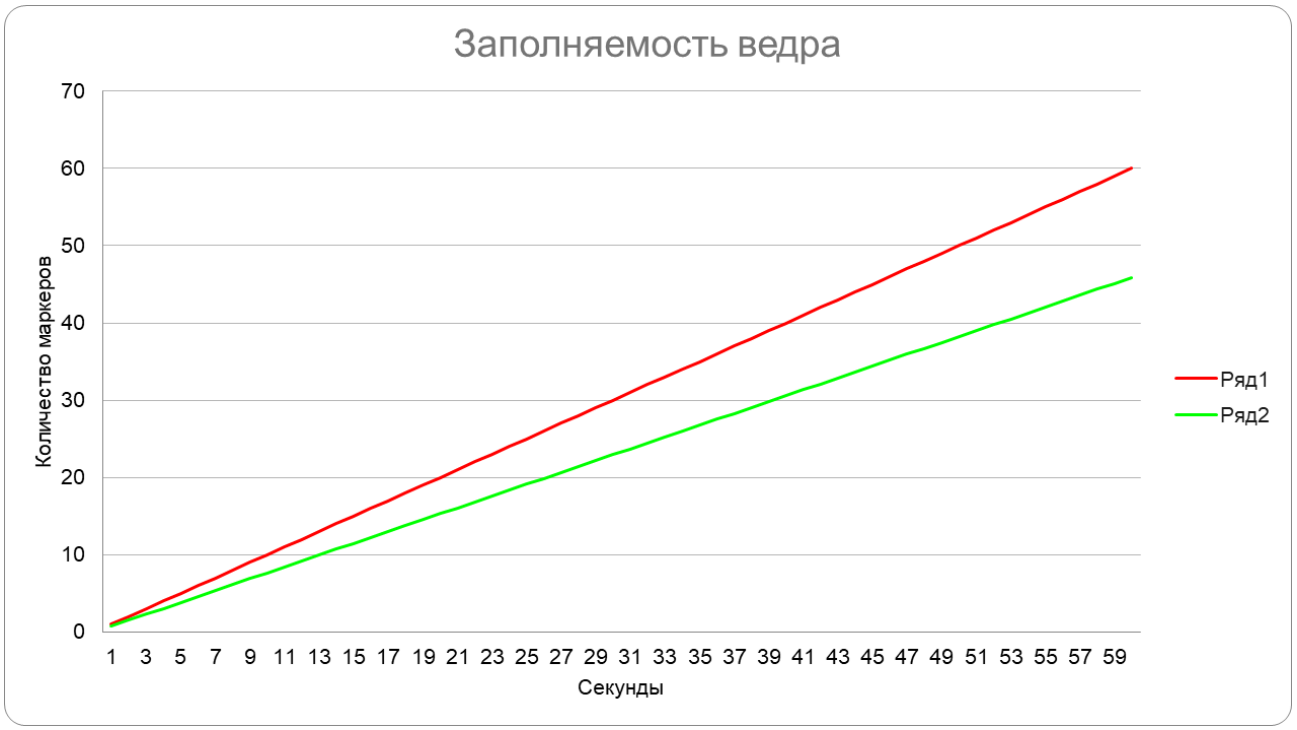

Рисунок 245 – Заполняемость ведра

Но если мы примем скорость истечения маркеров из ведра равной 6, а число маркеров, добавляемых в ведро при каждом запросе равным 20,5, то при такой настройке атакующий также будет заблокирован на 60 секунде, а легитимный пользователь уже на 340 (см. рисунок 246).

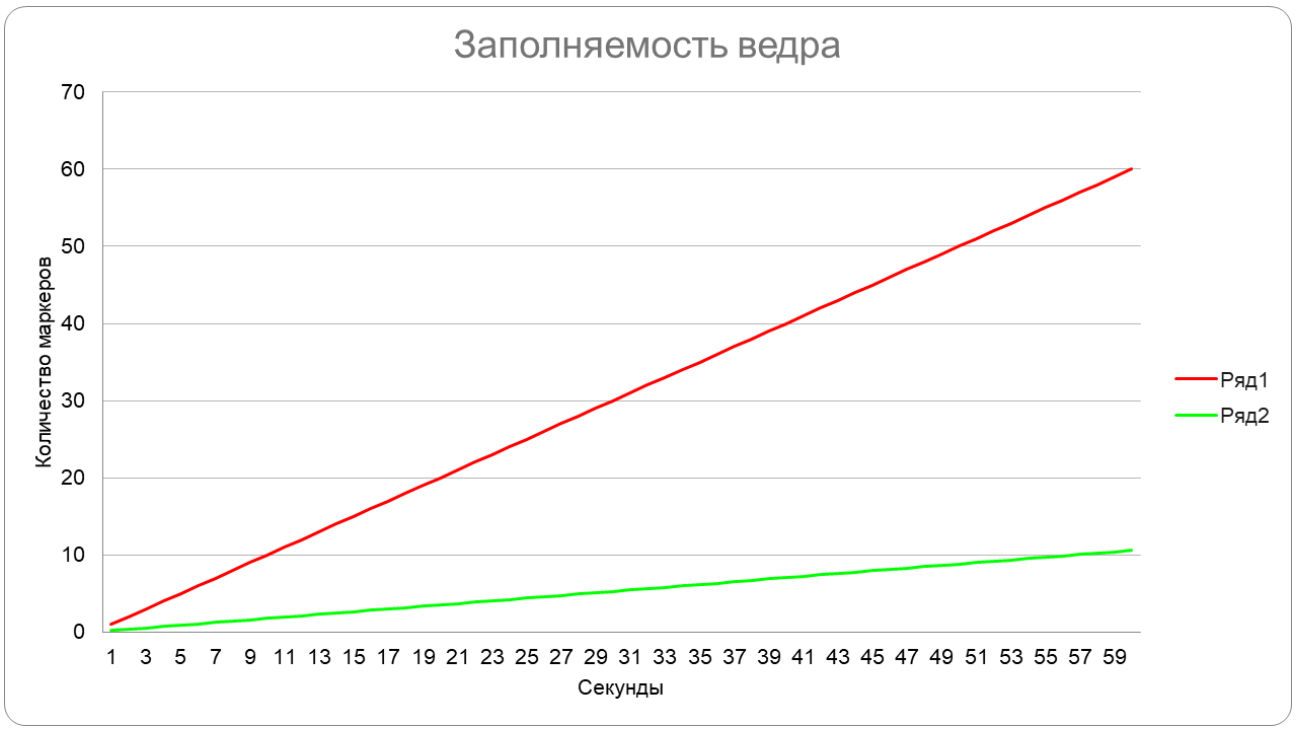

Рисунок 246 – Заполняемость ведра

Примечание: в реальных условиях равномерное распределение запросов может быть достигнуто только с использованием средств автоматизации. Поэтому в данных расчетах в качестве RPM стоит использовать не среднее значение количества запросов в секунду, а медиану. Если нет возможности подсчета медианы, то можно увеличить RPM на 25%, чтобы избежать преждевременной блокировки из-за неравномерности распределения запросов пользователей.

Ручная настройка параметров для детектора переборных атак для 20 RPM показана на рисунке 247.

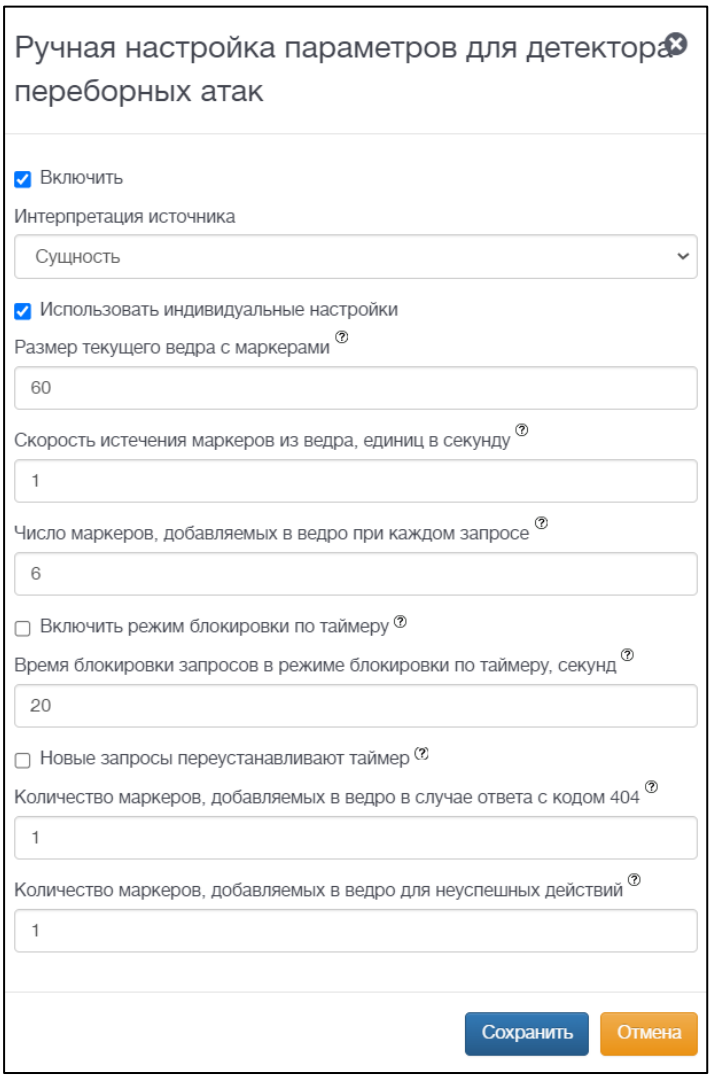

Рисунок 247 – Ручная настройка параметров для детектора переборных атак

4. Создать правило (создание правил описано в разделе 21), в результате работы которого будут блокироваться запросы в зависимости от настройки параметров для детектора переборных атак. Настройка аномалии для детектора переборных атак показана на рисунке 248.

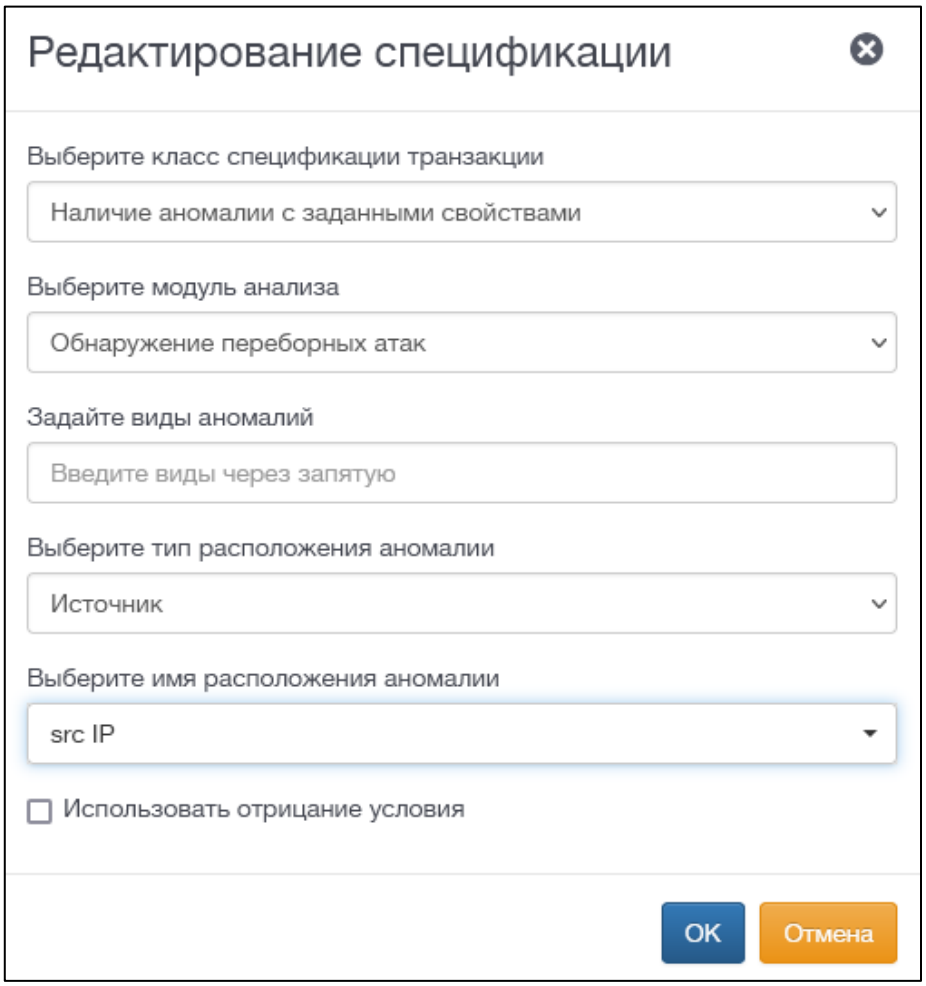

Рисунок 248 – Настройка аномалии правила для обнаружения переборных атак

Для правила необходимо выбрать цель – проверка веб-приложения, а также само защищаемое приложение (см. рисунок 249).

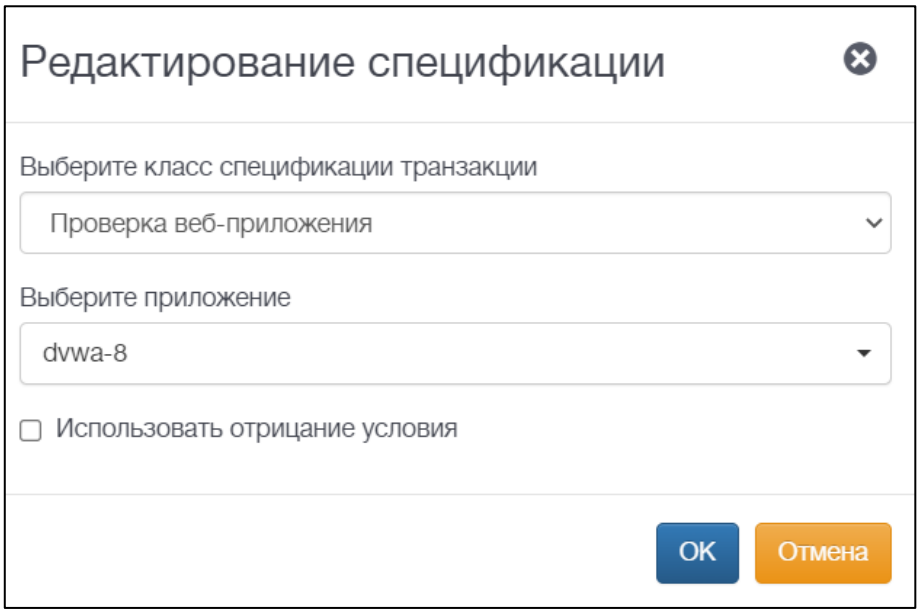

Рисунок 249 – Цель с классом спецификации проверка веб-приложения

Выбрать действие, для которого создавался детектор переборных атак (см. рисунок 250).

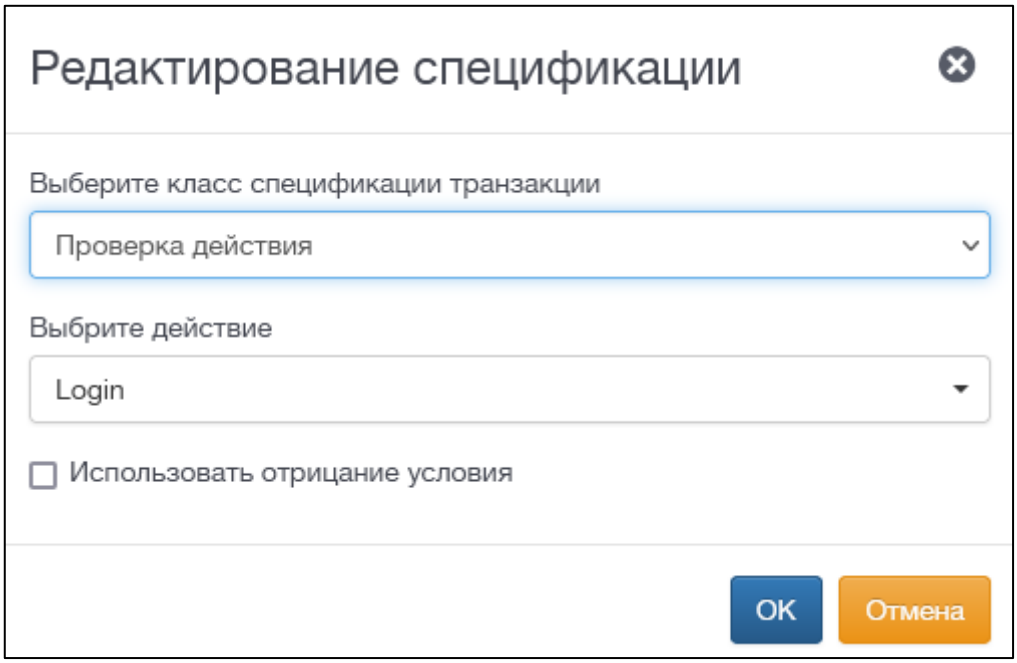

Рисунок 250 – Выбор действия

В редактировании действия для правила необходимо выбрать действие блокировки транзакции (см. рисунок 251).

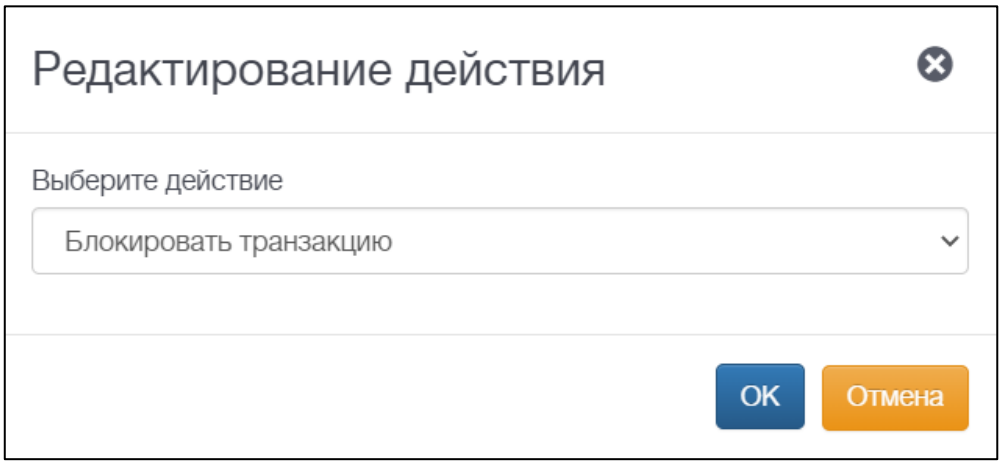

Рисунок 251 – Редактирование действия для правила

Настроенное правило для блокировки запросов с перебором формы авторизации показано на рисунке 252.

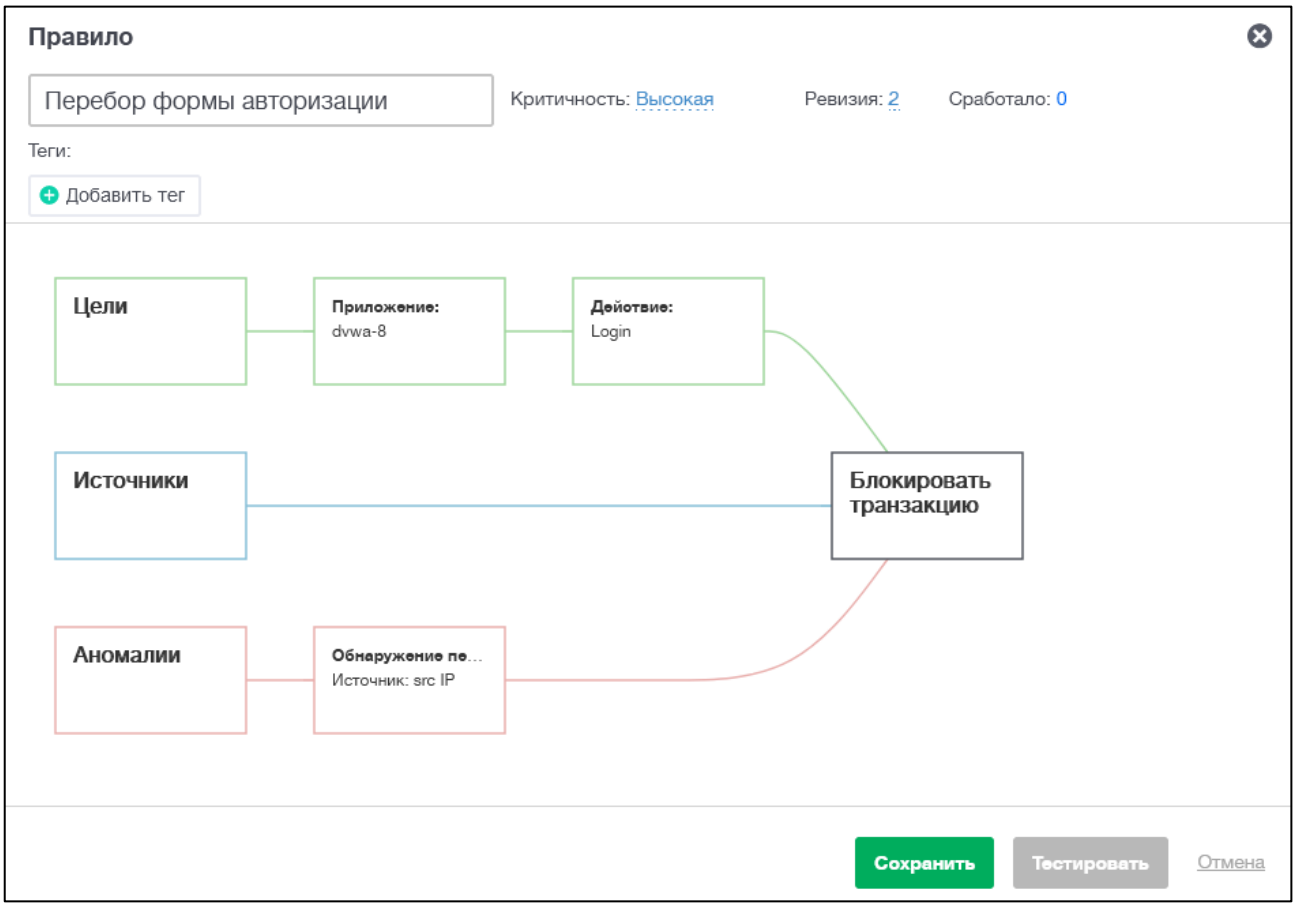

Рисунок 252 – Настройка правила на блокировку перебора формы авторизации

25.2. Настройка детекторов переборных атак «Действие\Источник\Цель»

Для примера настройки детекторов переборных атак «Действие\Источник/Цель» используем настроенное в разделе 25.1 правило, которое блокирует переборы поля логина для формы ввода логина\пароля на приложении (см. рисунок 243) с одного IP адреса.

Для этого нужно:

1. Создать действие на форму ввода логина/пароля (создание действий описано в разделе 15). Созданное действие для формы ввода пароля показано на рисунке 244.
2. Создать цель на поле логина/пароля (создание цели описано в разделе 14). Созданная цель для поля ввода логина показана на 253.

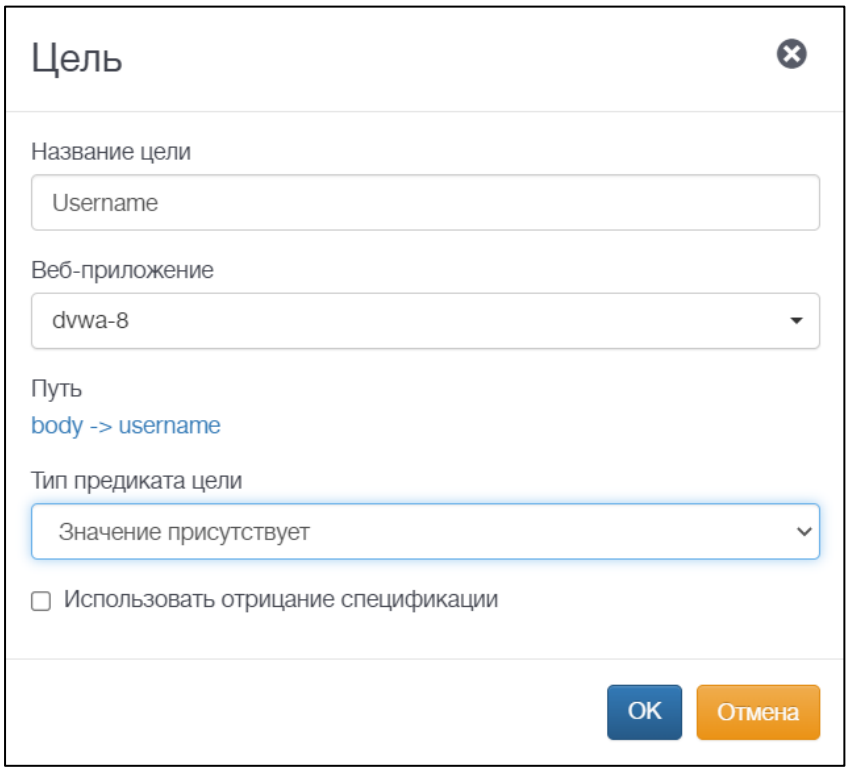

Рисунок 253 – Настройка цели для поля Username

3. Создать источник на поле IP-адреса (создание источника описано в разделе 13). Созданный источник для поля «src_ip» показан на 254.

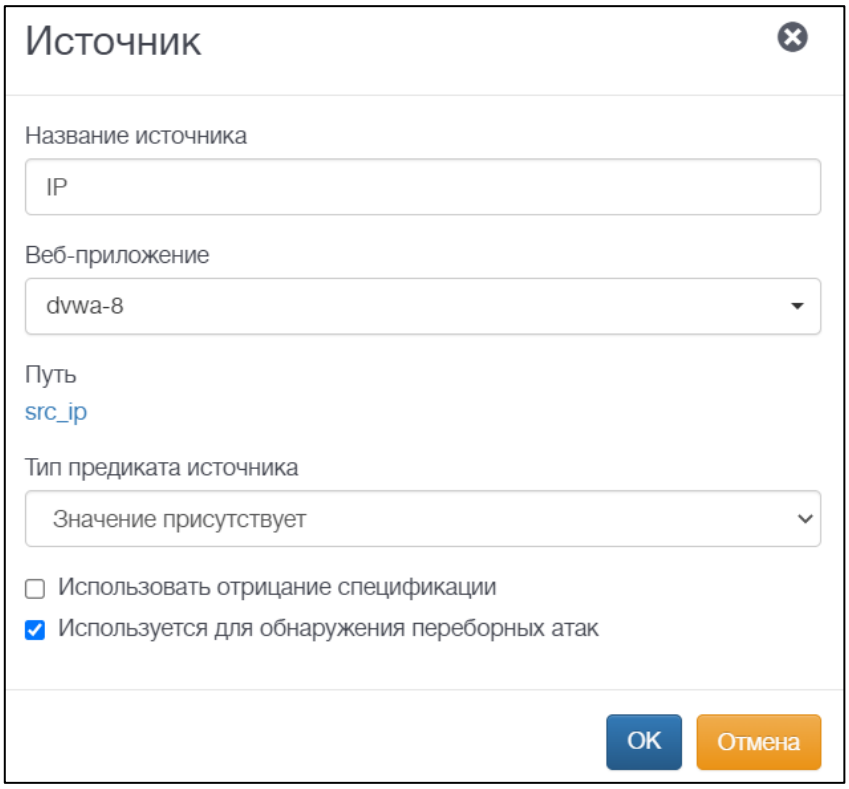

Рисунок 254 – Источник на поле «src_ip»

4. Создать детектор переборных атак «Действие\Источник\Цель» (создание детектора переборных атак «Действие\Источник» описано в разделе 16.1**Ошибка! Источник ссылки не найден.**). Далее н еобходимо настроить детектор переборных атак на 5 RPM (5 запросов за минуту), т.е. если пользователь вводит более 5 разных значений username для формы логина с одного IP-адреса, то следующий подобный запрос будет заблокирован детектором переборных атак. Ручная настройка параметров для детектора переборных атак для 5 RPM показана на рисунок 255.

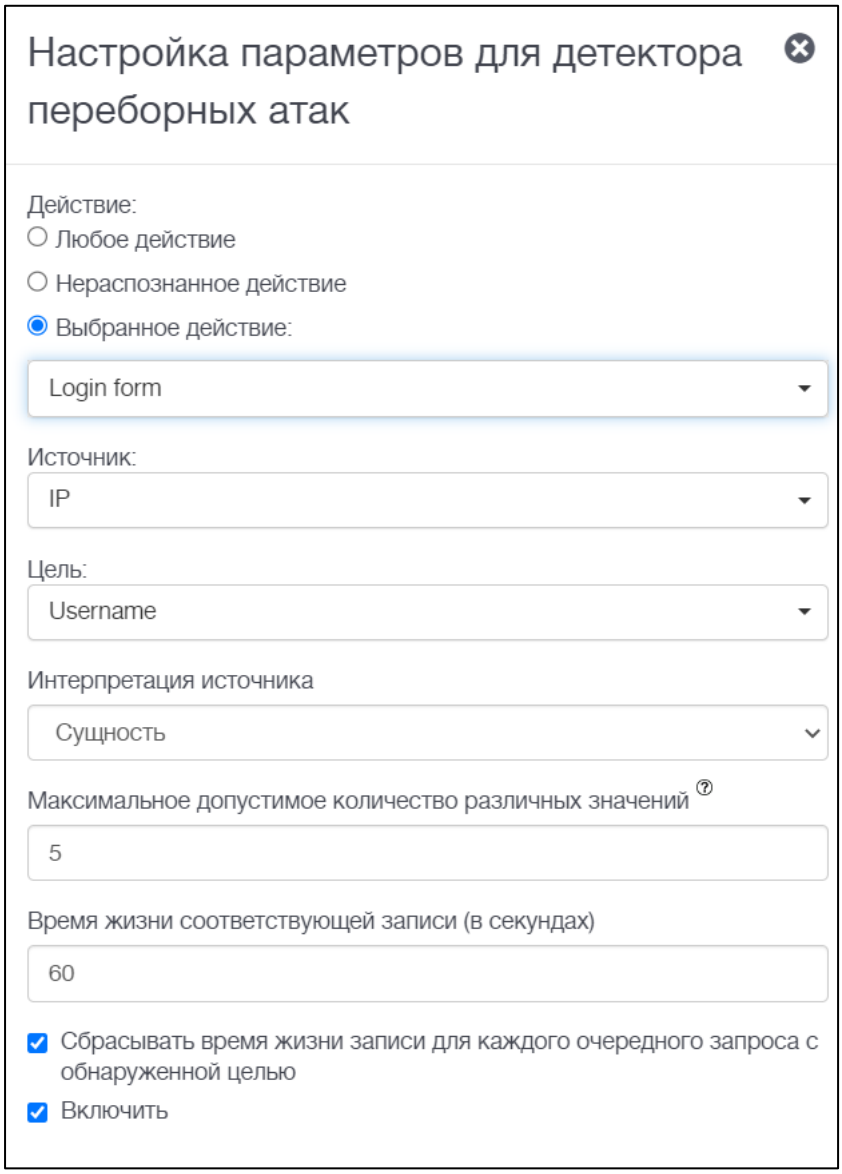

Рисунок 255 – Ручная настройка параметров для детектора переборных атак

5. Создать правило (создание правил описано в разделе 21), в результате работы которого будут блокироваться запросы в зависимости от настройки параметров для детектора переборных атак. Настройка аномалии для детектора переборных атак показана на рисунке 256.

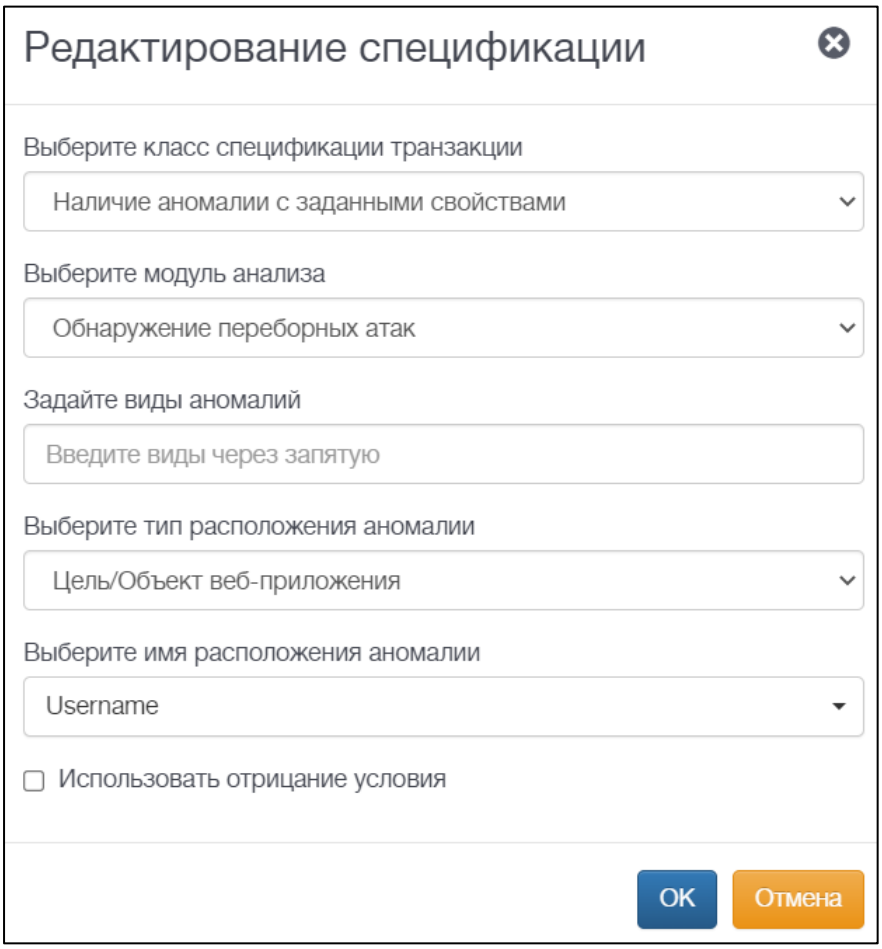

Рисунок 256 – Настройка аномалии правила для обнаружения переборных атак

Для правила необходимо выбрать цель - проверка веб-приложения, а также само защищаемое приложение (см. рисунок 257).

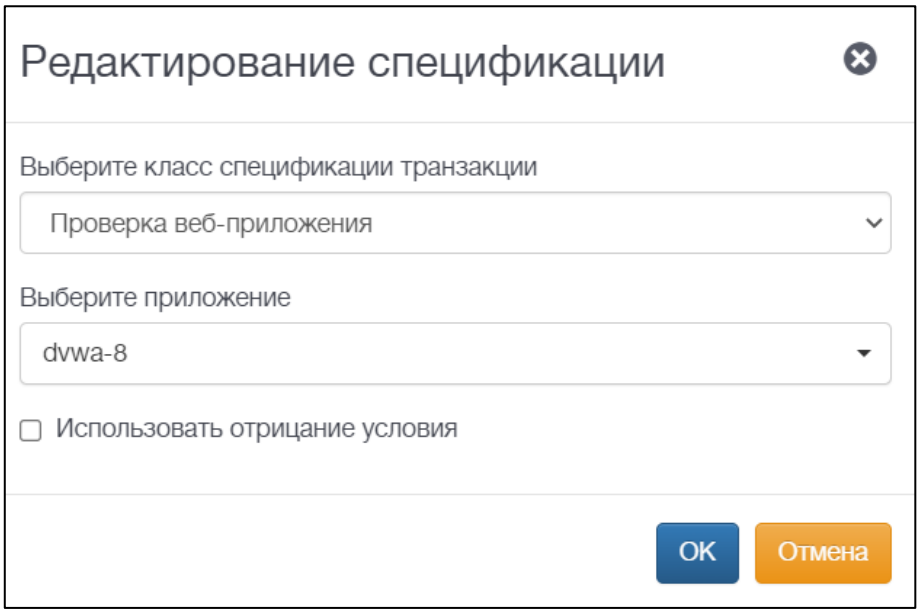

Рисунок 257 – Цель с классом спецификации проверка веб-приложения

В редактировании действия для правила необходимо выбрать действие блокировки транзакции (см. рисунок 258).

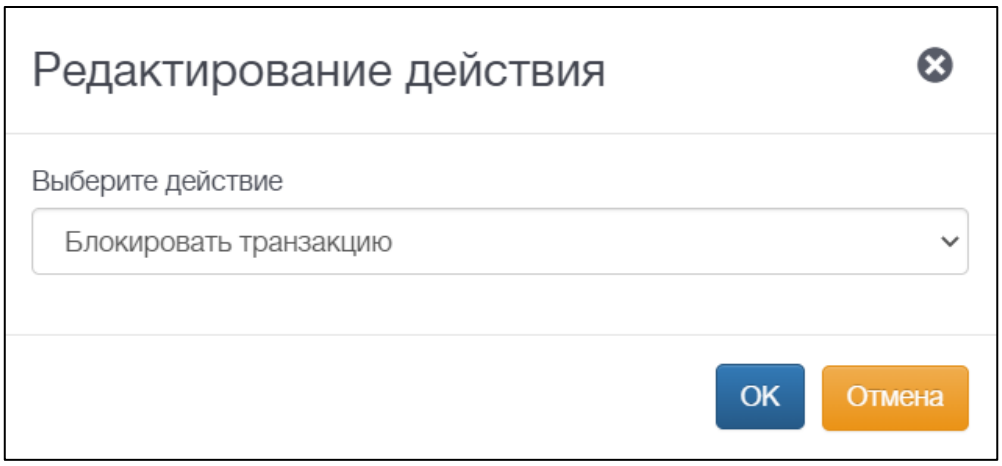

Рисунок 258 – Редактирование действия для правила

Настроенное правило для блокировки запросов с перебором формы логина показано на рисунке 259.

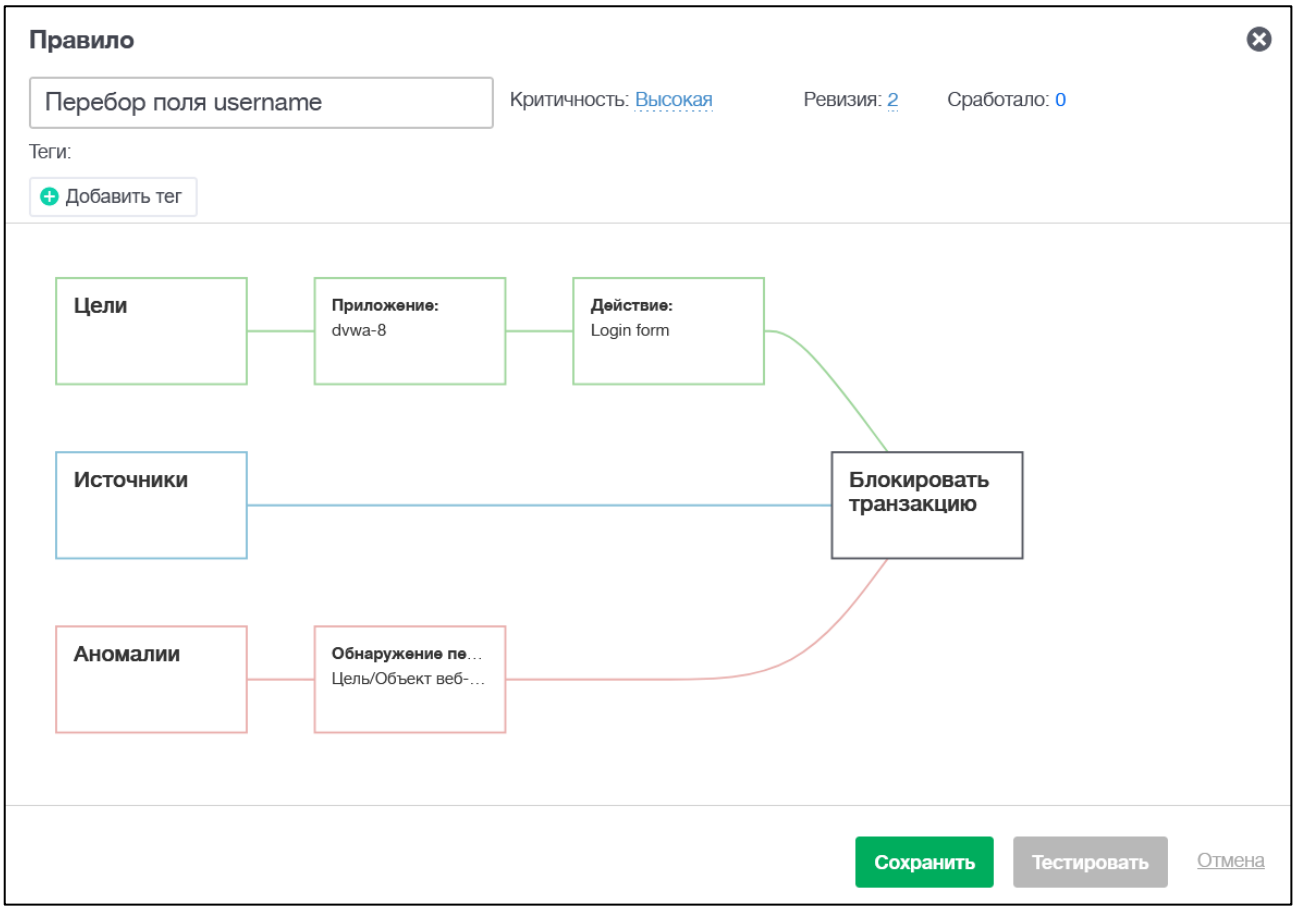

Рисунок 259 – Настройка правила на блокировку перебора поля username с одного IP

25.3. Разбор элементов дерева разбора

Рассмотрим разбор элементов дерева разбора на примере разбора заголовка authorization (разбор дерева запросов подробно описан в разделе 10). Подобный запрос можно отправить следующим образом:

```
curl                                    waf_ip                                  -
d'authorization=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3
ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4
fwpMeJf36POk6yJV_adQssw5c'  -H"x-real-ip:8.8.8.8"  -H"referer:http://dvwa"
-H"host:dvwa"
```

Отправленный запрос показан на рисунке 260.

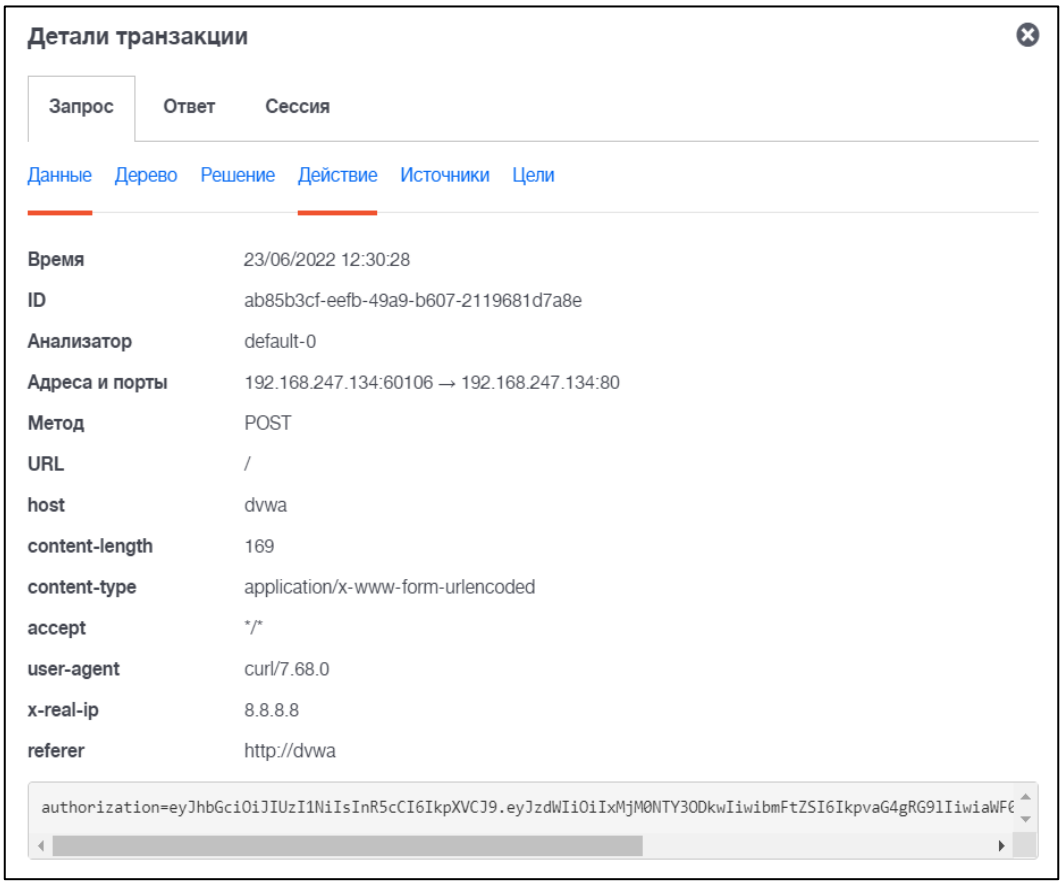

Рисунок 260 – Запрос с полем Authorization

Для разбора поля authorization необходимо:

1. Перейти на вкладку «Приложения» -> «Запросы» (см. рисунок 261).

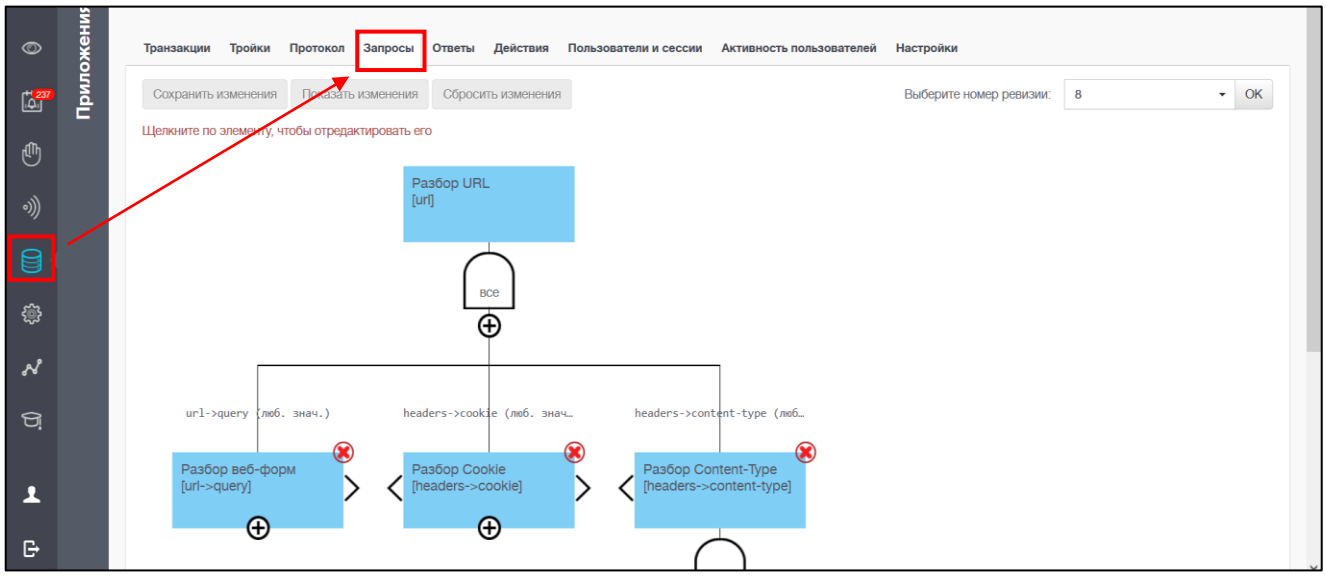

Рисунок 261 – Окно «Запросы»

2. Для того чтобы углубить дерево разбора необходимо нажать на иконку «⊕» в той части, где необходимо дополнить дерево разбора - в данном случае к блоку «Разбор URL». Настройки данного блока показана на рисунок 262.

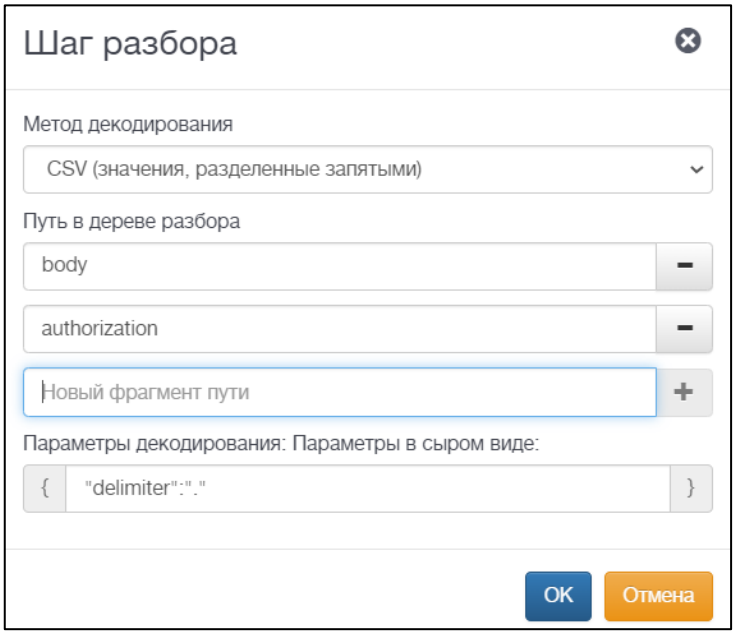

Рисунок 262 – Окно «Шаг разбора»

3. Далее декодируем первую часть запроса при помощи Base64 декодера. Его настройки можно увидеть на рисунке 263.

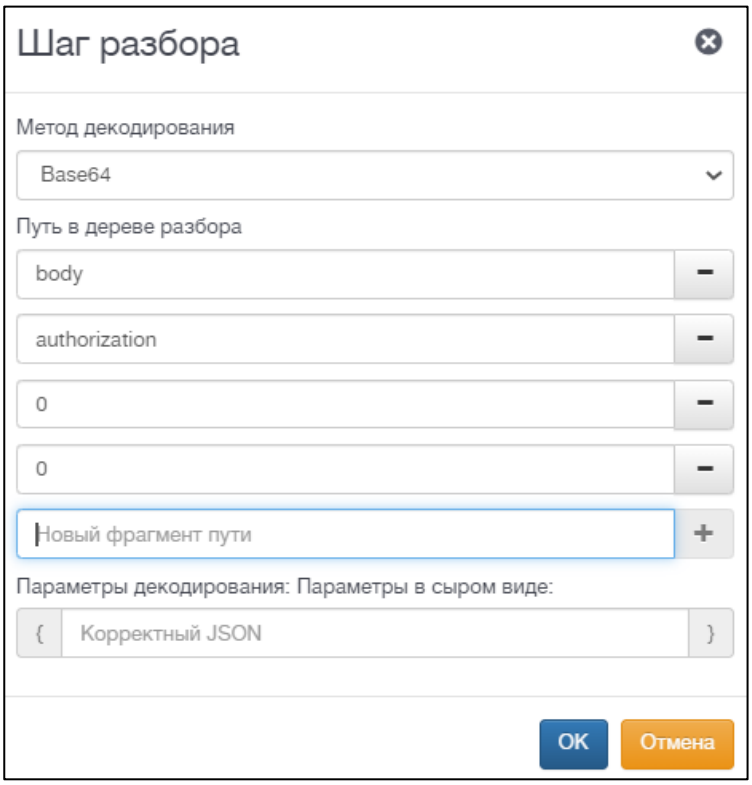

Рисунок 263 – Настройка блока разбора запроса

4. Декодированное значение дополнительно разбираем с помощью метода декодирования JSON (см. рисунок 264).

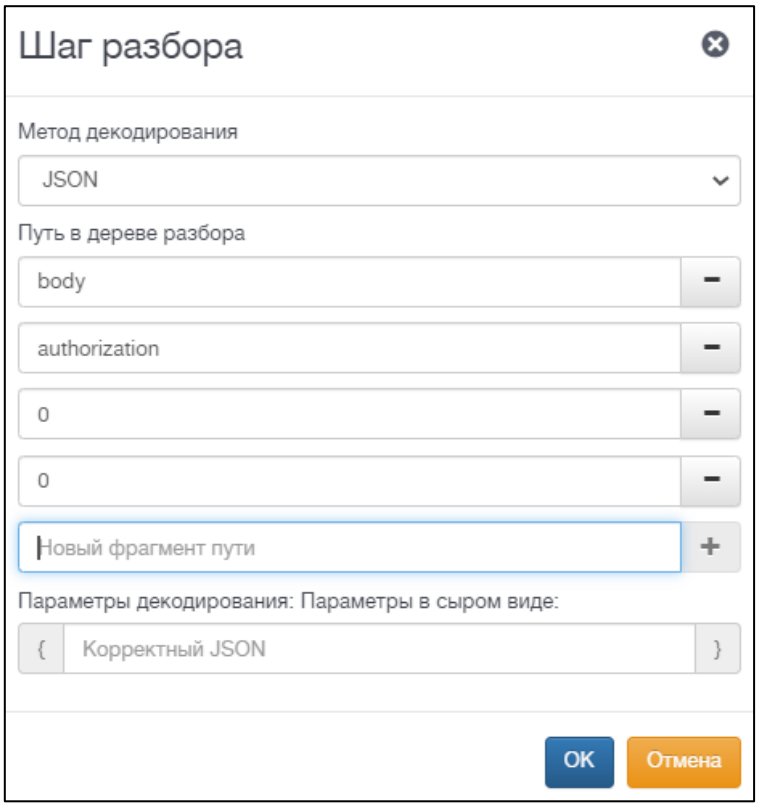

Рисунок 264 – Настройка блока разбора запроса

5. Пункты 3 и 4 повторяются для второго блока. В результате модель разбора данных запроса будет выглядеть как на рисунке 265.

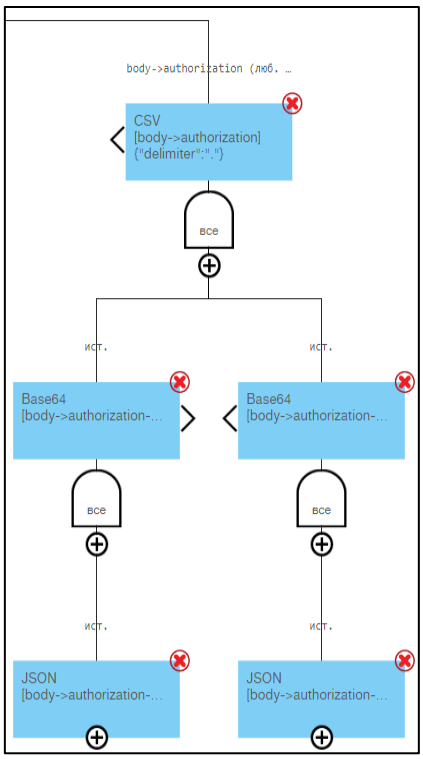

Рисунок 265 – Дерево разбора данных для запроса с jwt-токеном

В результате в дереве разбора будет разобран jwt-токен и отобразится раскодированное из Base64 значение параметров (см. рисунок 266).

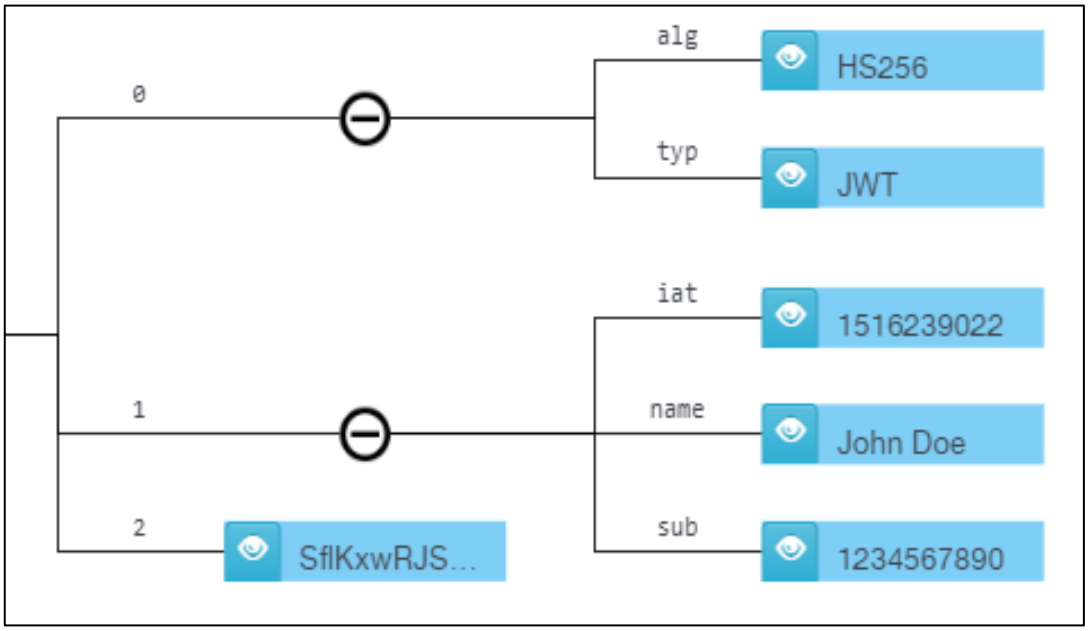

Рисунок 266 – Дерево разбора для запроса с jwt токеном

25.4. Блокировка запросов по геолокации

Для блокировки запросов по геолокации необходимо:

1. Создать правило (создание правил описано в разделе 21), где источник имеет класс спецификации транзакции «Проверка страны пользователя» (см. рисунок 267). В разделе редактирования спецификации также необходимо указать страну, транзакции которой будут блокироваться соответствующим правилом. Также есть возможность использовать отрицание условия. В данном примере стоит цель блокировать все запросы не из России, поэтому следует использовать отрицание условия.

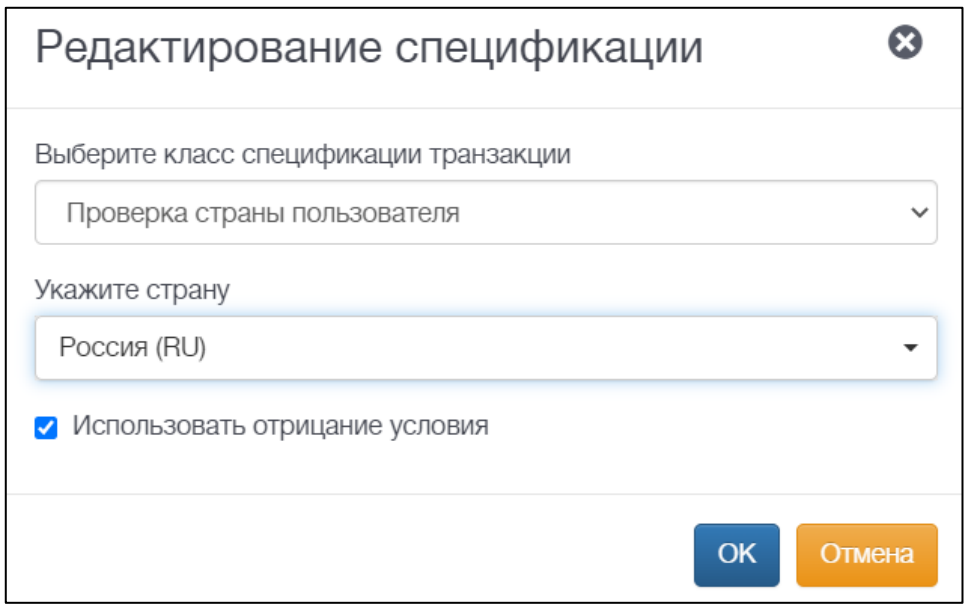

Рисунок 267 – Источник с классом спецификации проверка страны пользователя

2. Для правила необходимо выбрать цель - проверка веб-приложения, а также само защищаемое приложение (см. рисунок 268).

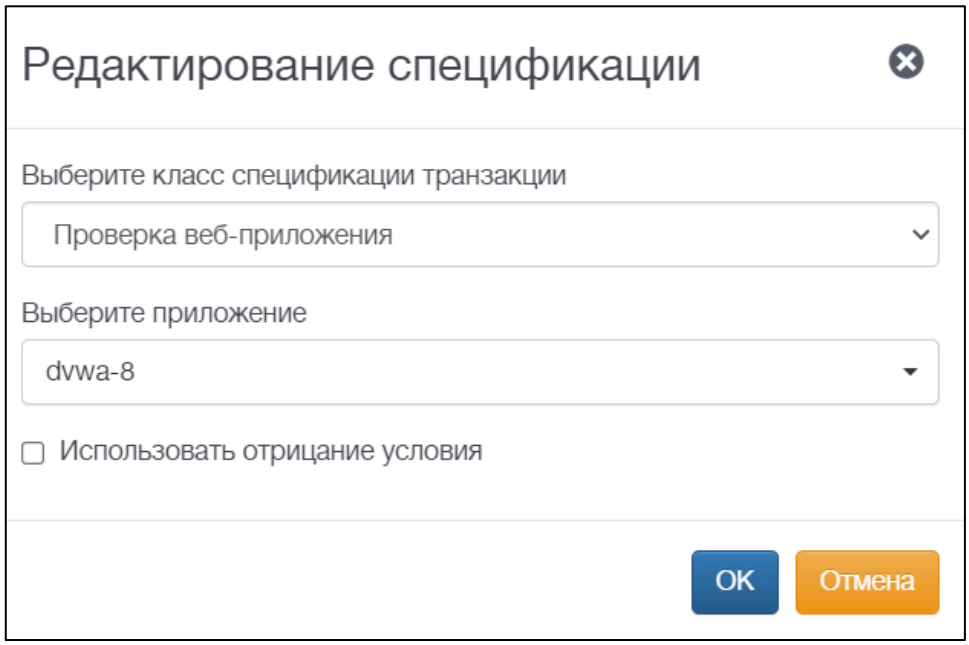

Рисунок 268 – Цель с классом спецификации проверка веб-приложения

3. В редактировании действия для правила необходимо выбрать действие блокировки транзакции (см. рисунок 269).

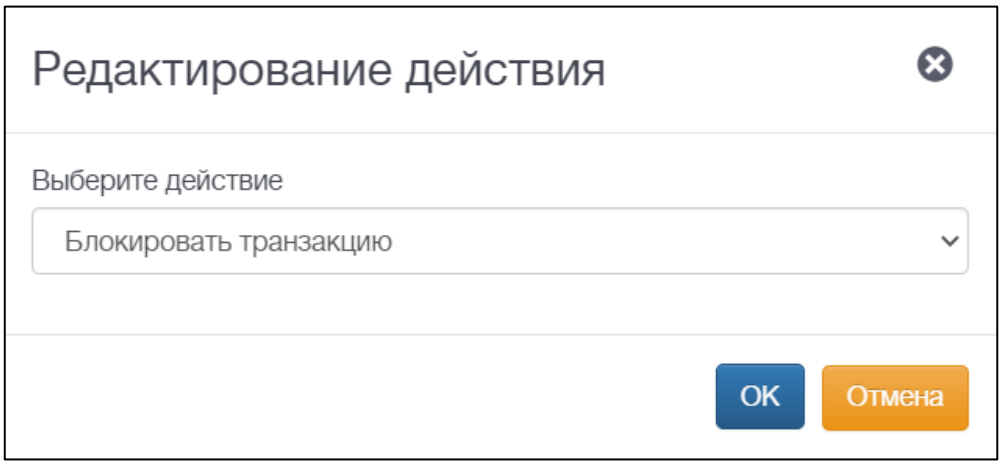

Рисунок 269 – Редактирование действия для правила

Настроенное правило для блокировки запросов не из России показано на рисунке 270.

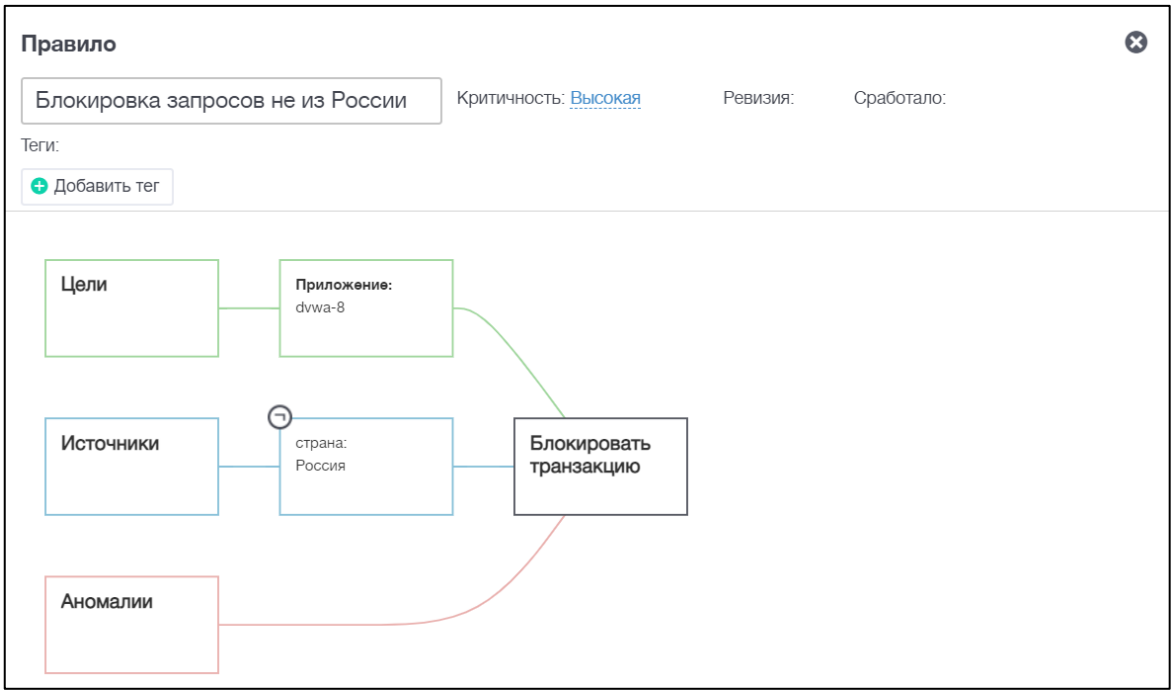

Рисунок 270 – Правило для блокировки запросов не из России

25.5. Включение\выключение правил

Для некоторых приложений бывает необходимым выключать некоторые правила, т.к. их работа приводит к множеству ложных сработок. Например, приложение не может содержать в себе признаки CSRF-атаки, но запросы всё равно блокируются детектором CSRF-атак. В этом случае будет правильным выключить данное правило для приложения. Для этого необходимо перейти в раздел «Правила», найти нужное правило и передвинуть переключатель в правом верхнем углу блока правила (см. рисунок 271).

Для включения правила необходимо повторить те же действия для выключенного правила.

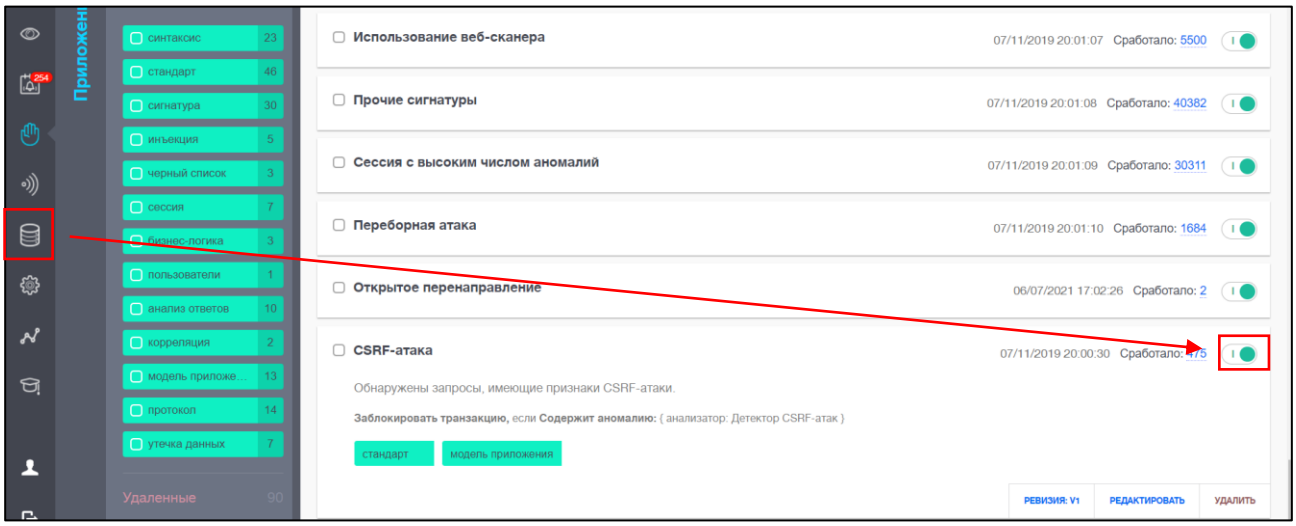

Рисунок 271 – Механизм включения\выключения правила

25.6. Настройка параметров действия

В качестве примера разберём настройку параметров действия для формы ввода ID пользователя на приложении (см. рисунок 272). В данное поле вводятся различные значения ID пользователя, т.е. значение этого поля может быть только целым числом.

Рисунок 272 – Форма ввода ID пользователя

Для настройки параметров действия необходимо:

1. Создать действие на форму ввода ID пользователя (создание действий описано в разделе 15). Для редактирования параметров действия необходимо нажать на «✎» в верхнем левом углу созданного действия (см. рисунок 273).

Рисунок 273 – Редактор параметров действия

2. Перейти в настройки параметров действия для поля ID (см. рисунок 274).

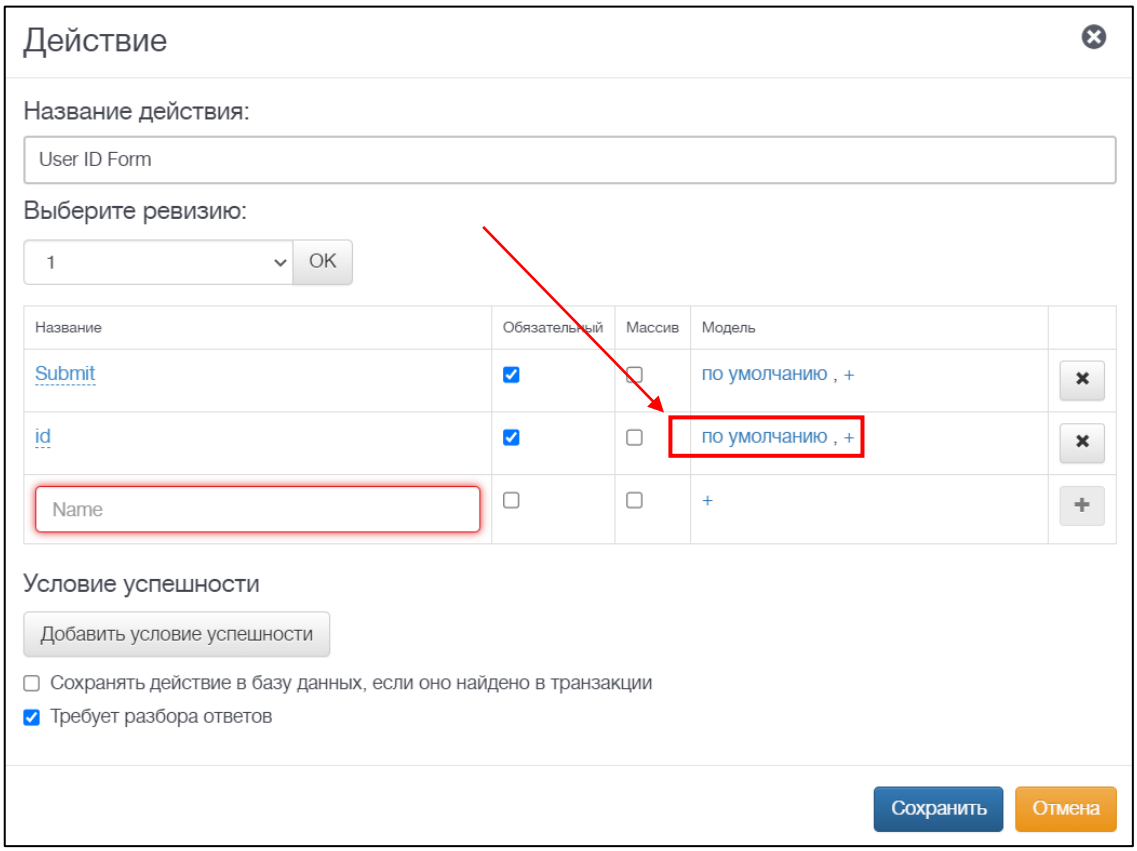

Рисунок 274 – Настройка параметров действия

3. Выбрать класс модели «Число» и нажать «Сохранить» (см. рисунок 275).

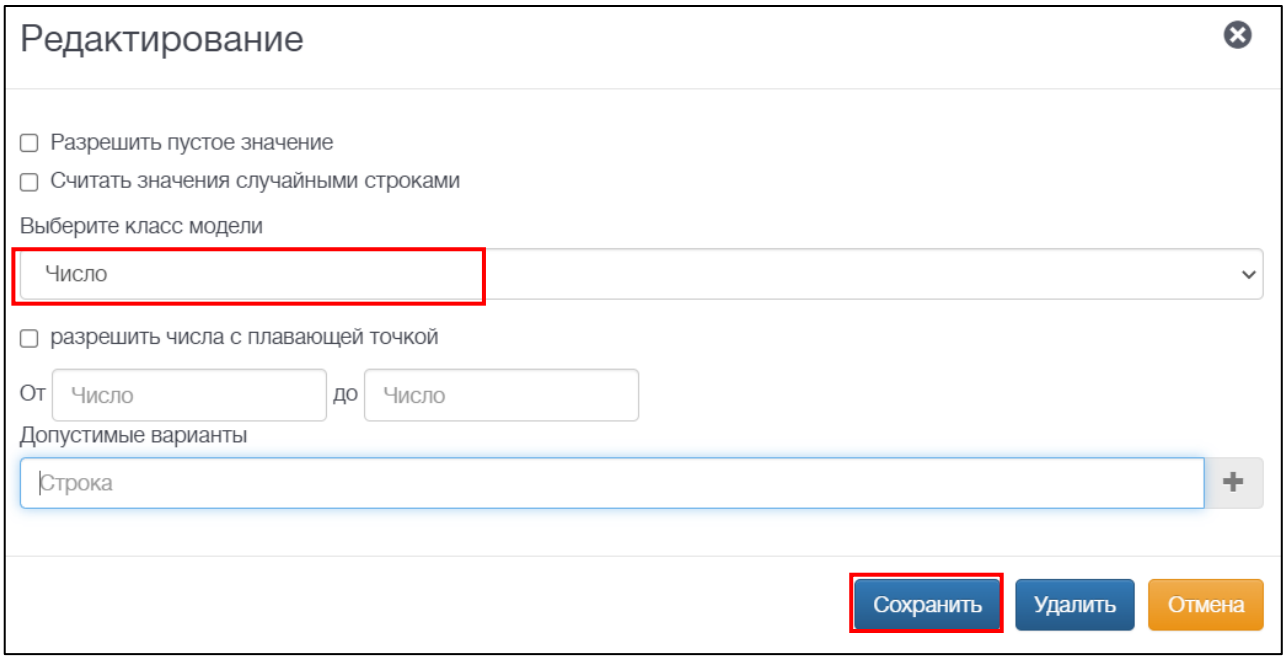

Рисунок 275 – Редактирование модели для поля ID

Действие с настроенными параметрами модели для поля ID показано на 276.

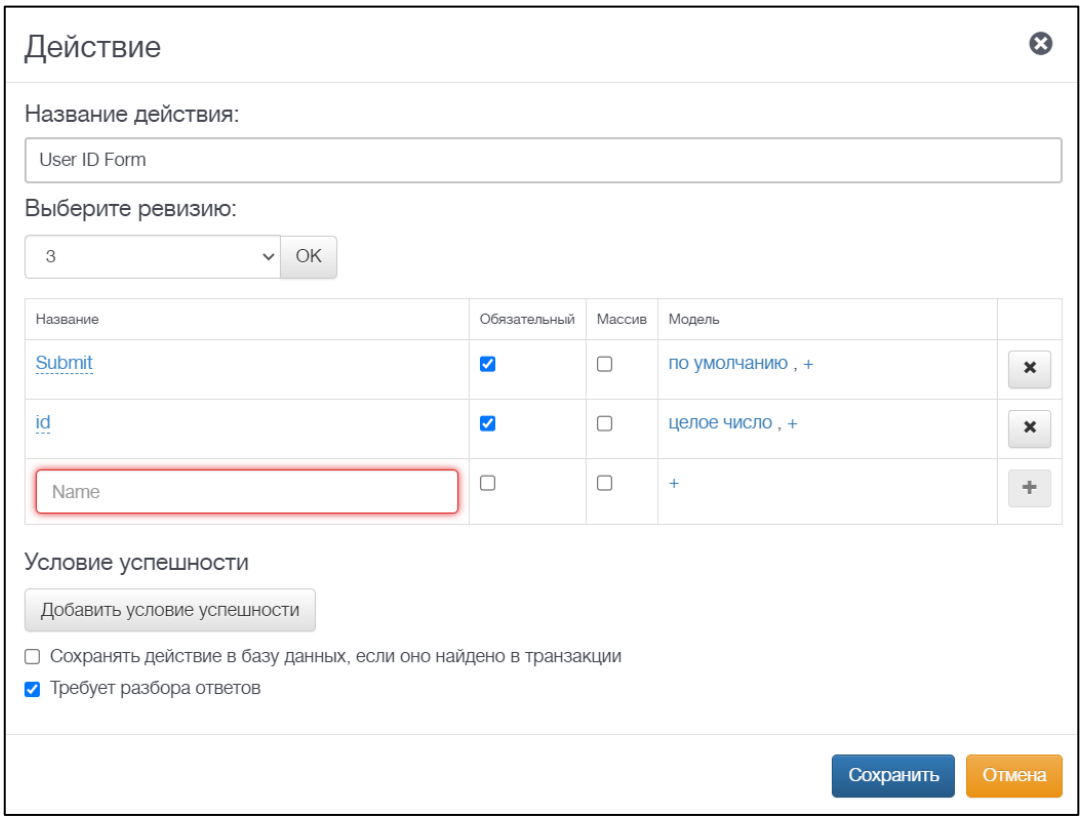

Рисунок 276 – Действие с настроенными параметрами

В результате настройки в последующих запросах, которые нарушают созданную модель, будут вызывать аномалии детектора ActionParameterValidator и запрос будет блокироваться.

25.7. Добавление IP-адреса пользователя в белый\чёрный список

Для добавления IP-адреса пользователя в белый\чёрный список необходимо:

1. Создать список (создание списка описано в разделе 12.1). Для того чтобы создать список необходимо перейти на вкладку «Источники, списки, цели» -> «Списки» и нажать на кнопку «Добавить список» (см. рисунок 277).

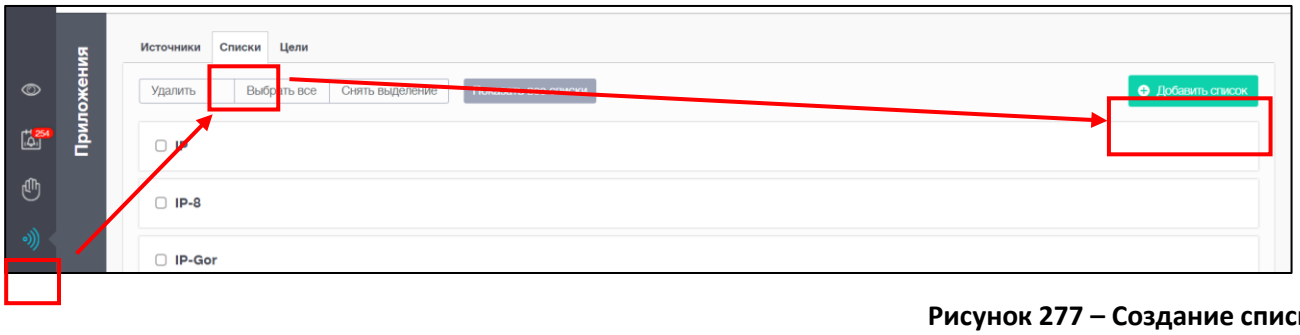

Рисунок 277 – Создание списка

2. После нажатия на кнопку создания списка появляется окно создания нового списка. Необходимо ввести название списка, выбрать веб-приложение и тип элементов. В данном случае используется тип элемента IP-адрес. После этого добавить элемент списка (см. рисунок 278).

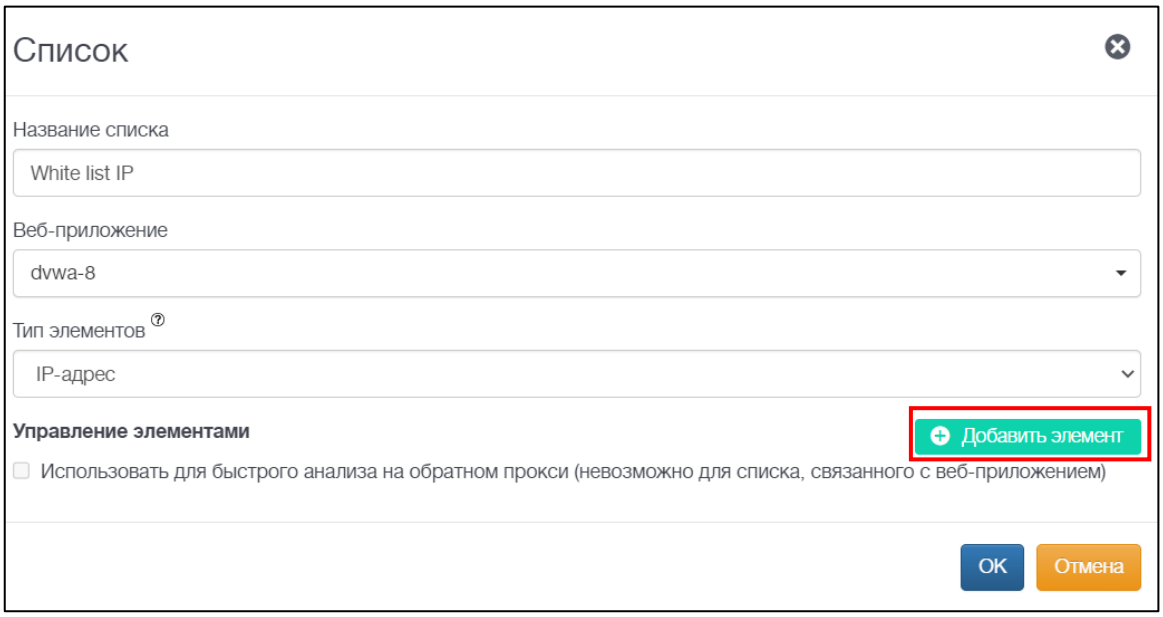

Рисунок 278 – Редактирование списка

3. Для добавления нового элемента в список необходимо ввести его название, ввести значение, время активации (по желанию) и добавить описание элемента списка (по желанию) (см. рисунок 279). В результате появиться список с добавленным элементов (см. рисунок 280).

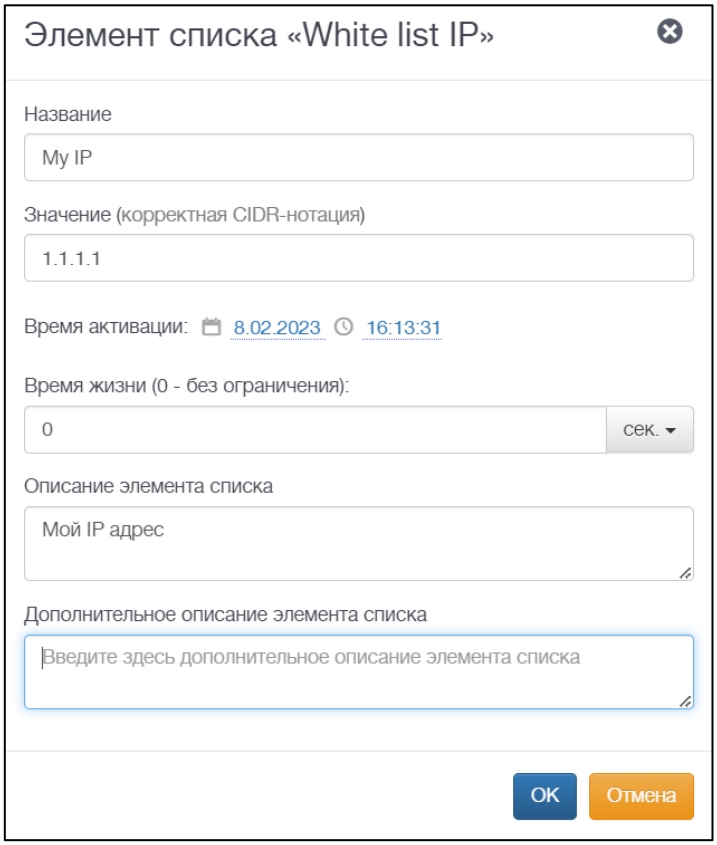

Рисунок 279 – Добавление элемента в список

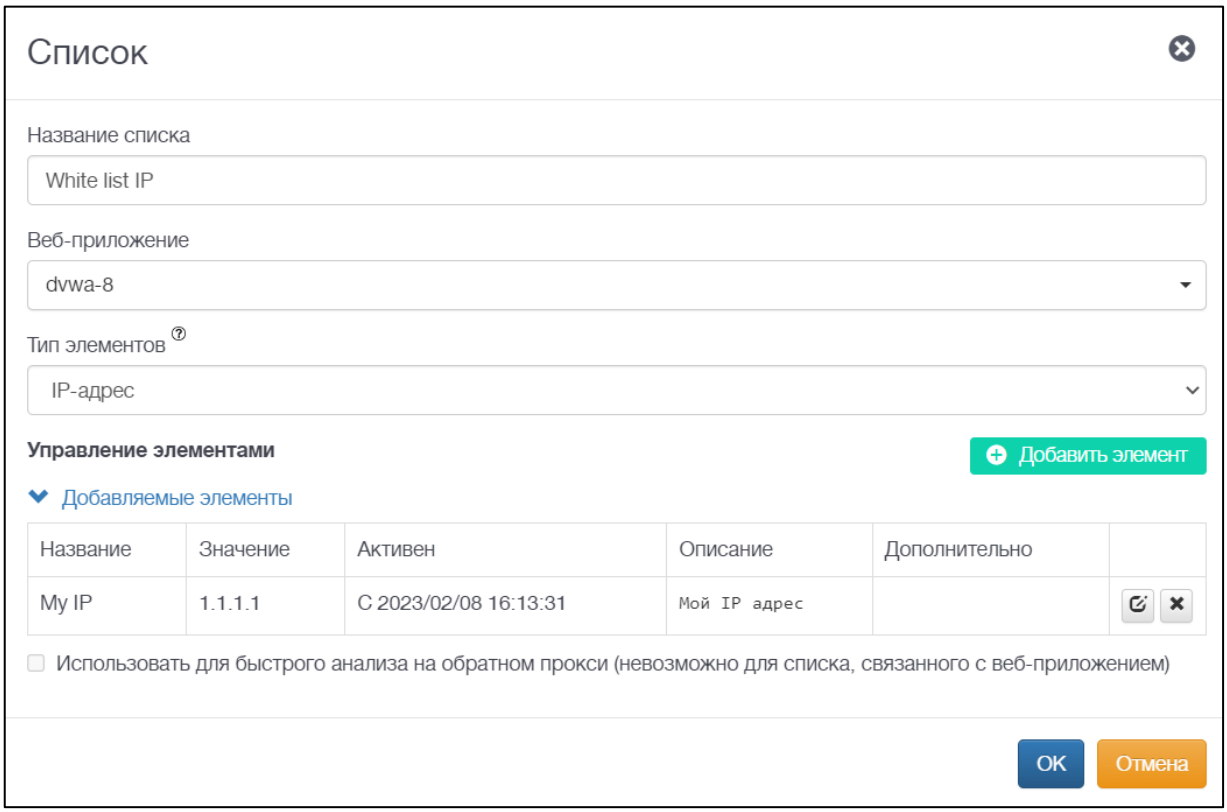

Рисунок 280 – Настроенный список

4. Далее необходимо создать источник для настроенного списка (создание источника описано в разделе 13.1). Для того чтобы создать источник необходимо перейти на вкладку «Источники, списки, цели» -> «Источники» и нажать на кнопку «Добавить источник» (см. рисунок 281).

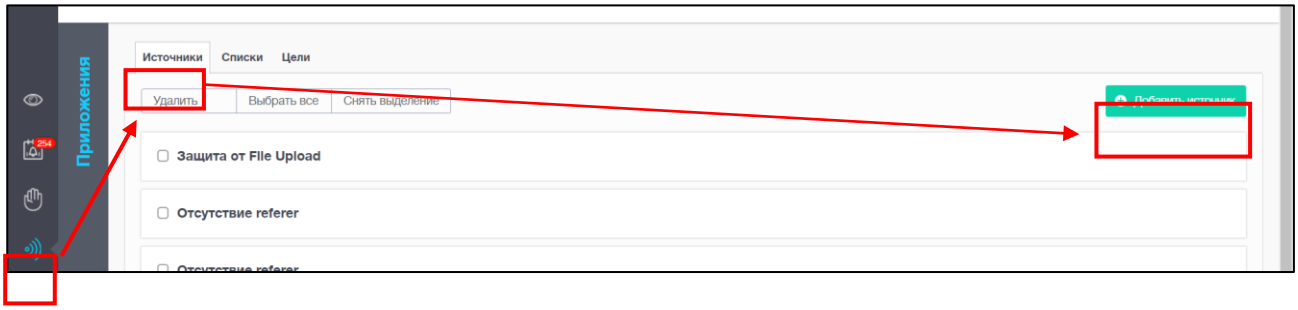

Рисунок 281 – Создание источника

5. После нажатия на кнопку создания источника появляется окно создания нового источника. Необходимо ввести его название, выбрать веб-приложение, указать путь до IP-адреса, выбрать тип предиката источника «Содержится в списке» и выбрать сам список (см. рисунок 282).

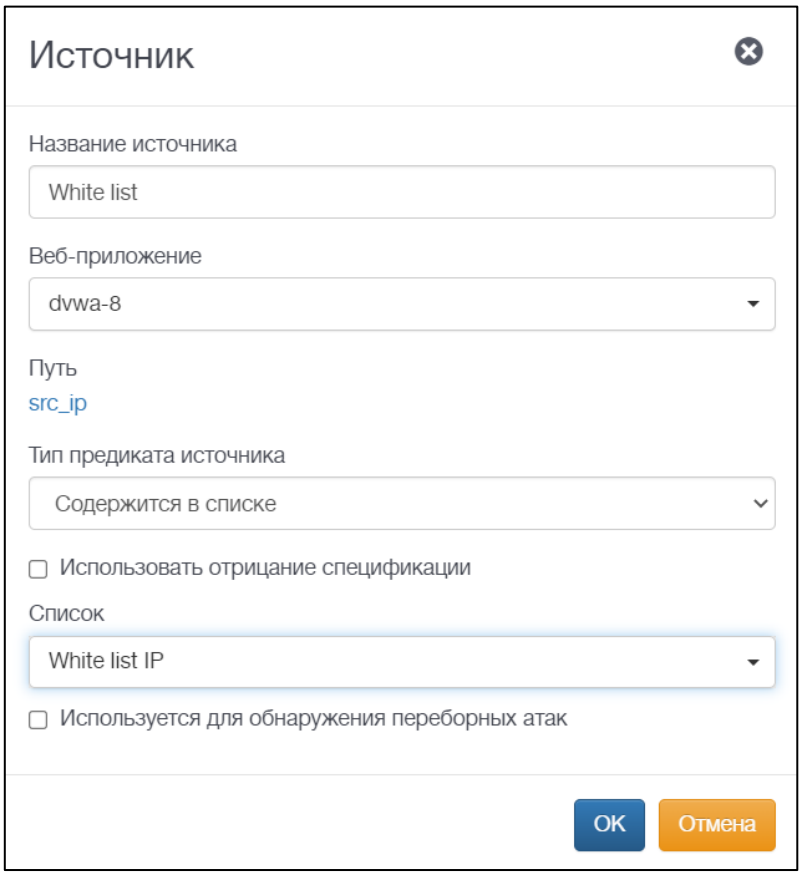

Рисунок 282 – Настроенный источник

6. Создать правило (создание правил описано в разделе 21), в результате работы которого не будут блокироваться запросы от IP-адресов, которые находятся в настроенном списке. Далее необходимо настроить источник для правила, для этого необходимо ввести класс спецификации транзакции «Проверка источника (любое значение)» и указать сам источник (см. рисунок 283).

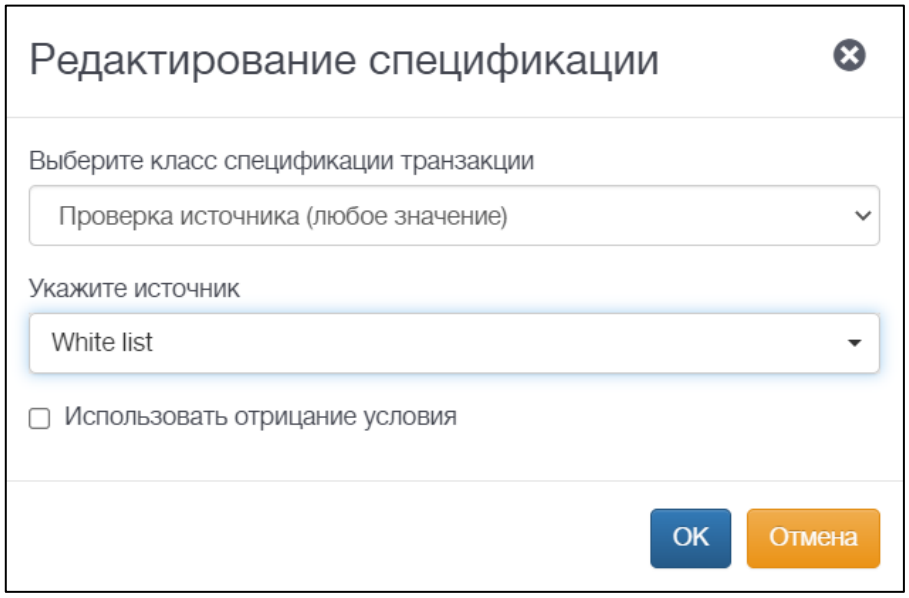

Рисунок 283 – Настроенный источник для правила

7. Для правила необходимо выбрать цель - проверка веб-приложения, а также само защищаемое приложение (см. рисунок 284).

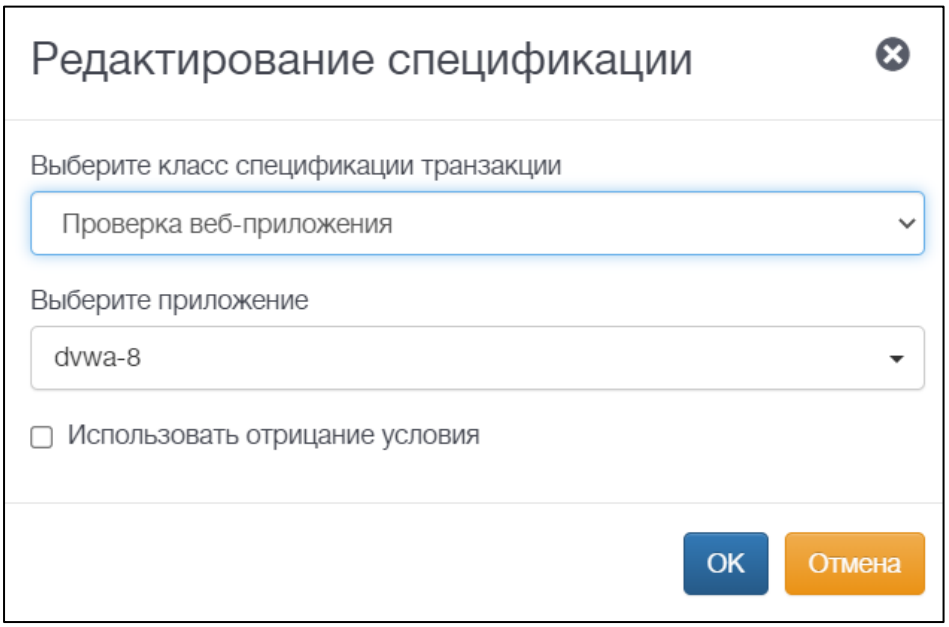

Рисунок 284 – Цель с классом спецификации проверка веб-приложения

8. В редактировании действия для правила необходимо выбрать действие разрешить транзакцию (см. рисунок 285).

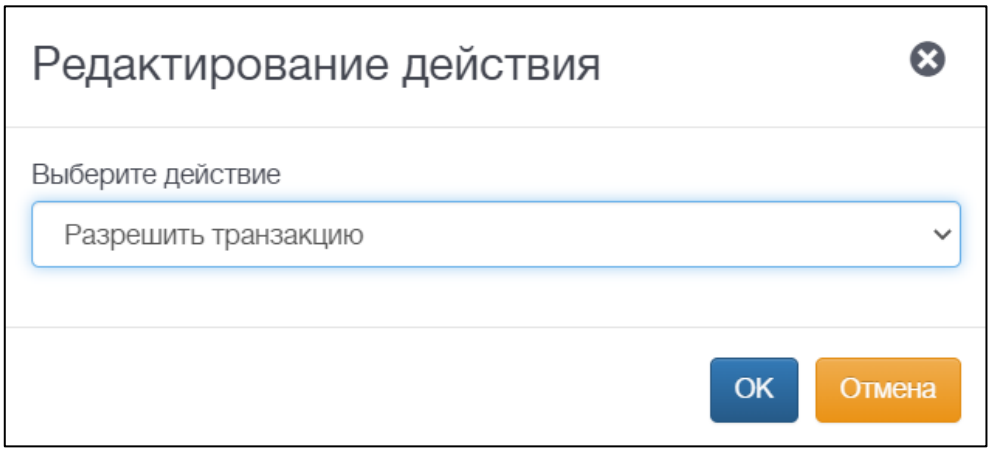

Рисунок 285 – Редактирование действия для правила

Настроенное правило для работы с белым списком показано на рисунке 286. Для работы с чёрным списком необходимо повторить те же действия, но выбрать действие для правила «Блокировать транзакцию».

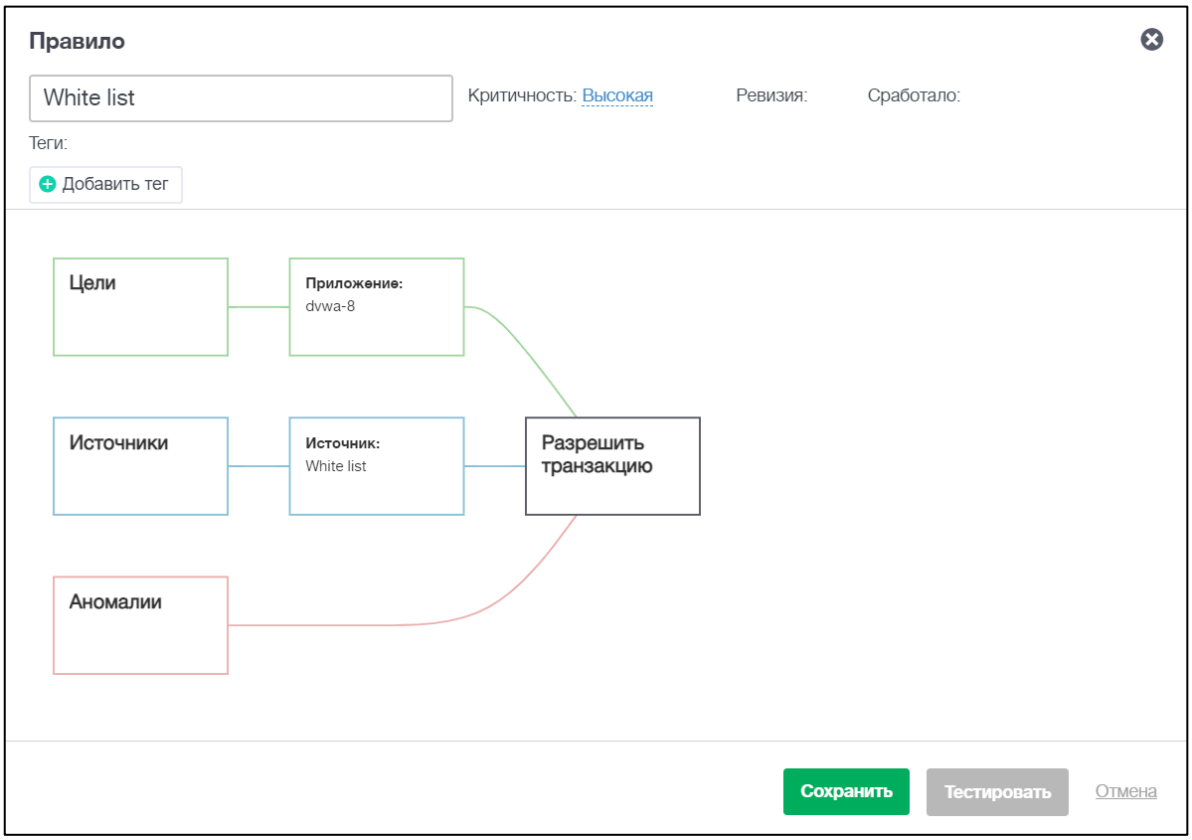

Рисунок 286 – Правило для работы с белым списком

25.8. Добавление в список при срабатывании правила

В качестве примера добавления в список при срабатывании правила разберём работу с правилом «Блокировка запросов по геолокации». При срабатывании правила «Блокировка запросов по геолокации» необходимо добавить IP-адреса этих запросов в список.

Для этого необходимо:

1. Создать список (создание списка описано в разделе 12.1). Для того чтобы создать список необходимо перейти на вкладку «Источники, списки, цели» -> «Списки» и нажать на кнопку «Добавить список» (см. рисунок 287).

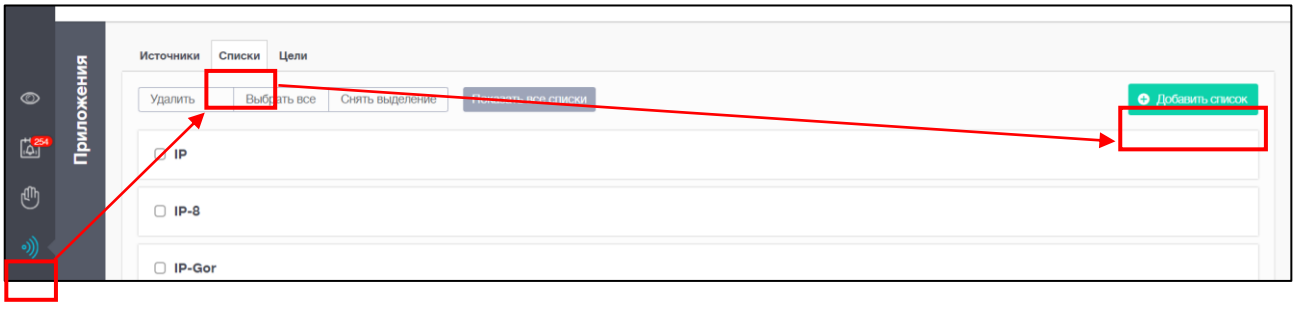

Рисунок 287 – Создание списка

2. После нажатия на кнопку создания списка появляется окно создания нового списка. Необходимо ввести название списка, выбрать веб-приложение и тип элементов. В данном случае используется тип элемента IP-адрес (см. рисунок 288).

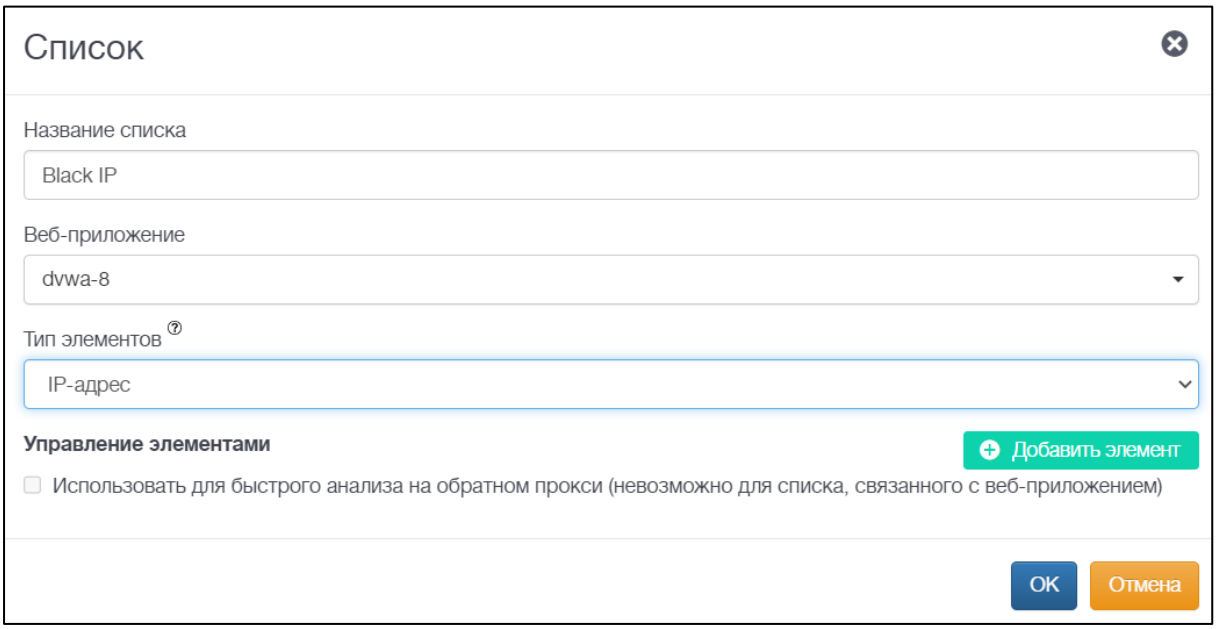

Рисунок 288 – Редактирование списка

3. Далее необходимо создать источник для настроенного списка (создание источника описано в разделе 13.1). Для того чтобы создать источник необходимо перейти на вкладку «Источники, списки, цели» -> «Источники» и нажать на кнопку «Добавить источник» (см. рисунок 289).

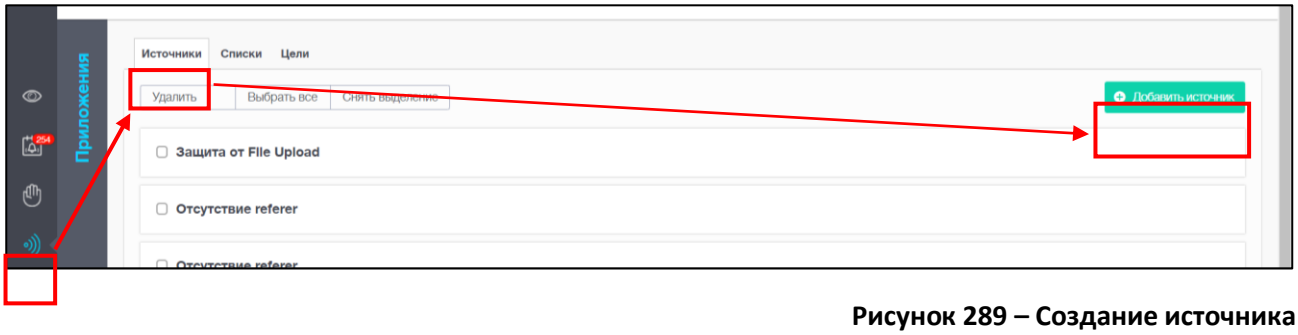

Рисунок 289 – Создание источника

4. После нажатия на кнопку создания источника появляется окно создания нового источника. Необходимо ввести его название, выбрать веб-приложение, указать путь до IP-адреса, выбрать тип предиката источника «Значение присутствует» (см. рисунок 290).

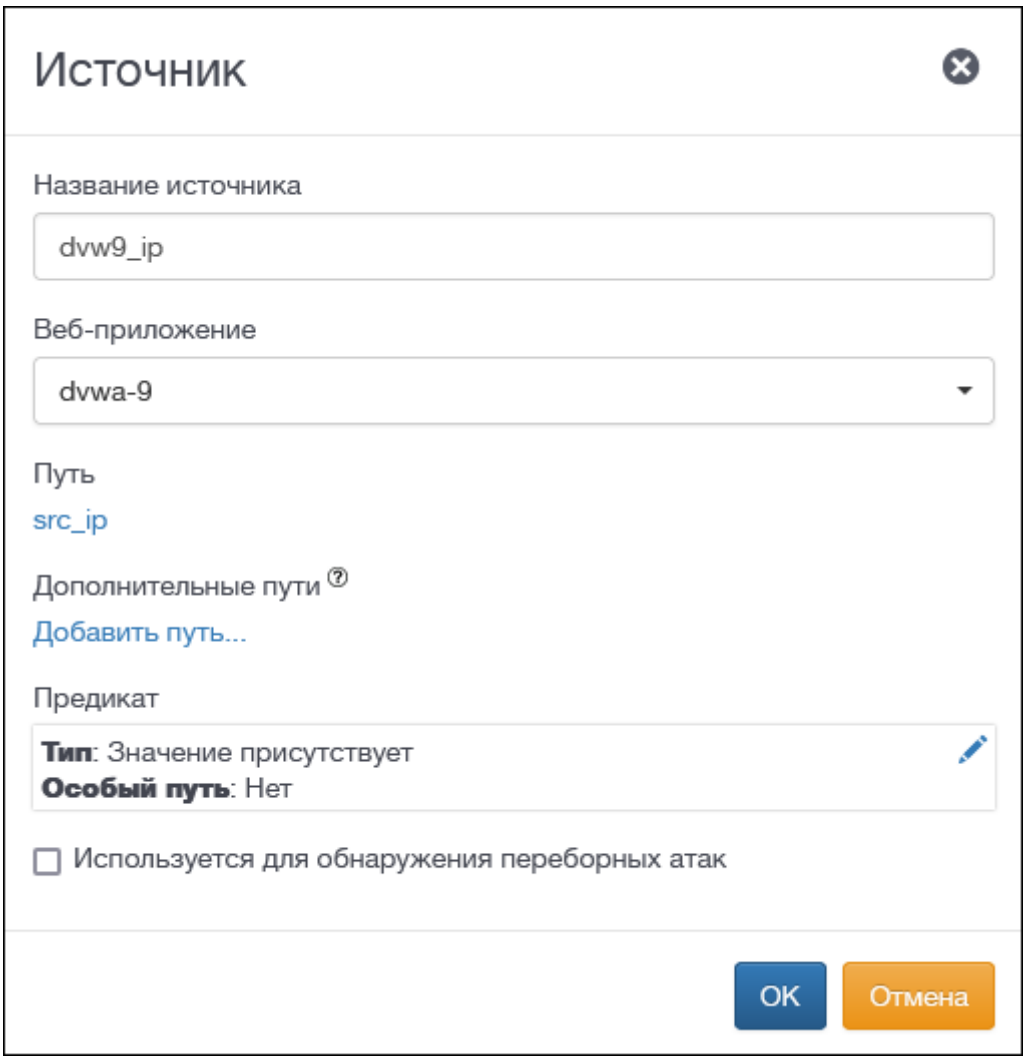

Рисунок 290 – Редактирование источника

5. Создать правило (создание правил описано в разделе 21), где источник имеет класс спецификации транзакции «Проверка страны пользователя» (см. рисунок 291). В разделе редактирования спецификации также необходимо указать страну, транзакции которой будут блокироваться соответствующим правилом. Также есть возможность использовать отрицание условия. В данном примере стоит цель блокировать все запросы не из России, поэтому следует использовать отрицание условия.

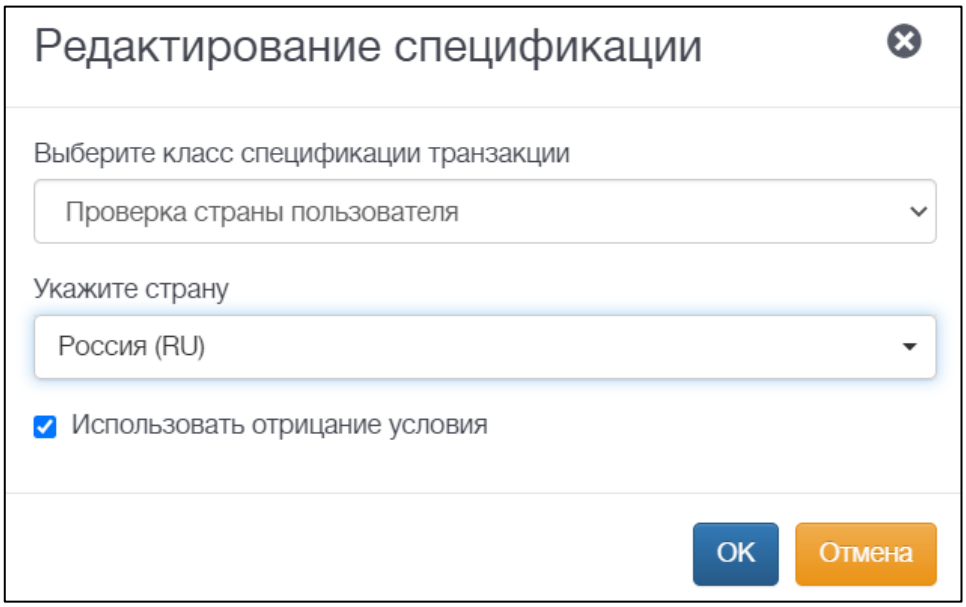

Рисунок 291 – Источник с классом спецификации проверка страны пользователя

6. Для правила необходимо выбрать цель – «Проверка веб-приложения», а также само защищаемое приложение (см. рисунок 292).

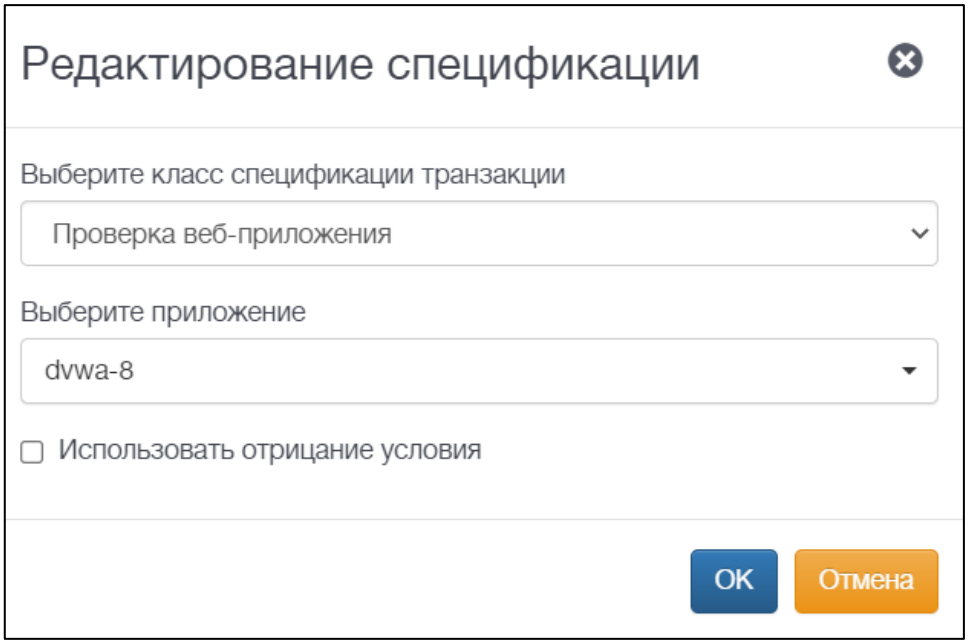

Рисунок 292 – Цель с классом спецификации проверка веб-приложения

7. В редактировании действия для правила необходимо выбрать действие «Добавить значение источника в список». Также необходимо указать решение для транзакции, выбрать источник, который будет добавляться в список и указать название списка. Дополнительно можно указать описание добавляемого элемента и время его жизни (см. рисунок 293).

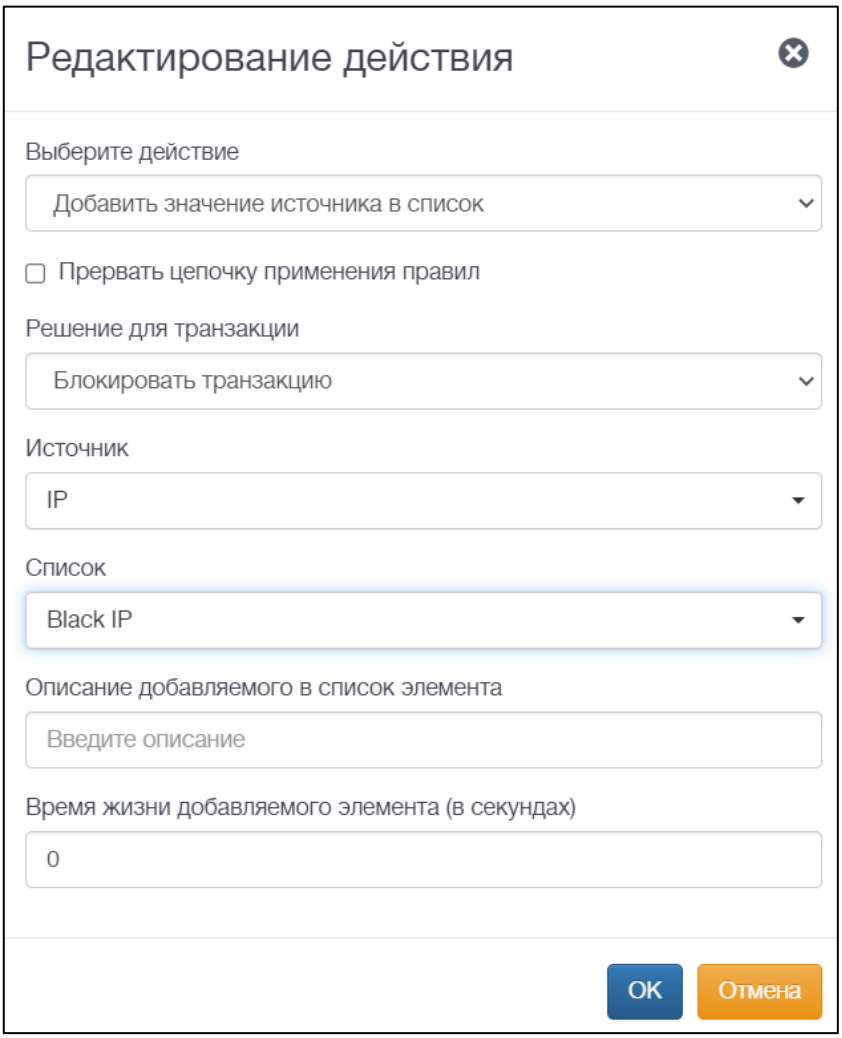

Рисунок 293 – Редактирование действия для правила

Настроенное правило для добавления IP-адресов запросов не из России в список показано на рисунке 294.

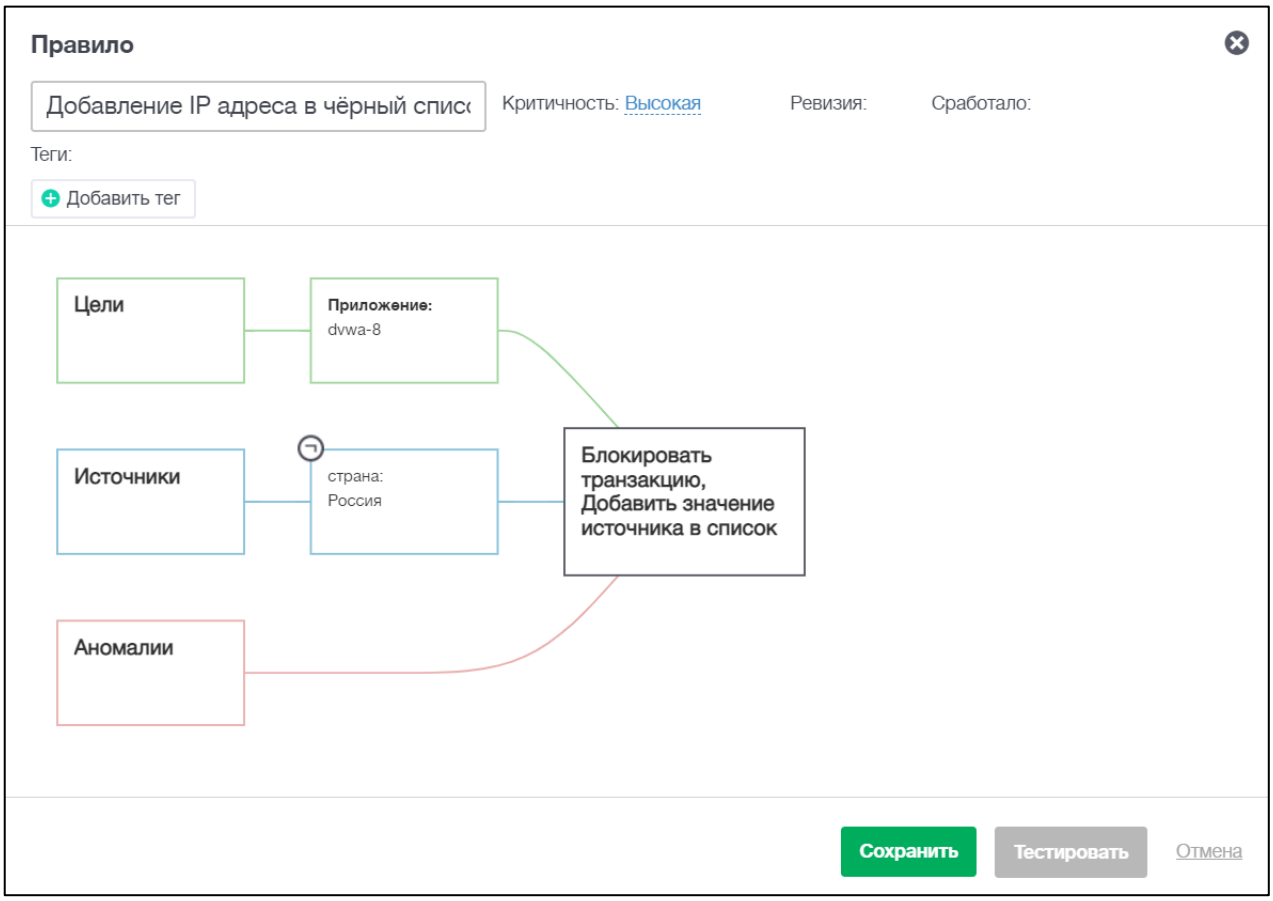

Рисунок 294 – Правило для добавления в список IP-адресов при его срабатывании

26. Сценарий работы

В данном разделе представлен общий сценарий работы с продуктом:

1. Заведение приложения за WAF:
   1.1. Создать конфигурационный файл NGINX (см. раздел 4).
   1.2. Добавить приложение в веб-интерфейсе (см. раздел 5).
2. При необходимости настраивается мультитенантная модель (см. раздел 6).
3. Проверка заведения приложения. Для этого необходимо перейти на вкладку транзакции, включить автообновление (см. раздел 3.5.1), отправить тестовый запрос и убедиться в том, что он прошел через WAF.
4. Перевести трафик на WAF.
5. Произвести первичную настройку:
   5.1. Настроить дерево разбора запроса\ответа (см. раздел 10).
   5.2. Настроить фильтрацию запросов к статическим ресурсам (см. раздел 8).
   5.3. При необходимости настроить маскирование критичных данных (см. раздел 11).
6. Подавить ложно-позитивные срабатывания (см. раздел 23).
7. Произвести тонкую настройку приложения (общие кейсы по тонкой настройке приложения находятся в разделе 25):
   7.1. Настроить протокольную валидацию (см. раздел 9).
   7.2. Настроить модель бизнес-логики (см. раздел 15).
   7.3. Настроить детекторы переборных атак на критичные действия (см. раздел 16).
   7.4. При необходимости настроить сессионную модель (см. раздел 18).
   7.5. Создать правила реагирования (см. раздел 21).
8. Организовать мониторинг на предмет ложно-позитивных срабатываний (см. раздел 23);
9. При достижении допустимого числа ложно-позитивных срабатываний, перевести приложение в активную блокировку (см. раздел 3.5.1).

27. Глоссарий