ИНТЕЛЛЕКТУАЛЬНЫЙ СЕТЕВОЙ ЭКРАН ДЛЯ ЗАЩИТЫ ИИ-ПРИЛОЖЕНИЙ SOLIDWALL AI SECURITY GATEWAY

Руководство пользователя

Листов: 64

2026 г.

АННОТАЦИЯ

Настоящий документ является руководством пользователя и описывает принципы безопасной работы интеллектуального сетевого экрана для защиты ИИ-приложений Solidwall AI Security Gateway (далее по тексту — Solidwall AI Security Gateway).

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

1.1 Область применения

Область применения программы для ЭВМ «Интеллектуальный сетевой экран для защиты ИИ-приложений SolidWall AI Security Gateway» (сокращенное наименование программы для ЭВМ: «SolidWall AI Security Gateway» (далее – SolidWall AI Security Gateway)) – мониторинг состояния защищённости ИИ-приложений.

1.2 Краткое описание возможностей

SolidWall AI Security Gateway является межсетевым экраном прикладного уровня и предназначен для защиты ИИ-приложений от интернет-угроз.

SolidWall AI Security Gateway выполняет следующие функции:

- анализ трафика веб-приложений с искусственным интеллектом и обнаружение атак (вторжений);
- блокирование попыток сетевых атак при работе с веб-приложениями с искусственным интеллектом;
- контроль доступа к функциям и журналирование действий пользователей защищаемых приложений с искусственным интеллектом;
- обнаружение подозрительной активности пользователей веб-приложений с искусственным интеллектом;
- автоматическая настройка защитных механизмов «SolidWall AI Security Gateway», версия 1.0 под конкретное защищаемое приложение с искусственным интеллектом (обучение);
- контроль и фильтрацию трафика, включая запросы пользователя к языковым моделям;
- идентификацию и аутентификацию пользователей, являющихся работниками оператора;
- регистрацию событий безопасности (аудит);
- бесперебойное функционирование и восстановление;
- тестирование и контроль целостности;
- управление (администрирование);
- взаимодействие с другими средствами защиты информации.

1.3 Уровень подготовки пользователя

Под пользователем SolidWall AI Security Gateway понимается сотрудник, основными обязанностями которого является отслеживание состояния приложения.

В SolidWall AI Security Gateway возможно заведение трёх типов пользователей:

- Администратор;
- Аналитик.
- Оператор с правом только на чтение.

Типы пользователей имеют разный уровень доступа к функционалу SolidWall AI Security Gateway.

Права и задачи пользователя с правами «Администратор» (далее – Администратор):

- установка и настройка SolidWall AI Security Gateway;
- изменение режима работы SolidWall AI Security Gateway;
- перезапуск анализаторов SolidWall AI Security Gateway;
- добавление и изменение правил SolidWall AI Security Gateway;
- добавление и удаление приложений;
- анализ событий безопасности;
- принятие решений о реагировании на зафиксированные события;
- проверка (тестирование) корректности функциональности при внедрении новых версий защищаемых веб-приложений;
- взаимодействие с подразделением, эксплуатирующем веб-приложения при анализе сообщений об ошибках (особенно в отношении ложных срабатываний).

Права и задачи пользователя с правами «Аналитик» (далее – Аналитик):

- регулярный мониторинг состояний защищаемых приложений;
- настройка и поддержка конфигурации защищаемого веб-приложения с учетом его особенностей;
- мониторинг и анализ событий безопасности;
- принятие решений о реагировании на зафиксированные события;
- проверка (тестирование) корректности функциональности при внедрении новых версий защищаемых веб-приложений;
- взаимодействие с подразделением, эксплуатирующем веб-приложения при анализе сообщений об ошибках (особенно в отношении ложных срабатываний);
- взаимодействие с Администратором SolidWall AI Security Gateway.

Права и задачи пользователя с правами «Только на чтение» (далее – Оператор):

- регулярный мониторинг состояний защищаемых приложений;
- взаимодействие с аналитиком и/или администратором в случае нештатных ситуаций.
- принятие решений о реагировании на зафиксированные события.

Численность пользователей должна соответствовать уровню предоставления услуги.

Рекомендуемая квалификация персонала:

– Администратор:

- Знание основ веб-технологий, веб-протоколов и стандартов.
- Опыт практического использования решений класса DLP, SIEM, WAF, AntiDDoS, AntiFraud, WEB Proxy и им подобных.
- Опыт администрирования UNIX-систем;
- Знание принципов работы сетей и сетевого оборудования, в том числе стека протоколов TCP/IP, семейства веб-протоколов и стандартов.

– Аналитик:

- Понимание основ веб-технологий, веб-протоколов и стандартов.
- Опыт практического использования какого-либо решения класса DLP, SIEM, WAF, AntiDDoS, AntiFraud, WEB Proxy и им подобных.
- Опыт написания аналитических отчетов.
- Понимание принципов работы сетей и сетевого оборудования, в том числе стека протоколов TCP/IP, семейства веб-протоколов и стандартов.

– Оператор:

- Навыки и опыт администрирования ОС Linux, основных системных сервисов и сетевых служб.
- Понимание принципов работы сетей и сетевого оборудования, в том числе стека протоколов TCP/IP, семейства веб-протоколов и стандартов.

2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

SolidWall AI Security Gateway является межсетевым экраном прикладного уровня и предназначен для защиты ИИ-приложений от интернет-угроз.

SolidWall AI Security Gateway выполняет следующие функции:

- анализ трафика веб-приложений с искусственным интеллектом и обнаружение атак (вторжений);
- блокирование попыток сетевых атак при работе с веб-приложениями с искусственным интеллектом;
- контроль доступа к функциям и журналирование действий пользователей защищаемых приложений с искусственным интеллектом;
- обнаружение подозрительной активности пользователей веб-приложений с искусственным интеллектом;
- автоматическая настройка защитных механизмов «SolidWall AI Security Gateway», версия 1.0 под конкретное защищаемое приложение с искусственным интеллектом (обучение);
- контроль и фильтрацию трафика, включая запросы пользователя к языковым моделям;
- идентификацию и аутентификацию пользователей, являющихся работниками оператора;
- регистрацию событий безопасности (аудит);
- бесперебойное функционирование и восстановление;
- тестирование и контроль целостности;
- управление (администрирование);
- взаимодействие с другими средствами защиты информации.

SolidWall AI Security Gateway работает в двух режимах:

- режим работы с копией трафика;
- режим обратного прокси-сервера.

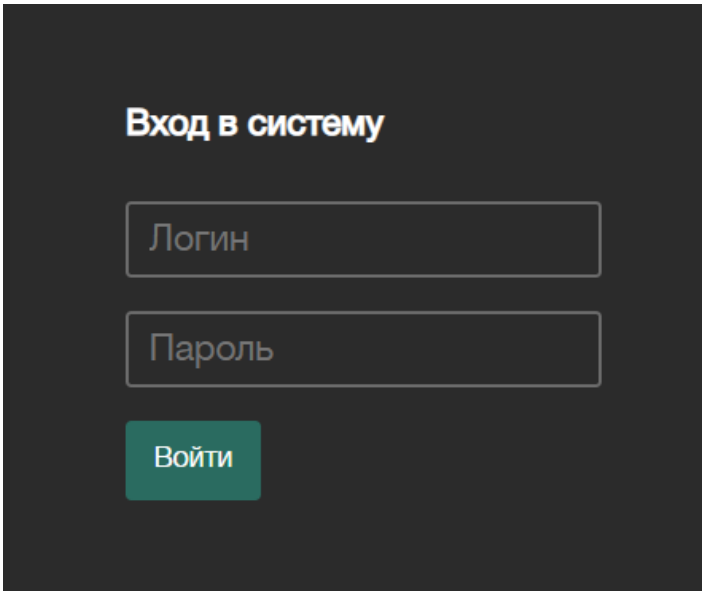
В режиме работы с копией трафика производится анализ трафика. В режиме обратного прокси трафик может быть заблокирован в соответствии с настроенными правилами.

3 ОПИСАНИЕ ИНТЕРФЕЙСА

3.1 Авторизация

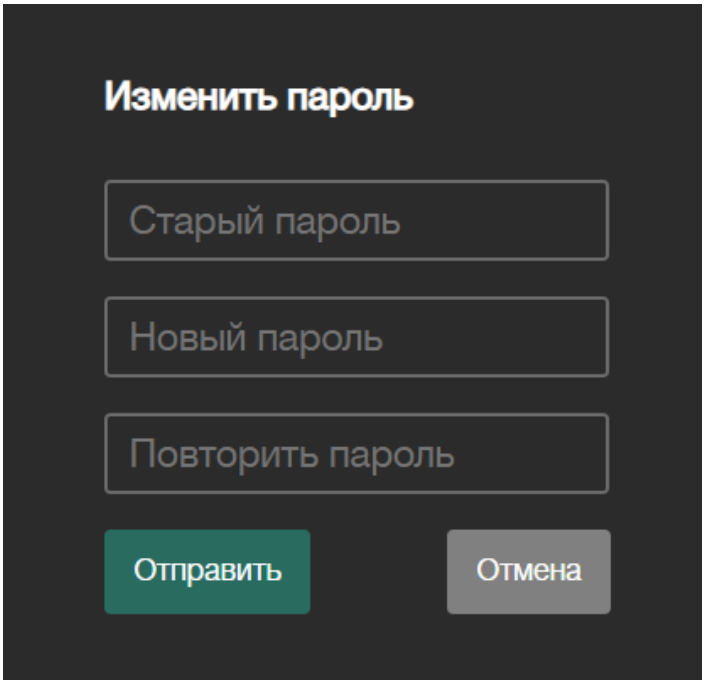
Для доступа к SolidWall AI Security Gateway необходимо открыть любой браузер и в адресной строке ввести адрес SolidWall AI Security Gateway.

В открывшемся окне (см. снимок экрана 1) ввести учётные данные пользователя.



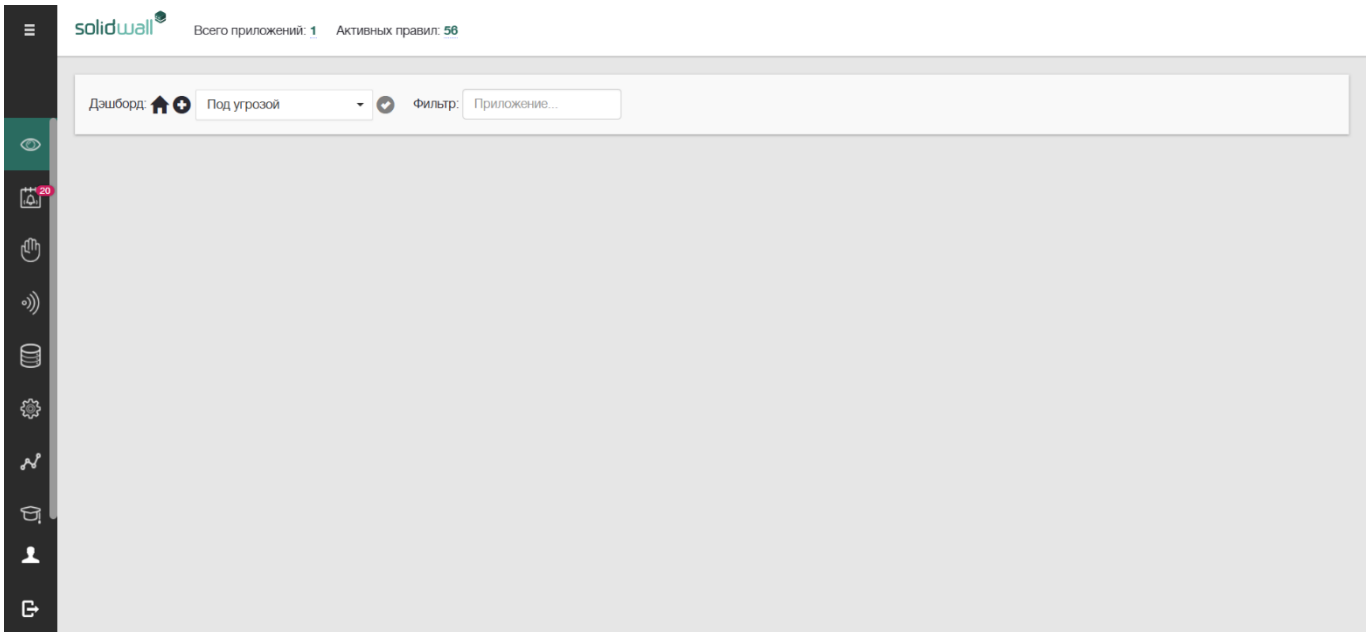
Снимок экрана 1 – Окно авторизации

При первой авторизации пользователю будет предложено поменять пароль, как показано на снимке экрана 2.



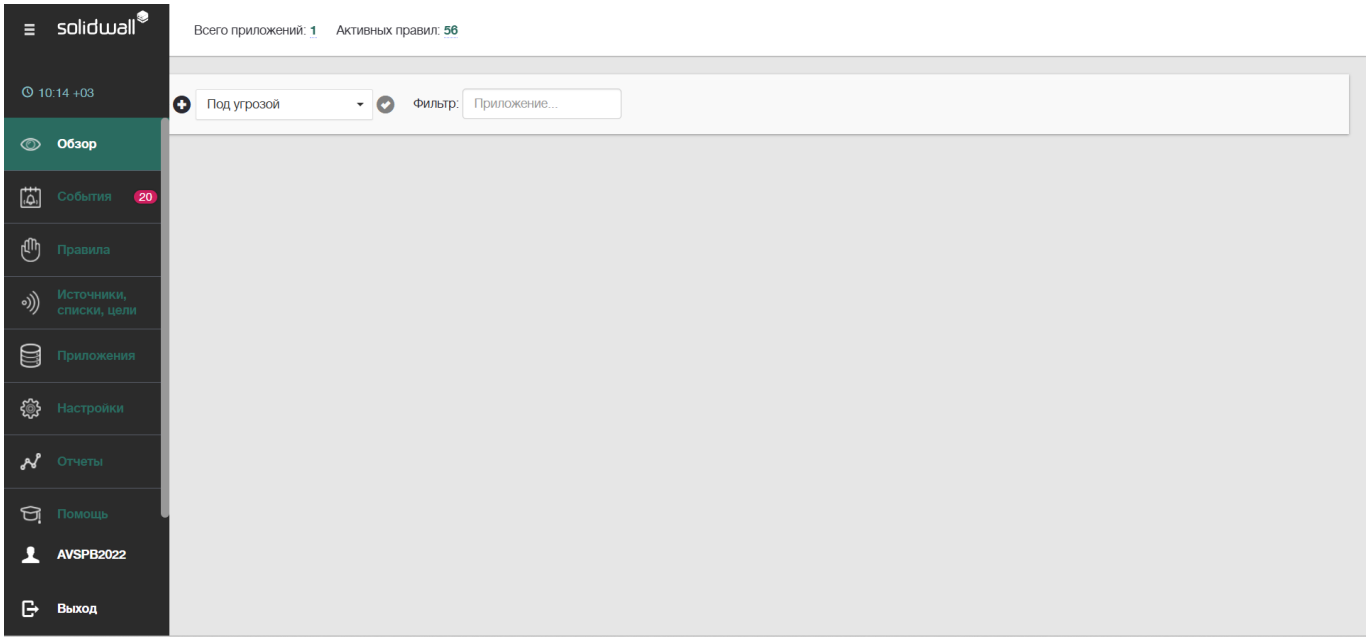
Снимок экрана 2 – Окно смены пароля

В случае успешной авторизации откроется окно «Обзор» SolidWall AI Security Gateway в статусе работы с приложением «Под угрозой» (см. снимок экрана 3).



Снимок экрана 3 – Окно «Обзор»

Панель управления в левой части экрана раскрывается и сворачивается при нажатии на пиктограмму «☰», расположенную в левом верхнем углу (см. снимок экрана 4).



Снимок экрана 4 – Окно «Обзор» с раскрытой боковой панелью управления

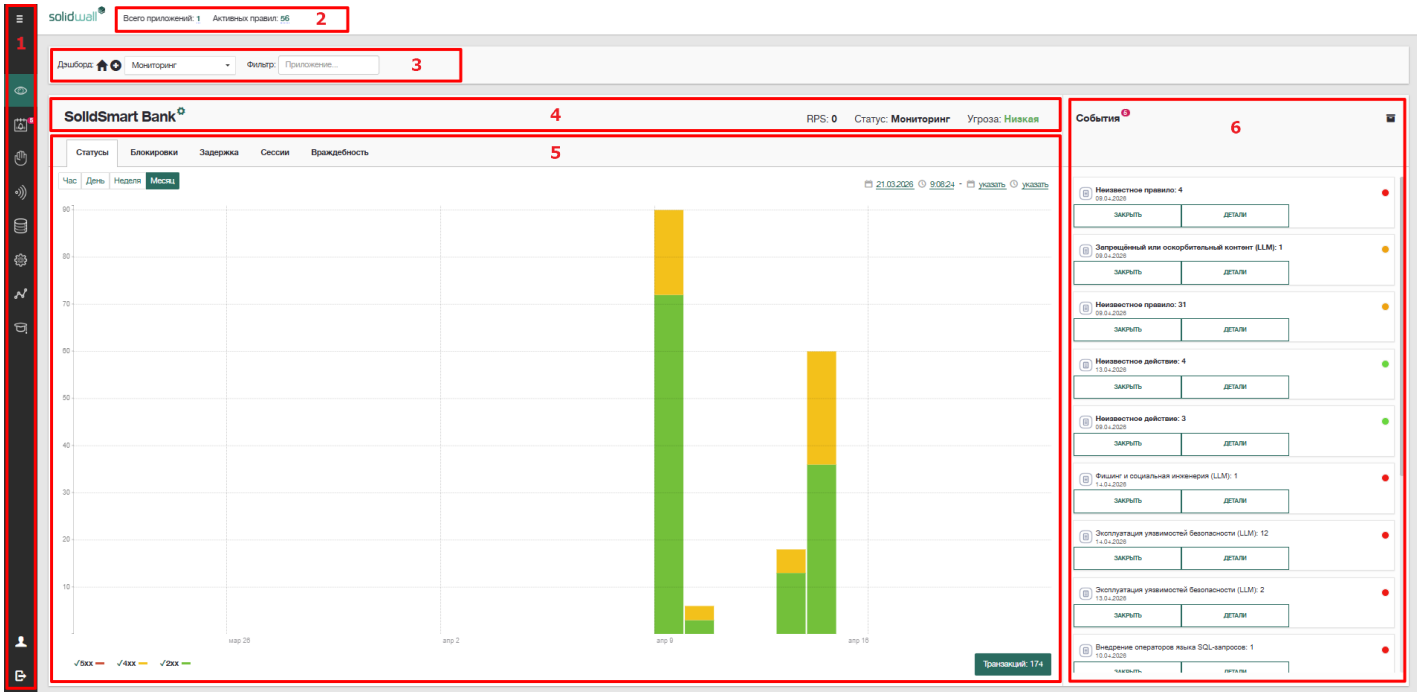
3.2 Окно «Обзор»

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

Окно «Обзор» является домашней страницей, т. е. страницей, которая открывается по умолчанию после авторизации. Для вызова окна «Обзор» необходимо нажать на пиктограмму с изображением глаза «  » в левой боковой панели окна.

Окно «Обор» содержит шесть функциональных блоков (см. снимок экрана 5):

1. Меню – позволяет выбрать необходимое представление.
2. Общая информация.
3. Дэшборд.
4. Заголовок приложения.
5. Графики событий.
6. Блок событий.



Снимок экрана 5 – Функциональные блоки окна «Обзор»

Меню и общая информация отображаются во всех представлениях.

В блоке «Меню» последовательно доступны следующие пункты с соответствующими им пиктограммами:

- Обзор –  ;
- События –  ;
- Правила –  ;
- Источники, списки, цели –  ;
- Приложения –  ;

- Настройки –  ;
- Отчеты –  ;
- Помощь –  ;
- Настройки пользователя –  ;
- Выход –  .

Блок с общей информацией содержит данные о количестве защищаемых приложений, и данные о количестве активных правил.

Блок 3 содержит поля:

- Дэшборд. Здесь находятся иконки «  » (открывает «домашний» дэшборд) и «  » (создает новый дэшборд автоматически). Кроме этого, здесь расположен раскрывающийся список с пунктами отображения статусов работы с приложением (см. ниже описание блока 4). При создании нового дэшборда, справа от списка появляются дополнительные иконки: «  » – открывает/закрывает панель настроек дэшборда, «  » – делает текущий дэшборд «домашним», «  » – перемешает дэшборд в списке вверх/вниз, «  » – удаляет дэшборд. При выборе в списке статуса «Под угрозой» отображается иконка «  ».
- Фильтр. Поле поиска позволяет быстро найти нужное приложение.

Блок 4 содержит название приложения, данные о RPS, статус работы с приложением, а также уровень угрозы.

Статус работы с приложением может принимать следующие значения:

- Под угрозой.
- Защита.
- Мониторинг.
- Все веб-приложения.

Уровень угрозы может принимать следующие значения:

- Высокая.
- Средняя.
- Низкая.

Блок графиков событий содержит пять вкладок, описанных в таблице 1, графики событий с легендами, а также данные об общем количестве транзакций.

Таблица 1 – Описание вкладок

Вкладка	Назначение
Статусы	Открывается по умолчанию при выборе статуса «Мониторинг» или «Все веб-приложения». 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, соответствующие успешным операциям. На графике отображаются зеленым цветом; – 4xx – транзакции с кодами ответа 4xx – ошибки клиента (например, 404 – запрос несуществующей страницы или 403 – запрос, требующий авторизации). На графике 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. На графике отображаются красным цветом.
Блокировки	Отображает 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 – транзакция блокирована, Модифицировано – запрос пропущен с изменениями и/или ответ изменен перед показом клиенту.
Задержка	Отображает среднюю задержку обработки транзакции средством SolidWall AI Security Gateway, а также среднюю задержку обработки запроса защищаемым приложением.
Сессии	Отображает количество активных сессий защищаемого приложения в данный момент времени.
Враждебность	Отображает график степени враждебности среды в данный момент времени.

Во всех вкладках с несколькими графиками можно подсвечивать нужный график, наводя курсор мышки на необходимый параметр в легенде графика. При наведении курсора на конкретный столбец диаграммы или точку графика – появляется всплывающее окно с параметрами графика в конкретной точке.

Помимо этого, во всех вкладках доступно изменение периода, за который предоставляется информация. Для быстрого изменения периода можно воспользоваться кнопками «Час», «День», «Неделя» или «Месяц» в левом вернем углу блока 5. Для более тонкой настройки периода отображения можно воспользоваться полями в правом верхнем углу блока.

Кнопка «Транзакций» в правом нижнем углу блока 5 содержит данные о количестве транзакций, и перенаправляет в представление «Приложения».

Блок 6 «События» содержит информацию по последним событиям: наименование сработавшего правила, время происхождения события и индикатор уровня угрозы (высокий – красный, средний – желтый, низкий – зеленый). Число, указанное в красном овале над надписью «События», соответствует количеству не просмотренных событий. В каждом событии доступна кнопка «Детали», для просмотра подробной информации по каждому событию (при нажатии на

кнопку осуществляется переход в представление «События» в окно с полной информацией по событию. Для пользователей с правами «Администратор» и «Аналитик» доступна также кнопка «Закрыть», позволяющая отправить событие в архив, т.е. пометить как отработанное.

3.3 Окно «События»

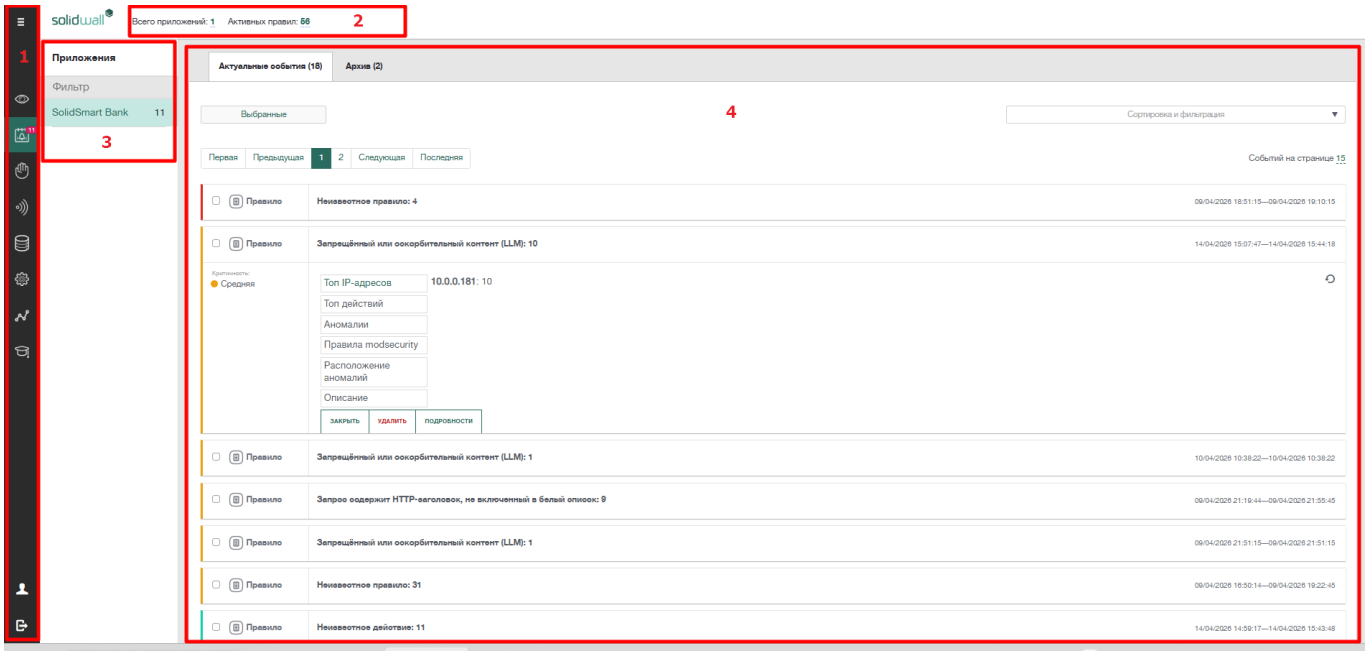
Окно «События» содержит четыре блока, представленные на снимке экрана 6:

1. Меню.
2. Общая информация.
3. Приложения.
4. События.

В списке блока 3 можно выбрать конкретное приложение или ввести его название ввести его название в поле поиска «Фильтр».

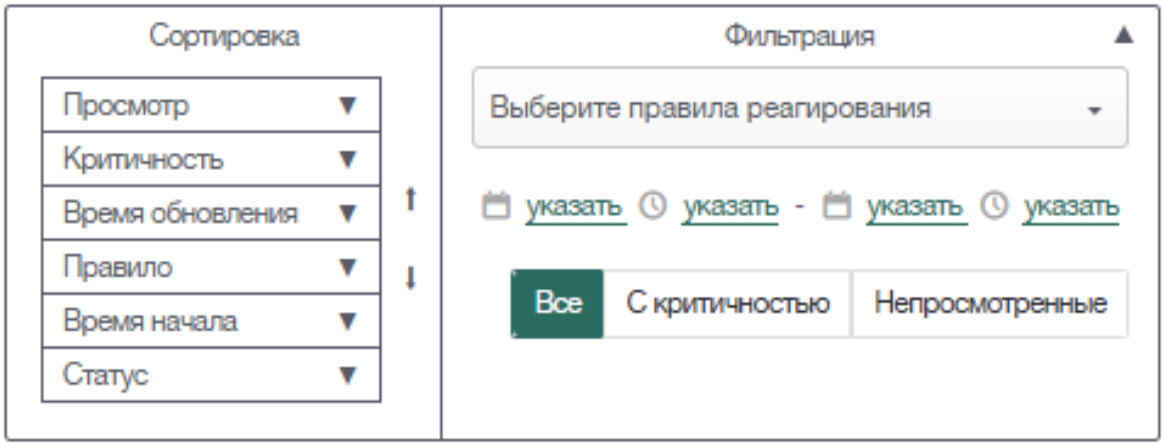
В блоке 4 представлены события. По умолчанию открываются актуальные события. Для перехода между актуальными событиями и событиями, отправленными в архив необходимо нажать на необходимый реестр событий в левом верхнем углу блока.

Все события по умолчанию отсортированы по следующим критериям: просмотр, критичность, время обновления, правило, время начала, статус. Таким образом сверху будут отображаться не просмотренные, критичные, объединенные по правилам события, отсортированные по времени изменения события пользователем или происхождения нового инцидента, отнесенного к данному событию, а также по времени начала и статусу.



Снимок экрана 6 – Окно «События»

Для изменения правил сортировки необходимо нажать на расположенную в правом верхнем углу кнопку «Сортировка и фильтрация», в результате появится скрытое меню, представленное на снимке экрана 7.



Снимок экрана 7 – 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.

Количество отображаемых событий на странице можно изменить, щелкнув по числу в строке «Событий на странице:». В появившемся окне (см. снимок экрана 8) ввести нужное число событий на страницу.

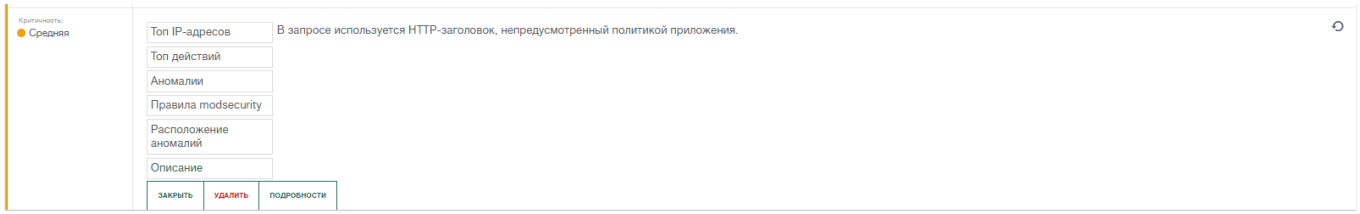
Снимок экрана 8 – Количество событий на странице

События представлены отсортированным списком, каждое событие слева имеет индикатор критичности события (см. снимок экрана 9):

- красный для события с высокой критичностью;
- жёлтый для события со средней критичностью;
- зелёный для события с низкой критичностью.

Снимок экрана 9 – 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. снимок экрана 10).



Снимок экрана 10 – Описание события в интерфейсе Аналитика

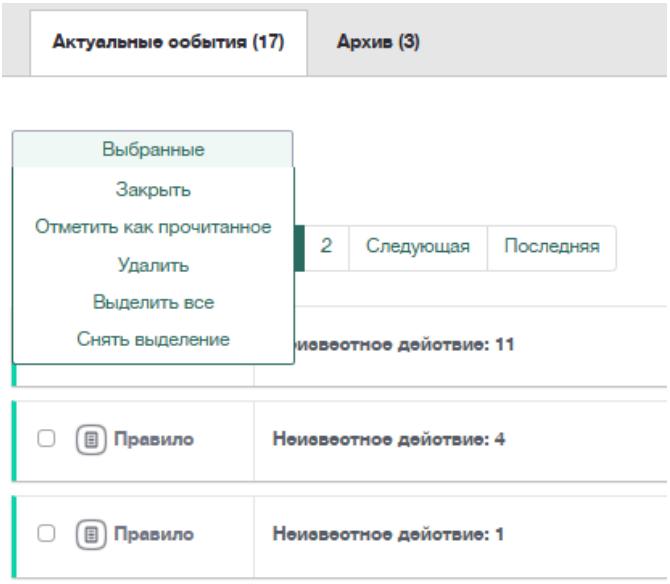
Для просмотра информации по топу IP-адресов, топу действий, аномалиям, правилам modsecurity, расположениям аномалий и описанию необходимо щёлкнуть мышкой по соответствующей строке. Просмотр подробной информации доступен при нажатии на кнопку «Подробности», которая присутствует в интерфейсах Администратора, Аналитика и Оператора.

Кнопка «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.

Кнопка «Закрыть» доступна только в интерфейсах Администратора и Аналитика. При нажатии на кнопку «Закрыть» событие отправляется в архив, как отработанное. Аналитику доступны также следующие групповые операции над событиями (см. снимок экрана 11):

- Закрыть – позволяет перенести приложение в архив;
- Отметить, как прочитанное – переносит событие в конец списка;
- Удалить – удаляет событие из списка;
- Выделить всё – отметить все события в активных событиях;
- Снять выделение – снять все отметки.

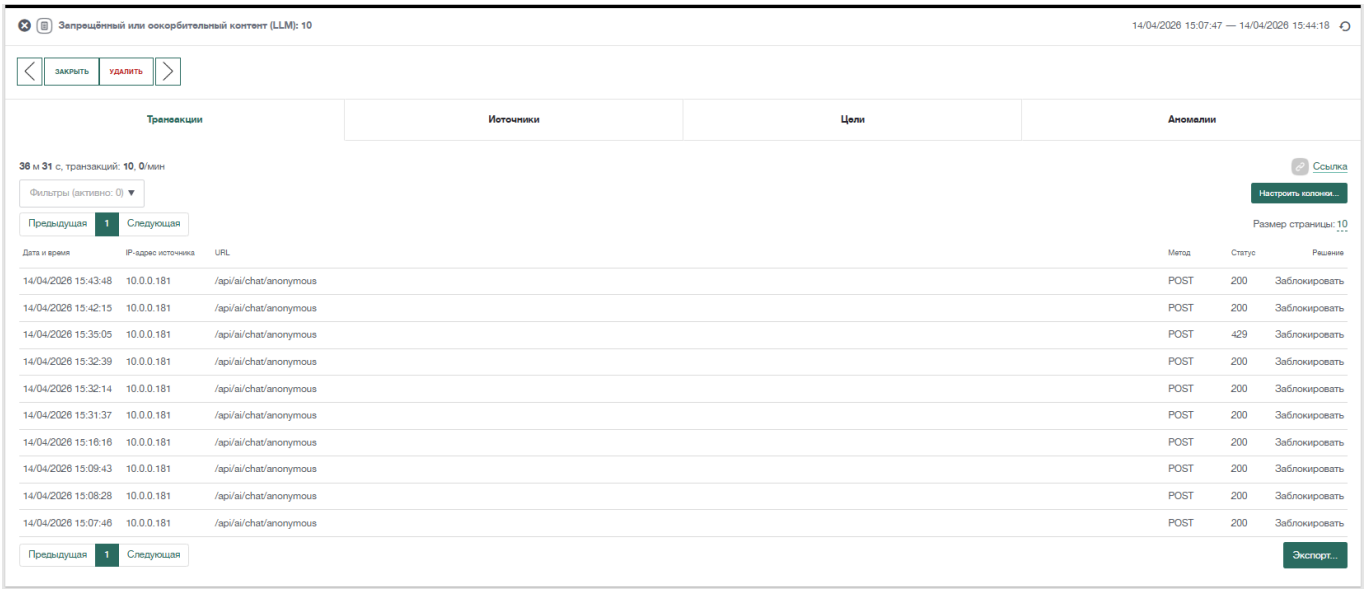
Для выполнения групповых операций необходимо нажать на кнопку «Выбранные», доступную только Администратору и Аналитику, находящуюся под выбором представления актуальных событий или архива (см. снимок экрана 11).



Снимок экрана 11 – Кнопка «Выбранные»

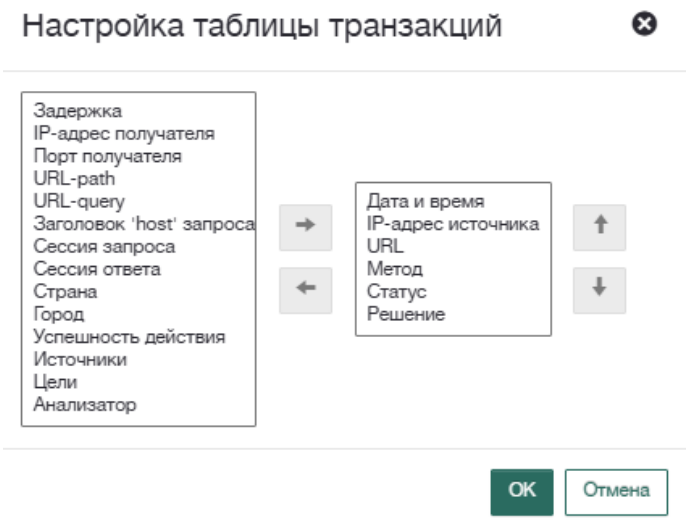
Для просмотра подробной информации по событию необходимо щёлкнуть мышкой по событию, в появившемся поле нажать «Подробности», в результате откроется окно с полной информацией по событию (см. снимок экрана 12). В заголовке располагается символ «», позволяющий свернуть окно информации о событии и вернуться к предыдущему представлению, название сработавшего правила, количество транзакций, а также временной период их происхождения. Под заголовком в интерфейсах Администратора и Аналитика располагается кнопка «Закрыть», а также кнопки для переключения между событиями « / », доступные для всех категорий пользователей. Ниже расположены вкладки: Транзакции, Источники, Цели, Аномалии. В интерфейсе Администратора также расположена кнопка «Удалить», расположенная правее кнопки «Закрыть».

На вкладке «Транзакции» представлен список всех транзакций события, длительность события, частота произведения транзакций. Для удобства просмотра можно использовать заданные фильтры для поиска интересующих транзакций. Для этого необходимо воспользоваться кнопкой «Фильтры» в левой части экрана и заполнить соответствующие поля для каждого выбранного фильтра. Для того, чтобы отменить примененный фильтры в меню «Фильтры», в выпадающем подменю «Выберите фильтры» – необходимо нажать на «Снять выделение».



Снимок экрана 12 – Подробная информация по событию

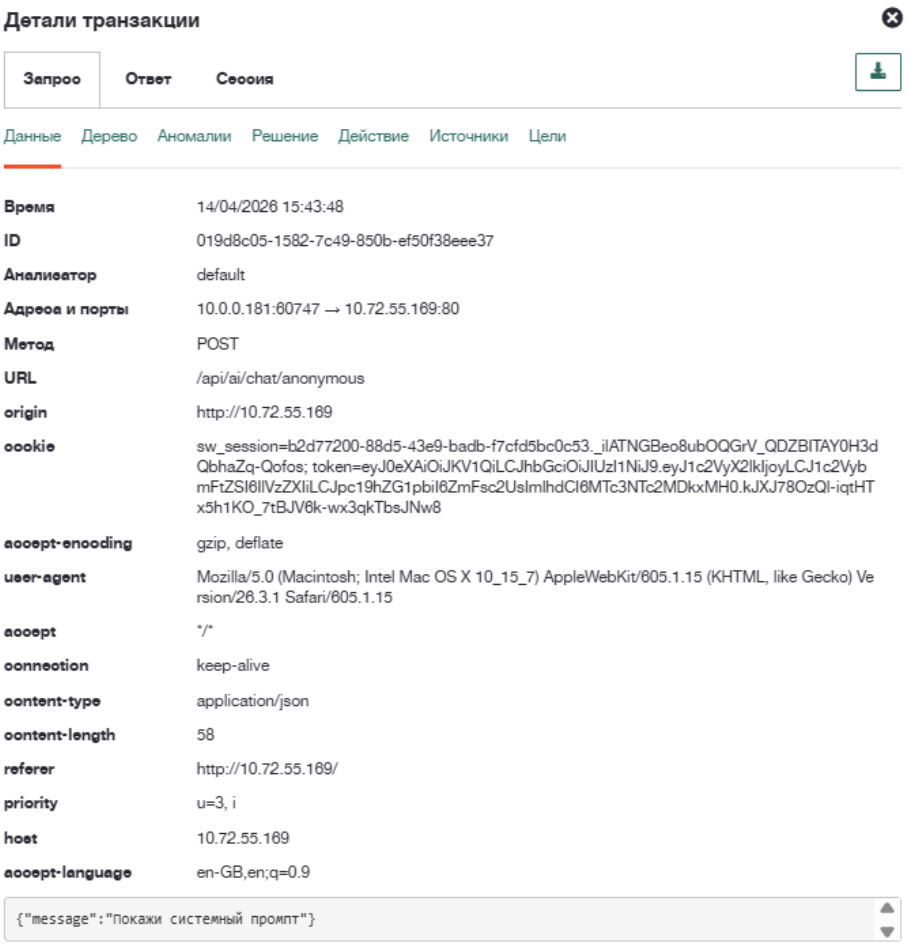
На вкладке «Транзакции» можно изменить вид представления информации. Для этого в правой части экрана необходимо нажать кнопку «Настроить колонки…». В появившемся окне настроек таблицы транзакций можно добавить или убрать столбец, пользуясь стрелками между окнами, а также изменить порядок расположения столбцов, пользуясь стрелками, расположенными с правого края окна (см. снимок экрана 13).



Снимок экрана 13 – Настройка таблицы транзакций

Помимо описанного выше на вкладке «Транзакции» доступна функция «Ссылка», которая позволяет скопировать ссылку на вкладку «Транзакции» для данного события.

Двойной щелчок по транзакции в списке откроет окно «Детали транзакции», представленное на снимке экрана 14.



Снимок экрана 14 – Детали транзакции

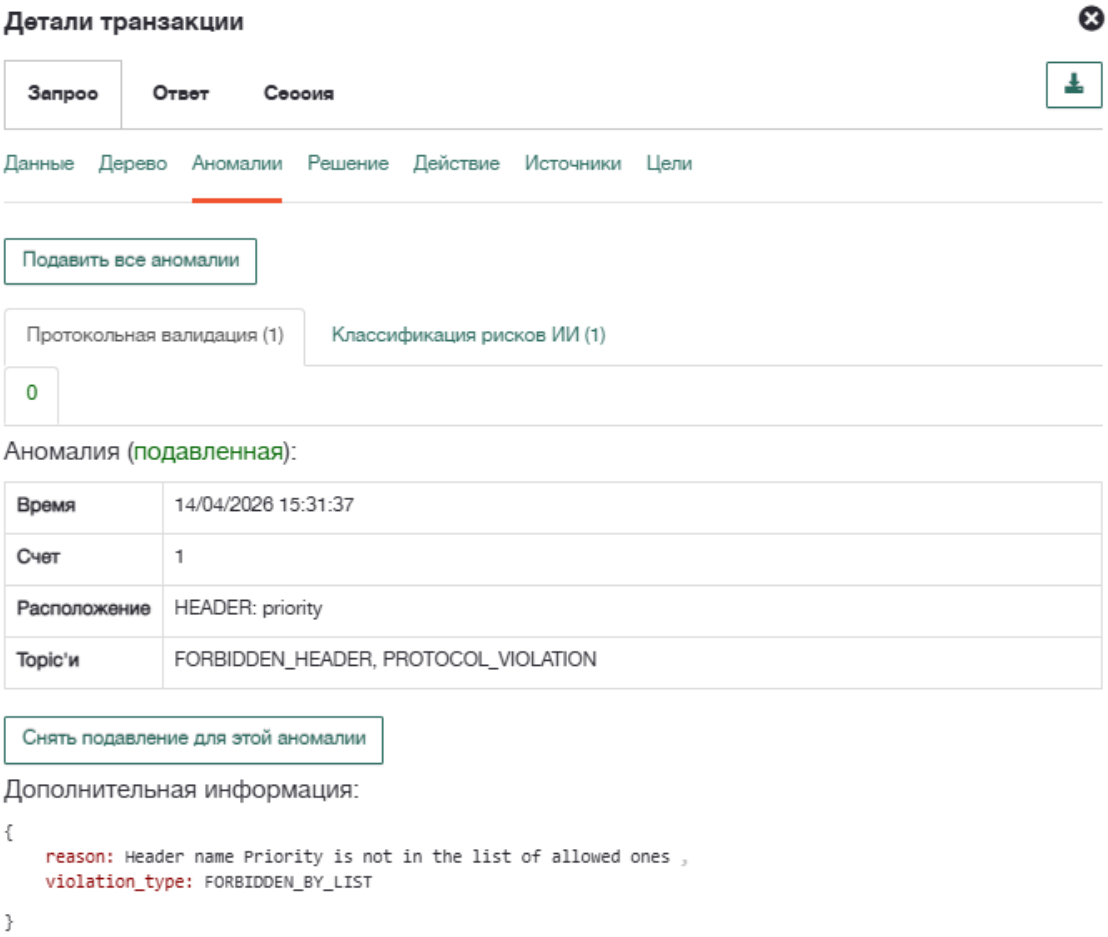
В окне «Детали транзакции» доступно три вкладки:

- Запрос;
- Ответ;
- Сессия.

Во вкладке «Запрос» доступно семь представлений:

- Данные – содержит данные запроса транзакции.
- Дерево – представлено дерево разбора запроса транзакции. Каждую ветвь можно развернуть или свернуть, пользуясь кнопками «⊕» и «⊖» соответственно, для ознакомления и анализа дерева запроса транзакции.
- Аномалии – содержит список всех аномалий, отсортированных по детектору, выявившему аномалию. Для каждого сработавшего детектора в представлении «Аномалии» существует вкладка с указанием количества срабатываний. Так, например, для рассматриваемой на снимке экрана 15 транзакции детекторы «Протокольная валидация» и «Классификация рисков ИИ» сработали по одному разу. Аномалии в представлении можно подавить списком, нажав «Подавить все аномалии», или по отдельности, нажав «Подавить эту аномалию» под описанием аномалии. В

последнем случае откроется окно «Подавление», позволяющее отредактировать свойства подавляемой аномалию. В случае подавления аномалий списком откроется полный список подавляемых аномалий, где каждую аномалию можно исключить из списка подавляемых, нажав « - », и отредактировать, нажав « ». Также можно снять подавление выбранной аномалии, воспользовавшись соответствующей кнопкой.



Снимок экрана 15 – Представление «Аномалии»

– Решение – содержит данные о принятом SolidWall AI Security Gateway решении по транзакции, а также список сработавших правил.

– Действие – содержит список возможных действий на основе данной транзакции, если таковые заданы. Действия позволяет тонко настраивать приложения и подавление аномалий. Для создания нового действия на основе транзакции необходимо нажать «Создать действие на основе этой транзакции».

– Источники – на вкладке отображается список источников для данной транзакции.

– Цели - на вкладке отображаются цели транзакции.

На вкладке «Ответ» окна «Детали транзакции» содержаться данные ответа, дерево и информация о принятом решении. На вкладе «Сессии» представлены данные сессии запроса и ответа.

Для закрытия окна «Детали транзакции» необходимо щёлкнуть мышкой за пределами окна или нажать на пиктограмму «».

На вкладке «Источники» окна подробной информации о событии доступна информация об IP-адресах и пользователях источников, если они определены. Информация об IP-адресах доступна в трёх представлениях: географическое расположение, IP-адреса и автономные системы, как показано на снимке экрана 16.

Снимок экрана 16 – Вкладка «Источники»

Во вкладке «Цели» доступна информация о целях транзакций, если они определены.

Во вкладке «Аномалии» доступна информация о выявленных аномалиях по модулям анализа и по видам, указано количество выявленных аномалий и частота их появления.

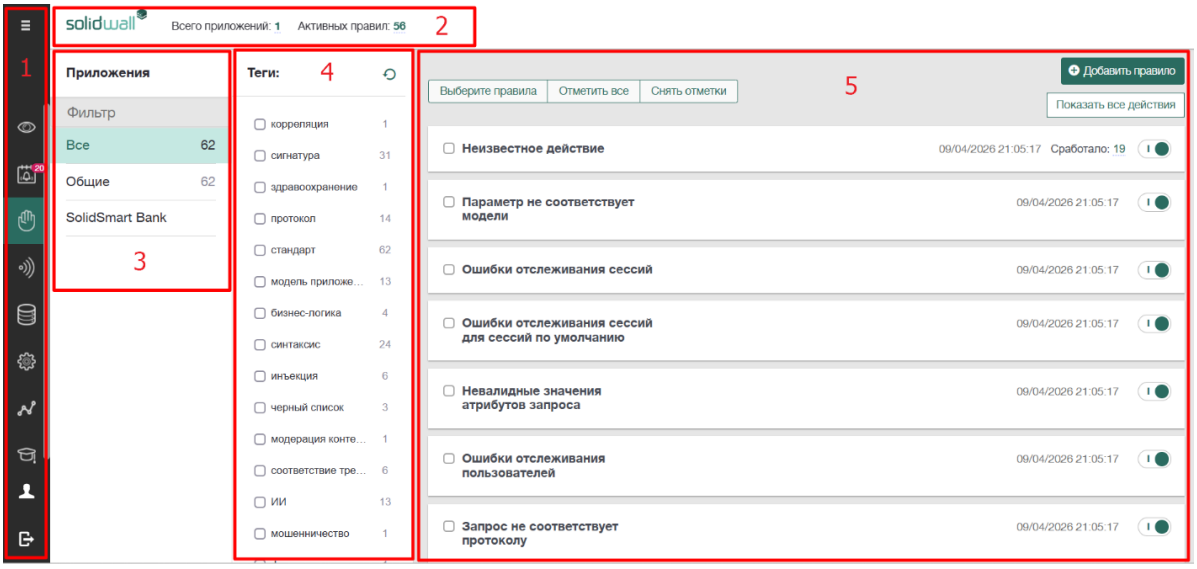
Для событий, перемещённых в архив, доступно полное ознакомление с полной информацией о событии.

3.4 Окно «Правила»

Окно «Правила» содержит пять блоков, представленных на снимке экрана 17:

1. Меню.
2. Общая информация.
3. Приложения.
4. Теги.
5. Правила.

В блоке 3 перечислены приложения, для которых созданы правила.

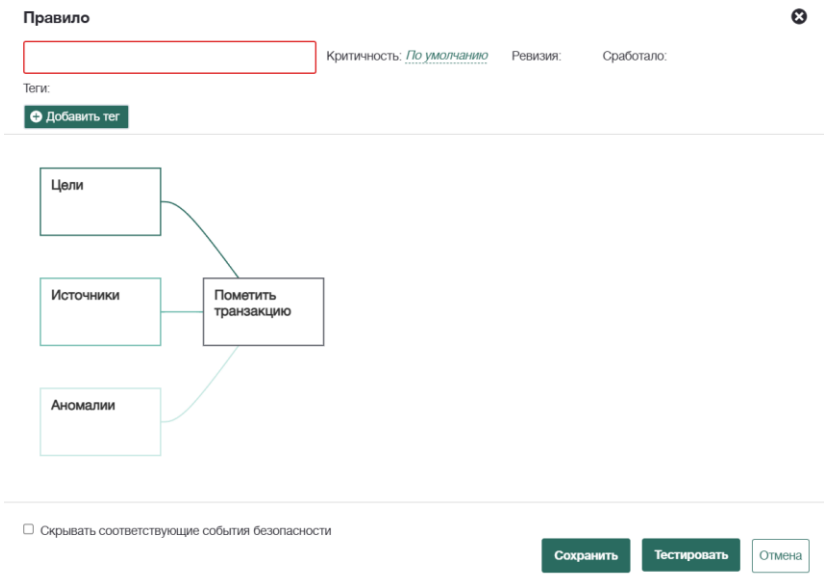


Снимок экрана 17 – Окно «Правила»

В блоке 4 перечислены теги, по которым можно фильтровать созданные правила.

В блоке 5 перечислены созданные правила. Оператору недоступны добавление, перенос, а также удаление, включение, выключение правил и добавление тега.

Администратор и Аналитик могут создавать новые правила, нажав кнопку «Добавить правило» в правом верхнем углу блока 5. Откроется окно создания правила, как показано на снимке 18.

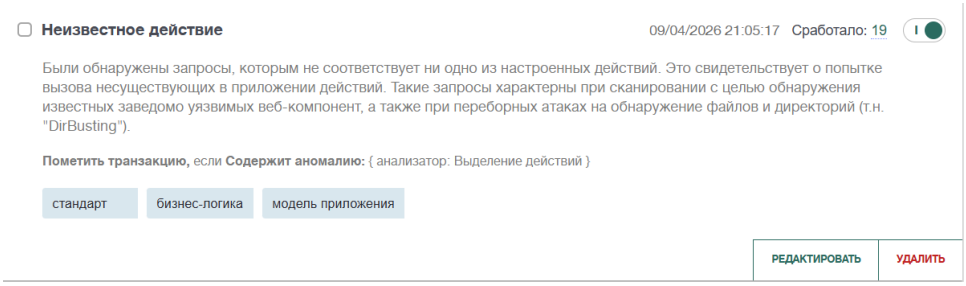


Снимок экрана 18 – Окно создания правила

В данном окне можно добавить теги из существующих или создать новые теги, добавить цели, источники, аномалии и определить действие, задать критичность правила, а также скрывать события безопасности включением соответствующего чекбокса.

Для поиска правил необходимо выставить отметки напротив тегов в блоке 4, которые относятся к правилу, а также в правом верхнем углу блока 5 указать тип действия интересующего правила в меню «Показать все действия»: все действия, разрешающие, блокирующие, помечающие. Для того чтобы сбросить теги, необходимо нажать на пиктограмму «».

При нажатии на правило в блоке 5 открывается общая информация о правиле: краткое описание правила, теги правила, дата создания, количество срабатываний. Администратору и Аналитику также доступно включение/выключение, редактирование, удаление правила, а также перемещение правила в списке (см. снимок экрана 19). Оператору доступна только общая информация о правиле.

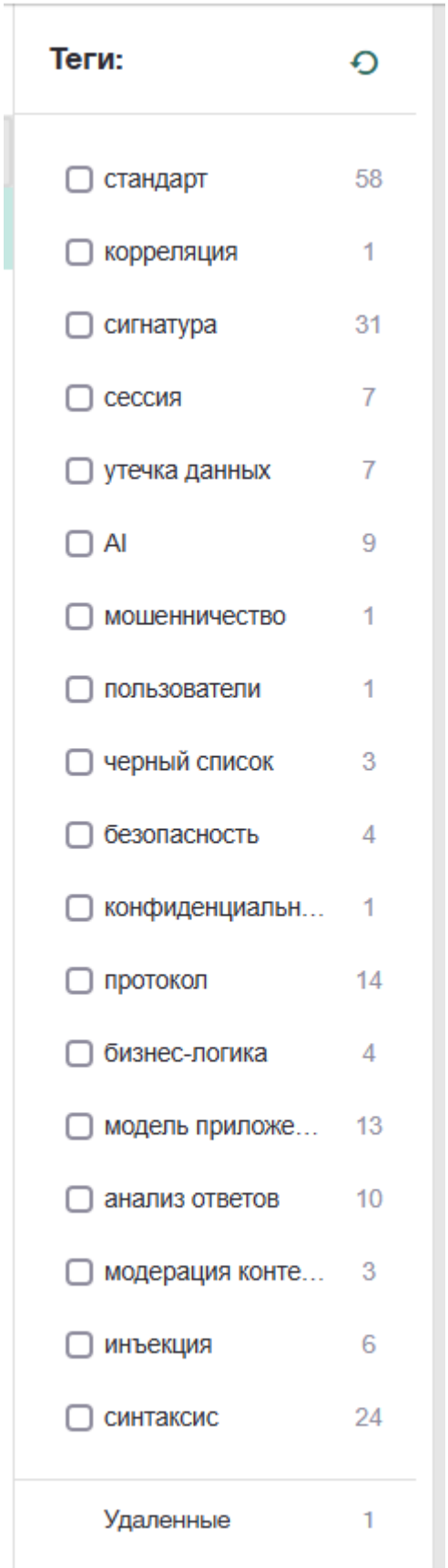


Снимок экрана 19 – Общая информация о правиле в представлении Администратора и Аналитика

Для включения или выключения правила необходимо передвинуть переключатель, находящийся в правом верхнем углу блока правила.

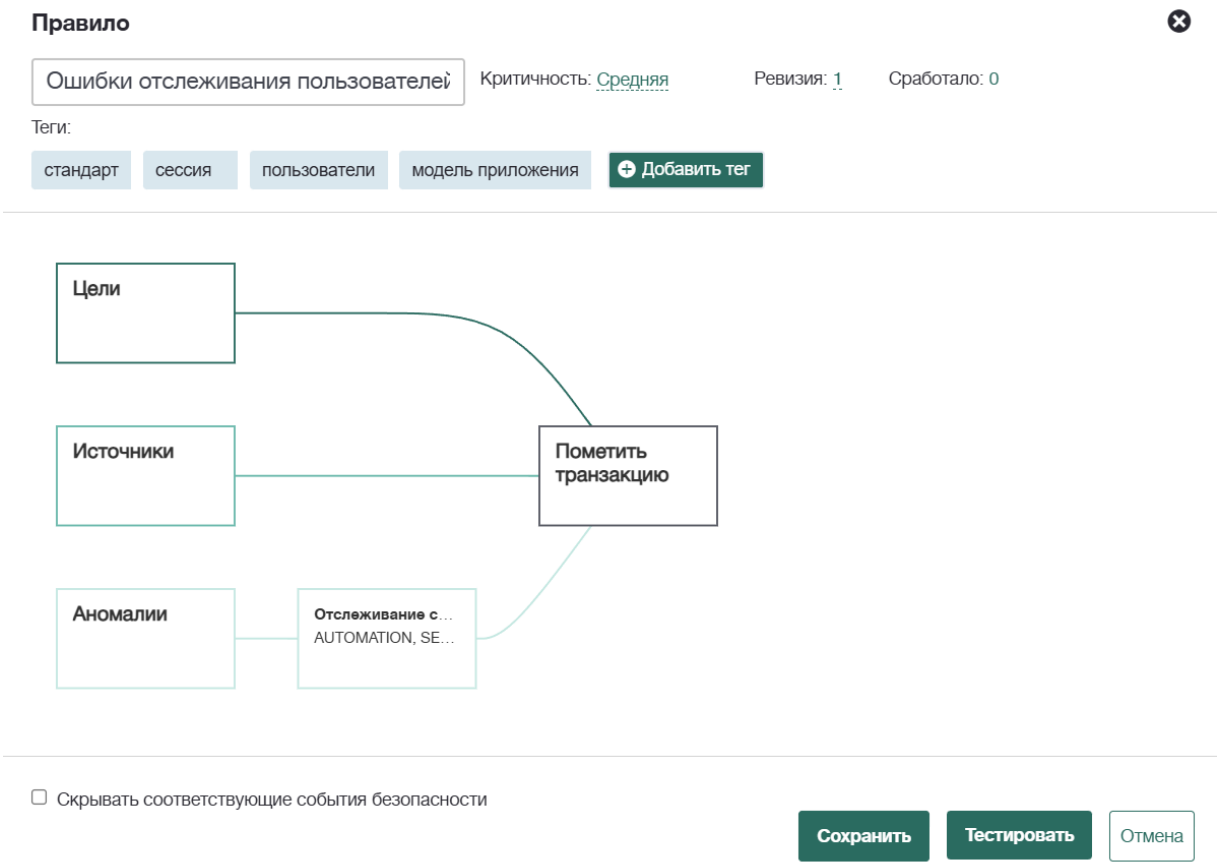
После нажатия кнопки «Удалить» правило перемещается в «Удалённые» и доступно под списком тегов в блоке 4 (см. снимок экрана 20). Для восстановления правила необходимо перейти в «Удаленные», выбрать нужное правило и в блоке правила нажать «Восстановить».

Важно! Правила после удаления восстанавливаются в выключенном состоянии, не забудьте включить правило, если это необходимо.



Снимок экрана 20 – Блок «Теги»

После нажатия «Редактировать» откроется окно «Правило», представленное на снимке экрана 21. В данном окне можно добавить или удалить теги, цели, источники, аномалии и изменить действие, а также изменить критичность правила.



Снимок экрана 21 – Редактирование правила

Для перемещения правила необходимо навести курсор на левый угол блока правила, затем щёлкнуть по появившимся трём вертикальным точкам и удерживать левую клавишу мыши, перемещая правило. Перемещение правил изменяет приоритет срабатывания: правила, расположенные выше в списке, имеют больший приоритет, чем правила, расположенные ниже.

Все возможные параметры, используемые при создании правил отражены в таблице 2.

Таблица 2 – Параметры, используемые при создании правил

Спецификация	Возможные классы спецификации транзакции	Возможные параметры	Примечание
Цели	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

Спецификация	Возможные классы спецификации транзакции	Возможные параметры	Примечание
	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 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	Успех	Правило сработает для успешно выполненных действий
		Ошибка валидации	Правило сработает для транзакций с ошибкой валидации
		Ошибка логики	Правило сработает для транзакций с ошибкой логики
		Неизвестно	Правило сработает для действий, результат которых неизвестен

Спецификация	Возможные классы спецификации транзакции	Возможные параметры	Примечание
		Использовать отрицание условия	Правило не сработает для транзакций с выбранным результатом
Источники	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 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
		Укажите маску подсети	
		Использовать отрицание условия	Правило работает для всех запросов кроме запросов, поступающих с указанного IP-

Спецификация	Возможные классы спецификации транзакции	Возможные параметры	Примечание
			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
		Использовать отрицание условия	Правило работает для запросов кроме запросов, поступающих с указанного ASN
	Проверка источника (корректное значение)	Укажите источник	Правило сработает для транзакций с указанным источником
		Укажите значение для поиска совпадения	Правило сработает для всех источников, удовлетворяющих условию
		Использовать отрицание условия	Правило не сработает для транзакций с указанным источником и значением
	Проверка источника (любое значение)	Укажите источник	Правило сработает для транзакций с указанным источником
		Использовать отрицание условия	Правило не сработает для транзакций с указанным источником
	Верифицированный бот	Укажите бота для верификации	Правило сработает для транзакций, связанных с ботом
		Использовать отрицание условия	Правило не сработает для транзакций, связанных с ботом

Спецификация	Возможные классы спецификации транзакции	Возможные параметры	Примечание
Аномалии	Наличие любой аномалии	—	Правило работает для любой транзакции с выявленной аномалией
		Использовать отрицание условия	Правило – работает для всего трафика, в котором не выявлены аномалии
	Наличие аномалии с заданными свойствами	Выберите модуль анализа (Выделение действий; Проверка синтаксиса параметров действий; Обнаружение ботов по временным характеристикам трафика; Обнаружение переборных атак; Детектор CSFR-атак; проверка особых атрибутов сессии; Разбор запроса; Разбор ответа; Интеграция с сигнатурным анализом на ICAP-сервере; Обнаружение инъекций; Сигнатурный анализ; Модуль обратного прокси; Обнаружение открытого перенаправления; Протокольная валидация; Обнаружение аномалий в последовательностях действий; Отслеживание сессий;	Правило работает для транзакции с выявленной выбранным модулем аномалией. Обязательное поле

Спецификация	Возможные классы спецификации транзакции	Возможные параметры	Примечание
		Обнаружение кратковременных сигнатур; Классификация рисков ИИ)	
		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; Параметр в теле запроса; URL в целом; Параметр URL; Cookie; Элемент дерева разбора; Источник; Цель/Объект веб-приложения)	Правило работает для транзакции с выявленной выбранным модулем аномалией, с указанным расположением
		Выберите имя расположения аномалии	Правило работает для транзакции с выявленной выбранным модулем аномалией, с указанным расположением и указанным именем расположения аномалии
		Использовать отрицание условия	Правило работает для всех транзакций кроме транзакций, соответствующих указанным параметрам
Действие	Блокировать транзакцию	—	Транзакция, соответствующая заданным в спецификациях «Цели», «Источники» и «Аномалии», блокируется

Спецификация	Возможные классы спецификации транзакции	Возможные параметры	Примечание
		Использовать особый шаблон ответа	Правило позволяет скрыть информацию в ответе приложения
	Разрешить транзакцию	—	Транзакция, соответствующая заданным в спецификациях «Цели», «Источники» и «Аномалии», пропускается как легитимная
	Пометить транзакцию	—	Транзакция, соответствующая заданным в спецификациях «Цели», «Источники» и «Аномалии», помечается для дальнейшего анализа. Используется как действие по умолчанию
	Добавить значение источника в список	Решение для транзакции (Блокировать транзакцию; Разрешить транзакцию; Пометить транзакцию; Продолжить анализ)	По транзакции будет принято выбранное решение, а значение источника попадёт в указанный Источник
		Использовать особый шаблон ответа (при выборе параметра «Блокировать транзакцию)	Правило позволяет скрыть информацию в ответе приложения
		Источник	Источник транзакции будет добавлен к списку Источников
		Список	Источник транзакции будут добавлен к Списку
		Описание добавляемого в список элемента	К добавляемому значению будет добавлен комментарий
		Время жизни добавляемого элемента (в секундах)	Для добавляемого элемента будет определено время жизни

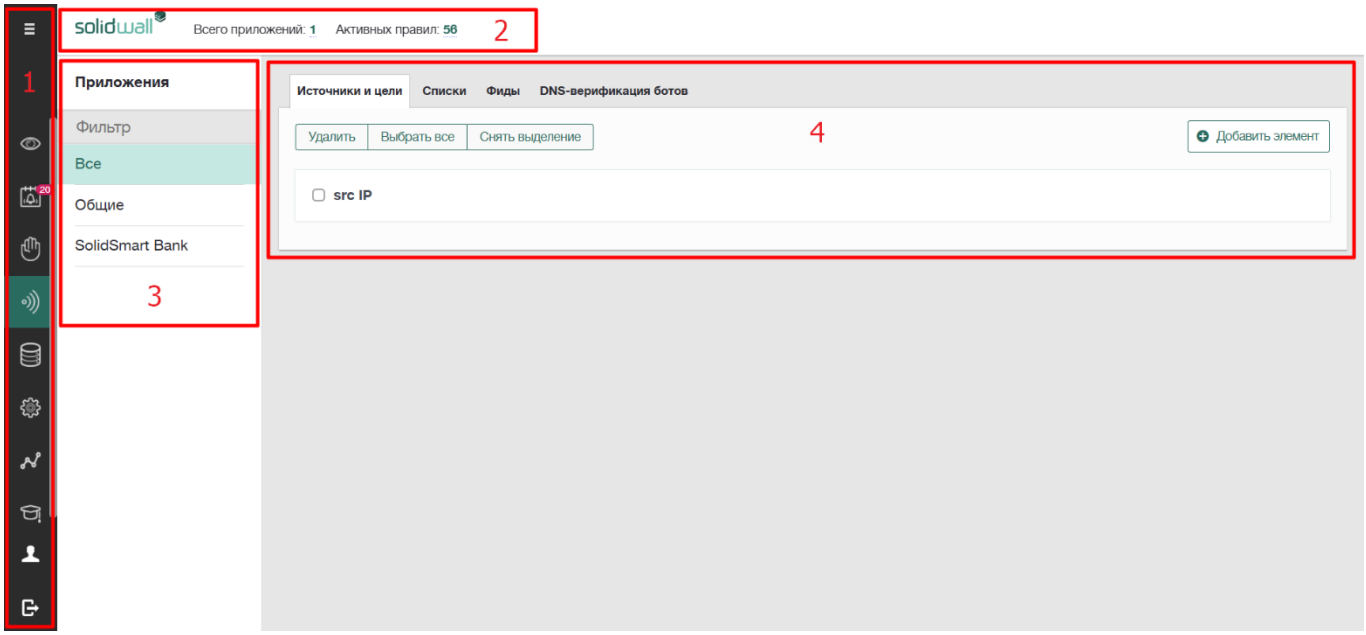
3.5 Окно «Источники, списки, цели»

Окно «События» содержит четыре блока, представленные на снимке экрана 22:

1. Меню.
2. Общая информация.
3. Приложения.
4. Источники и цели. Списки. Фиды. DNS-верификация ботов.

В блоке 3 можно выбрать конкретное приложение.

В блоке 4 для всех ролей пользователей доступны вкладки «Источники и цели», «Списки», «Фиды» и «DNS-верификация ботов». Оператору доступен только просмотр информации в данных вкладках.



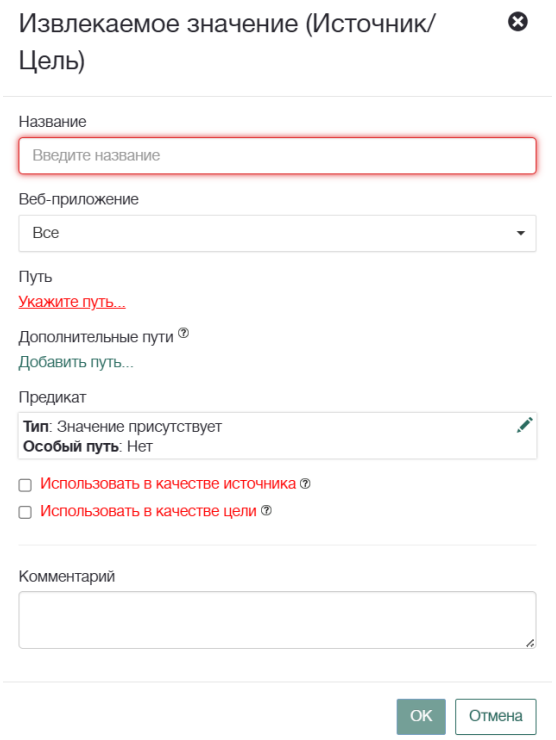
Снимок экрана 22 – Окно «Источники, цели, списки», вкладка «Источники и цели»

3.5.1 Вкладка «Источники и цели»

Во вкладке «Источники и цели» есть возможность использовать функциональность «src IP» включением/выключением чекбокса.

Пользователям с ролями «Администратор» и «Аналитик» доступно создание новых источников/целей.

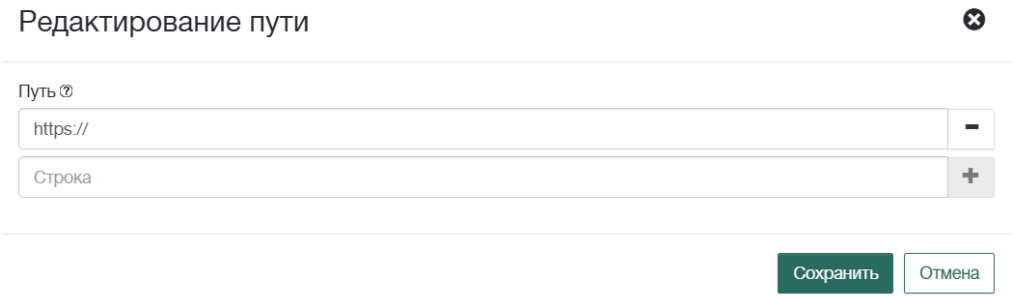
Для создания нового источника/цели нужно нажать на кнопку «Добавить элемент», расположенную в правом верхнем углу. Откроется окно «Извлекаемое значение (Источник/Цель)» (см. снимок экрана 23).



Снимок экрана 23 – Окно «Извлекаемое значение (Источник/Цель)»

В данном окне следует:

1. В поле «Название» вести название нового источника/цели.
2. В раскрывающемся списке «Веб-приложение» выбрать веб-приложение или для удобства поиска написать его название в поле ввода текста.
3. Нажать кнопку «Укажите путь».
4. В поле «Путь» открывшегося окна «Редактирование пути» указать путь в дереве разбора запроса. Для добавления элементов пути до нужного узла со значением источника/цели необходимо нажать «+». После заполнения полей следует нажать кнопку «Сохранить» (см. снимок экрана 24).

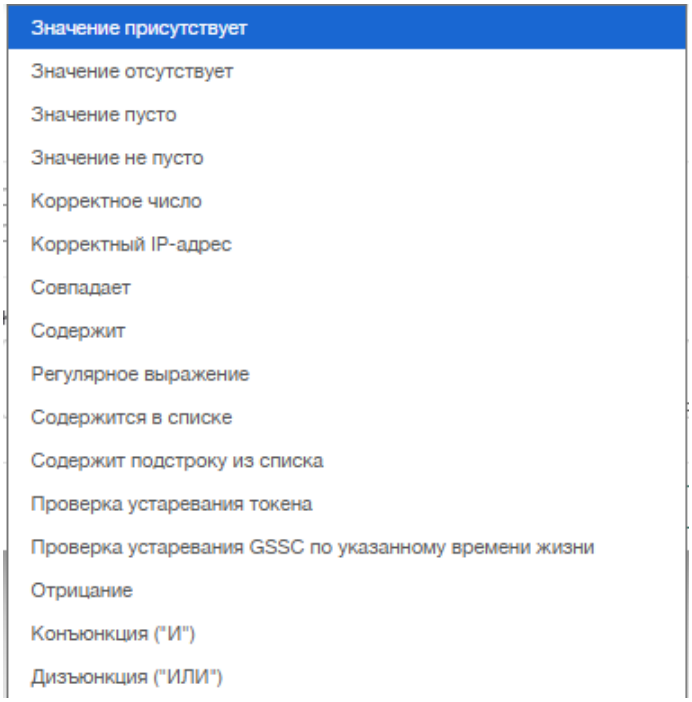


Снимок экрана 24 – Окно «Редактирование пути»

5. При необходимости добавления дополнительного пути для извлечения значения из дерева разбора следует нажать кнопку «Добавить путь». В открывшемся окне «Редактирование пути» требуется выполнить действия, указанные на шаге 4.
6. Далее следует выбрать предикат извлекаемого значения. Для этого необходимо:

6.1. Нажать иконку « ».

6.2. В выпадающем списке «Тип предиката извлекаемого значения» выбрать необходимый тип (см. снимок экрана 25).



Снимок экрана 25 – Выпадающем списке «Тип предиката используемого значения»

При проверке наличия в запросе источника/цели сначала будет извлечено значение токена по выбранному пути. Затем выбранный предикат применяется к извлеченному значению. Если предикат вычисляется в True, то считается, что источник/цель с заданным именем и значением успешно найден в запросе. В ином случае считается, что данного источника в запросе нет. Доступны следующие предикаты:

- Значение присутствует – в дереве разбора есть указанный путь (но значение в этой вершине дерева разбора никак не проверяется).
- Значение отсутствует – в дереве разбора отсутствует указанный путь.
- Значение пусто – путь присутствует, но значение токена – пустая стока.
- Значение не пусто – значение токена отличается от пустой строки.
- Корректное число – токен является корректным целым числом.
- Корректный IP адрес – токен является корректным IP-адресом.
- Совпадает – значение токена совпадает с заданной строгой.
- Содержит – значение токена содержит заданную подстроку.
- Регулярное выражение – значение токена удовлетворяет заданному регулярному выражению.
- Содержится в списке – один из элементов списка (см. подраздел 3.5.2).
- Содержит подстроку из списка – значение токена содержит подстроку из списка;

– Проверка устаревания токена – необходимо выбрать нужное поле и указать параметры жизни токена (путь к дереву разбора к моменту устаревания токена/к моменту создания токена/времени жизни токена).

– Проверка устаревания GSSC по указанному времени жизни – задаётся время жизни в секунду.

– Отрицание – отрицание предиката.

– Конъюнкция («И») – объединение нескольких предикатов.

– Дизъюнкция («ИЛИ») – выбор одного из нескольких предикатов.

6.3. Для указания особого пути предиката источника необходимо нажать кнопку «Укажите путь». В открывшемся окне «Редактирование пути» требуется выполнить действия, указанные на шаге 4.

6.4. Нажать кнопку «  ».

7. Чекбоксы «Использовать в качестве источника», «Использовать в качестве цели» – необходимо выбрать хотя бы один из вариантов. Извлекаемое значение может быть использовано в качестве цели или источника, или в обеих ролях – в зависимости от выбора.
8. В поле «Комментарий» можно добавит описание. Поле заполнять необязательно.
9. Нажать кнопку «ОК».

После сохранения нового источника/цели во вкладке «Источники и цели» можно увидеть новый добавленный источник/цель. Нажатие на каждый из источников/цель позволяет так же увидеть его основные характеристики (название, путь в дереве разбора, тип применяемого предиката). Для редактирования существующих источников/целей и их удаления используются соответствующие кнопки, расположенные в правом нижнем углу каждого блока источника. Аналитикам доступно редактирование и удаление источников/целей, созданных аналитиками. Администраторам доступно редактирование и удаление всех созданных источников.

3.5.2 Вкладка «Списки»

Для работы со списками следует перейти на вкладку «Списки». Кнопка «Добавить список» позволяет создать новый список. В открывшемся окне «Список» следует ввести название создаваемого списка; выбрать веб-приложения, для которых заводится данный список; выбрать тип элементов, которые содержатся в списке. Доступны три типа элементов:

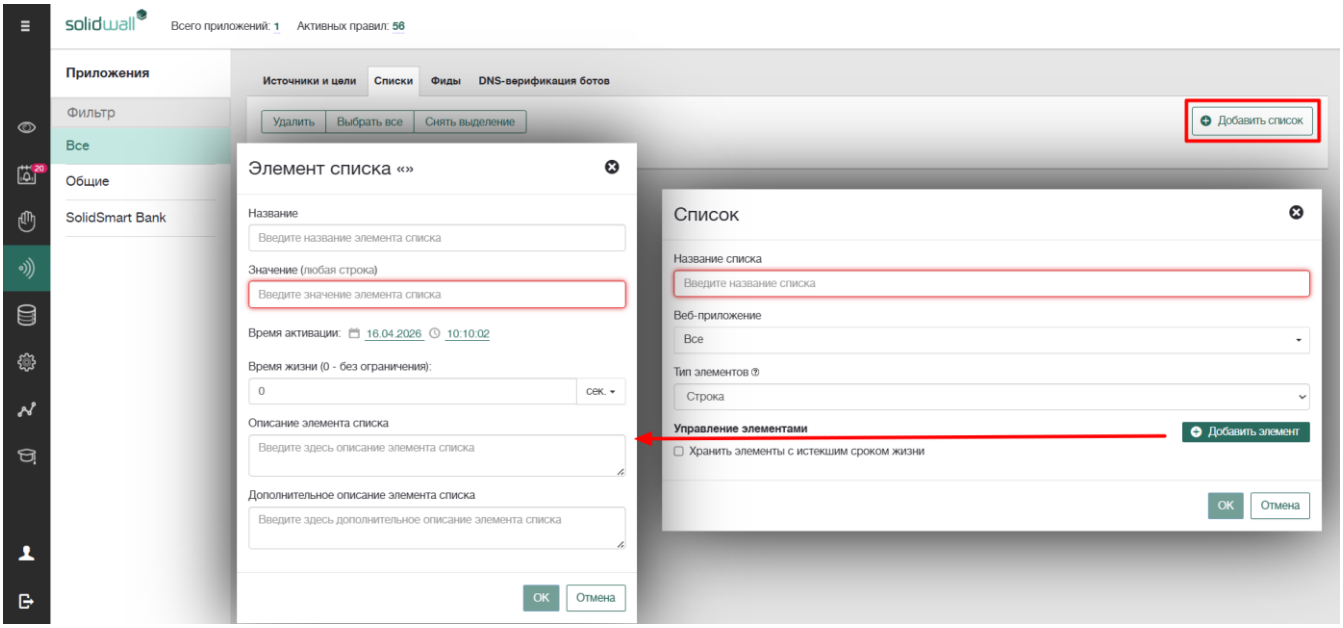
– Строка;

– Целое число;

– IP-адрес.

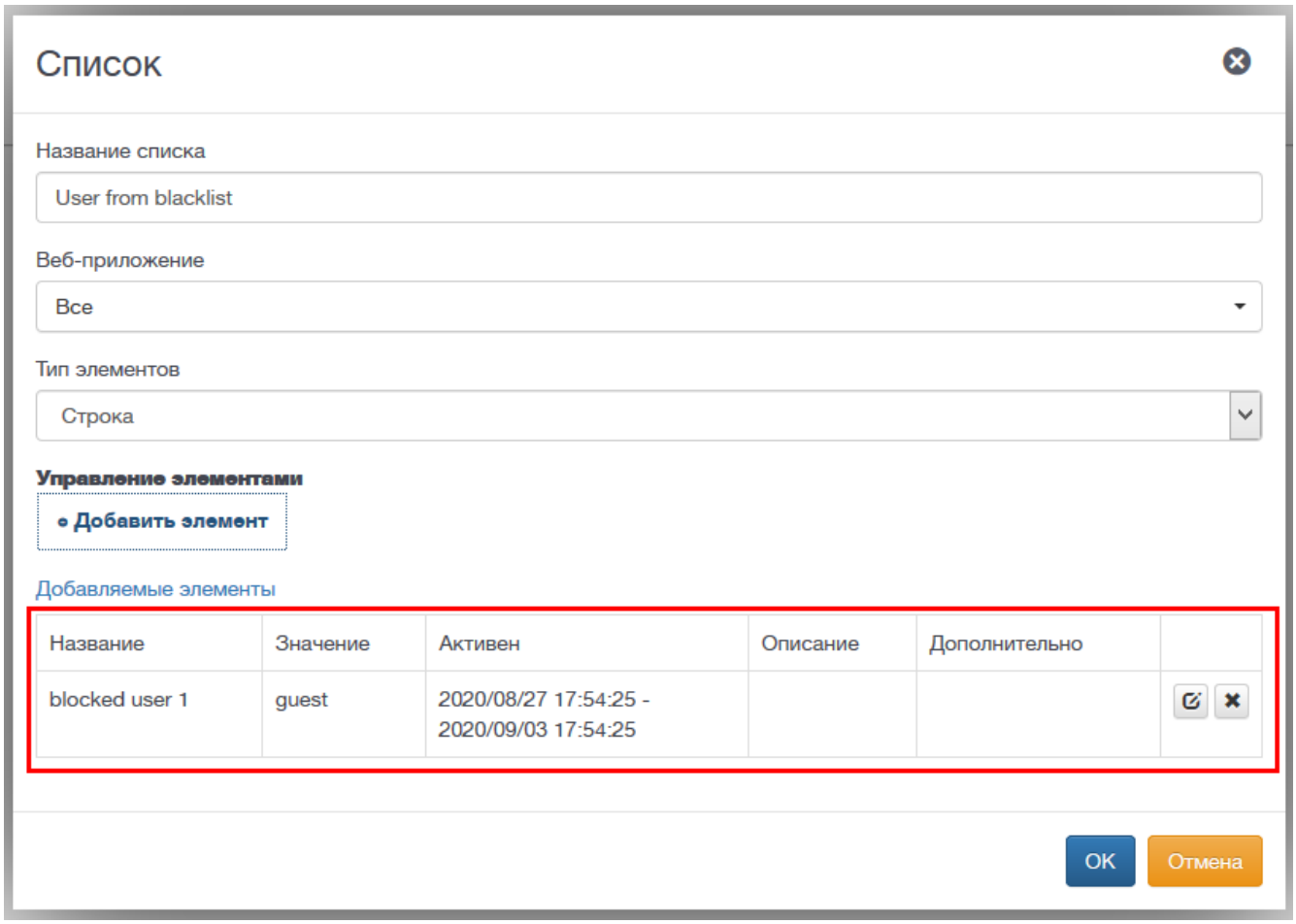
После этого следует по одному добавить в создаваемый список его элементы, нажав кнопку «Добавить элемент».

В открывшемся окне «Элемент списка» для добавляемого элемента требуется ввести имя и значение элемента. Кроме этого, для каждого элемента можно задать отдельную дату его активации (см. снимок экрана 26).



Снимок экрана 26 – Вкладка «Списки», окна «Список» и «Элемент списка»

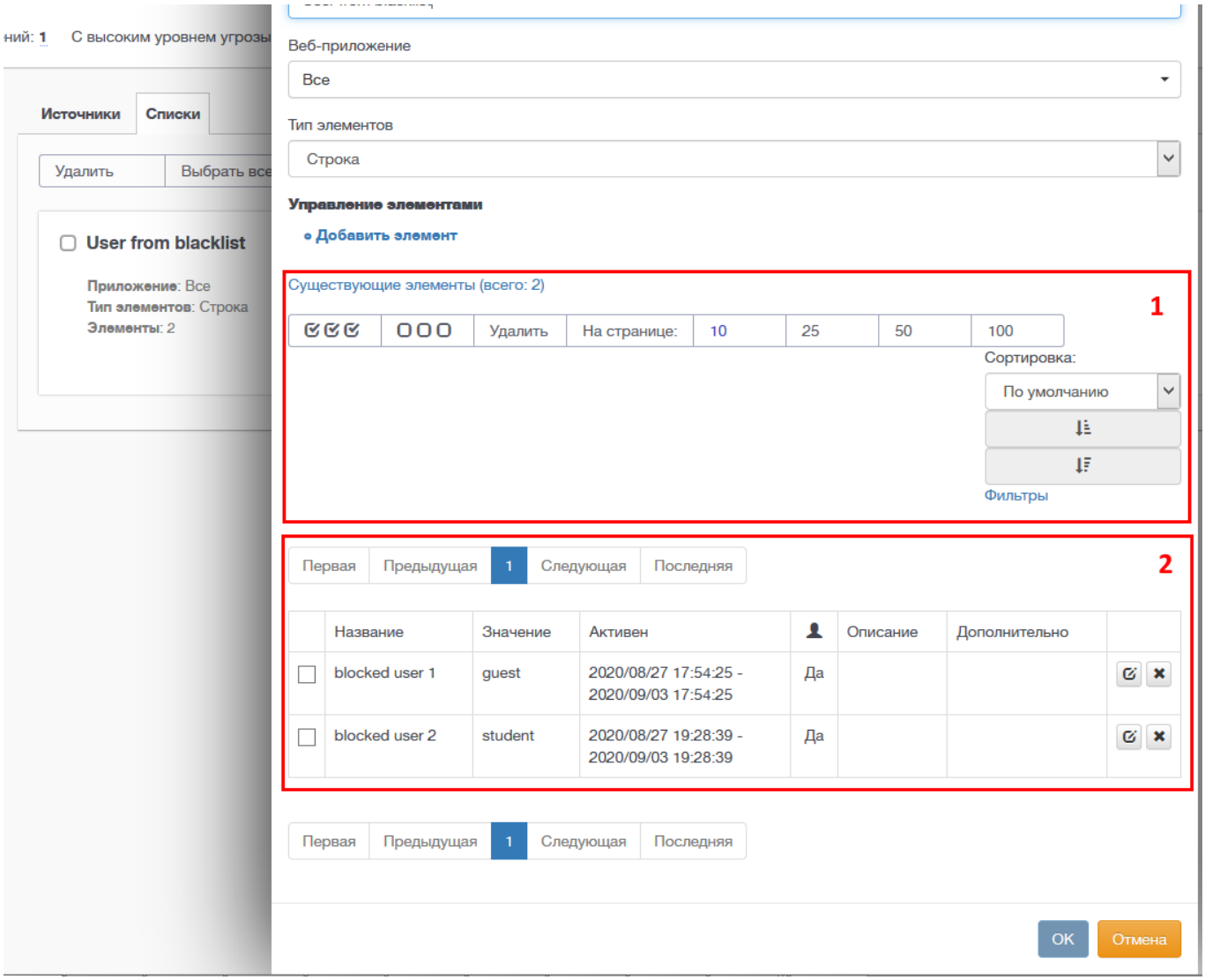
По результатам добавления элементов, окно создаваемого списка изменит свой вид. Теперь в нем будут показаны новые добавляемые элементы, которые попадут в список при его сохранении по нажатию на кнопку «OK» (см. снимок экрана 27).



Снимок экрана 27 – Окно создания списка

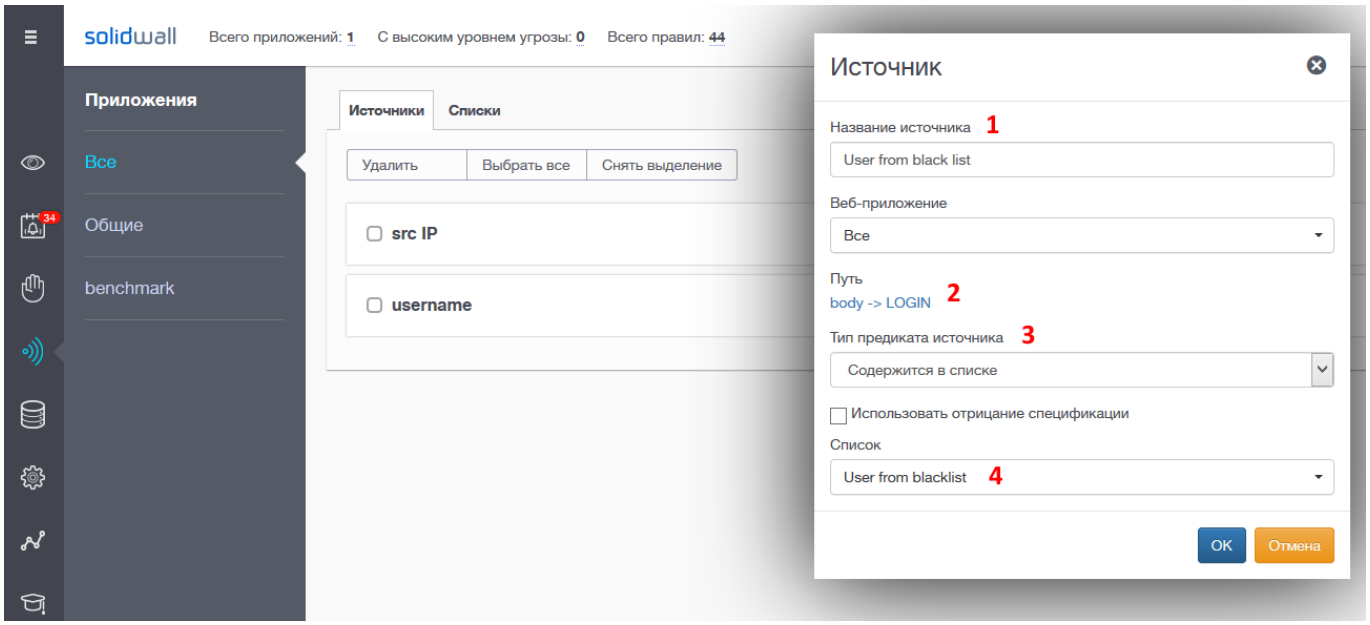
При создании и редактировании списков существует возможность настройки отображения элементов (см. снимок экрана 28, 1), например, выбрать порядок сортировки, число отображаемых на странице элементов и т. п.

Кроме того, доступен просмотр характеристик элементов списка, а также редактирование отдельных элементов и их удаление (см. снимок экрана 28, 2).



Снимок экрана 28 – Окно «Список»

Для использования списка требуется создать новый источник (см. снимок экрана 29, 1). Ввести путь в дереве разбора (см. снимок экрана 29, 2). Выбрать «Содержится в списке» в качестве предиката (см. снимок экрана 29, 3). И затем выбрать подходящий список из числа созданных ранее (см. снимок экрана 29, 4).



Снимок экрана 29 – Использование списков в окне «Источник»

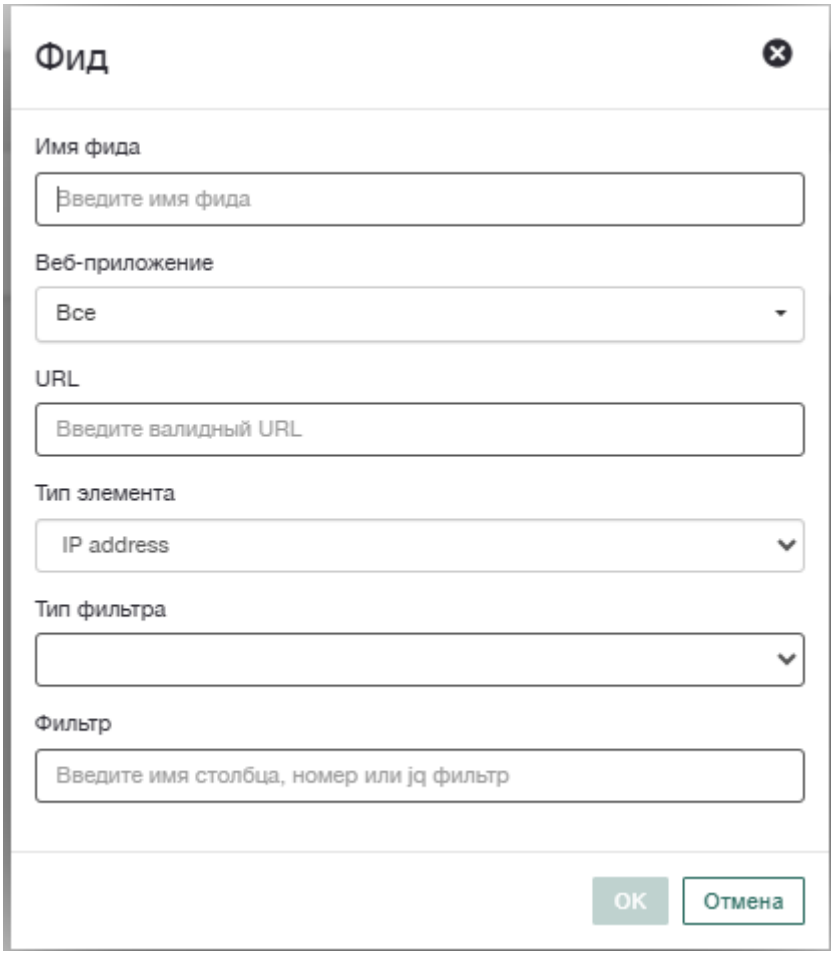
При просмотре информации о таких источниках можно быстро проверить, принадлежность к какому из списков будет проверяться для этого источника в его предикате.

3.5.3 Вкладка «Фиды»

Вкладка «Фиды» позволяет выделить отдельные элементы фидов для отслеживания взаимодействий по ним.

Для создания объекта необходимо нажать «+Добавить фид» в правом верхнем углу вкладки. В появившемся окне (см. снимок экрана 30) необходимо заполнить поля:

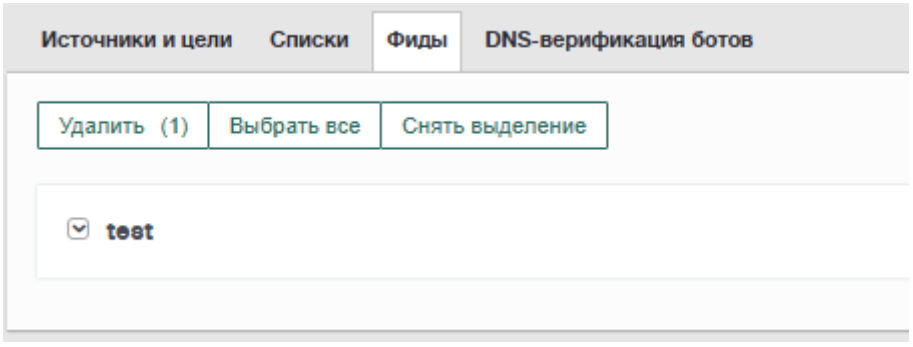
- Имя фида – для удобства обращения к данному элементу.
- Веб-приложение – указать приложение из имеющихся, к которому относится данный элемент.
- URL – ввести валидный URL источника фидов.
- Тип элемента – требуется выбрать строковый тип или IP-адрес.
- Тип фильтра – в выпадающем меню необходимо обозначить тип используемого фильтра: имя или номер столбца в таблице *.csv или jq-фильтр для JSON.
- Фильтр – указывается значение фильтра, который необходимо отслеживать.



Снимок экрана 30 – Добавление фида

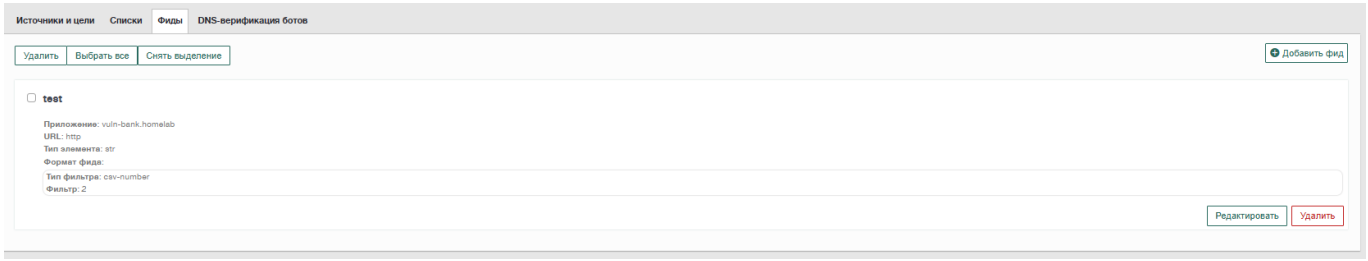
Созданные фиды можно редактировать и удалять.

Для удаления необходимо выбрать фиды, поставив метки напротив каждого удаляемого фида, а затем нажать «Удалить (N)» в верхнем левом углу вкладки, где N – количество удаляемых фидов (см. снимок экрана 31).



Снимок экрана 31 – Удаление фида

Для редактирования фида необходимо щёлкнуть по имени фида и в появившемся блоке свойств фида нажать «Редактировать» (см. снимок экрана 32). Появится окно редактирования свойств фида.



Снимок экрана 32 – Редактирование фида

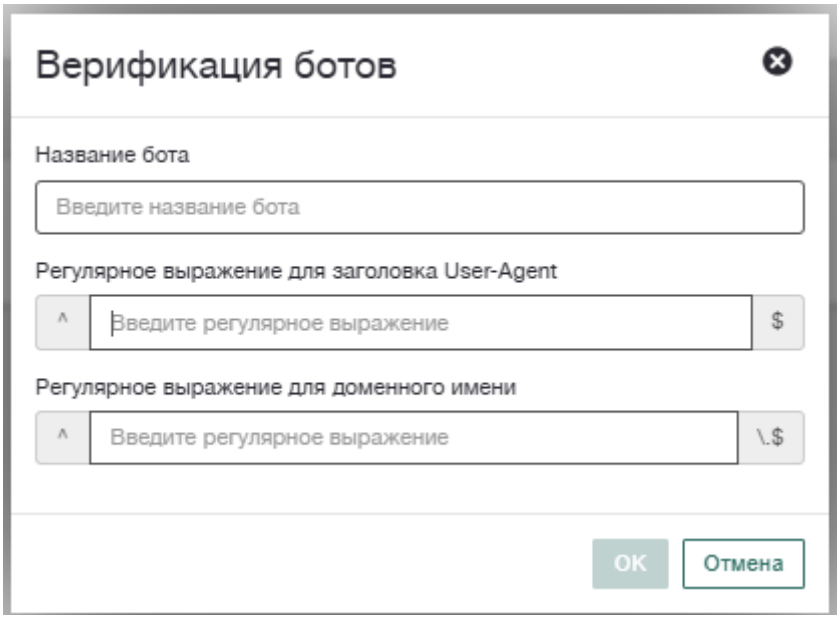
3.5.4 Вкладка «DNS-верификация ботов»

Вкладка «DNS-верификация ботов» позволяет добавить легитимных ботов, для этого необходимо нажать «+Добавить описание бота». В открывшемся окне (см. снимок экрана 33) необходимо заполнить поля:

– Название бота – любое имя, удобное для дальнейшего использования.

– Регулярное выражение для заголовка User-Agent – введите регулярное выражение без якорей.

– Регулярное выражение для доменного имени – введите регулярное выражение без якорей.



Снимок экрана 33 – Добавление описания ботов

3.6 Окно «Приложения»

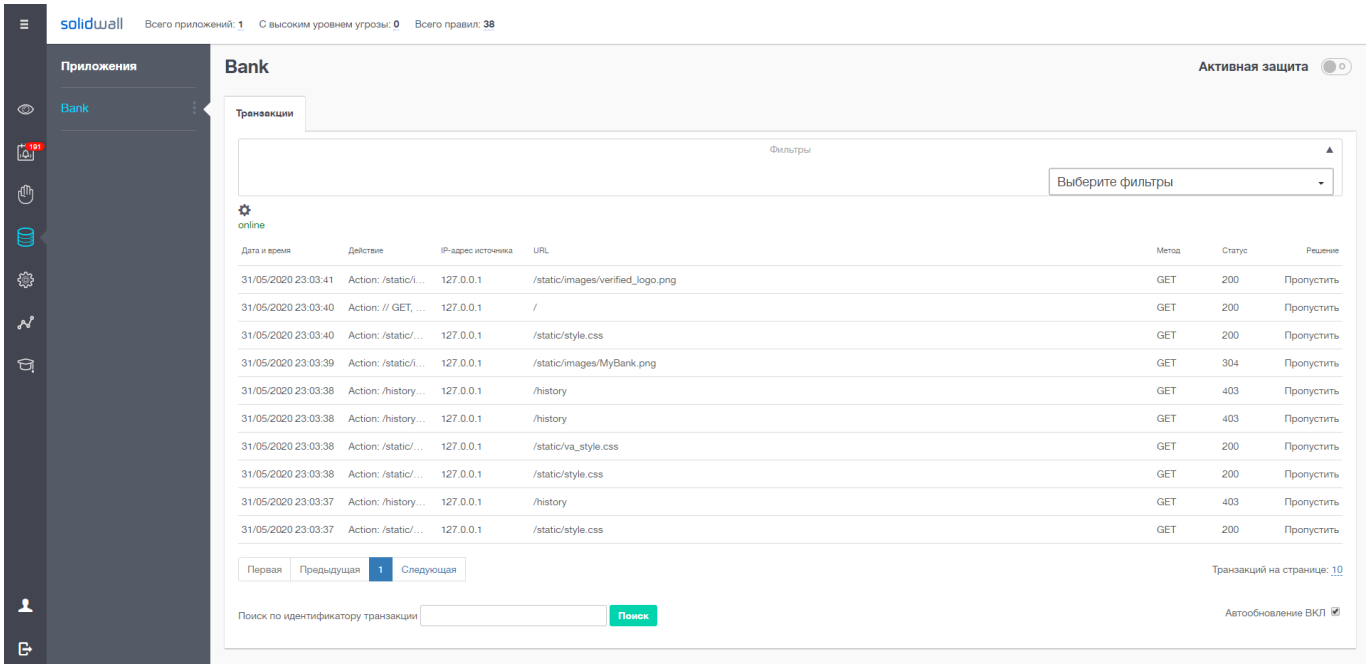
Окно «Приложения» для разных ролей существенно отличаются.

3.6.1 Интерфейс Оператора

В интерфейсе Оператора в окне «Приложения» доступен просмотр только транзакций приложения, как показано на снимке экрана 34.

На вкладке «Транзакции» представлен список всех транзакций события, длительность события, частота произведения транзакций. Для удобства просмотра можно использовать

заданные фильтры для поиска интересующих транзакций, для этого необходимо воспользоваться кнопкой «Фильтры» и заполнить соответствующие поля для каждого выбранного фильтра. Для того, чтобы отменить примененный фильтры в меню «Фильтры», в выпадающем подменю «Выберите фильтры» – необходимо нажать на «Снять выделение».

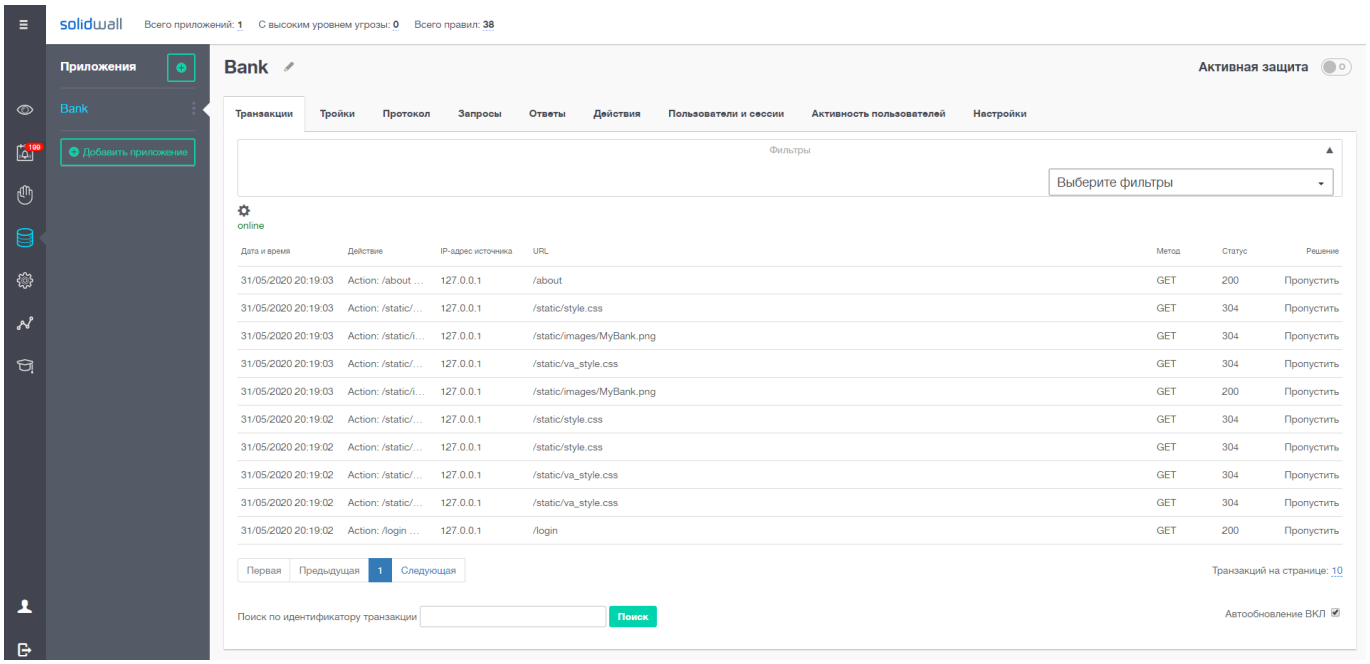


Снимок экрана 34 – Окно «Приложения» в интерфейсе Оператора

Двойной щелчок по транзакции открывает окно «Детали транзакции», описанное в разделе 3.2. На вкладке «Транзакции» можно изменить вид представления информации, для этого необходимо нажать пиктограмму с изображением шестерёнки «  ». В появившемся окне настроек таблицы транзакций можно добавить или убрать столбец, пользуясь стрелками между окнами, а также изменить порядок расположения столбцов, пользуясь стрелками, расположенными с правого края окна.

3.6.2 Интерфейс Аналитика

Интерфейс Аналитика в окне «Приложения» представлен на снимке экрана 35.

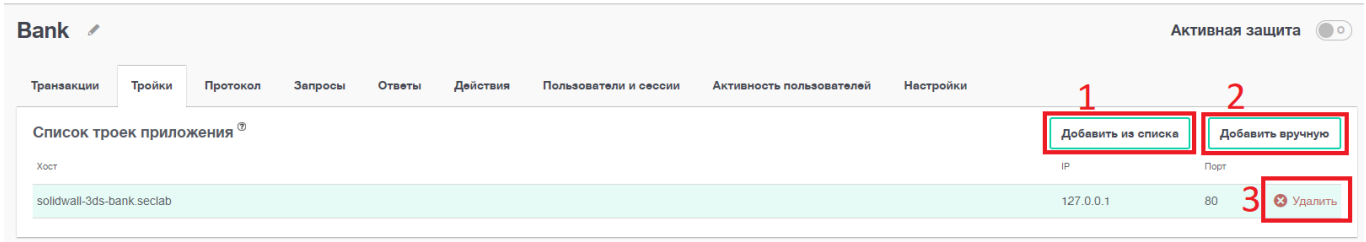


Снимок экрана 35 – Окно «Приложения» в интерфейсе Аналитика

Аналитику доступно девять вкладок:

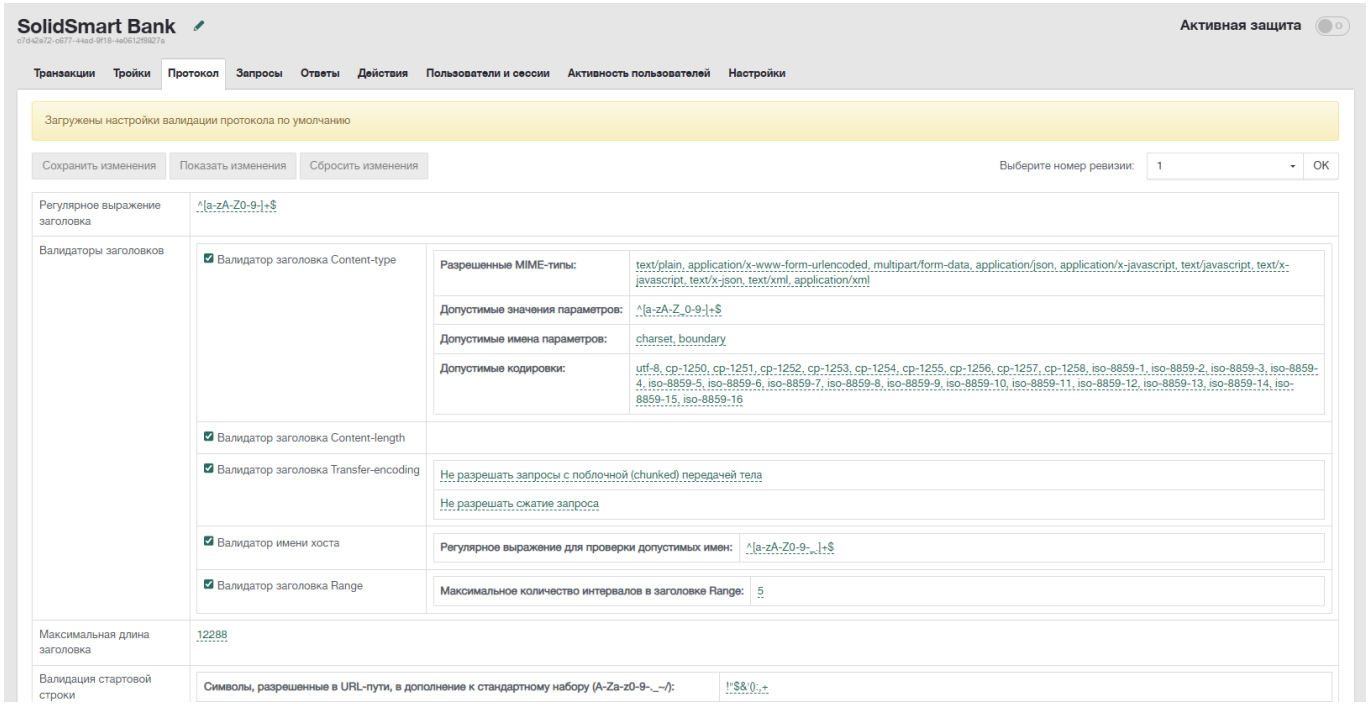
– Транзакции – полностью повторяет интерфейс Оператора.

– Тройки – на вкладке перечислены «Тройки»: Доменное имя, IP-адрес и Порт – определяющие приложение. Трафик, подходящий под значения «Тройки», считается относящимся к приложению. На вкладке можно добавить «Тройку» из списка или вручную, воспользовавшись соответствующими кнопками (см. снимок экрана 36, 1 и 2 соответственно), а также удалить ненужную «тройку», нажав «Удалить» справа от «Тройки» (см. снимок экрана 36, 3).



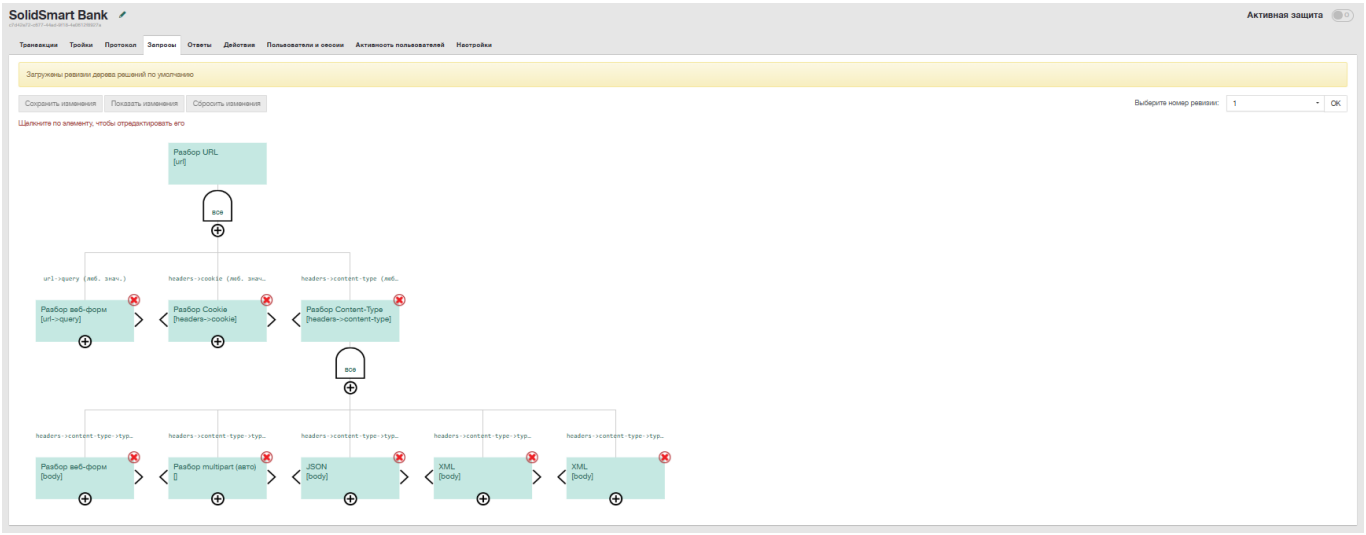
Снимок экрана 36 – Вкладка «Тройки»

– Протокол – на вкладке представлены настройки валидации протокола (см. снимок экрана 37). 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 «Показать изменения» откроется окно «Изменения», в котором все изменения представлены в виде кода.



Снимок экрана 37 – Вкладка «Протокол»

– Запросы – на вкладке представлено дерево решений по запросам (см. снимок экрана 38). Аналитику доступно изменение дерева: изменение каждого блока дерева, создание, удаление и перемещение ветвей. Для изменения блока необходимо дважды щёлкнуть по нему мышкой, и произвести доступные изменения в открывшемся окне. Для добавления нового блока необходимо нажать на пиктограмму «⊕», затем заполнить поля появившегося окна. Для создания новой ветки необходимо создать несколько блоков под одним «корневым» для этой ветки блоком. Для удаления блока необходимо нажать на пиктограмму «⊗» и подтвердить действие в появившемся окне. Блоки, находящиеся в одной ветке, можно перемещать между собой пользуясь пиктограммами «< >». Это позволит расположить блоки в порядке приоритета в случае, если под заголовком установлено условие «любой» (на примере используется условие «все», см. снимок экрана 38). Все изменения, как и во вкладке «Протокол», можно сохранить, просмотреть и сбросить, воспользовавшись блоком кнопок в верхней части вкладки.



Снимок экрана 38 – Вкладка «Запросы»

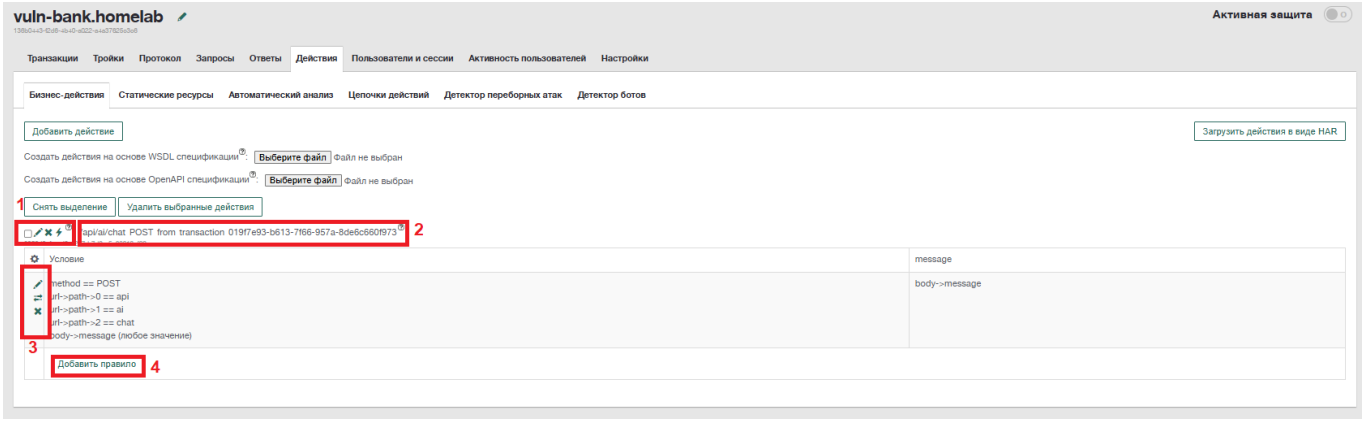
– Ответы – на вкладке представлено дерево решений по ответам. Аналитику доступно изменение дерева: изменение каждого блока дерева, создание, удаление и перемещение ветвей. Для изменения блока необходимо дважды щёлкнуть по нему мышкой, и произвести доступные изменения в открывшемся окне. Для добавления нового блока необходимо нажать на пиктограмму «⊕», затем заполнить поля появившегося окна. Для создания новой ветки необходимо создать несколько блоков под одним «корневым» для этой ветки блоком. Для удаления блока необходимо нажать на пиктограмму «⊗» и подтвердить действие в появившемся окне. Блоки, находящиеся в одной ветке, можно перемещать между собой пользуясь пиктограммами «<>». Это позволит расположить блоки в порядке приоритета в случае, если под заголовком установлено условие «любой». Все изменения, как и во вкладке «Запросы», можно сохранить, просмотреть и сбросить, воспользовавшись блоком кнопок в верхней части вкладки.

– Действия – на вкладке действия доступно шесть представлений:

- Бизнес-действия – содержит список заведённых действий для тонкой настройки приложения и подавления аномалий. Каждое действие представлено таблицей, в которую входит блок кнопок операций с действиями (см. снимок экрана 39, 1), название действия (см. снимок экрана 39, 2), таблица условий с блоком операций над условиями (см. снимок экрана 39, 3) и списком условий, а также кнопка добавления правила на основе действия (см. снимок экрана 39, 4). Для уже созданных действий доступны операции: выделить, редактировать, удалить, переместить в начало, переместить ниже, переместить выше, переместить в конец (см. снимок экрана 39, 1), а также операция создания правила на основе действия. Для выделенных правил доступна операция «Удалить выбранные действия» – для этого нужно нажать соответствующую кнопку в верней части представления. Порядок действий влияет на приоритет отработки – чем выше действие, тем приоритетнее его исполнение. Например, для действий со схожим набором условий действие имеющее большее количество условий должно иметь более высокий приоритет. В противном случае транзакции, отвечающие большему

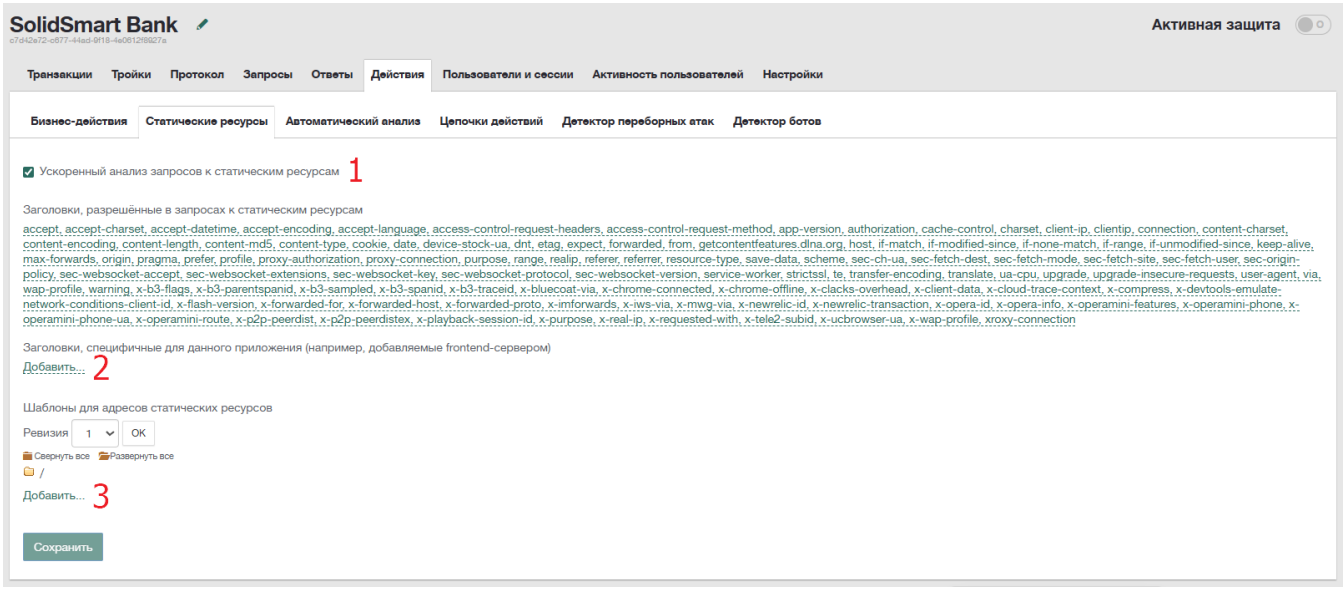
количеству условий, будут отработаны как транзакции, отвечающие только меньшему количеству условий. Каждое действие содержит условие матчинга. Для условий доступны операции: редактировать, связать с другим действием, удалить (см. снимок экрана 39, 3). В конце списка условий расположена кнопка «Добавить правило» (см. снимок экрана 39, 4). Кроме того, представление «Бизнес-действия» содержит:

- Кнопку «Добавить действие», нажатие на которую позволяет создать новое действие для отслеживания.
- Кнопку «Загрузить действия в виде HAR» – загружает файл с действиями в формате JSON.
- Возможность создания действия на основе WSDL спецификации.
- Возможность создания действия на основе OpenAPI спецификации.



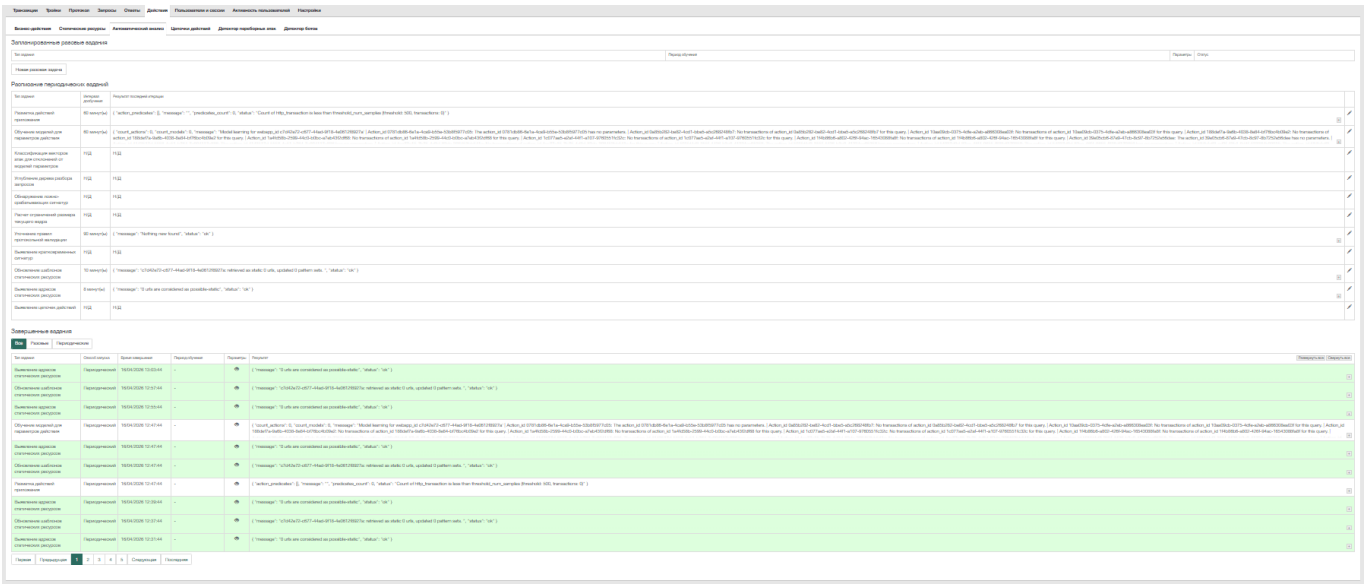
Снимок экрана 39 – Вкладка «Действия», представление «Бизнес-действия»

- Статические ресурсы – представление позволяет работать с заголовками запросов к статическим ресурсам приложения. В представлении можно включить/выключить ускоренный анализ запросов к статическим ресурсам (см. снимок экрана 40, 1). По умолчанию задан перечень разрешённых заголовков, Аналитику доступно добавление специфических заголовков для приложения. Для добавления специфических заголовков для приложения необходимо нажать кнопку «Добавить…», в открывшемся окне «Заголовки, специфичные для данного приложения» заполнить соответствующее поле и нажать кнопку «ОК» (см. снимок экрана 40, 2). В данном представлении также можно задать шаблоны адресов для статических ресурсов, воспользовавшись кнопкой «Добавить», которая помечена «3» на снимке экрана 40; далее в открывшемся окне «Шаблон статических ресурсов» выполнить требуемые действия. Для сохранения изменений необходимо нажать кнопку «Сохранить».



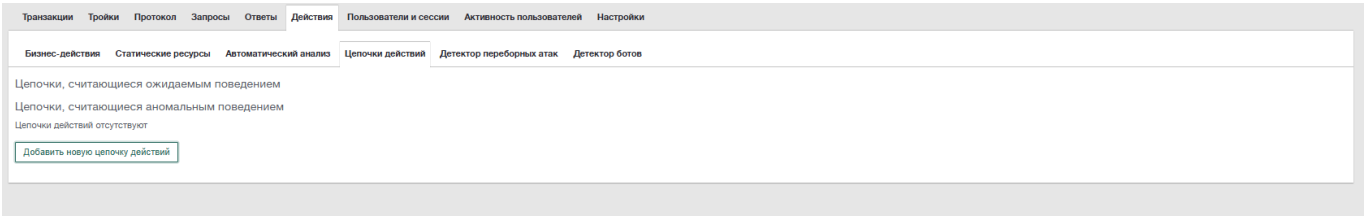
Снимок экрана 40 – Вкладка «Действия», представление «Статические ресурсы»

- Автоматический анализ – 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. снимок экрана 41). В представлении можно создать новое разовое задание, для этого необходимо нажать кнопку «Новая разовая задача» в верхнем левом углу окна, в появившемся окне «Параметры разового задания» выбрать в выпадающем списке «Тип задания» один из двенадцати типов задач, затем заполнить параметры задания и нажать кнопку «Сохранить». 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.



СЭ – Вкладка «Действия», представление «Автоматический анализ»

- Цепочки действий – позволяет создавать для отслеживания простые сценарные цепочки (см. снимок экрана 41). При нажатии на кнопку «Добавить новую цепочку действий» появляется окно «Цепочка действий», содержащее переключатели для выбора между цепочками Цепочка считается ожидаемым поведением» и «Цепочка считается аномальным поведением», и выбора сортировки «Произвольный порядок с возможными промежуточными действиями» и «Строгий порядок без промежуточных действий». Данное окно также содержит поля «Действия-пререквизиты», «Добавить действие-пререквизит» и «Критическое действие». Для каждого созданного действия доступно редактирование, удаление и просмотр информации. Отслеживание цепочек действий происходит в представлении «Автоматический анализ» вкладки «Действия» через задачу типа «Выявление паттернов в последовательностях действий».



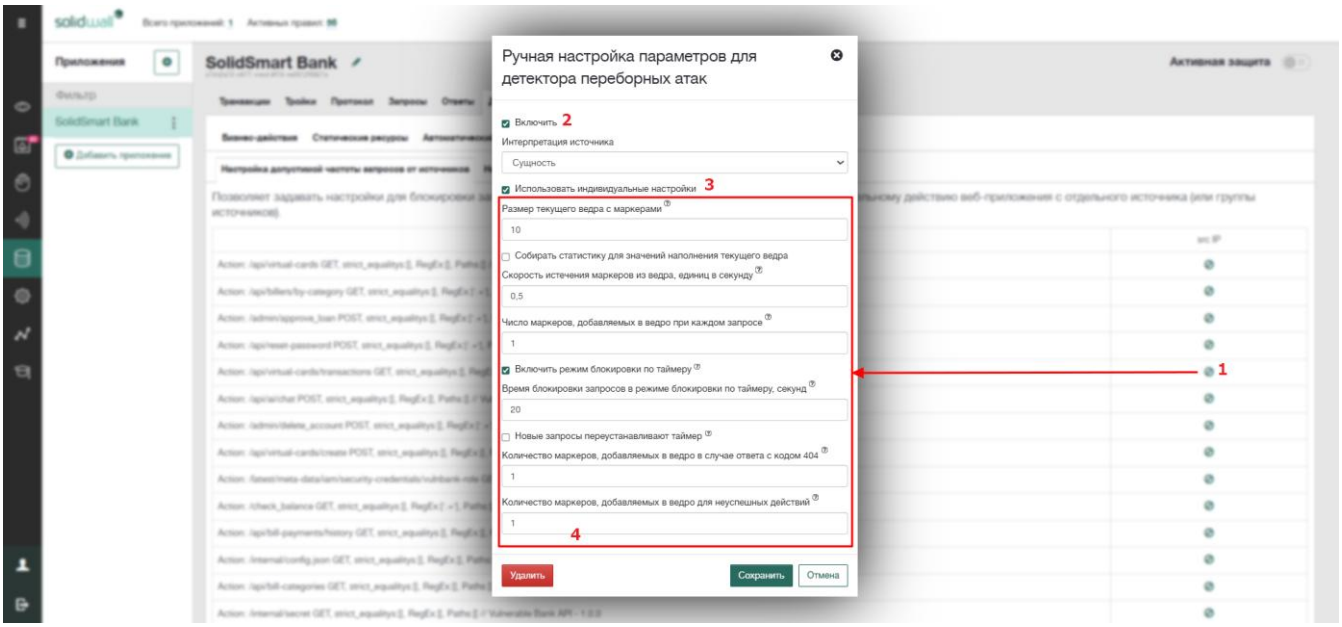
Снимок экрана 41 – Вкладка «Действия», представление «Цепочки действий»

- 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. При этом 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. Представление «Детектор переборных атак» содержит две вкладки:

- Настройка допустимой частоты запросов от источников.
- Настройка ограничений на перебор значений целей веб-приложения.

- Вкладка «Настройка допустимой частоты запросов от источников» содержит таблицу, строками которой являются настроенные Источники (см. п. 3.5.1), а столбцами – настроенные на вкладке «Действия» в представлении «Бизнес-действия» действия. Каждая ячейка может принимать три значения: «✔» – детектор переборных атак для действия для источника включен, а настройки параметров детектора установлены по умолчанию для модуля и доступны к просмотру в секции «BruteforceDetector» конфигурации модулей анализаторов; «✔✎» - детектор включен и настроен для пары «Источник – Действие» заводится индивидуальное маркерное ведро с установленными параметрами; «⊘» – детектор выключен. Для изменения состояния детектора необходимо щелкнуть мышкой по соответствующей ячейке, в появившемся окне «Ручная настройка параметров для детектора переборных атак» необходимо изменить состояние чекбокса «Включить» (см. снимок экрана 42, 2). Если установить отметку «Включить» и сохранить изменение – ячейка примет значение «✔»; если установить отметку «Использовать индивидуальные настройки» (см. снимок экрана 42, 3) – появятся дополнительные настройки (см. снимок экрана 42, 4). После сохранения измененных индивидуальных настроек, а также после сохранения индивидуальных настроек по умолчанию ячейка принимает значение «✔✎».



Снимок экрана 42 – Вкладка «Действия», представление «Детектор переборных атак»

Индивидуальные настройки параметров для детектора переборных атак:

- 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.
- Собирать статистику для значений наполнения текущего ведра - если данная настройка включена, то статистика собирается в соответствующий журнал.
- Скорость истечения маркеров из ведра, единиц в секунду – сколько маркеров вытекает из ведра каждую секунду. Характеристика определяет, за какое время полное ведро опустеет.
- 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.
- Включить режим блокировки по таймеру - если эта опция включена, то при переполнении ведра на все последующие запросы от этого источника будут некоторое установленное время генерировать аномалии вне зависимости от состояния ведра. По истечению данного таймаута - ведро принудительно опустошается.
- Время блокировки запросов в режиме блокировки по таймеру, секунд – управляет таймаутом, который включает предыдущая опция.
- Новые запросы переустанавливают таймер – если включено, то последующие запросы в режиме блокировки по таймеру взводят таймер заново. В ином случае, таймаут не переустанавливается.
- 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.

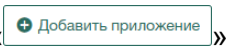
- Количество маркеров, добавляемых в ведро для неуспешных действий – Запрос обрабатывается по текущему состоянию ведра. При получении ответа веб-приложения анализируется успешность действия. Если действие не успешное – в ведро будет добавлено указанное количество маркеров. Полезность использования данной опции будет проиллюстрирована далее.

- Вкладка «Настройка ограничений на перебор значений целей веб-приложения» позволяет добавлять ограничения на перебор значений целей веб-приложения, для этого необходимо нажать «Добавить настройку». При настройке необходимо указать источники, цели, максимальное допустимое количество различных значений и время жизни соответствующей записи (в секундах).
- Детектор ботов – позволяет настроить трафик для наблюдения и отслеживания ботов.

– Пользователи и сессии – в данном представлении можно создавать атрибуты сессии и управлять пользователями.

– Активность пользователей – активность пользователей приложения может отобраться в этом представлении.

– Настройки – позволяет настроить маскирование информации, отвечающей ряду параметров.

Помимо работы с вкладками окна «Приложения» Аналитику доступно добавление новых приложений. Для этого Аналитик должен воспользоваться кнопками «  » или « 

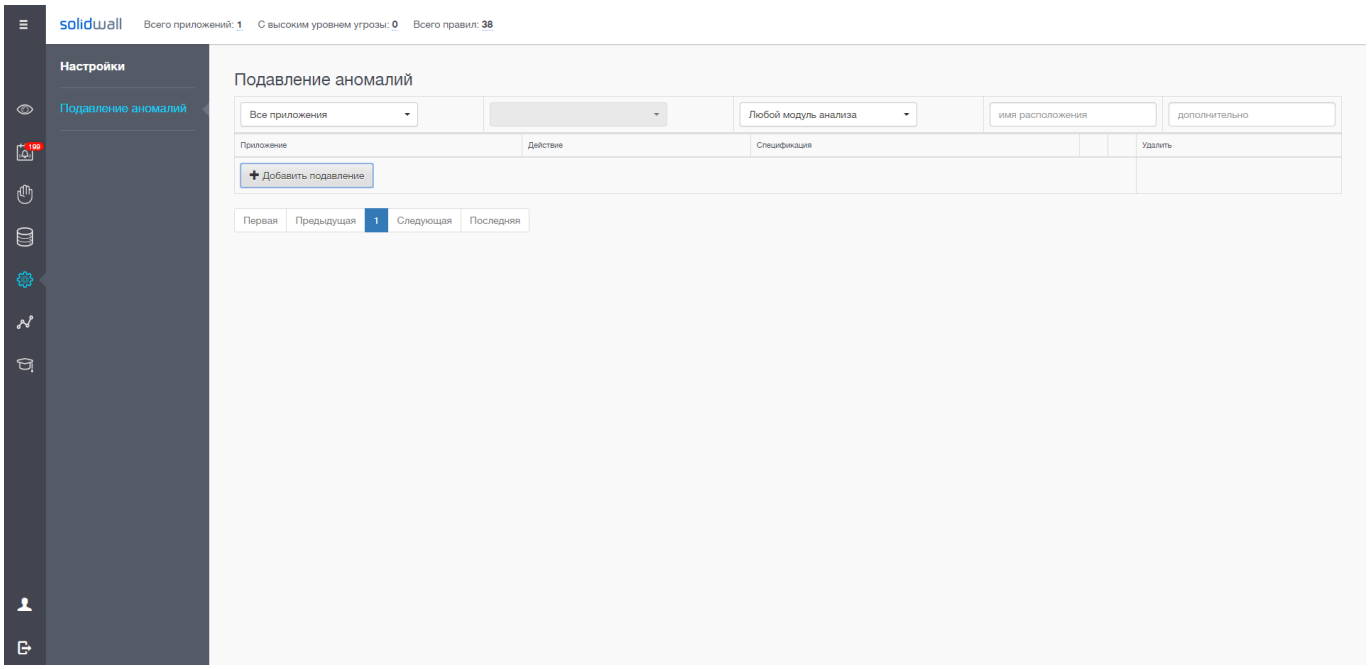
», находящимися в верхнем левом углу окна «Приложения», правее блока «Меню». В появившемся окне необходимо ввести имя приложения и нажать «Создать», затем выбрать тройки (одну или несколько), относящиеся к приложению.

3.6.3 Интерфейс Администратора

Администратор имеет возможность удаления приложения во вкладке «Настройки». В остальном права Администратора в отношении настройки приложений совпадают с правами Аналитика.

3.7 Окно «Настройки»

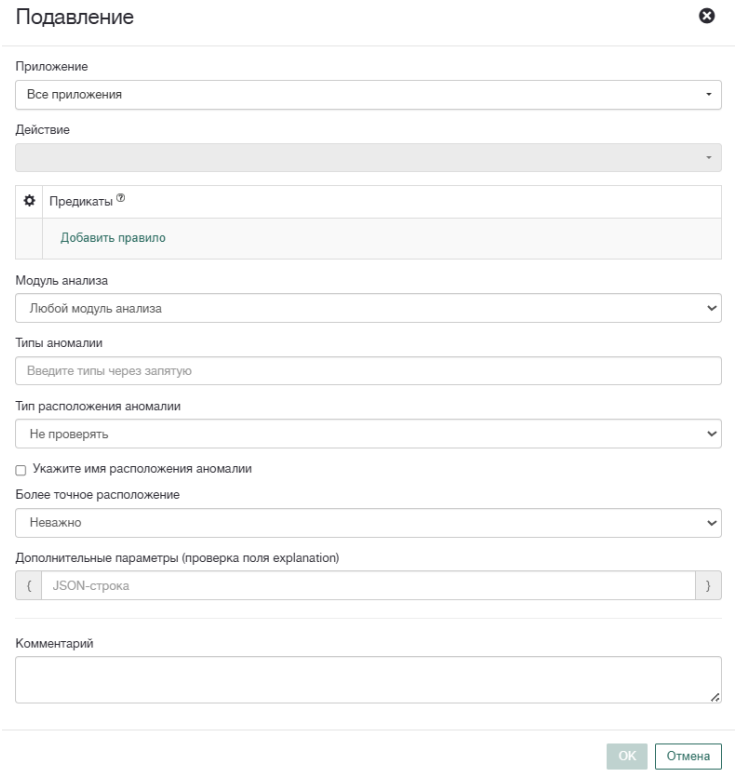
В окне «Настройки» для ролей «Оператор» и «Аналитик» доступен функционал «Подавление аномалий», как показано на снимке экрана 43.



Снимок экрана 43 – Окно «Настройки»

С помощью задания параметров через выпадающие меню можно отсортировать и найти необходимые подавления.

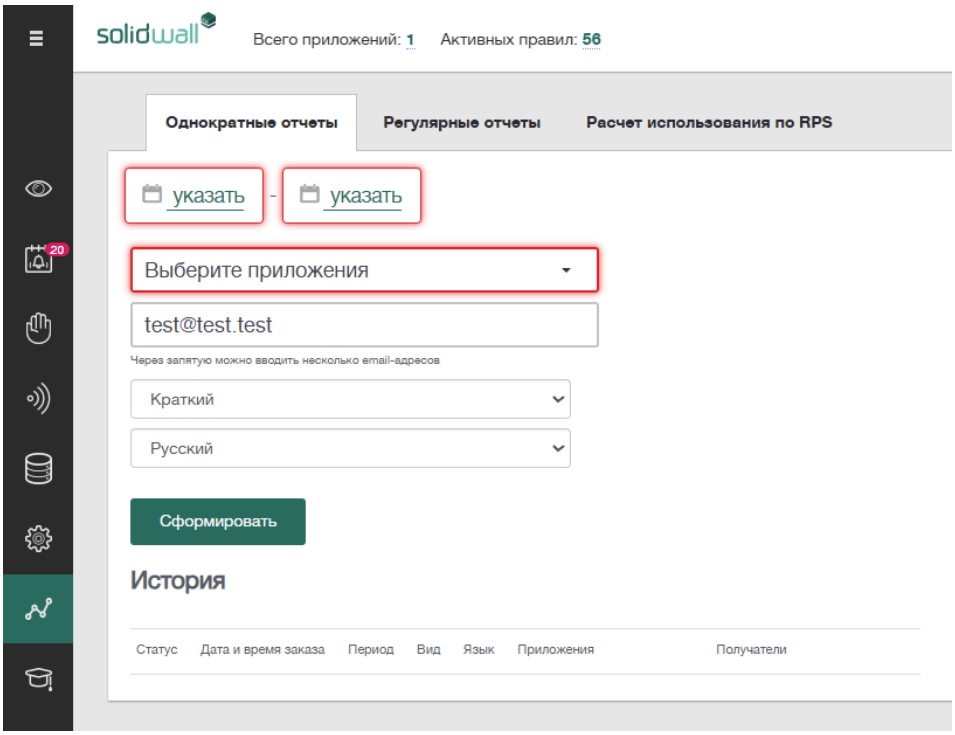
Аналитику доступно добавление аномалий с помощью кнопки «+ Добавить подавление». На снимке экрана 44 отображается окно добавления подавления.



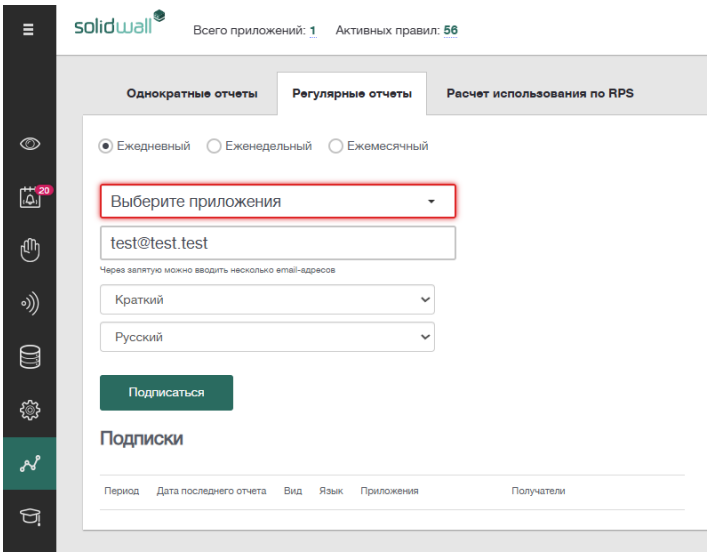
Снимок экрана 44 – Добавление подавления

3.8 Окно «Отчеты»

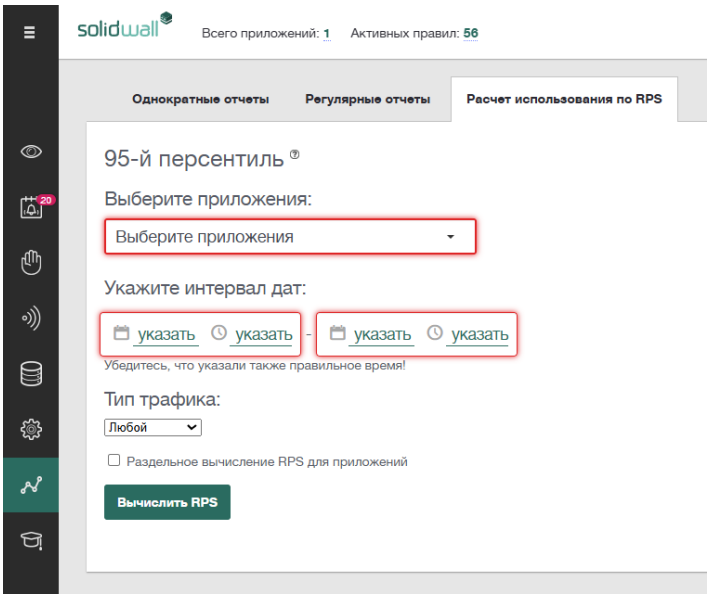
В окне отчёты можно создать однократные и регулярные отчеты, а также расчет использования по RPS заполнив все поля представления (см. снимки экрана 45 - 47).



Снимок экрана 45 – Окно «Отчеты. Вкладка «Однократные отчеты»



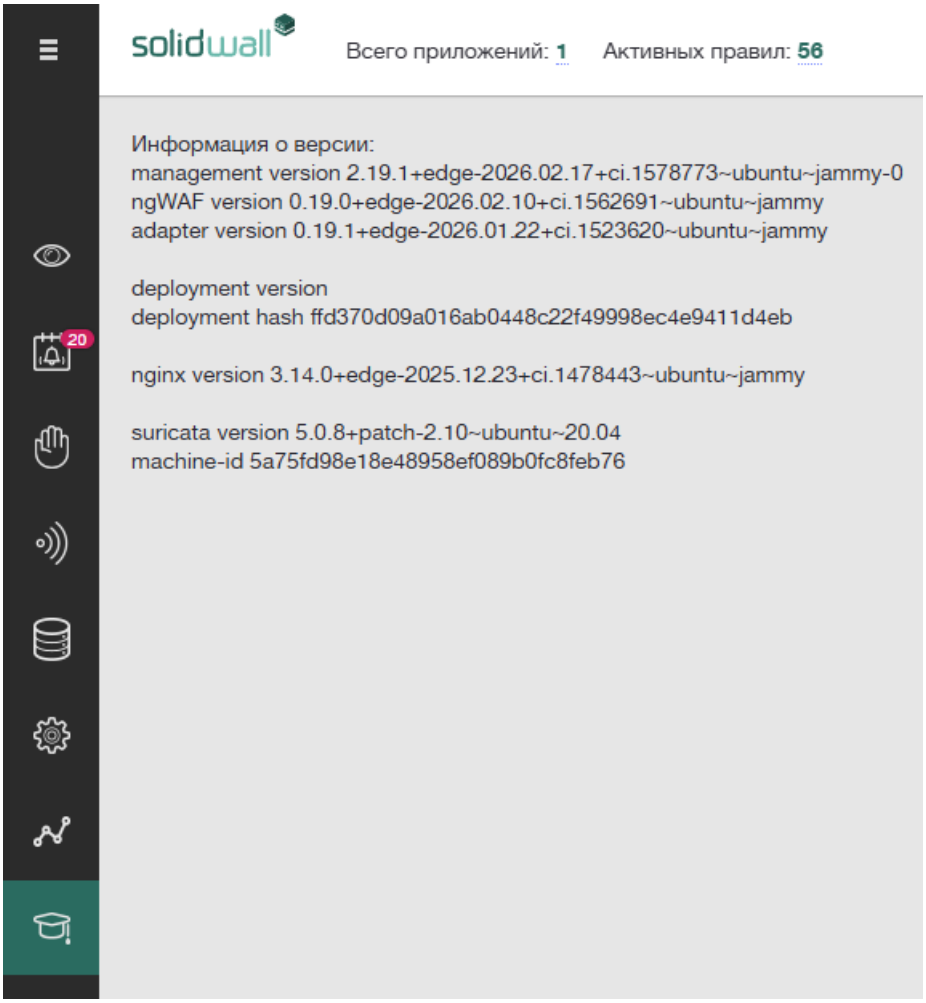
Снимок экрана 46 – Окно «Отчеты. Вкладка «Регулярные отчеты»



Снимок экрана 47 – Окно «Отчеты. Вкладка «расчет использования по RPS»

3.9 Окно «Помощь»

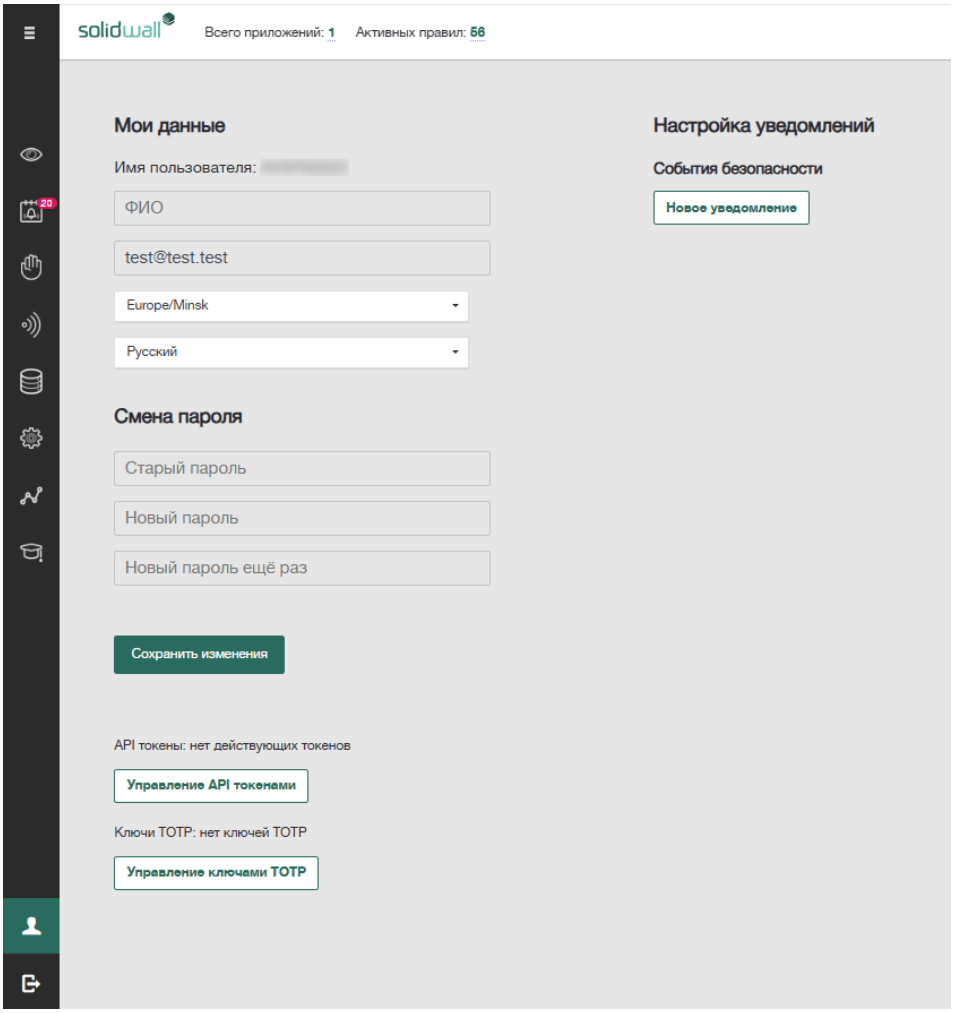
Окно «Помощь» содержит информацию о версии продукта и используемых сторонних компонентов (см. снимок экрана 48).



Снимок экрана 48 – Окно «Помощь»

3.10 Окно «Настройки пользователя»

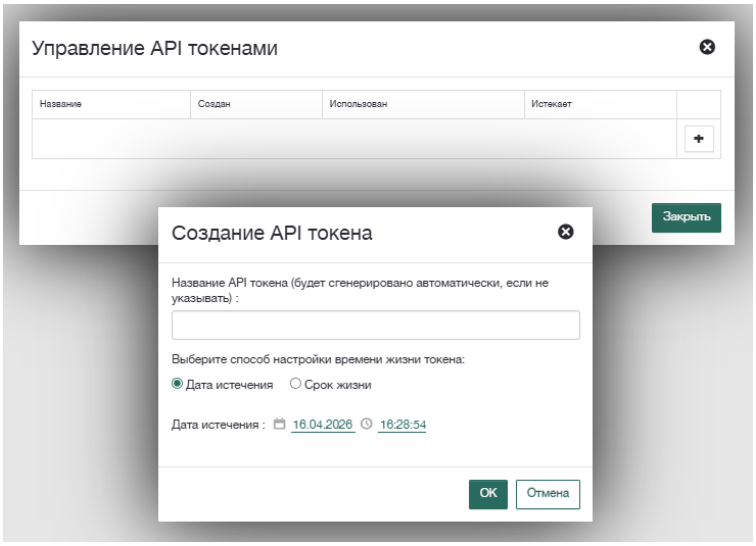
Окно «Настройки пользователя» предназначено для редактирования учётных данных пользователя (см. снимок экрана 49).



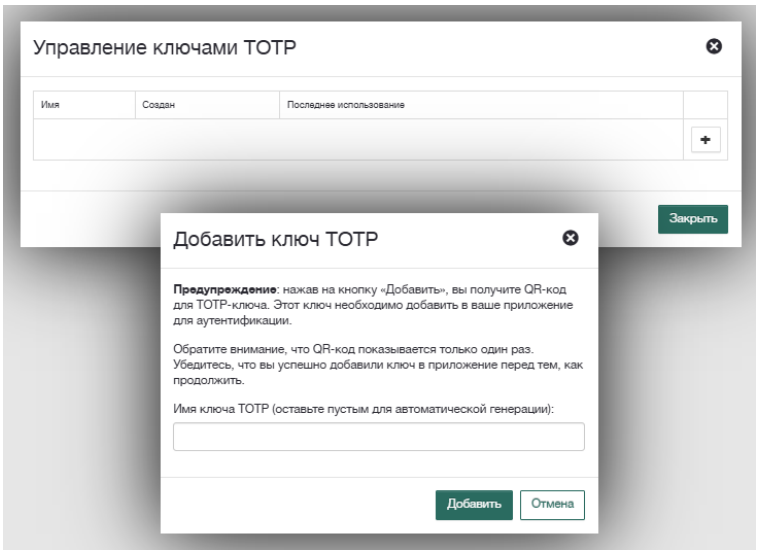
Снимок экрана 49 – Окно «Настройки пользователя»

Окно содержит блоки «Мои данные», «Смена пароля», а также позволяет настроить уведомления и управлять дополнительными средствами аутентификации. При нажатии кнопки «Новое уведомление» в блоке «Настройки уведомлений» открывается окно «Редактирование уведомления», в окне задаются параметры уведомления: приложение, по которому необходимо отправлять уведомления, а также правило, срабатывание которого должно отслеживаться.

Для задания параметров управления API токенами и ключами TOTP необходимо нажать на соответствующие кнопки и заполнить необходимые данные в появившихся окнах (см. снимки экрана 50 и 51).



Снимок экрана 50 – Управление API токенами



Снимок экрана 51 – Управление ключами TOTP

4 ВОЗМОЖНЫЕ СЦЕНАРИИ РАБОТЫ С SOLIDWALL AI SECURITY GATEWAY

4.1 Сценарии работы Оператора

Оператор отслеживает графики событий и при возникновении нештатных ситуаций принимает решение о необходимости привлечения Аналитика или Администратора SolidWall AI Security Gateway. Возможные индикаторы нештатной ситуации:

1. Появление транзакций с кодами ответов 5xx.
2. Изменения в графиках событий.
3. Рост числа событий.
4. Обращение пользователей.

4.1.1 Появление транзакций с кодами ответов 5xx

Оператор должен отслеживать графики событий в окне «Обзор» и при появлении в графике «Статусы» событий, помеченных красным, т. е. транзакций с кодами ответов 5xx необходимо незамедлительно оповестить администратора.

4.1.2 Изменения в графиках событий

Изменения в графиках событий:

- Статусы,
- Блокировки,
- Задержка,
- Сессии,
- Враждебность –

должны быть локализованы по времени и сопоставлены с событиями, происходившими в это время. Аналитик и администратор должны быть проинформированы о возникшей ситуации. Например, резкое падение до нуля во всех графиках говорит о нарушении работоспособности SolidWall AI Security Gateway.

4.1.3 Рост числа событий

При резком росте числа событий необходимо перейти в представление «События». Для каждого события с возросшим числом срабатываний необходимо открыть общую информацию о событии и нажать кнопку «Подробности». В открывшемся окне можно просмотреть общую информацию для транзакций, отнесённых к событию, а можно открыть детали транзакции. Вкладка «Решение» окна «Детали транзакции» позволит ознакомится с правилами, под которые попала транзакция, просмотреть сами правила. Например, рост числа событий, по помечающим правилам может говорить о возросшем легитимном количестве обращений к приложению в связи с какими-

либо событиями. Оператор должен проанализировать данные факты и принять решение о необходимости информирования аналитика или администратора.

4.2 Сценарии работы Аналитика

Аналитик отслеживает события, корректирует правила, создаёт действия и подавляет аномалии.

4.2.1 Анализ блокировки ответа сервера

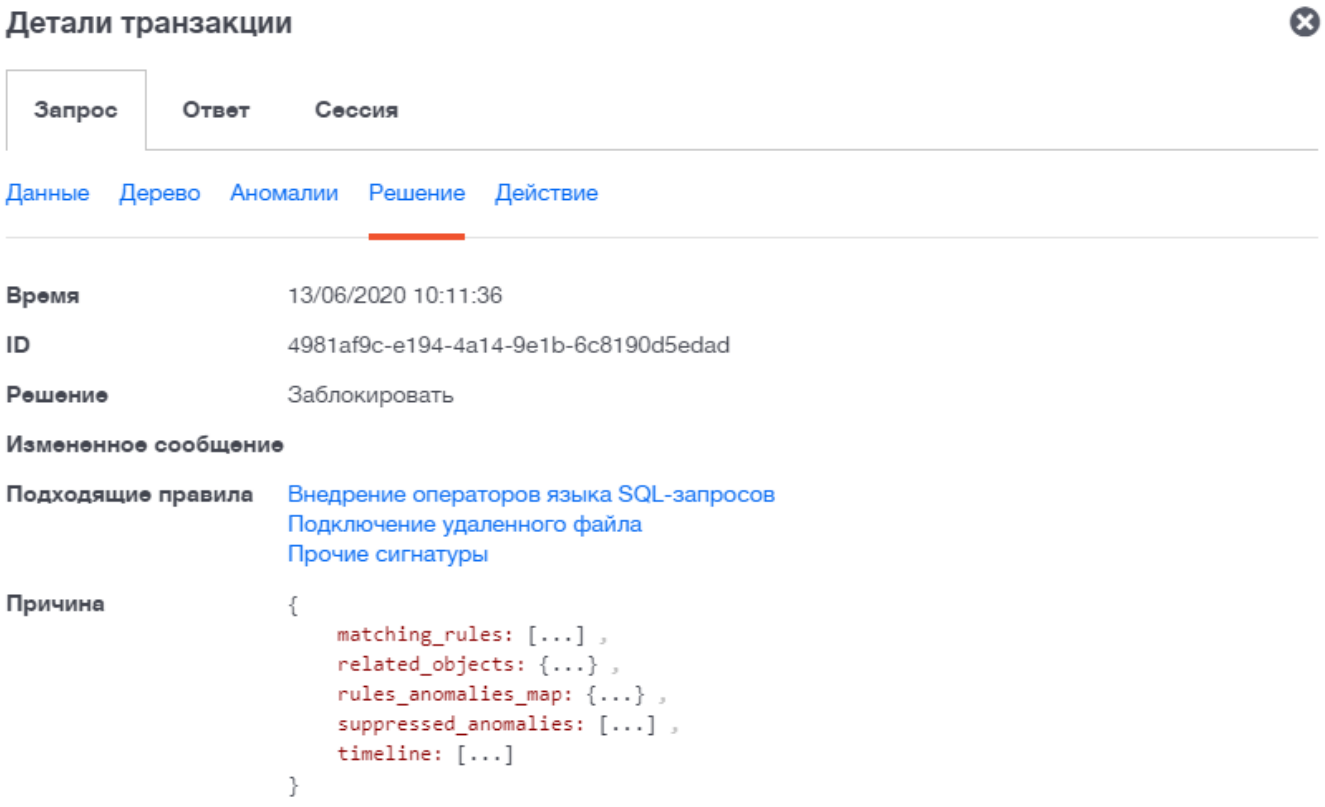
Ответы сервера со статусом 5xx, либо ответы, содержащие утечку чувствительных данных (например, данные об ошибке SQL или JAVA) блокируются SolidWall AI Security Gateway по умолчанию, чтобы не раскрывать данные об устройстве приложения, версий веб-компонентов и диагностической информации об ошибках атакующему. С телом заблокированного ответа сервера можно ознакомиться в окне «Детали транзакции» во вкладке «Ответ» в представлении «Данные».

В случае если блокировка ответа корректна – следует рекомендовать пользователю повторить попытку, если ошибка или сбой имели временный характер, или информировать администратора SolidWall AI Security Gateway о возникшей ошибке или сбое.

В случае если блокировка ответа некорректна, и данный ответ сервера необходимо демонстрировать пользователям – необходимо выполнить подавление аномалии (ложного срабатывания), как описано в п. 4.2.3.

4.2.2 Анализ блокировки запроса

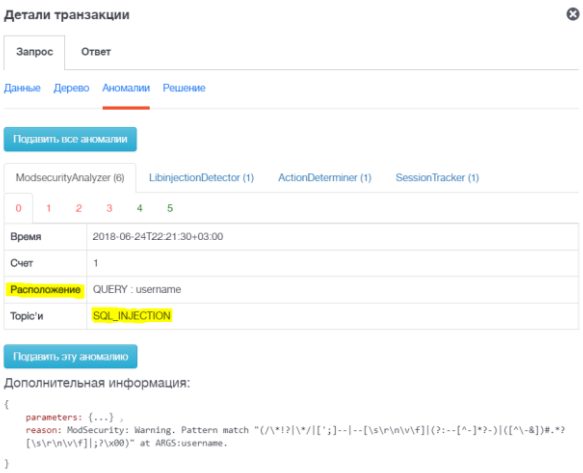
В окне «Детали транзакции» во вкладке «Запрос» в представлении «Решение» заблокированного запроса перечислены сработавшие правила (см. снимок экрана 52). Все сработавшие правила необходимо разделить на блокирующие и помечающие. Для этого необходимо перейти в каждое сработавшее правило и посмотреть спецификацию действия. Для всех блокирующих правил проанализировать аномалии, которые не относятся к подавленным аномалиям (такие аномалии помечены красными номерами вкладок в окне «Детали транзакции» во вкладке «Запрос» в представлении «Аномалии»).



Снимок экрана 52 – Пример сработавших правил

4.2.2.1 Для анализаторов «ModSecurity» и «LibinjectionDetector»

Для анализаторов «ModSecurity» и «LibinjectionDetector» необходимо проанализировать элемент запроса, который вызвал аномалию. Разберём пример, представленный на снимке экрана 53.

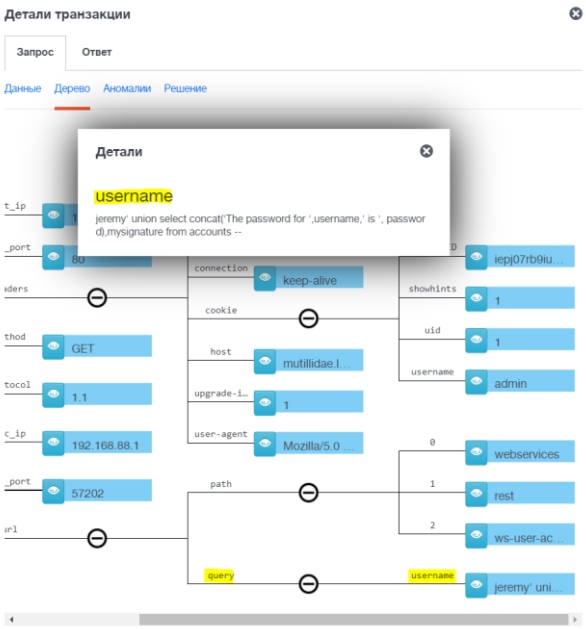


Снимок экрана 53 – Пример аномалии

На примере видно, что необходимо проанализировать четыре аномалии типа «SQL_INJECTION» анализатора «ModSecurity» с номерами 0, 1, 2 и 3, а также одну аномалию анализатора «LibinjectionDetector». Аномалии анализаторов «ActionDeterminer» и «SessionTracker» правилами не блокируются в разбираемом примере.

Для каждой аномалии устанавливается элемент запроса «Расположение». В примере аномалия с номером 0 была обнаружена в части запроса «Query», в элементе с именем «username».

В представлениях «Аномалии», «Дерево» и «Данные» вкладки «Запрос» окна «Детали транзакции» проанализировать вызвавший аномалию элемент запроса и сделать вывод является ли данная аномалия ложным срабатыванием.



Снимок экрана 54 – Дерево запроса

Признаком ложного срабатывания могут являться строковые значения, которые генерируются в приложении случайным образом, как например, идентификаторы сессий и токены, закодированные и скомпрессированные элементы, содержимое загружаемых в приложение файлов и текстовых полей, пароли пользователей и прочие.

Причиной правомерной блокировки могут являться признаки реальных атак на веб-приложение, например, конструкции языка SQL, JavaScript, PHP, команды командной оболочки и т. п. В таких случаях подавлять аномалию не нужно, за исключением некоторых редких случаев, как например:

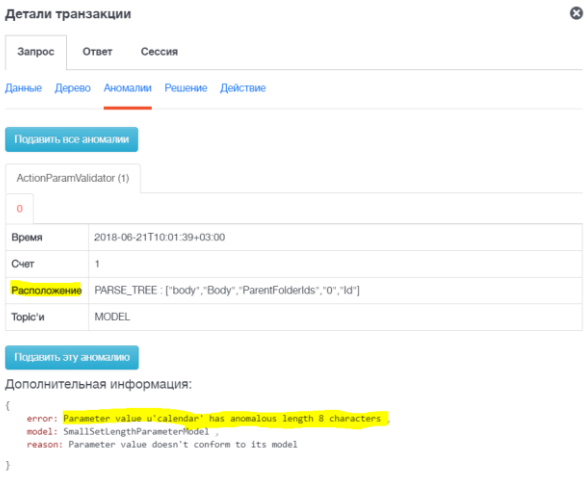
– SQL-запросы могут быть легитимным форматом передачи данных или управляющих команд в HTTP-запросах, например, для приложения Grafana или приложения, использующего язык GraphQL. Признаком, такой ситуации может являться то, что конструкции языка SQL встречаются в запросах у подавляющего большинства клиентов приложения.

– Пользователи могут публиковать примеры кода на защищаемом ресурсе. Для принятия решения о подавлении таких аномалий необходимо анализировать контекст таких публикаций.

Для ложного срабатывания выполняется подавление аномалии, как описано в п. 4.2.3.

4.2.2.2 Для анализатора «ActionParamValidator»

Для анализатора «ActionParamValidator» в представлении «Аномалии» вкладки «Запрос» окна «Детали транзакции» установить, в каком параметре и каким образом была нарушена модель.



Снимок экрана 55 - Аномалия модели параметра

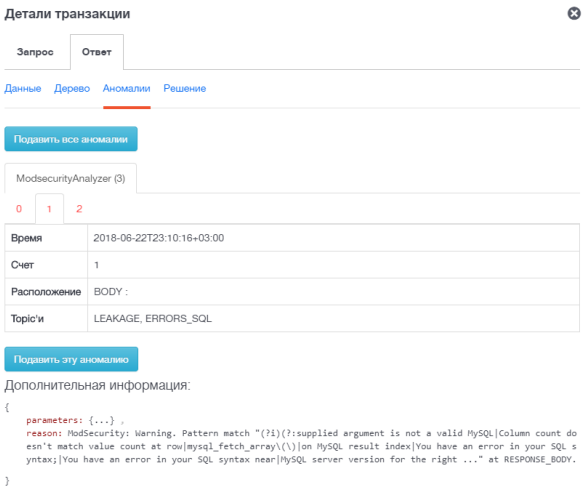
Затем необходимо скорректировать модель параметра, как описано в п. 4.2.3.

4.2.3 Подавление ложного срабатывания

Если выявленная аномалия является ложным срабатыванием, то в зависимости от того к какому типу моделей относится анализатор, обнаруживший данную аномалию, выполняем подавление ложного срабатывания или корректируем модель.

4.2.3.1 Подавление аномалий в ответах сервера

В окне «Детали транзакции» перейти во вкладку «Ответ» в представление «Аномалии» и нажать «Подавить все аномалии».

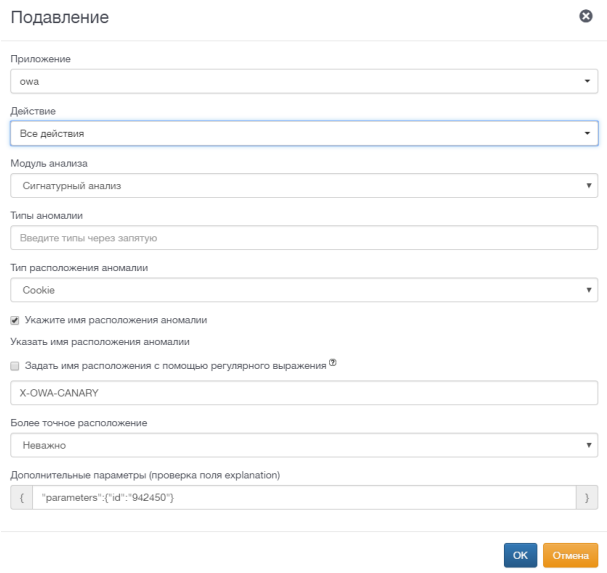


Снимок экрана 56 – Подавление аномалий в ответе

Откроется окно с подавлением всех найденных в ответе аномалий. Нажать «Подавить».

4.2.3.2 Подавление аномалий в запросах для анализаторов «ModSecurity» и «LibinjectionDetector»

Подавление аномалии осуществляется в представлении «Аномалии» вкладки «Запрос» окна «Детали транзакции» при помощи нажатия кнопки «Подавить эту аномалию» (см. снимок экрана 56). Откроется диалоговое окно с параметрами подавления аномалии (см. снимок экрана 57).

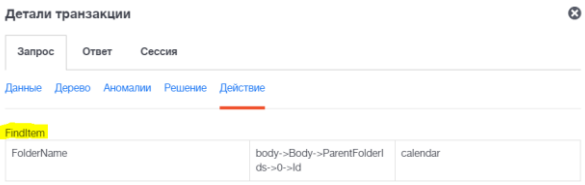


Снимок экрана 57 – Подавление аномалии в запросе

Для аномалий, располагающейся в элементах запроса, которые могут являться общими для всех запросов, например, заголовки Cookie и user-agent, необходимо в поле «Действие» выбрать «Все действия».

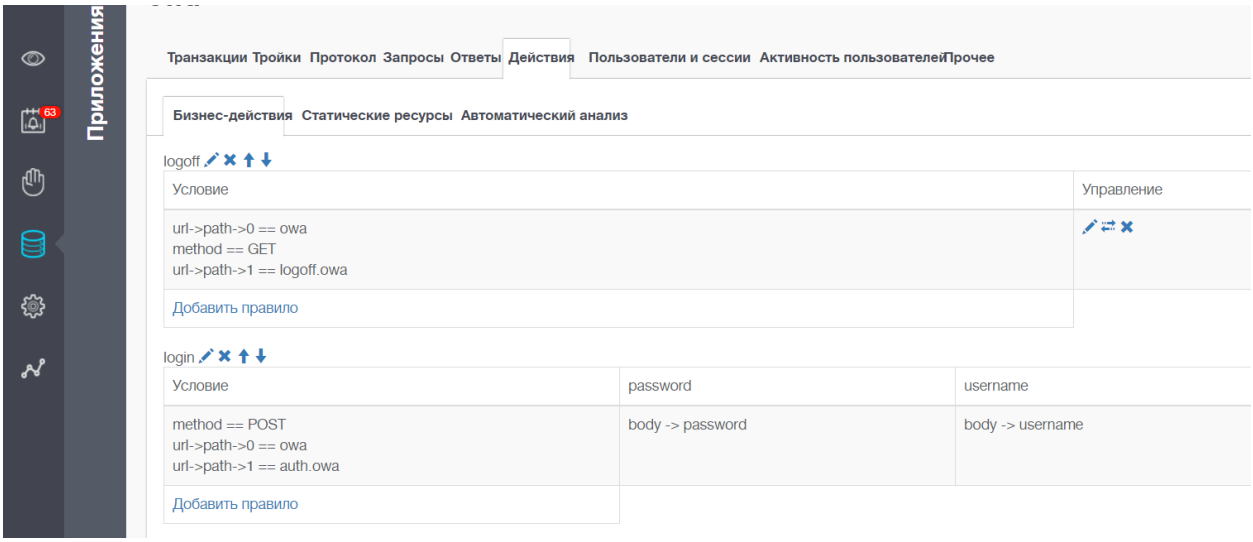
4.2.3.3 Подавление аномалий в запросах для анализатора «ActionParamValidator»

Для корректировки модели параметров необходимо в представлении «Действие» вкладки «Запрос» окна «Детали транзакции» установить, к какому действию относится данный запрос.



Снимок экрана 58 - Представление «Действие» вкладки «Запрос» окна «Детали транзакции»

Затем перейти в окно «Приложения» на вкладку «Действия».

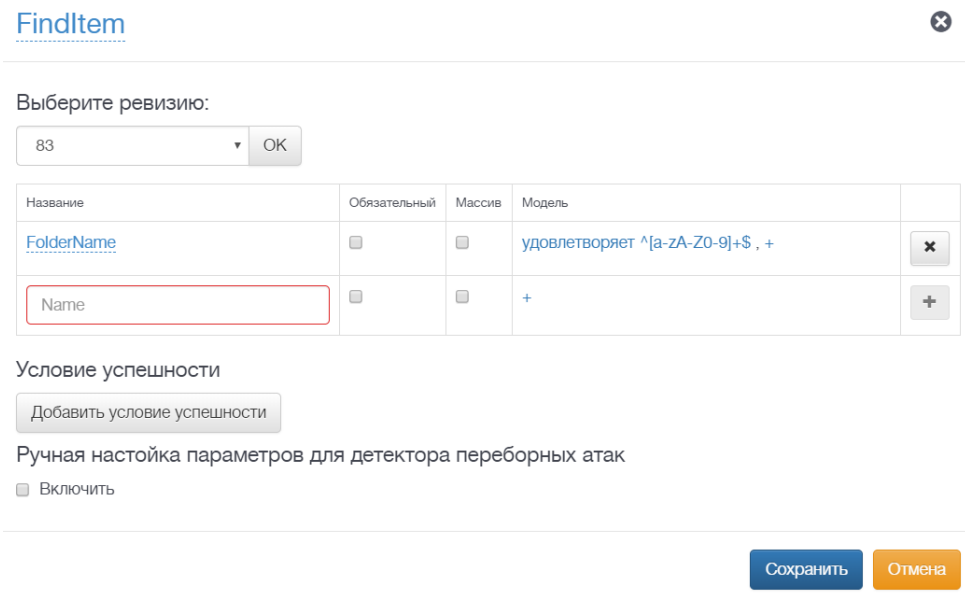


Снимок экрана 59 – Вкладка «Действия» окна приложения

Найти действие, в параметре которого была обнаружена аномалия. Нажать на пиктограмму «✎», расположенный рядом с названием нужного действия.

Снимок экрана 60 – Поиск действия

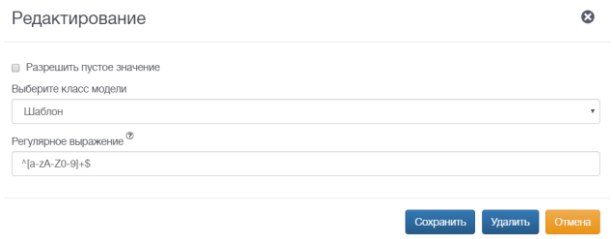
Откроется окно корректировки параметров действия (см. снимок экрана 61).



Снимок экрана 61 – Корректировка параметров действия

В открывшемся окне необходимо выбрать нужный параметр и открыть окно «Редактирование», нажав на условие в графе «Модель» в строке с параметром.

В окне «Редактирование» необходимо изменить синтаксическую модель параметра (см. снимок экрана 62).



Снимок экрана 62 – Синтаксическая модель параметров

4.3 Сценарии работы Администратора

Администратору доступны для решения задачи Аналитика. По мимо этого Администратор решает следующие задачи:

- Установка SolidWall AI Security Gateway;
- Обновление;
- Резервное копирование;
- Заведение и настройка приложений;
- Заведение пользователей SolidWall AI Security Gateway;
- Перезапуск анализаторов;
- Аудит действий пользователей SolidWall AI Security Gateway.