ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

АКЦИОНЕРНОЕ ОБЩЕСТВО «ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ»

(АО «ПМ»)

СИСТЕМА ВЫЯВЛЕНИЯ И ПРЕДУПРЕЖДЕНИЯ АТАК НА ВЕБ-РЕСУРСЫ «AML WEB PROTECTION»

Инструкция по эксплуатации

На 124 листах

Москва 2025

Аннотация

Настоящий документ является описывает эксплуатационные характеристики Системы выявления и предупреждения атак на веб-ресурсы «AML Web Protection» (далее – «AML», Система).

Содержание

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе применяют следующие сокращения:

АО «ПМ»	–	Акционерное общество «Перспективный мониторинг»
«AML»	–	Система выявления и предупреждения атак на веб-ресурсы «AML Web Protection»

1 Общие сведения

Основным направлением деятельности АО «ПМ» является оценка практической защищенности информационных систем, выявление их уязвимостей при помощи средств инструментального и ручного анализа, реагирование на инциденты безопасности, разработка программных продуктов в области информационной безопасности. Система выявления и предупреждения атак на веб-ресурсы «AML Web Protection» также является разработкой компании.

Задача «AML» – защитить внутренние и внешние веб-ресурсы организации от компьютерных атак. Для решения данной задачи Система взаимодействует напрямую с журналами веб-сервера и не анализирует содержимое сетевого трафика. «AML» использует алгоритмы поведенческого анализа для выявления атакующих сессий по записям журнала веб-сервера и синхронизируется с веб-сервером для блокировки вредоносной активности.

2 Начало работы с Системой

2.1 Авторизация в Системе

Для входа в «AML» потребуется запросить у администратора Системы следующие данные:

– ссылку/IP-адрес для входа в интерфейс продукта;

– логин и пароль для учетной записи пользователя.

Далее необходимо выполнить следующие действия:

1) ввести в адресной строке ссылку/IP-адрес для входа в интерфейс Системы, откроется страница авторизации. С помощью элементов управления можно изменить язык, а также включить/выключить видимость вводимого пароля (Рисунок 1);

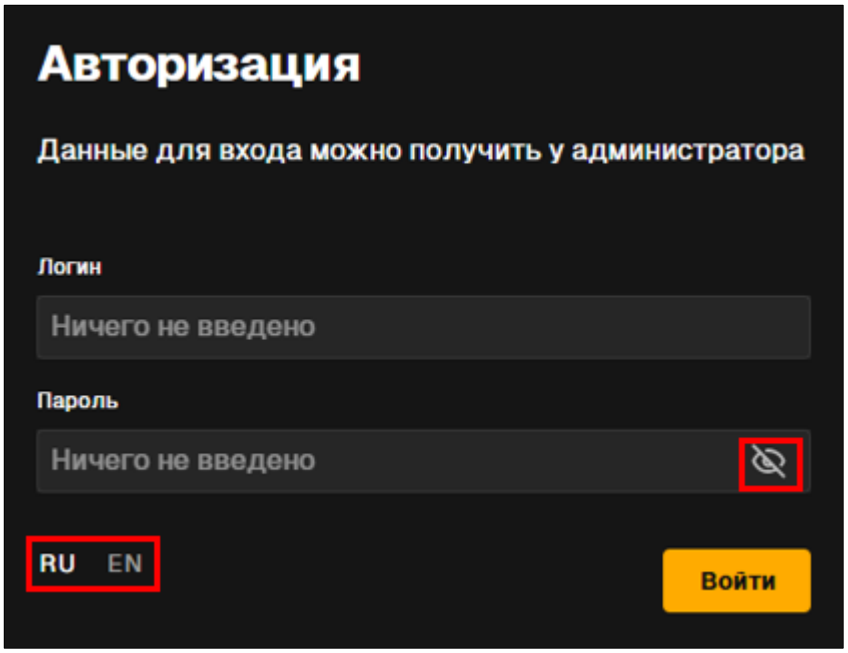

Рисунок 1 – Страница авторизации

2) для первого входа в форме авторизации ввести логин и пароль учетной записи, которые предоставляет системный администратор;

3) далее следует нажать кнопку «Войти». Если указанные данные верны, то откроется стартовая страница. Иначе Система выдаст сообщение об ошибке (Рисунок 2).

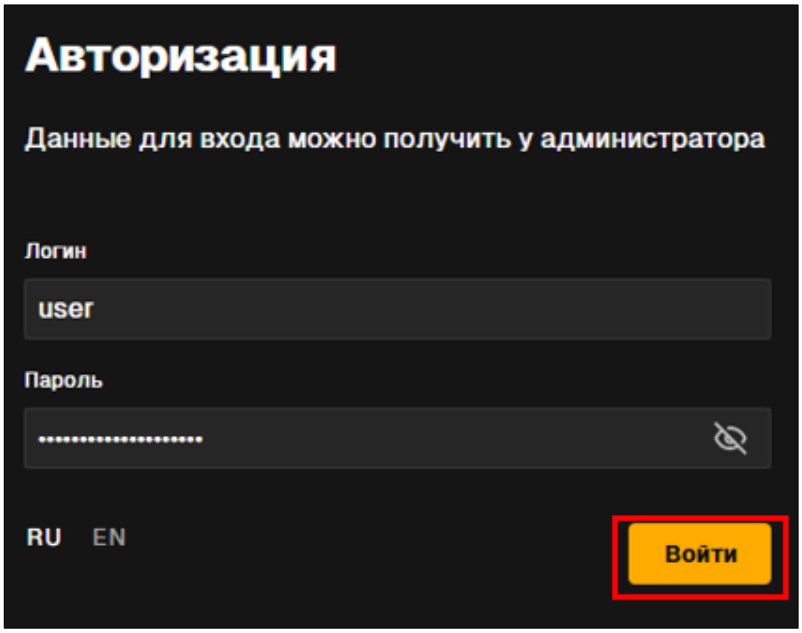

Рисунок 2 – Заполненная форма авторизации

2.2 Изменение цвета темы

Для удобства работы с Системой можно изменить цветовую тему интерфейса с помощью следующих действий:

1) Перейти в раздел «Настройки» (Рисунок 3);

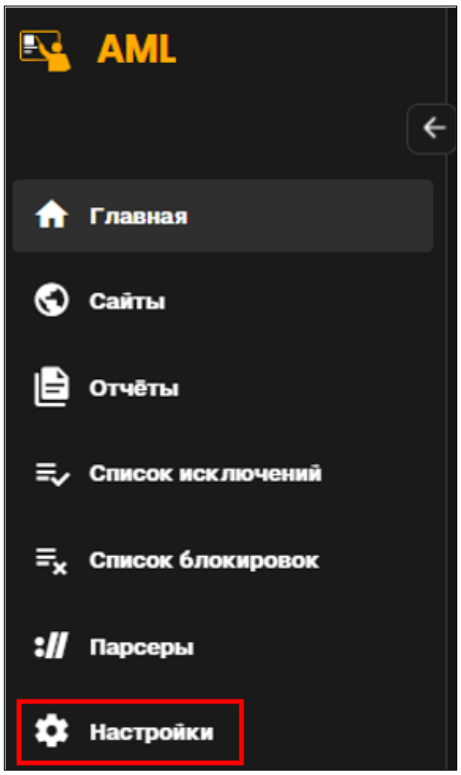

Рисунок 3 – Меню «AML»

2) в блоке «Тема» будут отображены два вида доступных для выбора тем: темная и светлая. У активной на данный момент темы активен чекбокс и цветовая подсветка. Для переключения нужно выбрать другую тему и активировать чекбокс (Рисунок 4);

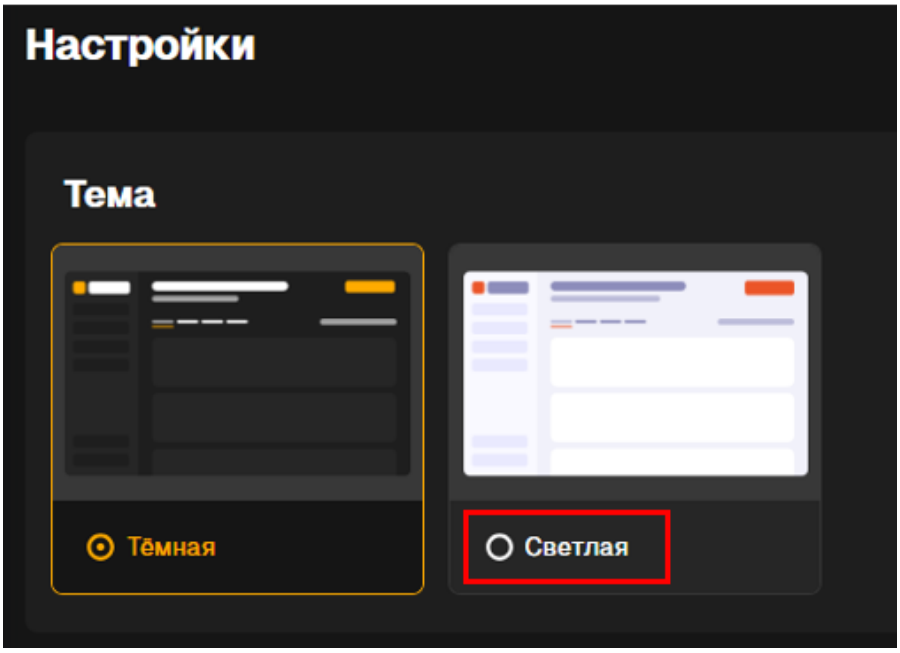

Рисунок 4 – Изменение цвета темы

3) после переключения системные цвета изменятся на выбранные.

2.3 Смена языка

Для удобства работы с Системой можно изменить настройки локализации – сменить системный язык с русского на английский с помощью следующих действий:

1) перейти в раздел «Настройки» (Рисунок 5);

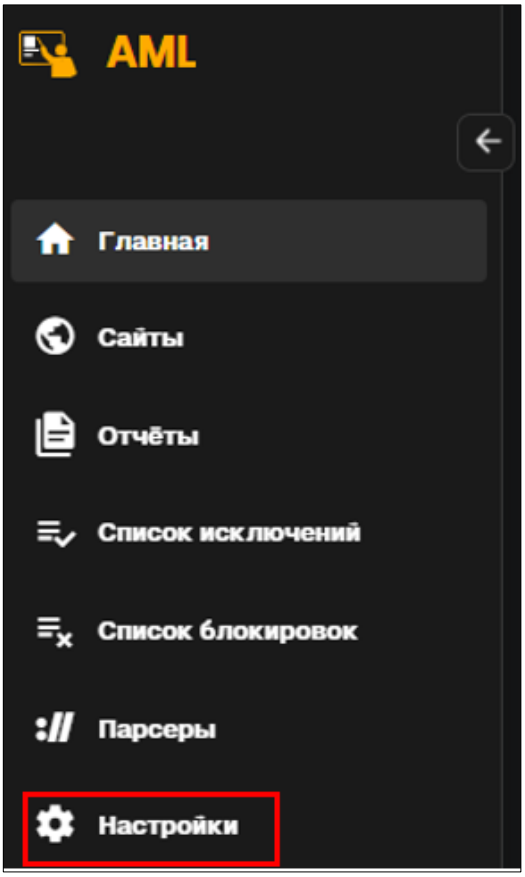

Рисунок 5 – Меню «AML»

2) в блоке «Локализация» отобразится выпадающий список, в котором выбрано значение текущего системного языка. После нажатия на поле выпадающего списка будут отображены другие варианты локализации (Рисунок 6);

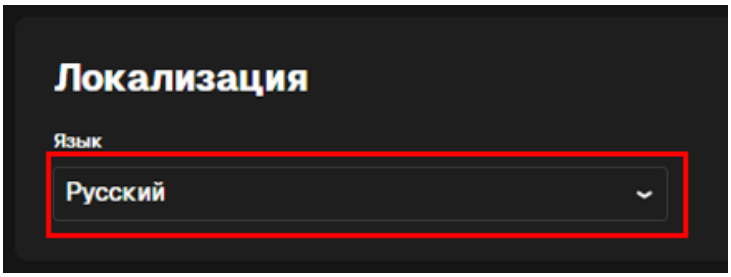

Рисунок 6 – Параметры выбора языка

3) в списке можно выбрать нужный язык (Рисунок 7);

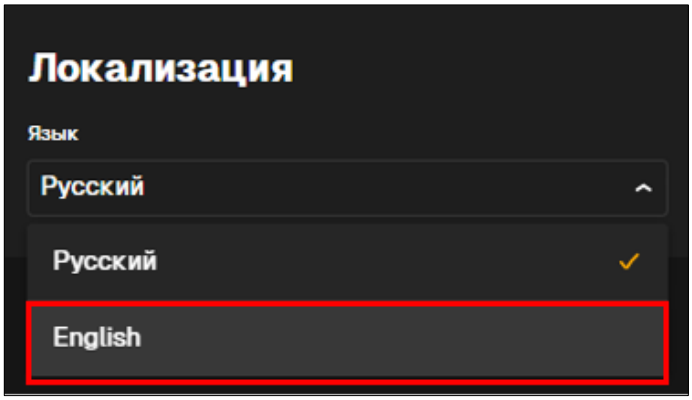

Рисунок 7 – Выпадающий список для выбора языка

2.4 Просмотр данных личного кабинета

В личном кабинете можно получить информацию о своей учетной записи – логин для входа в Систему, фамилию, имя. Для получения информации необходимо выполнить следующие действия:

1) в левой части меню нажать на иконку профиля (Рисунок 8);

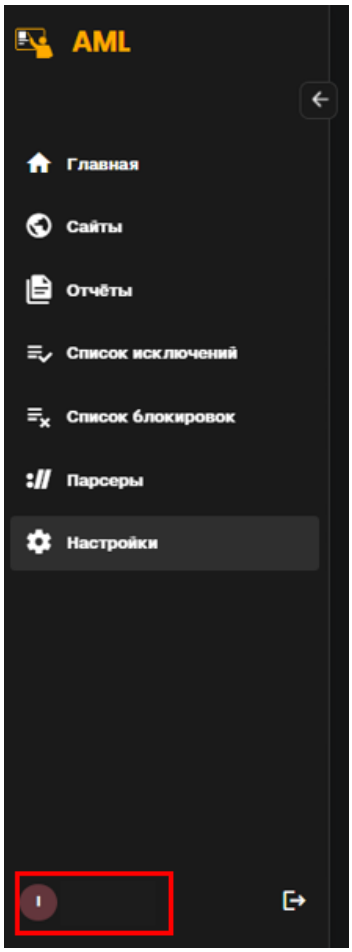

Рисунок 8 – Иконка профиля в меню «AML»

2) откроется страница с отображением личной информации пользователя (Рисунок 9);

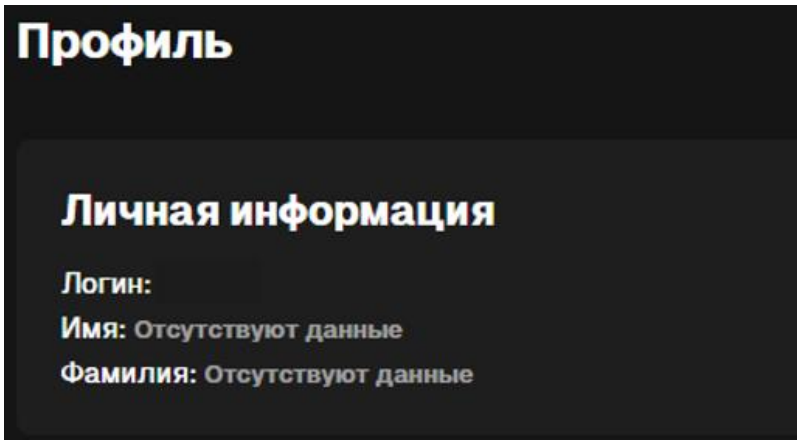

Рисунок 9 – Просмотр данных личного кабинета

2.5 Выход из Системы

После завершения работы с Системой или для смены учетной записи необходимо осуществить выход из учетной записи пользователя с помощью следующих действий:

1) в левой части меню навести курсор на иконку профиля;

2) далее откроется всплывающее поле с кнопками перехода к профилю и выхода из Системы, нажать на кнопку «Выйти» (Рисунок 10);

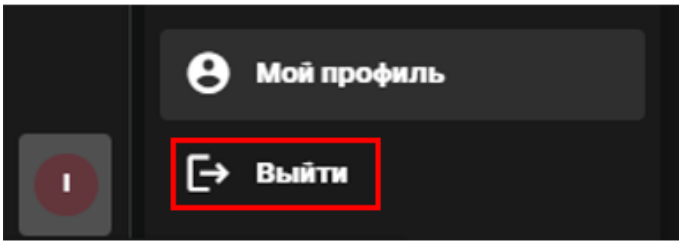

Рисунок 10 – Выход из Системы

3) пользователь будет перенаправлен на страницу авторизации.

3 Раздел «Главная»

В разделе «Главная» отображается сводная статистика по работе «AML». В данном разделе пользователь может ознакомиться с данными по результатам или процессу обработки журналов доступных сайтов.

3.1 Счетчик сайтов и переход к последнему загруженному журналу

В разделе «Главная» можно изучить количество доступных пользователю сайтов и перейти к последнему загруженному журналу с помощью следующих действий:

1) перейти в раздел «Главная» (Рисунок 11);

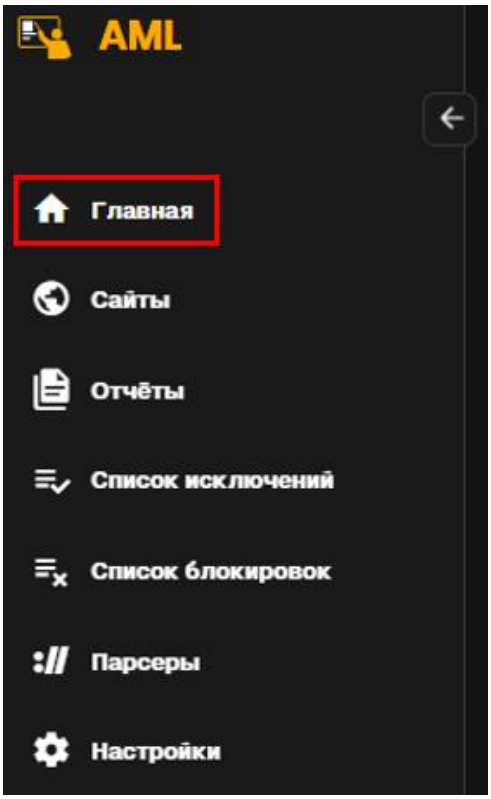

Рисунок 11 – Переход в раздел «Главная»

2) далее отобразится раздел со статистикой по всем доступным сайтам (Рисунок 12);

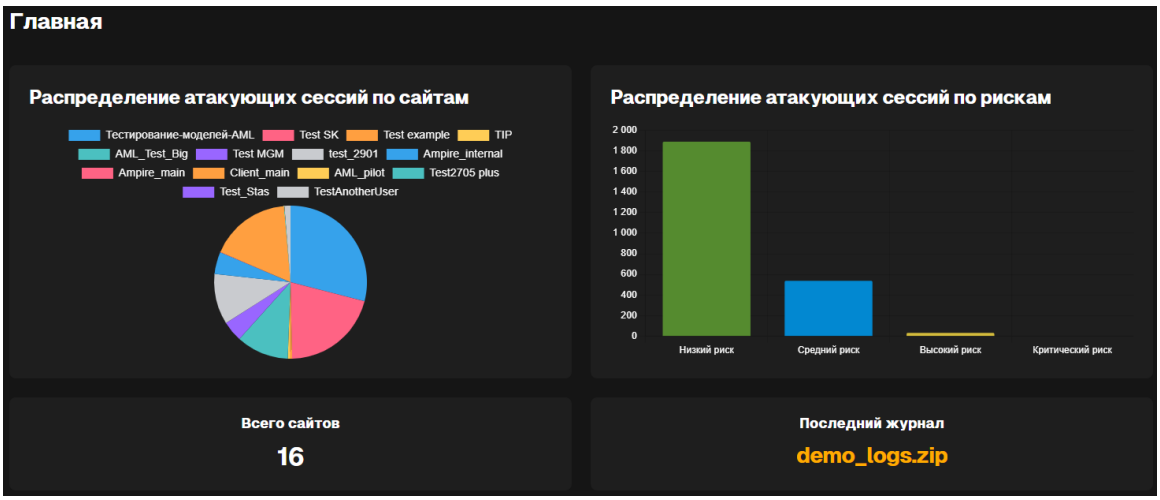

Рисунок 12 – Раздел со статистикой по всем доступным сайтам

3) в блоке «Всего сайтов» отображено количество сайтов, доступных пользователю (Рисунок 13);

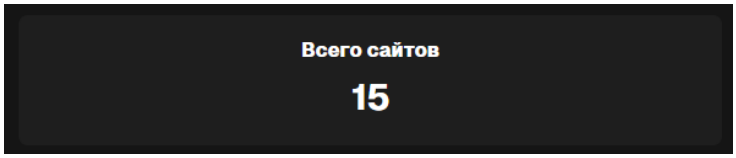

Рисунок 13 – Блок «Всего сайтов»

4) в блоке «Последний журнал» отображен журнал, который последним добавлен к доступным пользователю сайтов (Рисунок 14);

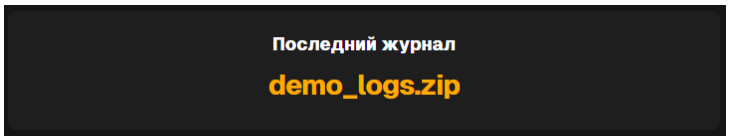

Рисунок 14 – Блок «Последний журнал»

5) для перехода к последнему добавленному журналу нужно нажать на наименование последнего журнала в блоке.

3.2 Просмотр распределения атакующих сессий по сайтам

В разделе «Главная» можно просматривать распределение атакующих сессий по сайтам, доступным пользователю. В данной статистике учитываются атакующие сессии с любым уровнем риска. Для просмотра распределения необходимо выполнить следующие действия:

1) перейти в раздел «Главная»;

2) отобразится раздел со статистикой по всем доступным сайтам;

3) в блоке «Распределение атакующих сессий по сайтам» отобразится круговая диаграмма с распределением атакующих сессий (Рисунок 15);

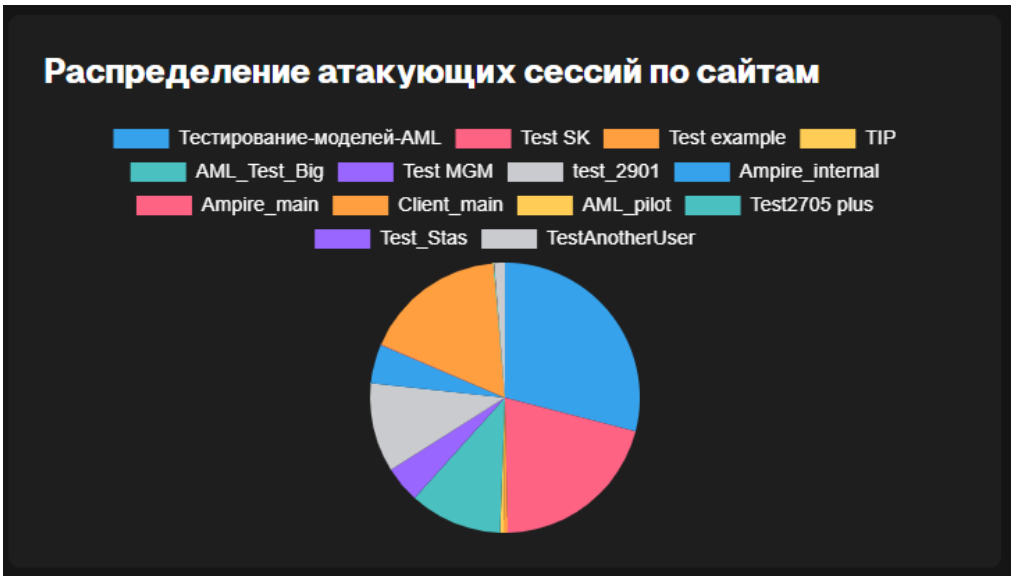

Рисунок 15 – Круговая диаграмма атакующих сессий

4) после нажатия на наименование сайта в легенде диаграммы сайт будет удален из отображения, наименование в легенде для данного сайта становится зачеркнутым (Рисунок 16);

Рисунок 16 – Выбор сайтов для отображения на круговой диаграмме

5) при наведении курсора мыши на область диаграммы будет отображено наименование сайта и количество выявленных для указанного сайта атакующих сессий (Рисунок 17).

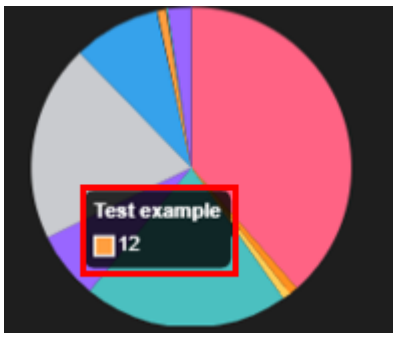

Рисунок 17 – Отображение данных о сайте на круговой диаграмме

3.3 Просмотр распределения атакующих сессий по рискам

В разделе «Главная» можно просматривать распределение атакующих сессий по уровню риска. Статистика строится для всех доступных пользователю сайтов. Для просмотра распределения необходимо выполнить следующие действия:

1) перейти в раздел «Главная»;

2) далее отобразится раздел со статистикой по всем доступным сайтам;

3) в блоке «Распределение атакующих сессий по риску» отображена гистограмма с распределением атакующих сессий (Рисунок 18);

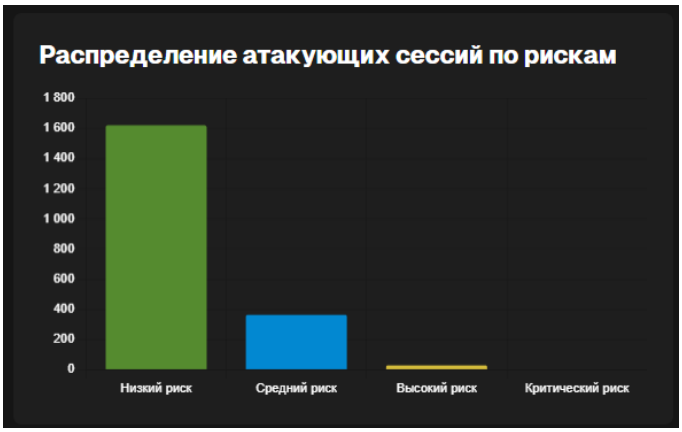

Рисунок 18 – Блок «Распределение атакующих сессий по риску»

4) при наведении курсора мыши на столбец гистограммы будет отображен риск, соответствующий столбцу и количество атакующих сессий с данным риском (Рисунок 19).

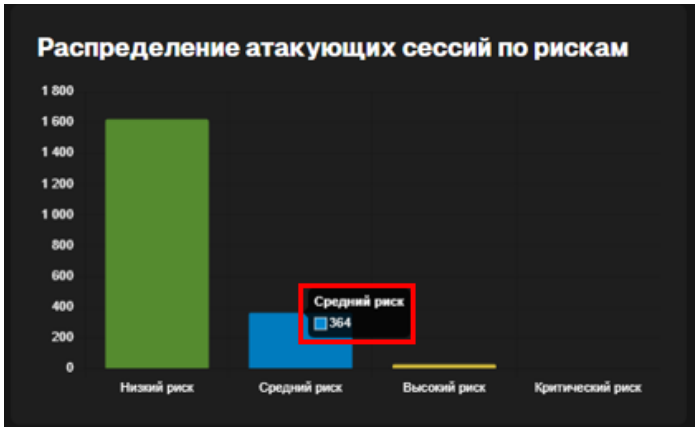

Рисунок 19 – Просмотр деталей по сессиям определенного риска

3.4 Просмотр списка журналов, обрабатываемых в потоковом режиме обработки

В разделе «Главная» для доступных пользователю сайтов можно просматривать статистику по журналам, которые в данный момент обрабатываются в потоковом режиме. Для просмотра статистики необходимо выполнить следующие действия:

1) перейти в раздел «Главная»;

2) в блоке «Журналы» отобразится таблица, содержащая наименование журнала, текущий статус блокировки и обработки, количество строк в журнале, количество запросов в секунду, выявленные пользовательские и атакующие сессии. Также отобразится сумма количества строк и запросов для сайтов, доступных пользователю (Рисунок 20).

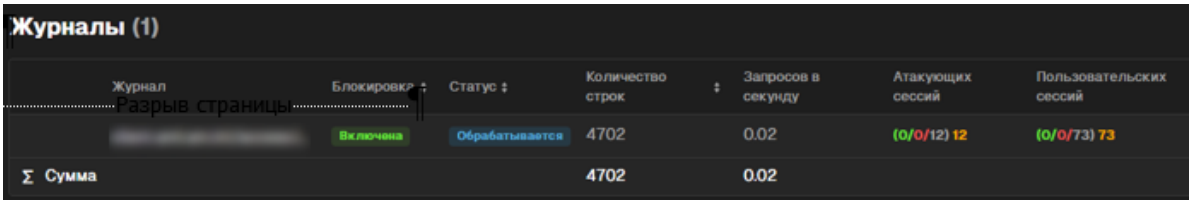

Рисунок 20 – Блок «Журналы»

4 Раздел «Сайты»

В разделе «Сайты» описана работа с сайтами, поставленными на обработку. В данном разделе пользователь может вести работу с доступными сайтами, а также добавлять или удалять сайты, являющиеся источником журналов для обработки.

4.1 Добавление сайта

Основная работа с «AML» начинается после добавления сайта. Для выполнения обработки журналов необходимо изначально добавить сайт. Далее добавить журналы, для которых будет выполняться обработка, с помощью следующих действий:

1) перейти в раздел «Сайты» (Рисунок 21);

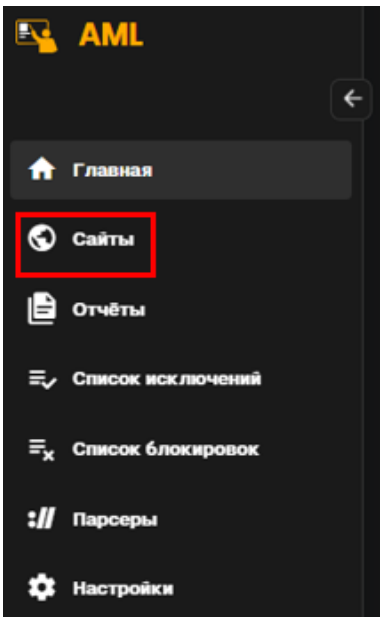

Рисунок 21 – Переход в раздел «Сайты»

2) нажать на кнопку «Добавить сайт» (Рисунок 22);

Рисунок 22 – Добавление сайта

3) в открывшемся модальном окне ввести «Название» и «Домен», также можно указать используемый «Технологический стек». Поле «Технологический стек» является необязательным, но может дать дополнительную информацию для оператора, который будет контролировать работу Системы (Рисунок 23);

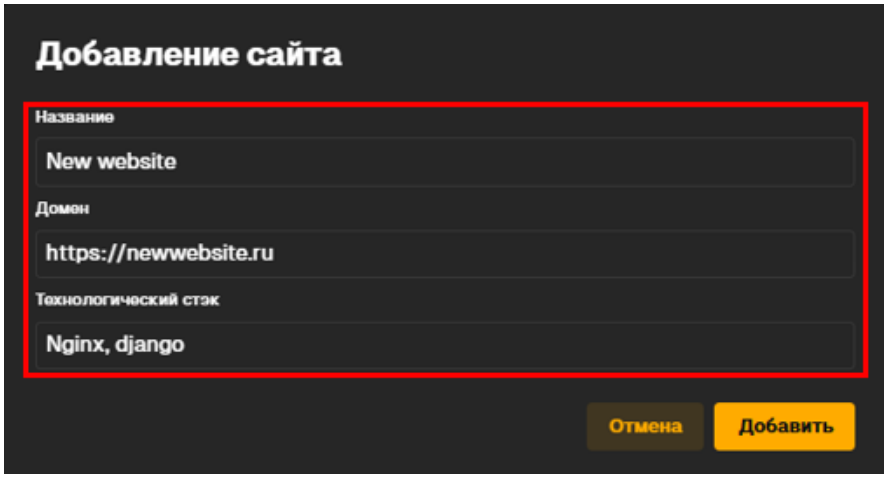

Рисунок 23 – Форма для добавления сайта

4) нажать на кнопку «Добавить» (Рисунок 24);

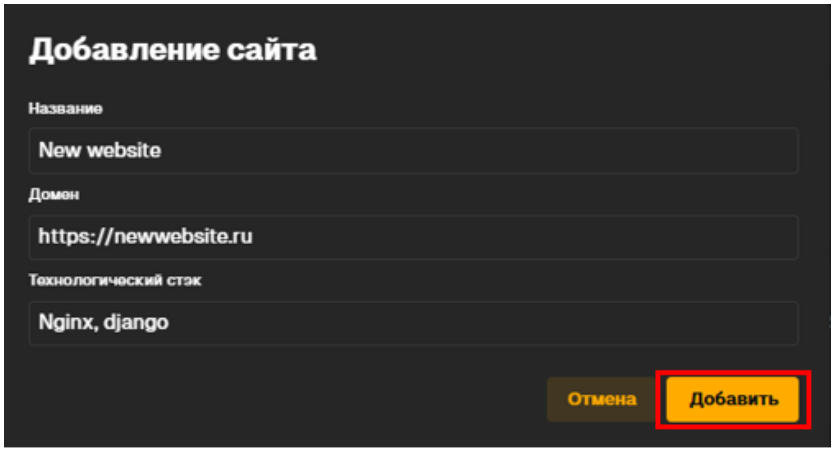

Рисунок 24 – Кнопка «Добавить»

5) будет создан сайт с указанным названием и доменом (Рисунок 25).

Рисунок 25 – Карточка добавленного сайта

4.2 Удаление сайта

В процессе работы могут возникнуть ситуации, когда нет необходимости в мониторинге ресурсов определенного сайта. В таком случае данный сайт можно удалить из «AML» с помощью следующих действий:

1) перейти в раздел «Сайты»;

2) навести курсор мыши на сайт, который нужно удалить. В правом верхнем углу отобразится иконка меню выбора действий (Рисунок 26);

Рисунок 26 – Иконка меню выбора действий

3) нажать на иконку для отображения перечня действий, в появившемся меню выбрать «Удалить» (Рисунок 27);

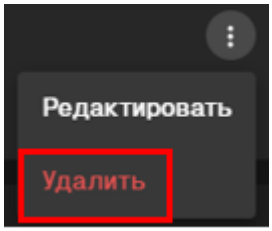

Рисунок 27 – Кнопка удаления сайта

4) в открывшемся модальном окне подтвердить удаление (Рисунок 28).

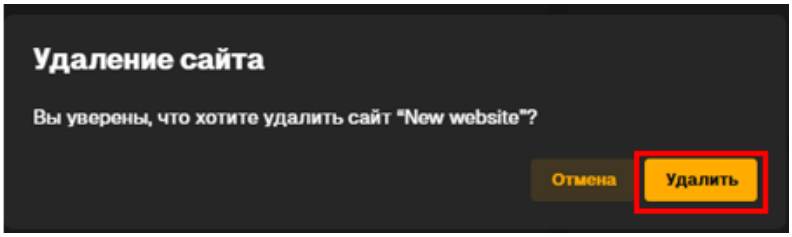

Рисунок 28 – Модальное окно для подтверждения удаления

4.3 Редактирование данных сайта

В процессе работы могут возникнуть ситуации, когда находящийся на мониторинге сайт меняется или при создании сайта была допущена ошибка. В таком случае данные указанного сайта можно отредактировать с помощью следующих действий:

1) перейти в раздел «Сайты»;

2) навести курсор мыши на сайт, который нужно отредактировать. В правом верхнем углу отобразится иконка меню выбора действий (Рисунок 29);

Рисунок 29 – Редактирование данных сайта

3) нажать на иконку для отображения перечня действий, в появившемся меню выбрать «Редактировать» (Рисунок 30);

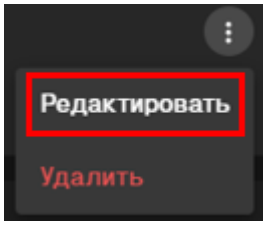

Рисунок 30 – Редактирование данных сайта

4) в открывшемся модальном окне внести изменения в данные сайта. Аналогично добавлению сайта «Название» и «Домен» являются обязательными полями при редактировании. После изменения данных нажать на кнопку «Сохранить» (Рисунок 31);

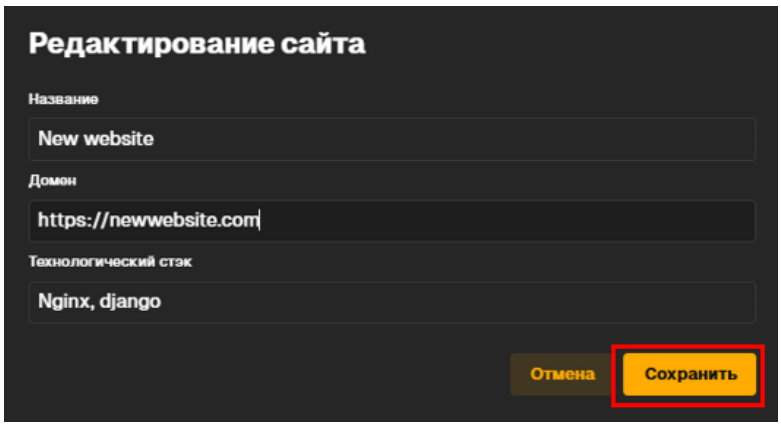

Рисунок 31 – Сохранение отредактированных данных

4.4 Чтение и изменение формата отображения перечня сайтов

В разделе «Сайты» пользователь может ознакомиться со всеми доступными сайтами, находящимися в обработке. Также пользователь может настроить вид отображения для своего удобства с помощью следующих действий:

1) перейти в раздел «Сайты», в котором будут отображены все доступные пользователю сайты;

2) после нажатия на кнопки «Таблица»/«Плитка» в правом верхнем углу можно изменить настройки отображения (Рисунок 32);

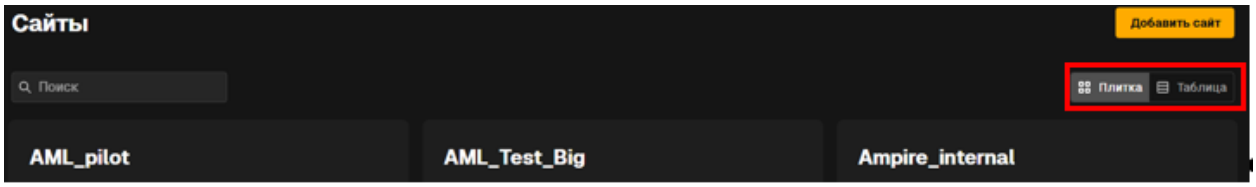

Рисунок 32 – Настройка вида отображения

3) после нажатия на кнопки выбора внешний вид страницы изменится (Рисунок 33).

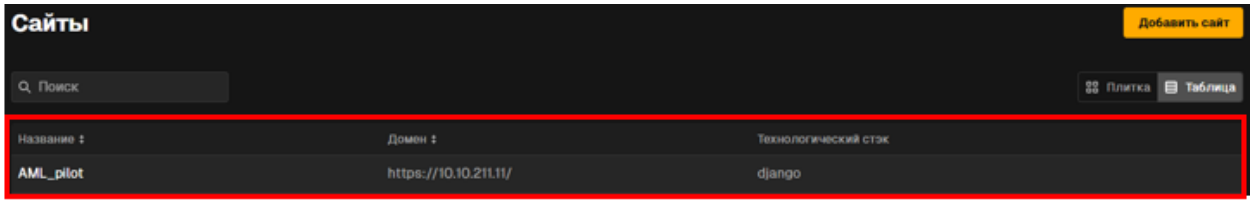

Рисунок 33 – Измененный вид отображения

4.5 Поиск по списку сайтов

Для ускорения работы с перечнем сайтов в разделе «Сайты» пользователь может выполнять поиск по списку доступных сайтов с помощью следующих действий:

1) перейти в раздел «Сайты»;
2) в поле поиска ввести искомое значение (Рисунок 34);

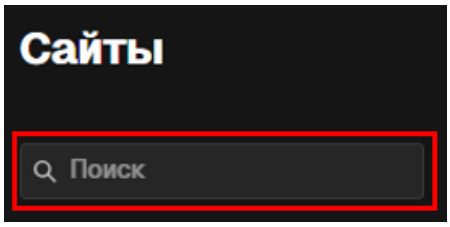

Рисунок 34 – Поиск по списку сайтов

3) далее Система выполнит поиск на вхождение искомого значения в полях «Название», «Домен» или «Технологический стек» (Рисунок 35).

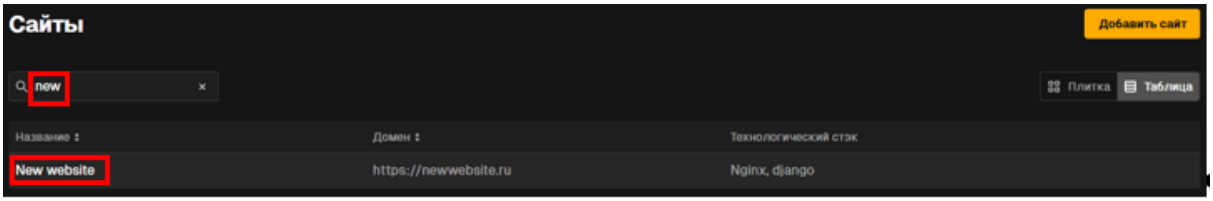

Рисунок 35 – Результат поиска

4.6 Переход к журналам сайта

Из раздела «Сайты» можно выполнить переход к журналам определенного сайта с помощью следующих действий:

1) перейти в раздел «Сайты»;
2) выбрать необходимый сайт (Рисунок 36);

Рисунок 36 – Переход к журналам сайта

3) нажать на блок с выбранным сайтом, пользователь будет перенаправлен на страницу журналов выбранного сайта (Рисунок 37).

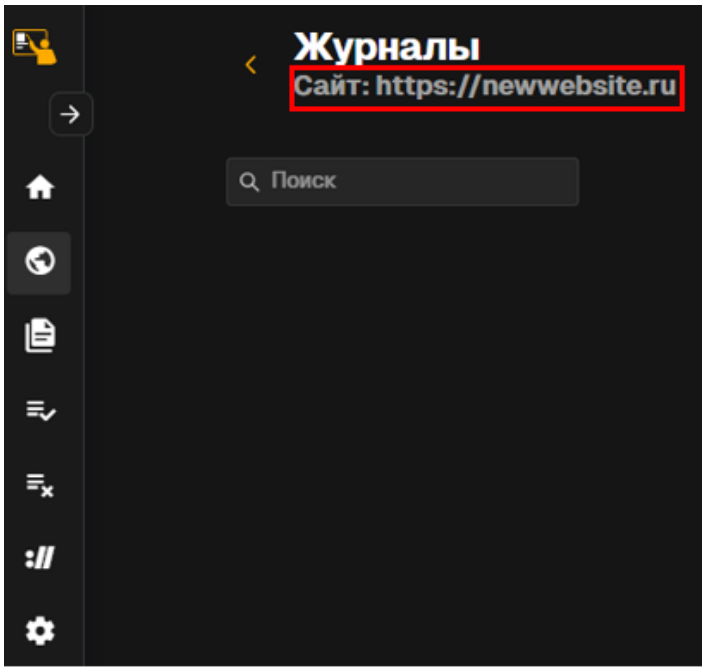

Рисунок 37 – Перенаправление на страницу журнала

5 Работа с журналами

В разделе «Сайты» пользователем может быть осуществлен переход к журналам доступного сайта. Из карточки журнала ведется работа по постановке на обработку новых журналов, просмотру результатов обработки, настройке параметров обработки.

5.1 Просмотр и настройка отображения журналов

В разделе «Сайты» при переходе к конкретному сайту можно изучить журналы, добавленные для обработки. Для просмотра и настройки отображения журналов необходимо выполнить следующие действия:

1) перейти к странице журналов сайта, что представлено в соответствующем описании (Подраздел 5.6);

2) по умолчанию перечень добавленных журналов будет отображен в формате «Плитка» (Рисунок 38);

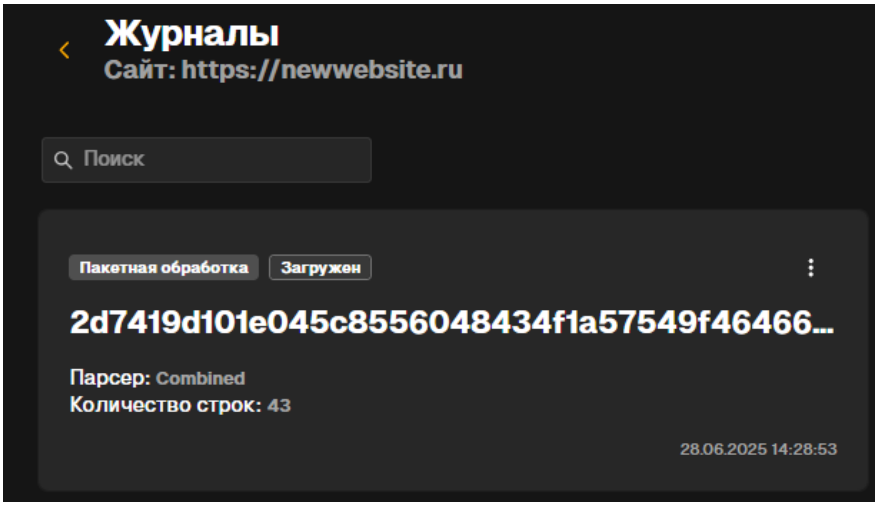

Рисунок 38 – Перечень добавленных журналов

3) для изменения отображения списка журналов необходимо в правом верхнем углу страницы выбрать формат отображения – «Таблица»/«Плитка» (Рисунок 39);

Рисунок 39 – Настройка отображения журналов

4) после нажатия на кнопки выбора внешний вид отображения будет изменен (Рисунок 40);

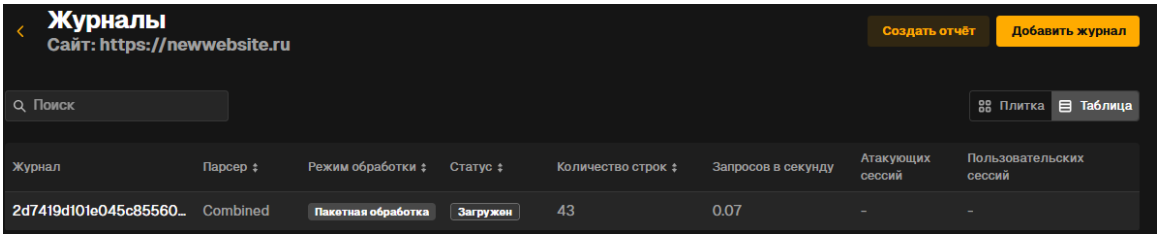

Рисунок 40 – Результат настройки отображения

5.2 Поиск по списку журналов

Для ускорения работы с журналами можно использовать поиск по списку журналов с помощью следующих действий:

1) перейти к странице журналов сайта;

2) в поле поиска ввести искомое значение (Рисунок 41);

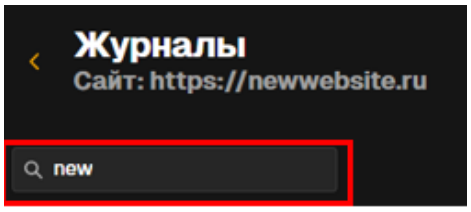

Рисунок 41 – Поиск по списку журналов

3) далее Система выполнит поиск на вхождение искомого значения в названии журнала (Рисунок 42);

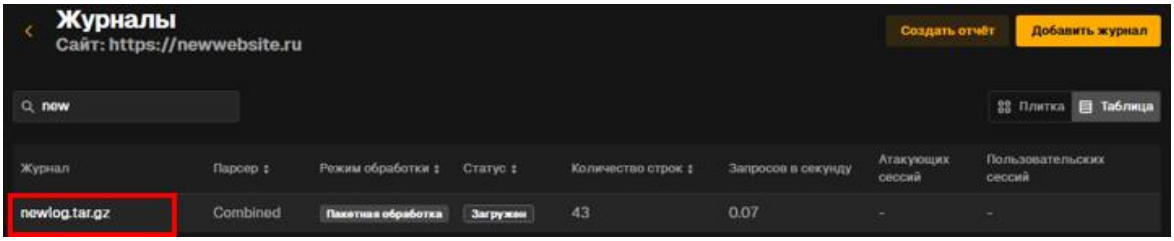

Рисунок 42 – Результат поиска

5.3 Добавление журнала для обработки в пакетном режиме

Для запуска обработки необходимо добавить в Систему файл с записями журнала веб-ресурса. Загрузка журнала, обрабатываемого в пакетном режиме, выполняется с помощью следующих действий:

1) перейти к странице журналов сайта;

2) нажать на кнопку «Добавить журнал» (Рисунок 43);

Рисунок 43 – Добавление журнала для обработки в пакетном режиме

3) в блоке «Режим обработки» выбрать чекбокс «Пакетная обработка» (Рисунок 44);

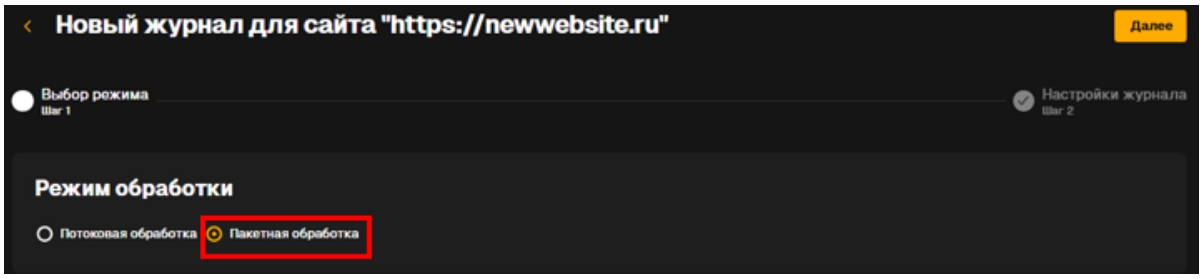

Рисунок 44 – Выбор пакетного режима обработки

4) в блоке «Файл с логами» перетащить в область или выбрать файл, содержащий журналы веб-сервера за необходимый период (Рисунок 45);

Рисунок 45 – Выбор файла с журналом событий

5) после загрузки файла лога будет осуществлен переход к шагу 2 «Настройки журнала» (Рисунок 46);

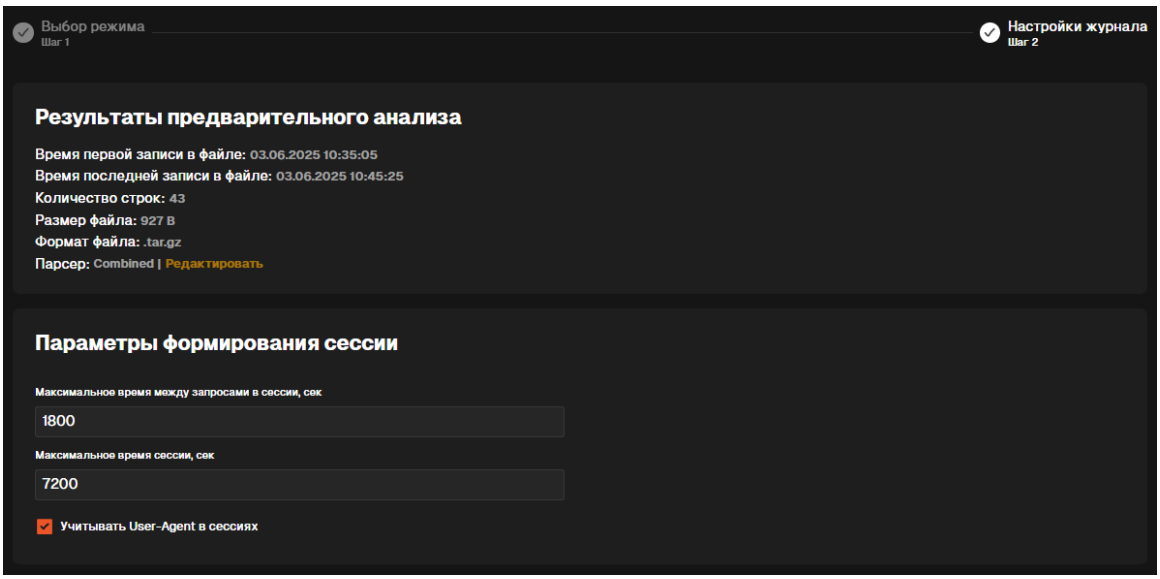

Рисунок 46 – Настройка обработки

6) в блоке «Результаты предварительного анализа» можно изменить автоматически подобранный Системой парсер на другой, заведенный в Системе, нажав на кнопку «Редактировать» (Рисунок 47);

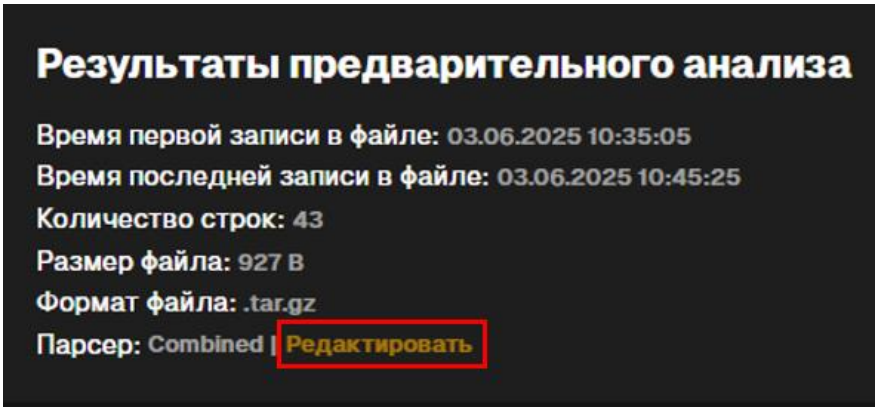

Рисунок 47 – Редактирование парсера для обработки журнала

7) в открывшемся модальном окне нужно выбрать необходимый парсер из выпадающего списка и нажать кнопку «Сохранить» (Рисунок 48, Рисунок 49);

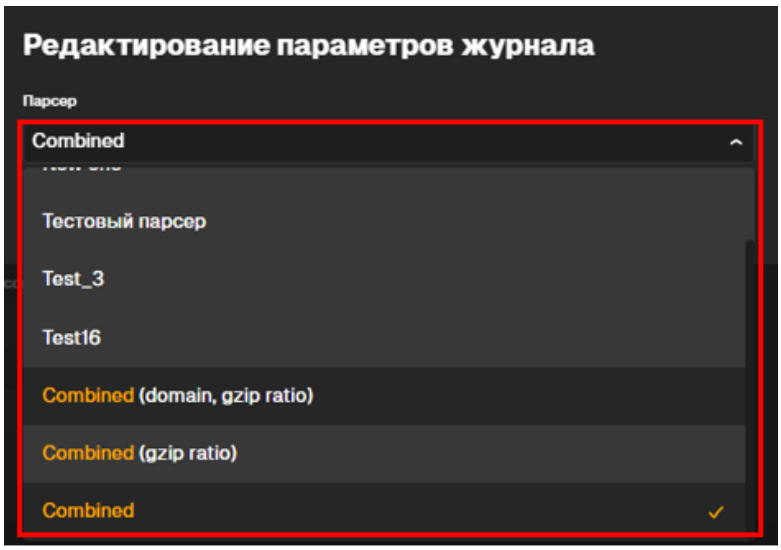

Рисунок 48 – Выбор парсера

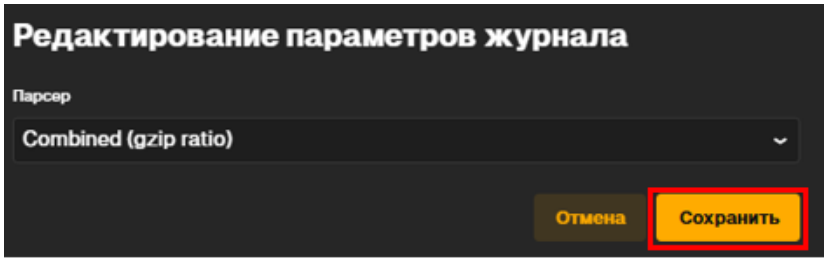

Рисунок 49 – Сохранение изменений при редактировании парсера

8) в блоке «Параметры формирования сессии» ввести максимальное время между запросами в сессии и максимальное время сессии. Рекомендуется не изменять установленные по умолчанию параметры при отсутствии бизнес-потребности (Рисунок 50);

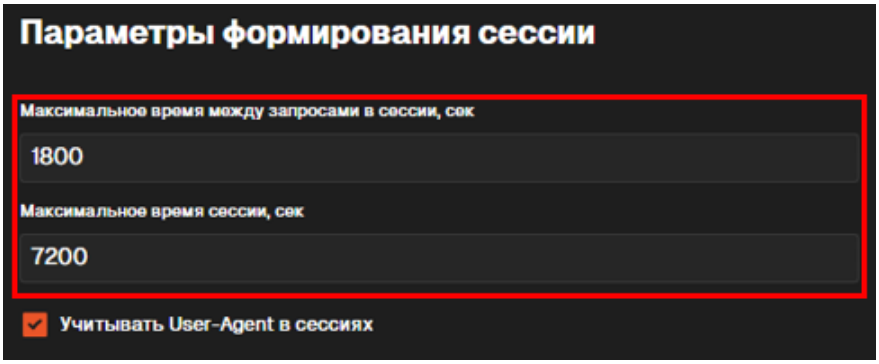

Рисунок 50 – Настройка параметров формирования сессии

9) при необходимости учета «User-Agent» при формировании сессии необходимо отметить соответствующий чекбокс (Рисунок 51);

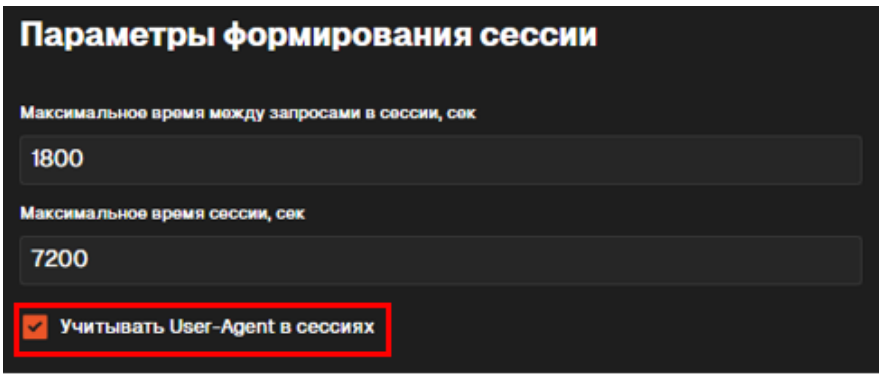

Рисунок 51 – Выбор признака учета «User-Agent» при формировании сессии

10) для завершения добавления журнала нажать кнопку «Сохранить» (Рисунок 52);

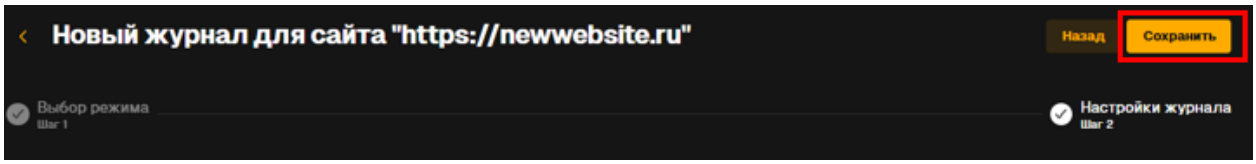

Рисунок 52 – Завершение добавления журнала

11) журнал будет добавлен в Систему и получит статус «Загружен» (Рисунок 53).

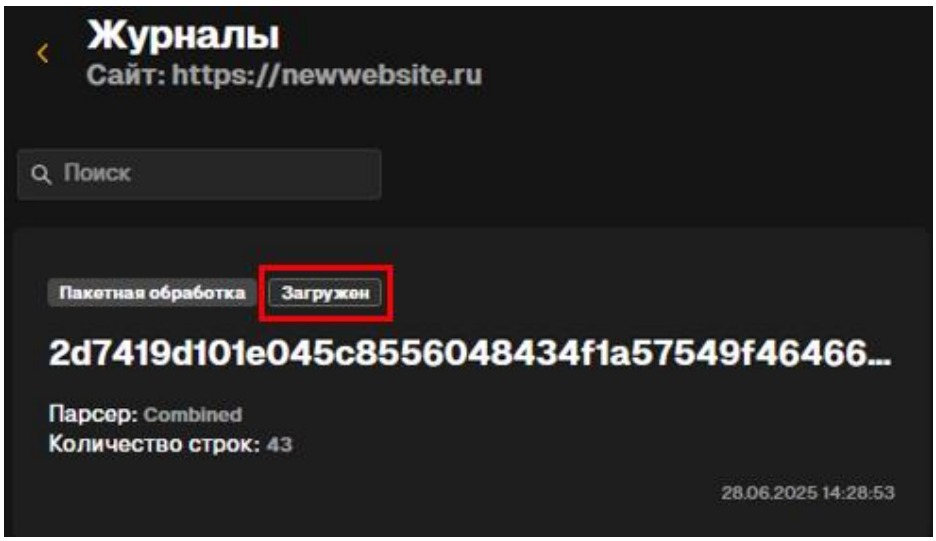

Рисунок 53 – Результат добавления нового журнала в пакетном режиме

5.4 Добавление журнала для обработки в потоковом режиме

Для запуска обработки необходимо добавить в Систему журнал, содержащий логи сайта. Загрузка журнала, обрабатываемого в потоковом режиме, выполняется с помощью следующих действий:

1) перейти к странице журналов сайта;

2) нажать на кнопку «Добавить журнал» (Рисунок 54);

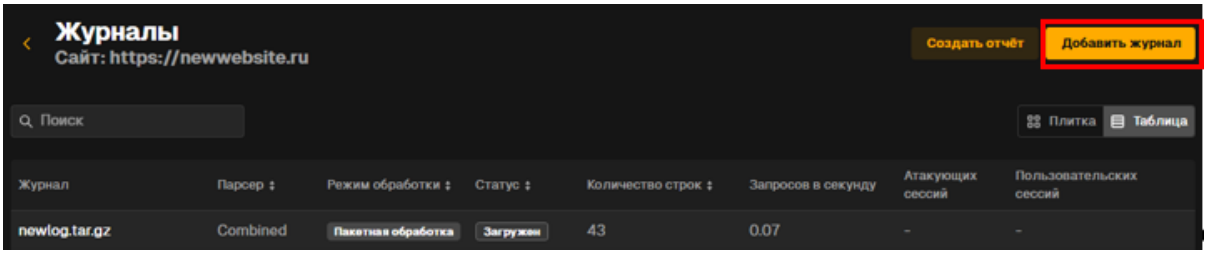

Рисунок 54 – Добавление журнала для обработки в потоковом режиме

3) в блоке «Режим обработки» выбрать чекбокс «Потоковая обработка» (Рисунок 55);

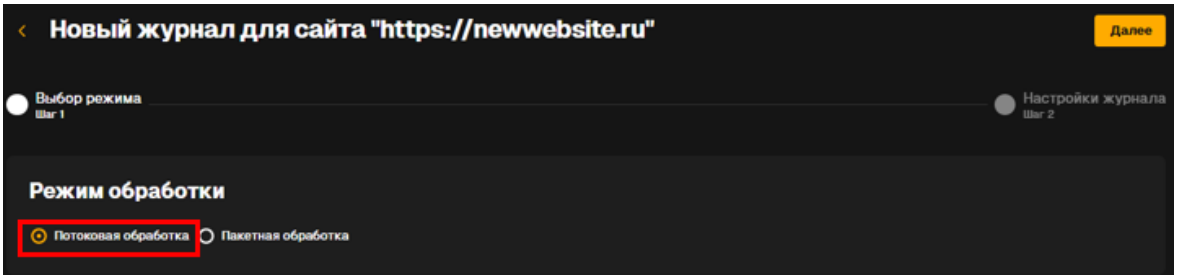

Рисунок 55 – Выбор потокового режима обработки при добавлении журнала

4) в блоке «Потоковая обработка» выбрать папку и файл записей с нужного веб-сервера. Для отображения файла в списке данные о сервере и пути до него должны быть предварительно внесены в Систему администратором (Рисунок 56);

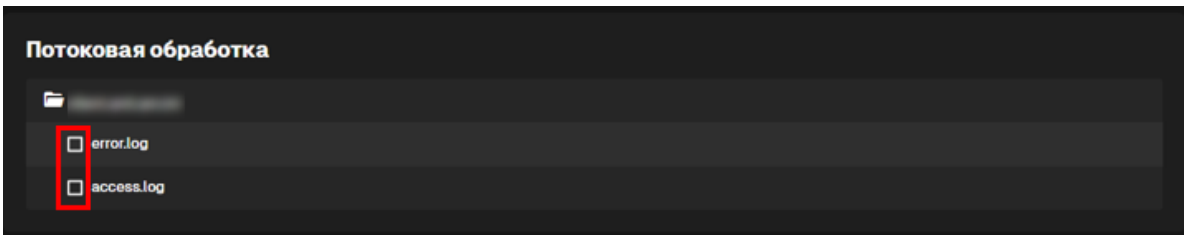

Рисунок 56 – Выбор пути до необходимого журнала событий

5) после выбора файла лога будет осуществлен переход к шагу 2 «Настройки журнала» (Рисунок 57);

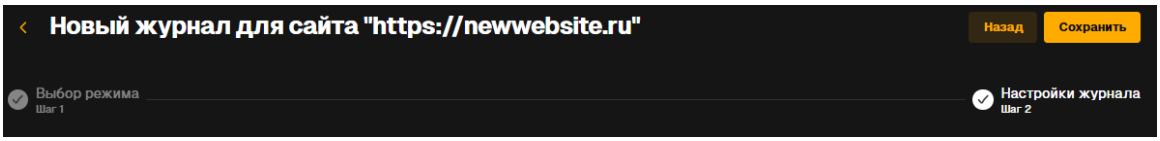

Рисунок 57 – Настройки журнала

6) в блоке «Результаты предварительного анализа» можно изменить автоматически подобранный Системой парсер на другой, подобранный Системой, нажав на кнопку «Редактировать» (Рисунок 58);

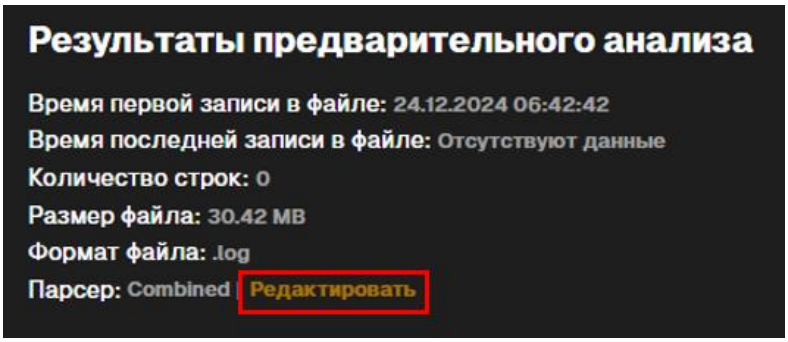

Рисунок 58 – Редактирование парсера при потоковой обработке журнала

7) в открывшемся модальном окне нужно выбрать необходимый парсер из выпадающего списка и нажать кнопку «Сохранить» (Рисунок 59, Рисунок 60);

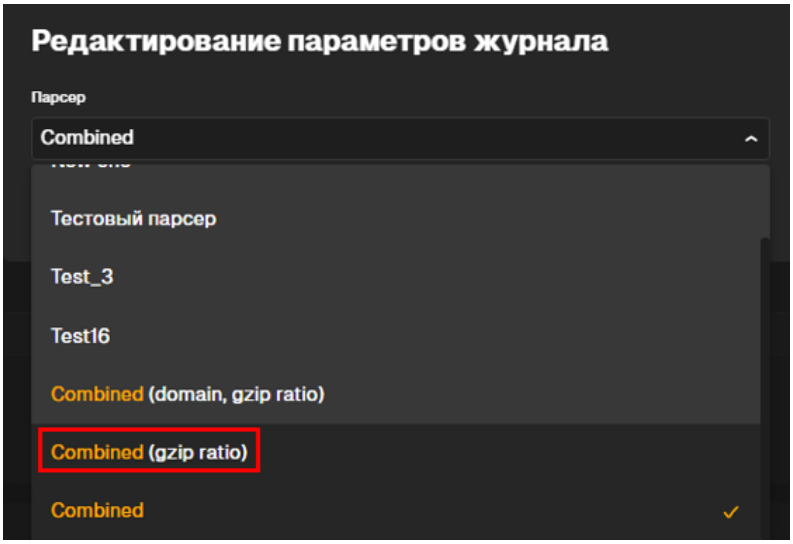

Рисунок 59 – Выбор парсера

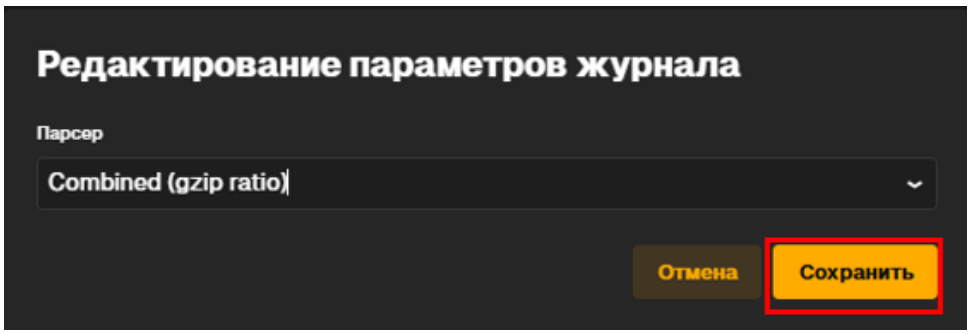

Рисунок 60 – Сохранение изменений при редактировании парсера

8) в блоке «Режим блокировки» можно активировать блокировку атакующих сессий. Для возможности блокировки атакующих сессий для указанного журнала системный администратор должен предварительно внести данные в панели администратора Системы. Если настройка выполнена, то можно активировать блокировку, изменив положение переключателя на активное (Рисунок 61);

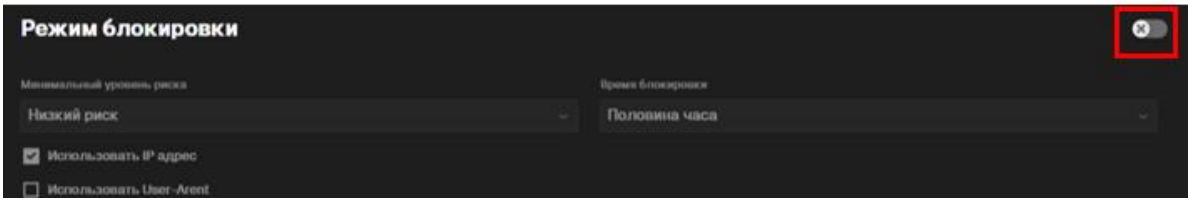

Рисунок 61 – Активация режима блокировки

9) после активации переключателя для блокировки можно указать «Минимальный уровень риска», «Время», на которое будет блокироваться атакующая сессия, а также выбрать параметр, по которому будет осуществляться блокировка – только «IP-адрес» или дополнительно «User-Agent» (Рисунок 62);

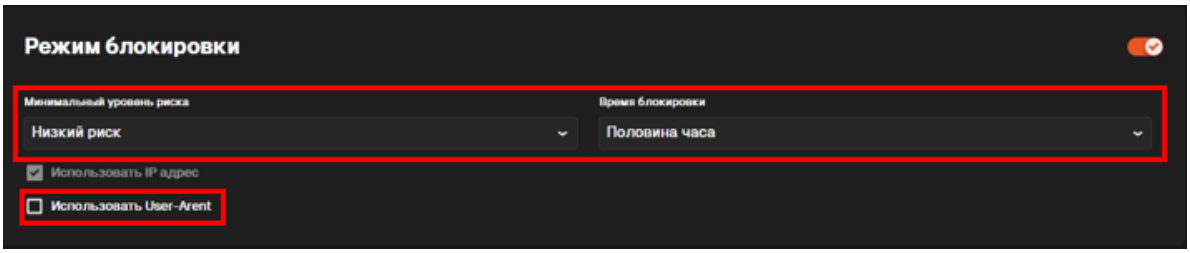

Рисунок 62 – Настройка блокировки на ресурсе

10) в блоке «Параметры формирования сессии» ввести «Максимальное время между запросами в сессии», «Максимальное время сессии», «Время хранения атакующих и пользовательских сессий» (в месяцах) (Рисунок 63);

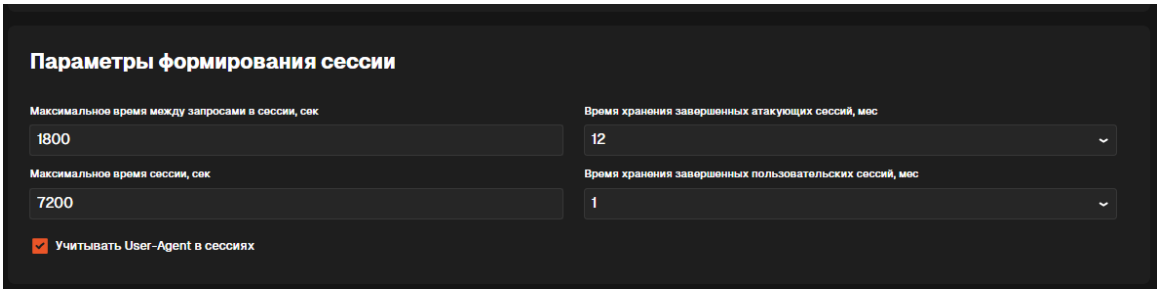

Рисунок 63 – Настройка параметров формирования сессии

11) при необходимости учета «User-Agent» при формировании сессии необходимо отметить соответствующий чекбокс (Рисунок 64);

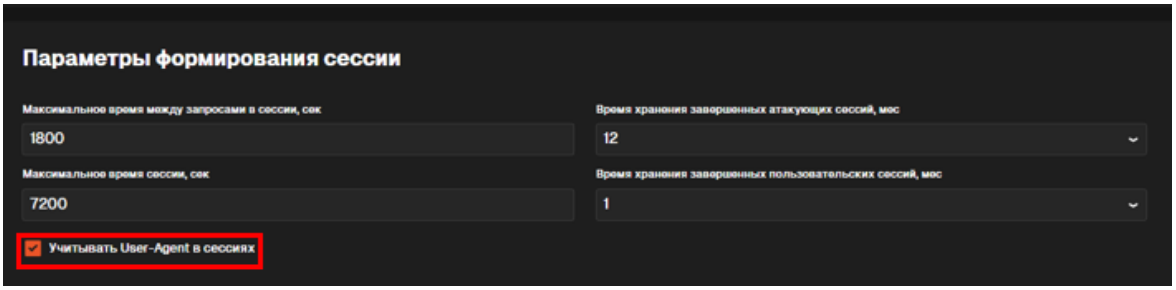

Рисунок 64 – Выбор признака учета «User-Agent» при формировании сессии

12) для завершения добавления журнала нажать кнопку «Сохранить» (Рисунок 65);

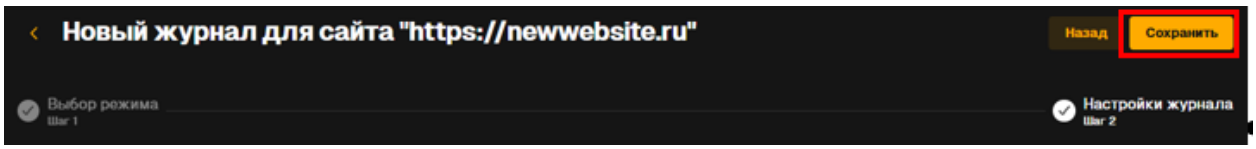

Рисунок 65 – Завершение добавления журнала для обработки в потоковом режиме

13) журнал будет добавлен в Систему и получит статус «Загружен».

5.5 Удаление журнала

При работе с Системой может возникнуть необходимость удаления журнала. Если журнал устарел или не считается актуальным, то можно выполнить удаление с помощью следующих действий:

1) перейти к странице журналов сайта;

2) навести курсор мыши на журнал, который пользователь намерен удалить. В правом верхнем углу журнала нажать на иконку меню выбора действий (Рисунок 66);

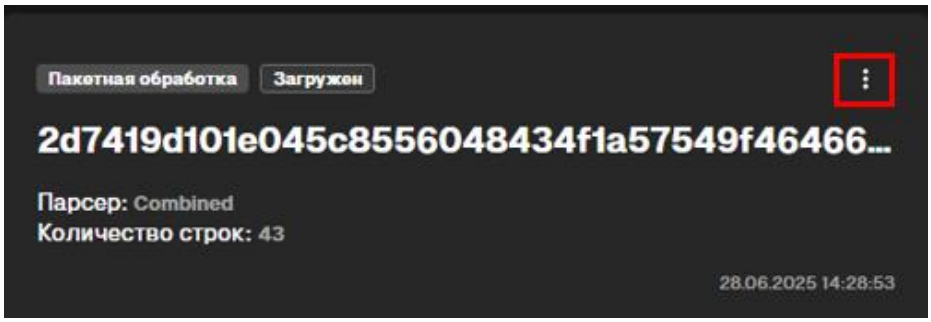

Рисунок 66 – Открытие меню действий

3) в появившемся меню нажать на пункт «Удалить» (Рисунок 67);

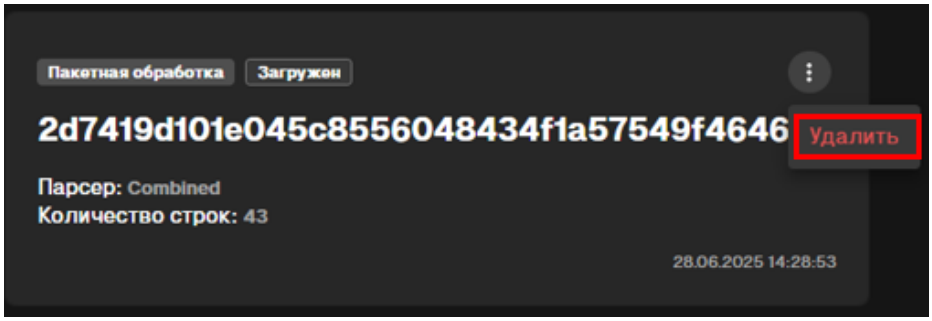

Рисунок 67 – Удаление журнала

4) в модальном окне подтвердить удаление (Рисунок 68).

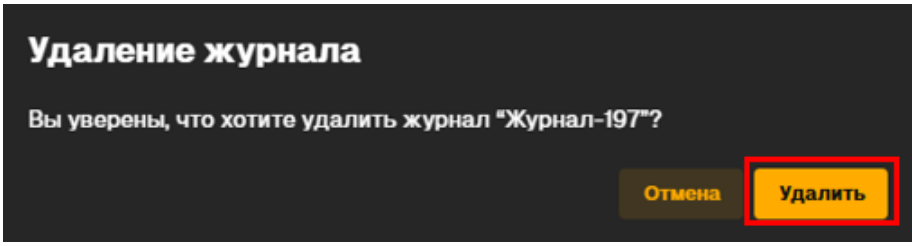

Рисунок 68 – Подтверждение удаления журнала

5.6 Просмотр общей информации и параметров журнала

Для просмотра выбранных настроек при добавлении журнала в Систему нужно перейти к просмотру информации об указанном журнале с помощью следующих действий:

1) перейти к странице журналов сайта;

2) нажать на журнал, для которого необходимо посмотреть информацию (Рисунок 69);

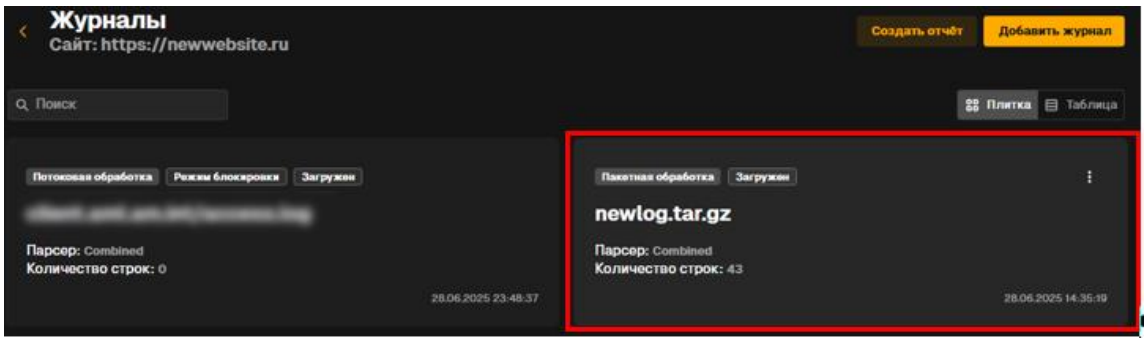

Рисунок 69 – Переход к странице параметров журнала

3) будет осуществлен переход к странице параметров журнала и результатов анализа (Рисунок 70).

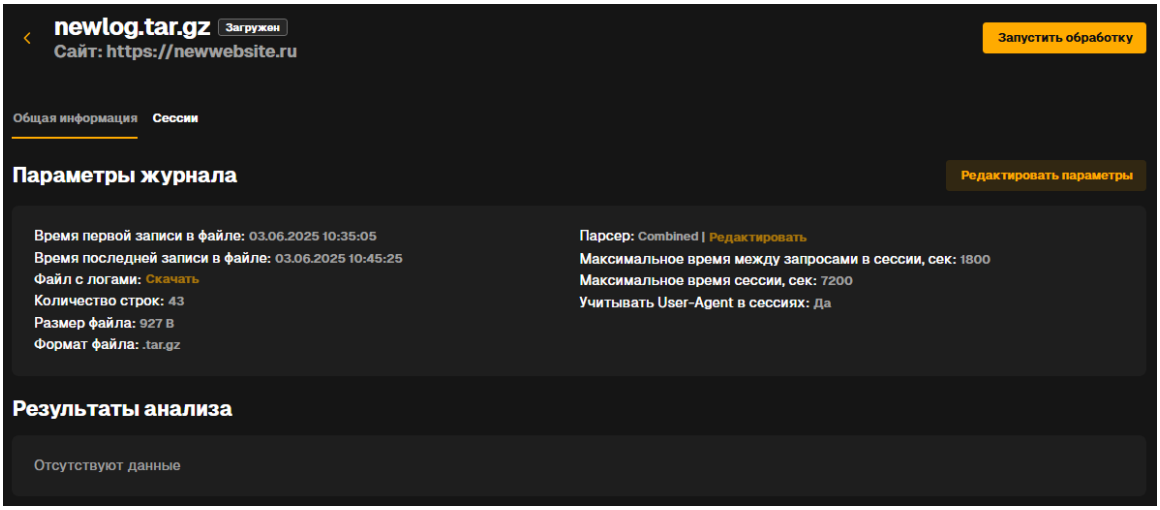

Рисунок 70 – Просмотр общей информации и параметров журнала

5.7 Редактирование параметров журнала

При необходимости изменения изначально заданных параметров журнала, что можно выполнить на странице просмотра подробной информации о журнале с помощью следующих действий:

1) перейти к странице просмотра параметров журнала, что представлено в соответствующем описании (Подраздел 5.6);

2) нажать на кнопку «Редактировать параметры» (Рисунок 71);

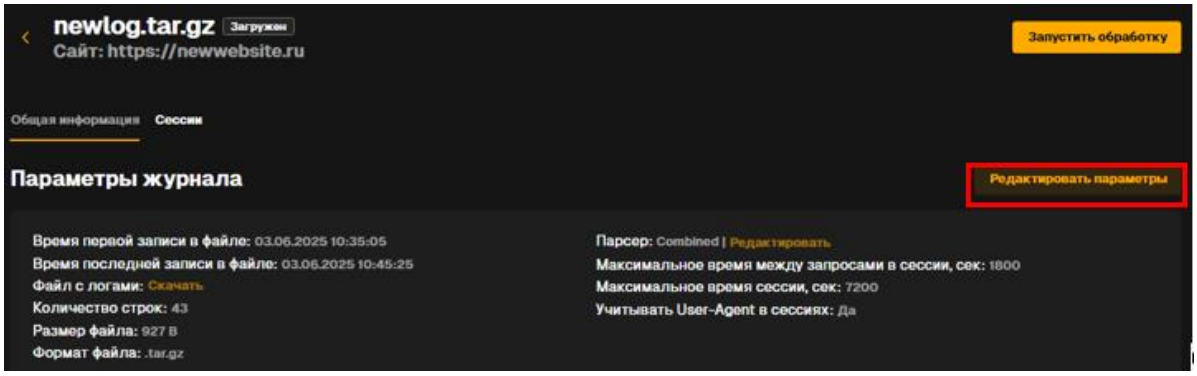

Рисунок 71 – Переход к редактированию параметров журнала

3) в модальном окне изменить параметры в полях «Максимальное время между запросами» и «Максимальное время сессии», а также изменив значение чекбокса «Учитывать User-Agent в сессиях» можно изменить параметры влияния «User-Agent» на формирование сессии (Рисунок 72);

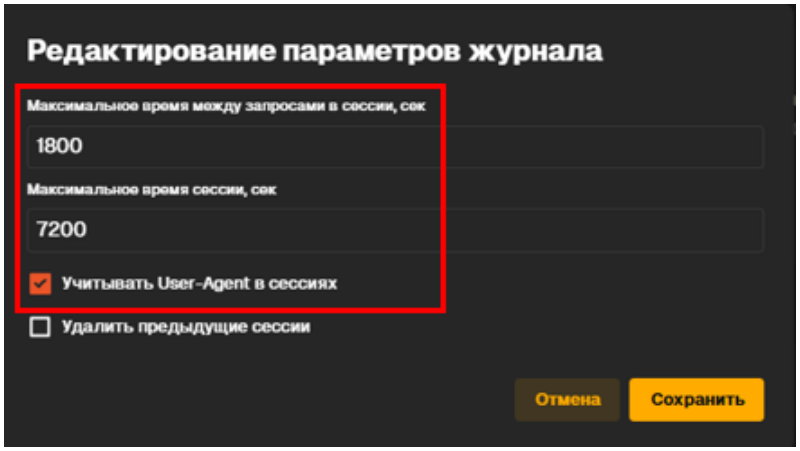

Рисунок 72 – Редактирование параметров журнала

4) отметив чекбокс «Удалить предыдущие сессии» можно стереть информацию о ранее сформированных сессиях в журнале, если указанные данные не требуются (Рисунок 73);

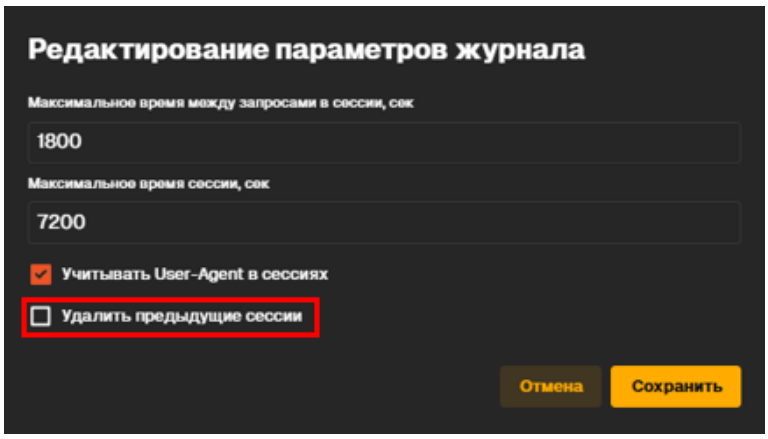

Рисунок 73 – Настройка удаления предыдущих сессий

5) после завершения редактирования нажать на кнопку «Сохранить».

5.8 Изменение парсера журнала

Если при добавлении журнала в Систему парсер логов выбран неверно или возникла необходимость изменения, то можно внести изменения на странице просмотра информации о журнале с помощью следующих действий:

1) перейти к странице просмотра параметров журнала;

2) в блоке «Параметры журнала» возле поля «Парсер» нажать на кнопку «Редактировать» (Рисунок 74);

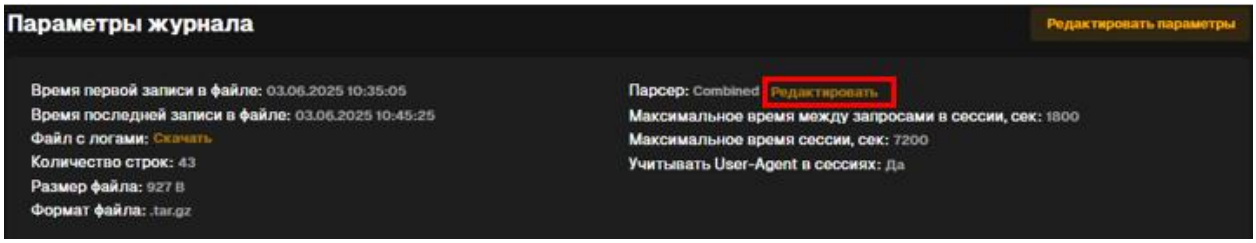

Рисунок 74 – Переход к изменению парсера журнала

3) в модальном окне выбрать значение нового парсера из выпадающего списка (Рисунок 75);

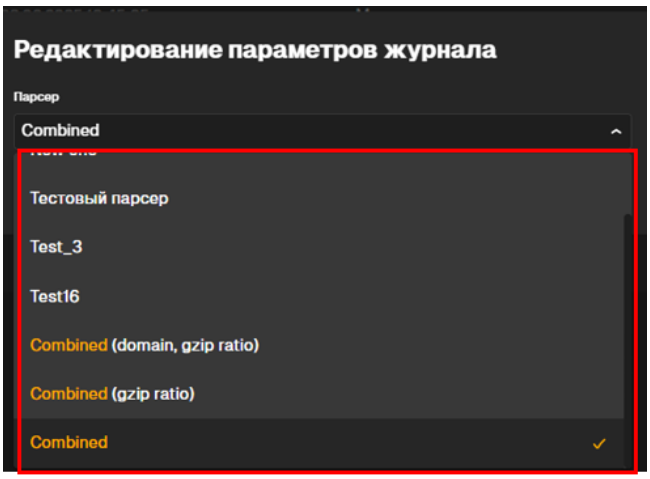

Рисунок 75 – Изменение парсера журнала

4) нажать на кнопку «Сохранить» (Рисунок 76);

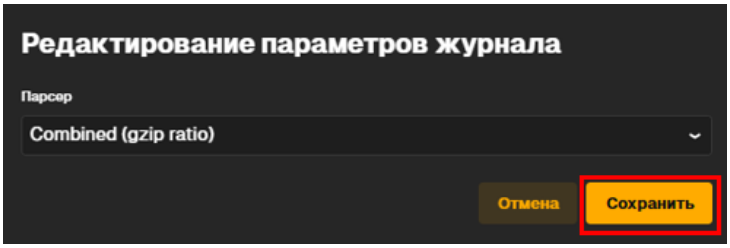

Рисунок 76 – Сохранение изменений парсера журнала

5) парсер для данного журнала будет изменен на новый.

5.9 Запуск обработки журнала

На странице параметров журнала можно запустить обработку журнала – анализ сессий в данном журнале на предмет наличия пользовательских и атакующих сессий, а также определение риска для атакующих сессий. Для запуска обработки журнала необходимо выполнить следующие действия:

1) перейти к странице просмотра параметров журнала;

2) в правом верхнем углу нажать на кнопку «Запустить обработку» (Рисунок 77);

Рисунок 77 – Запуск обработки журнала

3) журнал получит статус «В очереди»;

4) через некоторое время статус будет изменен на (Рисунок 78):

– «Обработан» – если журнал обрабатывается в пакетном режиме;

– «Обрабатывается» – если журнал обрабатывается в потоковом режиме;

– «Ошибка» – если обработка журнала прошла некорректно.

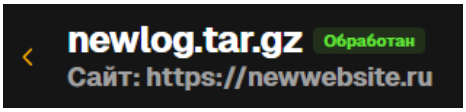

Рисунок 78 – Отображение статуса обработки журнала

5.10 Перезапуск пакетной обработки журнала

Для журналов, обрабатываемых в пакетном режиме можно повторно запустить обработку журнала. В перезапуске может возникнуть необходимость при изменении модели. Для перезапуска обработки журнала нужно выполнить следующие действия:

1) перейти к странице просмотра параметров журнала;

2) нажать на кнопку «Редактировать параметры» (Рисунок 79);

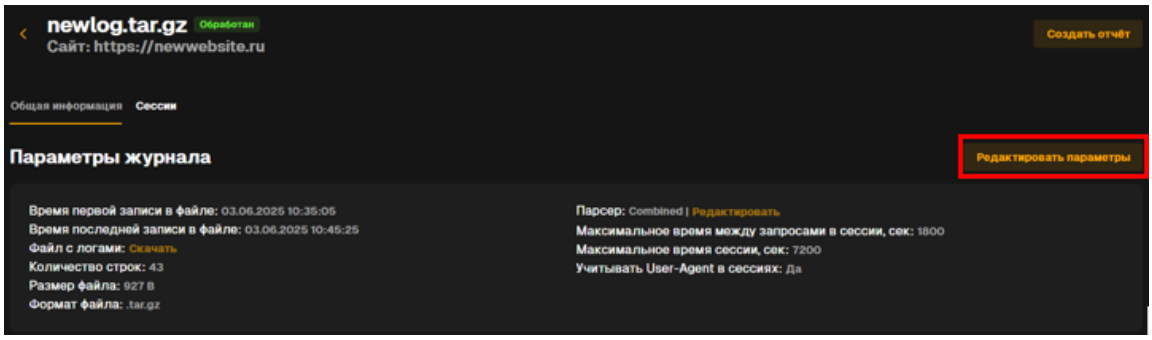

Рисунок 79 – Выполнение условий для перезапуска пакетной обработки журнала

3) в открывшемся модальном окне без внесения изменений нажать кнопку «Сохранить» (Рисунок 80);

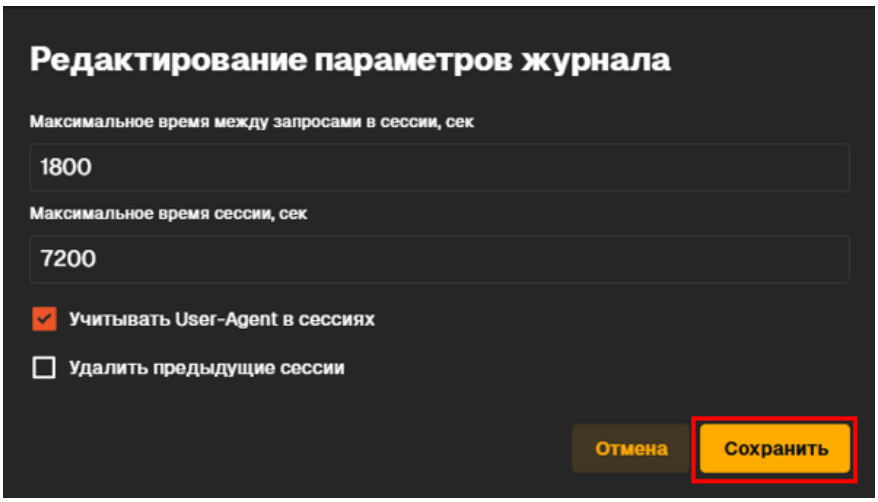

Рисунок 80 – Выполнение условий для перезапуска пакетной обработки журнала

4) после редактирования на странице параметров журнала можно повторно опустить обработку (Рисунок 81).

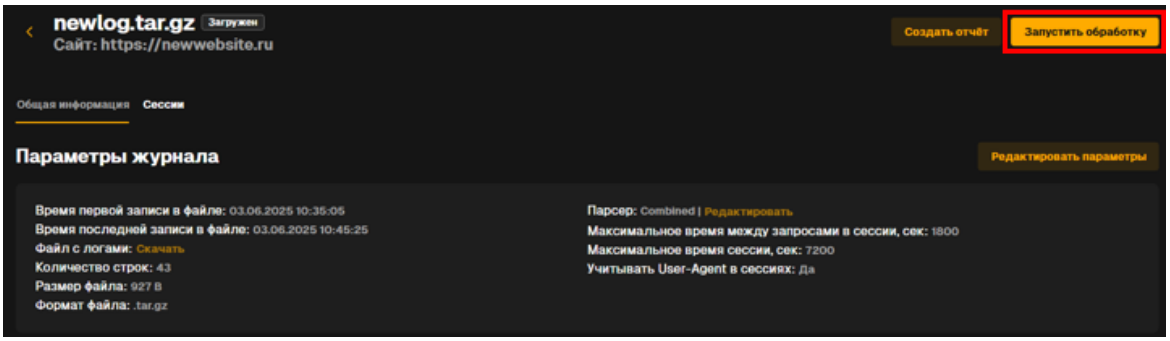

Рисунок 81 – Перезапуск пакетной обработки журнала

5.11 Перезапуск потоковой обработки журнала

Для журналов, обрабатываемых в потоковом режиме можно приостановить и повторно запустить обработку журнала с помощью следующих действий:

1) перейти к странице просмотра параметров журнала, который находится в статусе «Обрабатывается»;

2) в правом верхнем углу нажать на кнопку «Остановить обработку» (Рисунок 82);

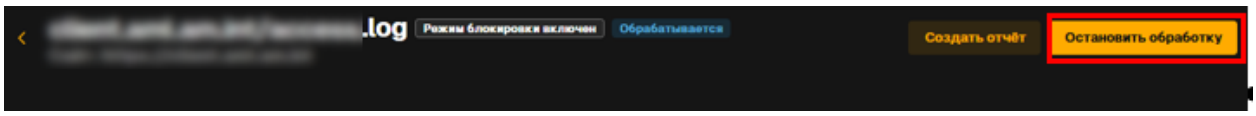

Рисунок 82 – Остановка обработки журнала

3) обработка журнала будет остановлена, а статус изменен на «Загружен»;

4) запустить обработку, что представлено в соответствующем описании (подраздел 5.9);

5) статус журнала изменится на «Обрабатывается», а анализ для данного журнала возобновится.

5.12 Просмотр результатов анализа

На странице журнала можно ознакомиться с результатами обработки логов данного журнала с помощью следующих действий (Рисунок 83):

1) перейти к странице просмотра параметров журнала;

2) в блоке «Результаты анализа» будет отображен датированный результат обработки выбранного журнала;

3) для каждого из запусков будут отображены следующие значения:

– «Количество IP» – подсчет IP-адресов в загруженном журнале событий;

– «Количество сессий» – подсчет объединенных в группы (по полям «IP-адрес» и «User-Agent») записей журнала»;

– «Атакующих сессий» – количественное выражение вида (M/N/P) Q, которое интерпретируется следующим образом: «Система выявила Q + N сессий данного типа, с M из которых пользователь согласен, с N из которых пользователь не согласен, P из которых пользователь не валидировал»;

– «Пользовательских сессий» – количественное выражение вида (M/N/P) Q, которое интерпретируется аналогично атакующим сессиям;

– «Процент атакующих сессий» – процентное соотношение атакующих сессий к общему количеству сессий;

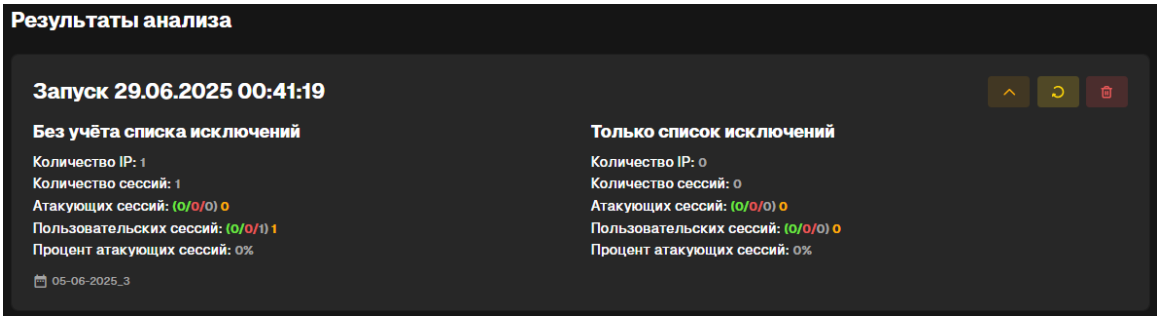

Рисунок 83 – Просмотр результатов анализа

4) результат отображается отдельно для каждого из запусков, по умолчанию в развернутом состоянии находится только самый последний запуск. Для отображения результатов предыдущих запусков нужно нажать на кнопку «Развернуть» (Рисунок 84);

Рисунок 84 – Просмотр более ранних результатов анализа

5) для каждого из результатов обработки показывается статистика распределения атакующих и пользовательских сессий без учета и с учетом исключений. Статистика для сессий исключений отображена в отдельном столбце и также включает распределение атакующих и пользовательских сессий (Рисунок 85).

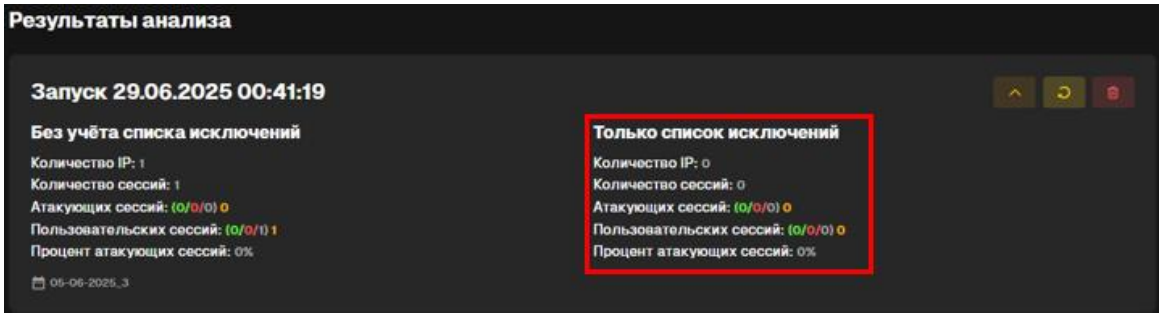

Рисунок 85 – Результаты анализа для адресов из списка исключений

5.13 Скачивание файла с логами

Иногда может понадобиться скачать файл, загруженный в Систему для анализа – если нужно убедиться в корректности загруженного файла или если файл загружен ранее другим пользователем. Для скачивания файла с логами необходимо выполнить следующие действия:

1) перейти к странице просмотра параметров журнала;

2) в блоке «Параметры журнала» найти пункт «Файл с логами» и нажать на кнопку «Скачать» (Рисунок 86);

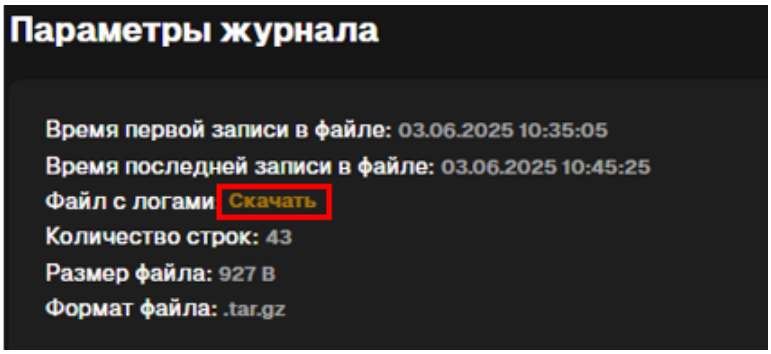

Рисунок 86 – Скачивание файла с логами

3) будет запущена загрузка файла журнала логов (Рисунок 87).

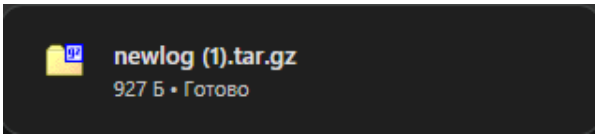

Рисунок 87 – Загрузка файла с логами

5.14 Скачивание файла с ошибками

При проведении анализа файла могут быть выявлены строки журнала, содержащие некорректные, ошибочные значения. Подобные ошибочные строки объединяются в один файл и могут быть выгружены из Системы для просмотра и анализа. При наличии данного файла для просмотра и скачивания необходимо выполнить следующие действия:

1) перейти к странице просмотра параметров журнала;

2) в блоке «Параметры журнала» найти пункт «Файл с ошибками. Нажать на кнопку «Скачать» (Рисунок 88);

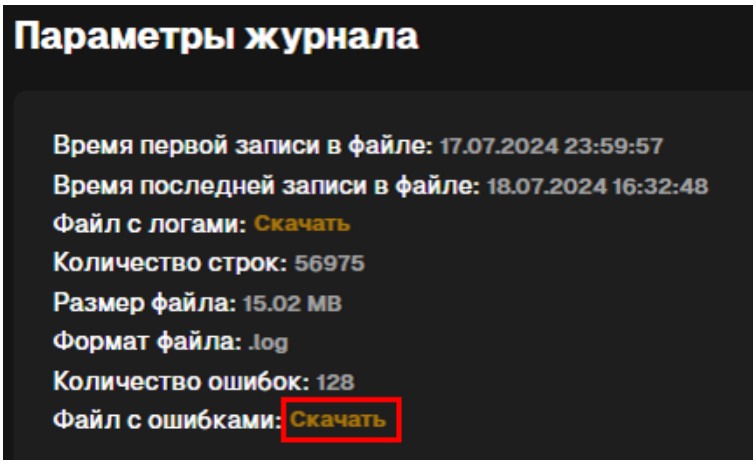

Рисунок 88 – Скачивание файла с ошибками

3) будет запущена загрузка файла ошибок.

5.15 Удаление результатов запуска обработки журнала

После завершения или перезапуска обработки журнала может понадобиться удалить старые результаты обработки журнала, что можно выполнить с помощью следующих действий:

1) перейти к странице просмотра параметров журнала;

2) в блоке «Результаты анализа» выбрать запуск, данные которого необходимо удалить;

3) нажать на иконку удаления в области необходимого запуска (Рисунок 89);

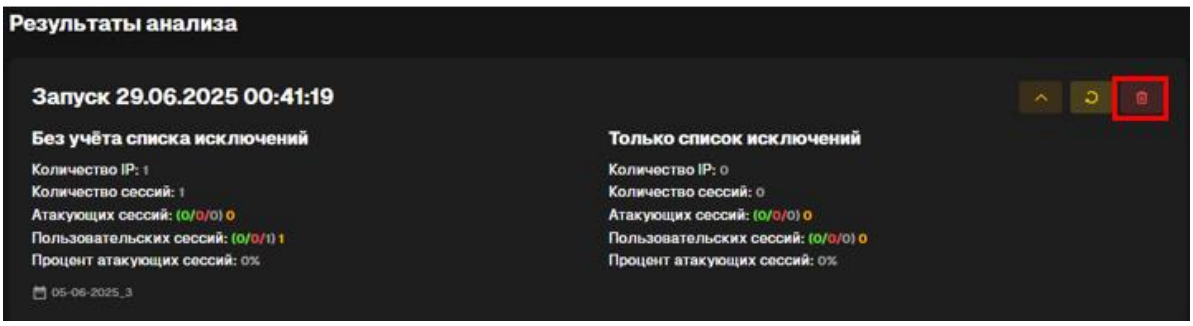

Рисунок 89 – Удаление результатов запуска обработки журнала

4) подтвердить удаление результата анализа. При удалении результата анализа сессии, сформированные для него, также будут удалены из Системы (Рисунок 90).

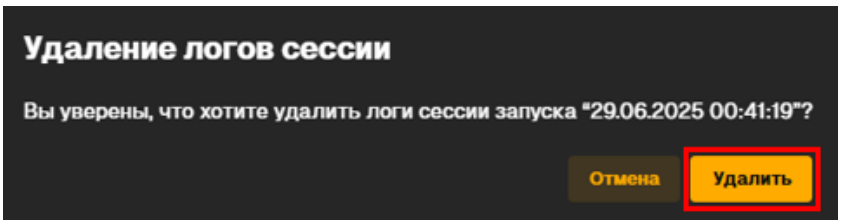

Рисунок 90 – Подтверждение удаления результатов запуска обработки журнала

5.16 Создание отчета

Для возможности ознакомления с результатами анализа журнала вне Системы можно выгрузить отчет, содержащий всю необходимую информацию, с помощью следующих действий:

1) перейти к странице журналов сайта или странице просмотра параметров конкретного журнала;

2) нажать на кнопку «Создать отчет» в правом верхнем углу страницы (Рисунок 91);

Рисунок 91 – Создание отчета

3) в открывшемся модальном окне указать журнал, тип результата обработки, выбрать запуск, по которому необходимо выгрузить отчет. Также необходимо указать период – за весь период или за произвольный период. После завершения ввода данных нажать кнопку «Создать» (Рисунок 92);

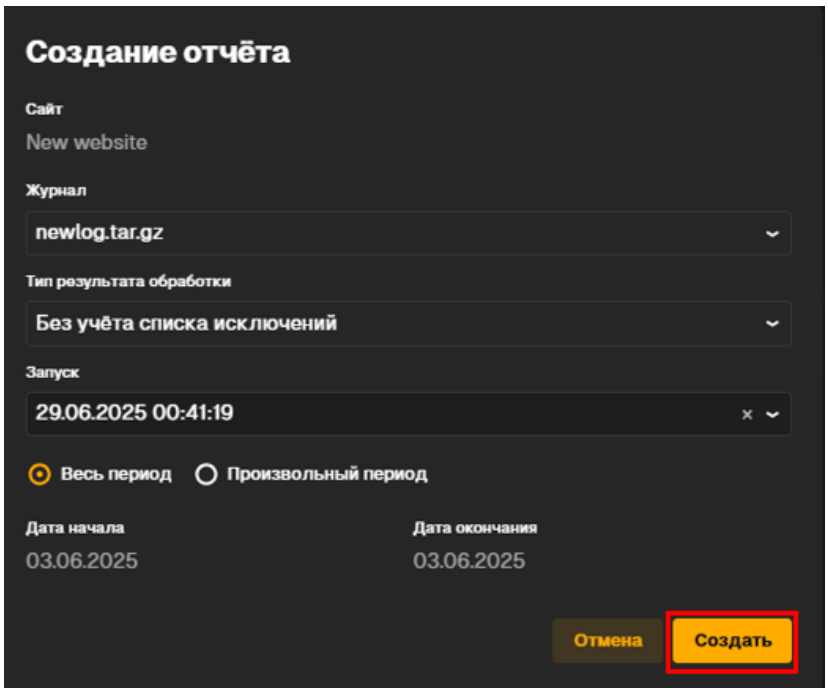

Рисунок 92 – Выбор информации при создании отчета

4) в новой вкладке откроется файл отчета в формате PDF (Рисунок 93);

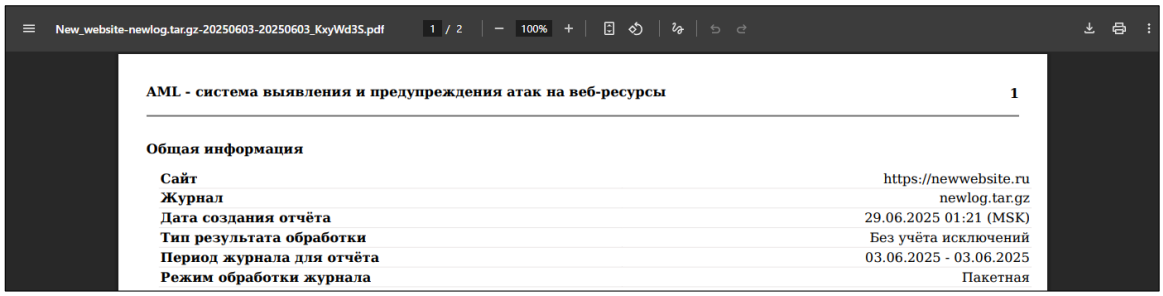

Рисунок 93 – Файл отчета

6 Работа с сессиями и логами

При работе с сессиями пользователь может:

– изучать подробности пользовательских и атакующих сессий;

– изучать логи, которые данную сессию формируют;

– выносить вердикт о корректности работы модели по выявлению атакующих сессий и определению их риска.

6.1 Просмотр и настройка отображения сессии

Для удобства работы с разделом пользователь может настроить формат отображения сессии, представив его в виде таблицы или в виде плиток, с помощью следующих действий:

1) перейти к просмотру журнала;

2) перейти к просмотру сессии (Рисунок 94):

– для пакетного режима – переключиться на вкладку «Сессии»;

– для потокового режима – переключиться на вкладку «Текущие сессии»;

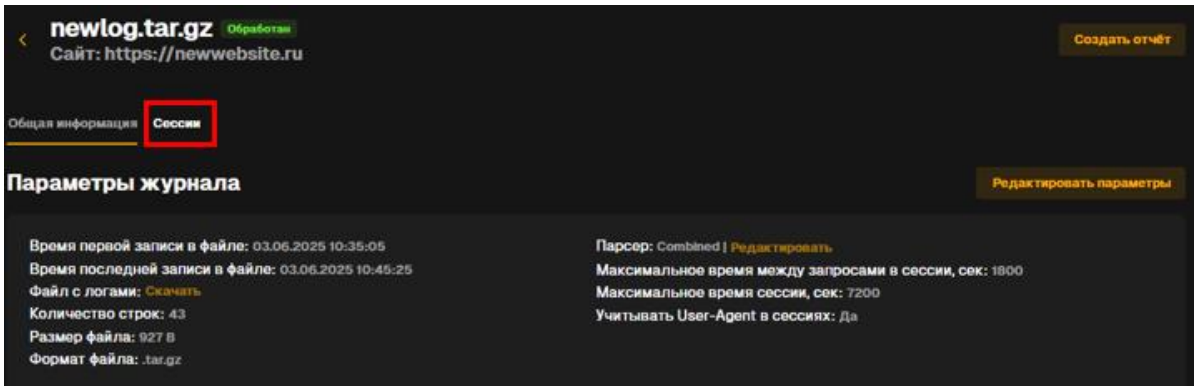

Рисунок 94 – Переход к сессиям журнала

3) по умолчанию список сессий отображается в виде таблицы, при необходимости можно изменить настройки визуализации – раскрыть выпадающий список в правом верхнем углу (Рисунок 95);

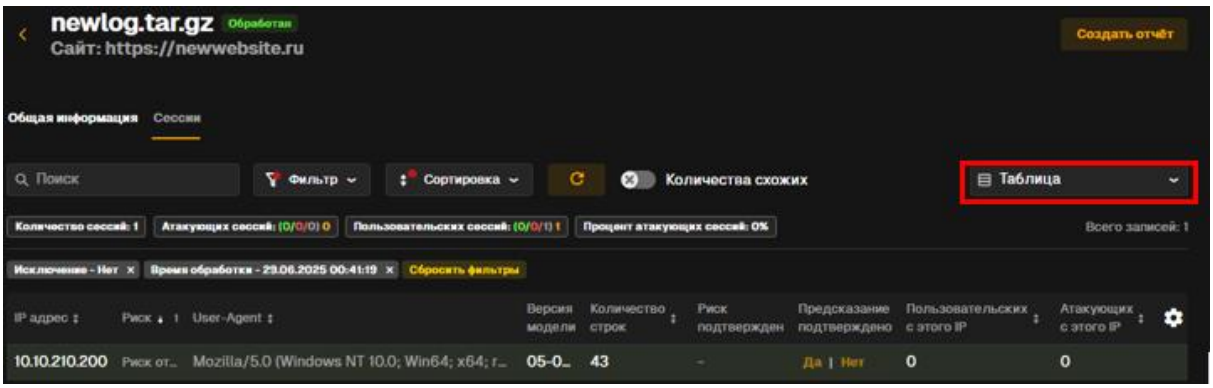

Рисунок 95 – Настройка отображения сессии

4) из появившегося списка выбрать необходимое отображение (Рисунок 96);

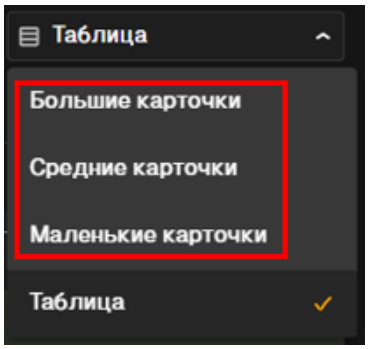

Рисунок 96 – Выбор отображения

5) табличное представление изменится на выбранное.

6.2 Подтверждение рисков и предсказаний из списка сессий

Для каждой из выявленных сессий проставляется предсказание на основе анализа модели. Предсказание выносит вердикт касательно того, является ли сессия атакующей или пользовательской. Для атакующих сессий выставляется риск в зависимости от различных показателей данной сессии – «IP-адрес», параметров запросов, «User-Agent» и т.д. Предсказание и риск могут быть вручную подтверждены или опровергнуты пользователем с помощью следующих действий:

1) перейти к просмотру сессий;

2) найти сессию, для которой необходимо подтвердить риск;

3) в столбце (в случае табличной визуализации страницы сессий) или в блоке сессии (в случае представления «Большие карточки») найти «Предсказание подтверждено». Для визуализации «Маленькие карточки» и «Средние карточки» подтверждение предсказания или риска невозможно (Рисунок 97);

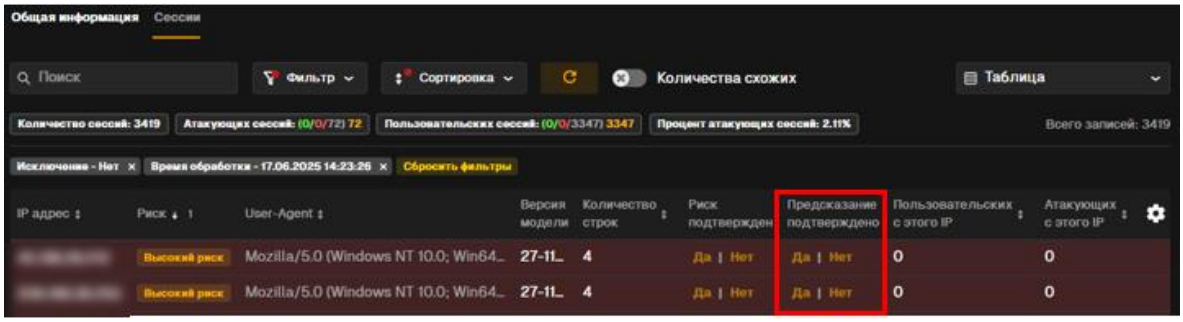

Рисунок 97 – Информация о текущем статусе подтверждения предсказания

4) нажать «Да», если пользователь согласен с предсказанием модели, или «Нет», если не согласен (Рисунок 98);

Рисунок 98 – Подтверждение предсказания

5) для атакующих сессий можно также подтвердить риск – в столбце (при табличной визуализации страницы сессий) или в блоке сессии (при представлении «Большие карточки») найти «Риск подтвержден» (Рисунок 99). Для визуализации «Маленькие карточки» и «Средние карточки» подтверждение предсказания или риска невозможно;

Рисунок 99 – Просмотр информации о текущем статусе подтверждения риска

6) нажать «Да», если пользователь согласен с предсказанным риском, или «Нет», если не согласен (Рисунок 100);

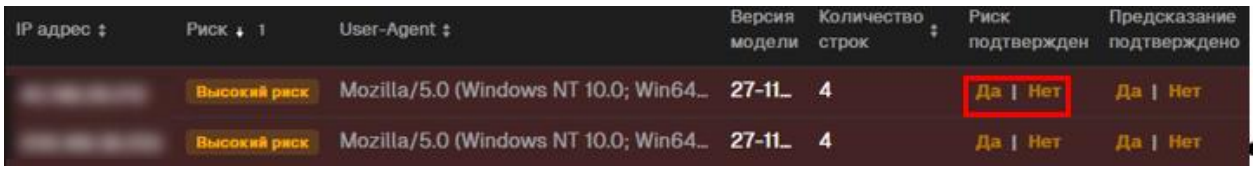

Рисунок 100 – Подтверждение риска

7) принадлежность подтвержденного пользователем риска/предсказания к атакующим или пользовательским сессиям может быть изменена из-за сделанного пользователем выбора. Изменения отобразятся в списке сессий (Рисунок 101).

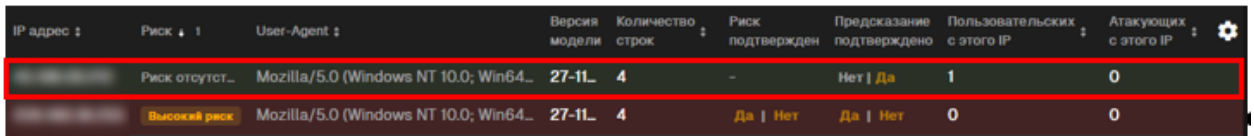

Рисунок 101 – Изменения в таблице сессий при изменении риска или предсказания

6.3 Подтверждение риска и предсказания из карточки сессии

Помимо подтверждения или опровержения риска сессии из списка аналогичные действия можно выполнить из карточки сессии. Поставить отметку о подтверждении риска можно с помощью следующих действий:

1) перейти к просмотру сессий;

2) выбрать сессию, для которой необходимо подтвердить риск и по нажатию на любой столбец строки, кроме столбца «IP-адрес» (в случае табличной визуализации страницы сессий) или на блок с сессией (в случае представления карточками), перейти на страницу сессии (Рисунок 102);

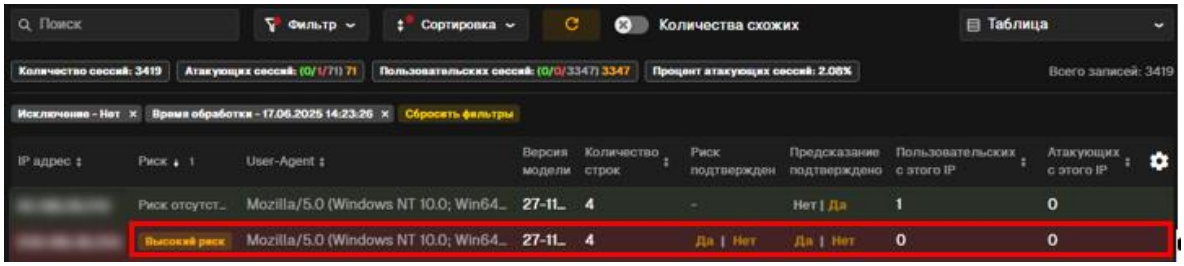

Рисунок 102 – Переход к просмотру карточки сессии

3) раскрыть блок «Общая информация» (Рисунок 103);

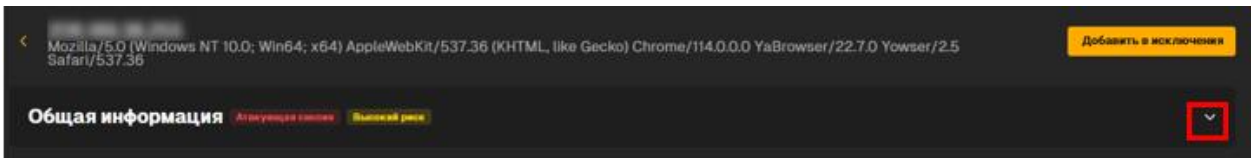

Рисунок 103 – Отображение общей информации о сессии

4) выбрать в пункте «Предсказание подтверждено» вариант «Да», если предсказание верно определено моделью или «Нет», если предсказание неверно (Рисунок 104);

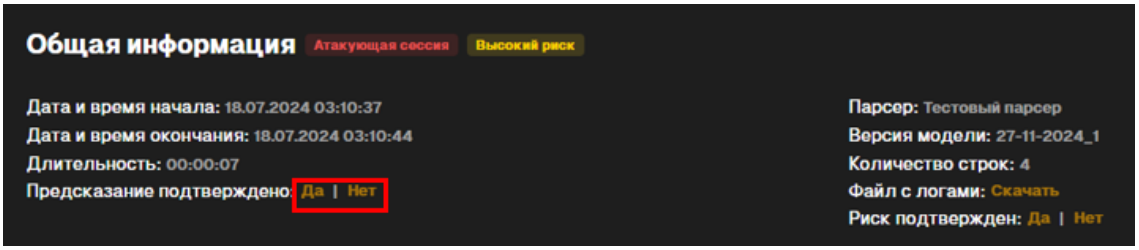

Рисунок 104 – Подтверждение предсказания

5) для атакующих сессий можно также подтвердить риск – нужно выбрать в пункте «Риск подтвержден» вариант «Да», если риск верно определен моделью или «Нет», если риск определен неверно (Рисунок 105);

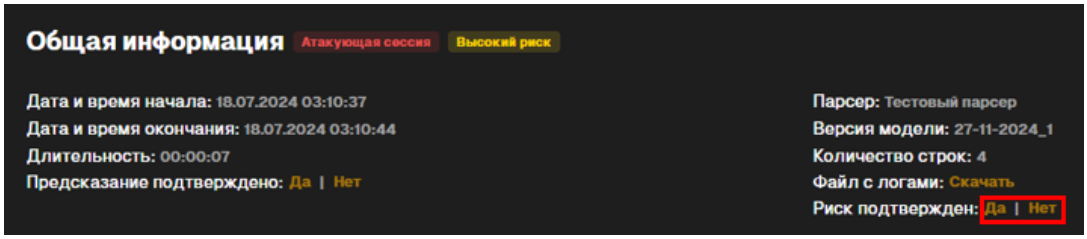

Рисунок 105 – Подтверждение риска

6) принадлежность подтвержденного пользователем риска/предсказания к атакующим или пользовательским сессиям может быть изменена из-за сделанного пользователем выбора. Изменения отобразятся в списке сессий (Рисунок 106);

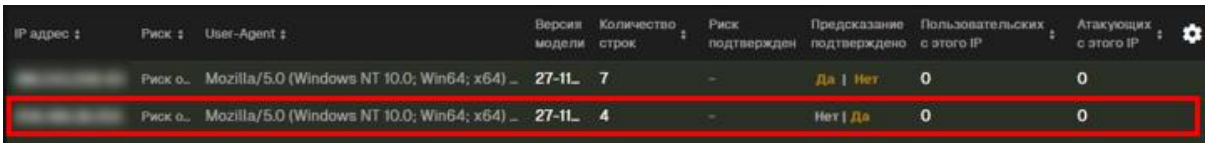

Рисунок 106 – Изменения в таблице сессий

6.4 Скачивание файла с логом сессии

При необходимости файл с логом сессии можно скачать из Системы для последующего изучения с помощью следующих действий:

1) перейти к просмотру сессии (Рисунок 107);

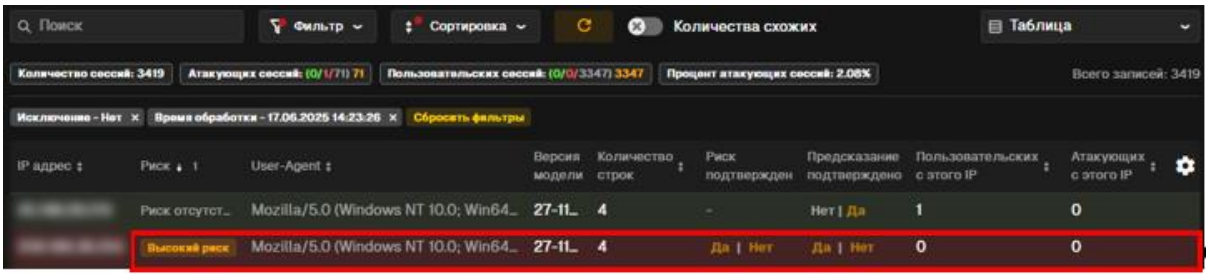

Рисунок 107 – Переход к карточке сессии

2) раскрыть блок «Общая информация» (Рисунок 108);

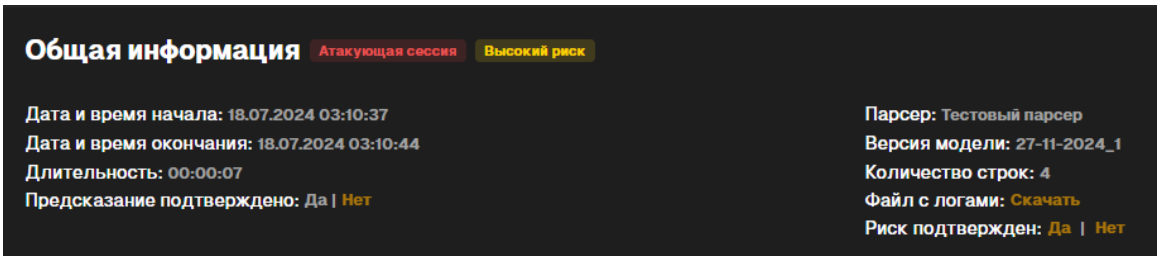

Рисунок 108 – Просмотр информации о сессии

3) в пункте «Файл с логами» нажать на кнопку «Скачать» (Рисунок 109);

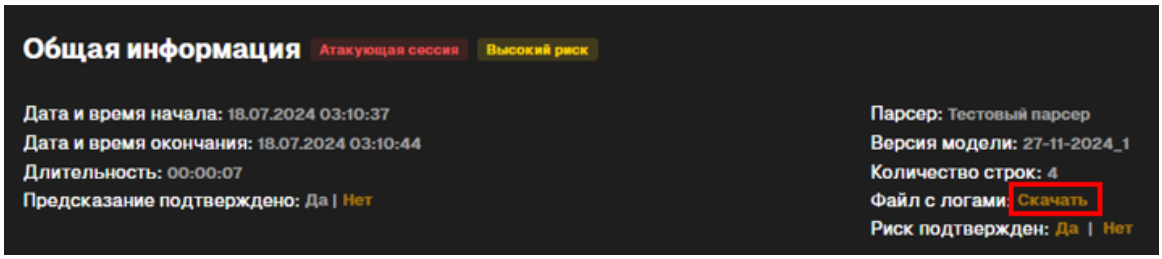

Рисунок 109 – Скачивание файла с логом сессии

4) будет запущено скачивание файла с логами в архиве .tar, содержащий файл в формате «tar.gz» (Рисунок 110);

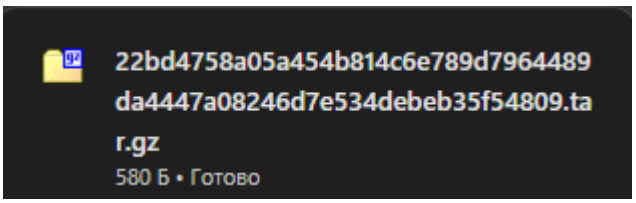

Рисунок 110 – Запуск загрузки файла с логом сессии

6.5 Изменение режима отображения лога

Для удобства ознакомления с логами сессии в Системе можно изменить формат их отображения с помощью следующих действий:

1) перейти к просмотру сессии;

2) в блоке «Логи сессии» в правом верхнем углу в выпадающем списке выбрать необходимый формат отображения, по умолчанию выбран формат «Строки» (Рисунок 111);

Рисунок 111 – Изменение режима отображения лога

3) в формате «Подсвеченные строки» Система отобразит логи сессии в строчном формате с цветовой дифференциацией. В данном представлении при нажатии одна из ячеек скопируется в буфер обмена. По двойному нажатию в буфер обмена будет скопирована вся строка (Рисунок 112);

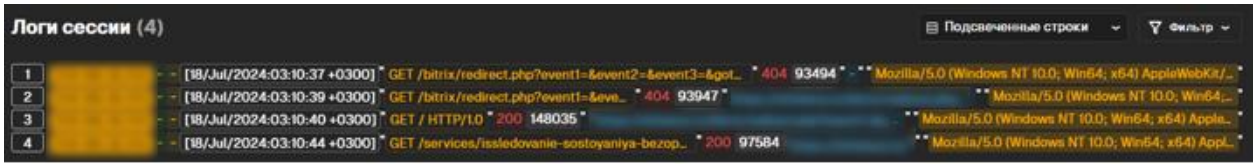

Рисунок 112 – Отображение в формате «Подсвеченные строки»

4) в формате «Таблица» Система отобразит логи сессии с разбиением и возможностью сортировки по столбцам (Рисунок 113).

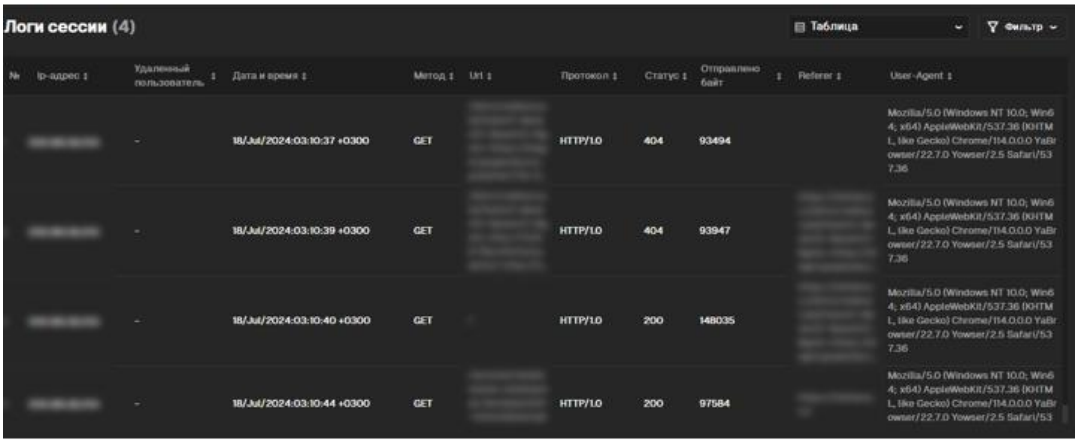

Рисунок 113 – Отображение в формате «Таблица»

6.6 Фильтрация при отображении лога

Логи сессии можно отфильтровать для удобства поиска необходимой информации с помощью следующих действий:

1) перейти к просмотру сессии;

2) в блоке «Логи сессии» в правом верхнем углу нажать на кнопку «Фильтр» (Рисунок 114);

Рисунок 114 – Фильтрация при отображении лога

3) в открывшемся окне ввести необходимые значения для фильтрации по полям «Метод», «URL», «Статус» и «Отправлено байт» (Рисунок 115);

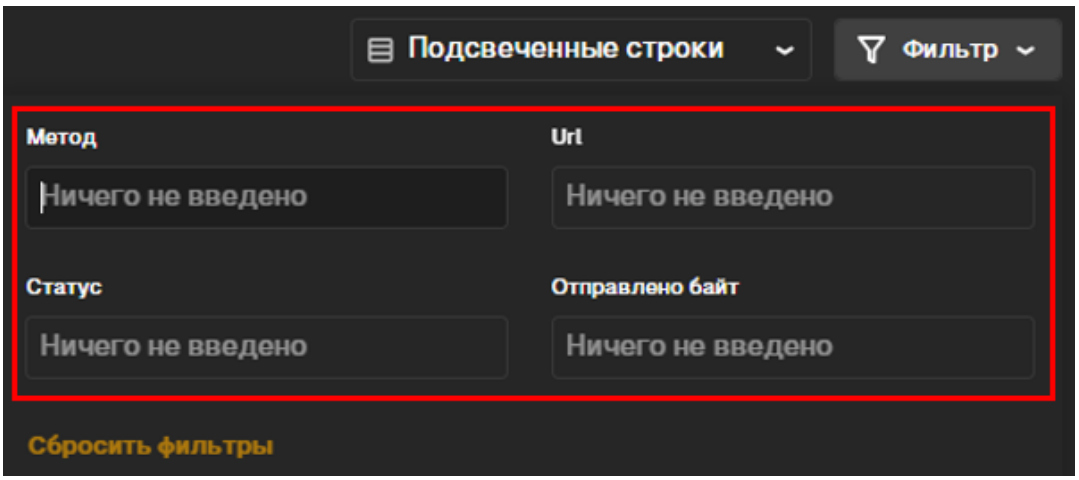

Рисунок 115 – Настройка фильтра

4) после ввода фильтры применятся автоматически (Рисунок 116);

Рисунок 116 – Пример работы фильтра

5) при необходимости все введенные фильтры можно удалить с помощью кнопки «Сбросить фильтры» (Рисунок 117).

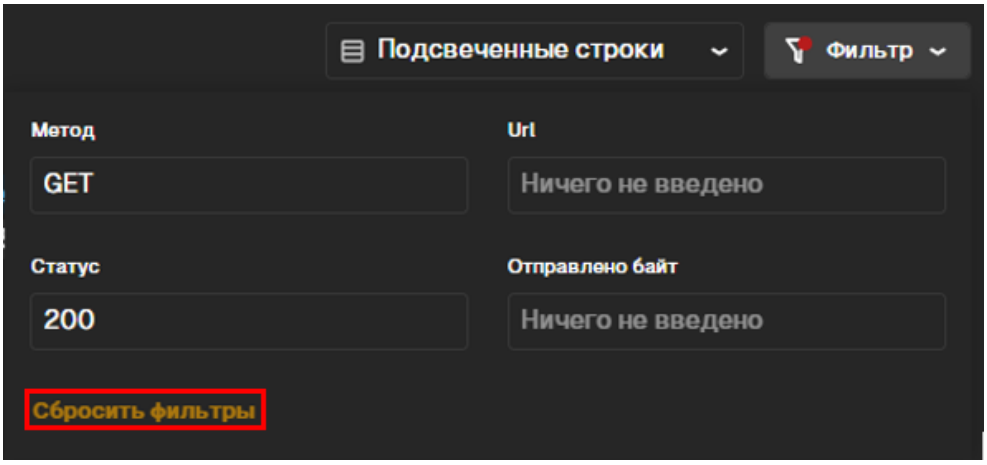

Рисунок 117 – Сброс фильтра

6.7 Изменение набора колонок в сессиях журнала

Пользователь может настроить перечень отображаемых столбцов при изучении информации о сессиях с помощью следующих действий:

1) перейти к просмотру журнала;

2) перейти к просмотру сессии:

– для пакетного режима – переключиться на вкладку «Сессии»;

– для потокового режима – переключиться на вкладку «Текущие сессии»/«Завершенные сессии» (Рисунок 118);

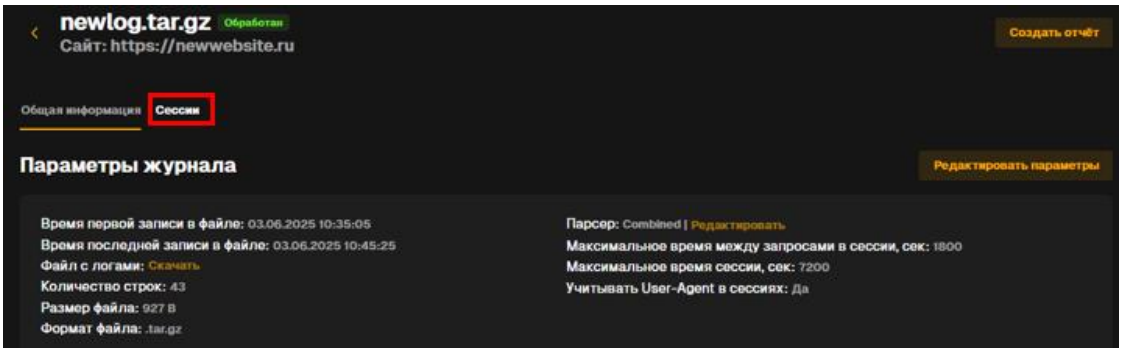

Рисунок 118 – Переход к сессиям журнала

3) в правой части шапки таблицы нажать на кнопку с изображением шестеренки (Рисунок 119);

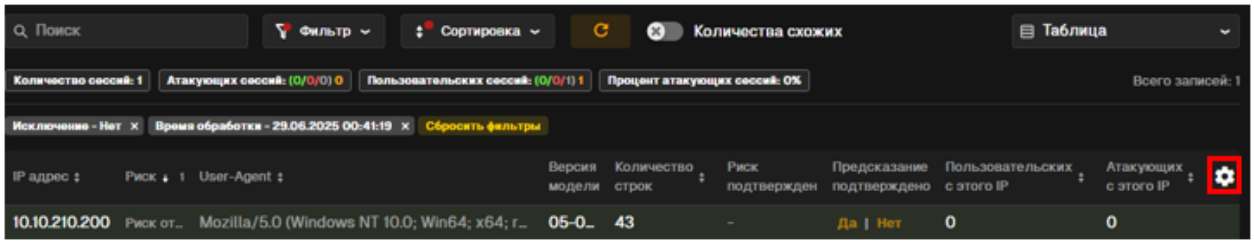

Рисунок 119 – Изменение набора колонок в сессиях журнала

4) в появившемся окне (Рисунок 120):

– выбрать чекбоксы для тех столбцов, которые необходимы в отображении;

– снять чекбоксы для тех столбцов, которые в отображении не нужны;

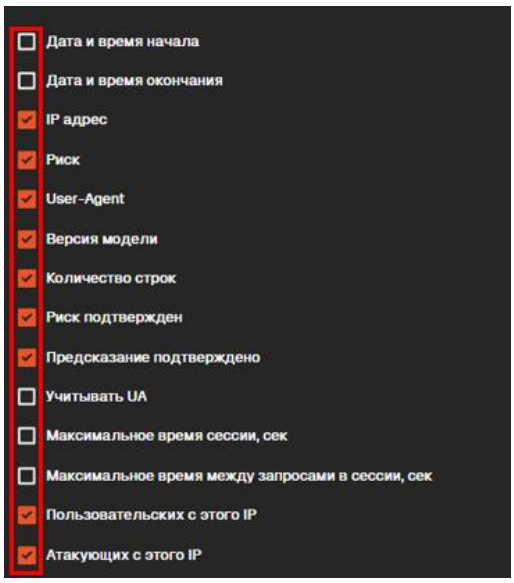

Рисунок 120 – Выбор возможных для отображения в таблице полей

5) изменения в таблице будут применены автоматически.

6.8 Ручное обновление списка текущих и завершенных сессий

Для потоковой обработки список текущих и завершенных сессий обновляется по мере появления новых записей в логах. При необходимости можно вручную обновить список текущих и завершенных сессий с помощью следующих действий:

1) перейти к просмотру журнала;

2) перейти к просмотру сессии:

– для пакетного режима – переключиться на вкладку «Сессии»;

– для потокового режима – переключиться на вкладку «Текущие сессии»/«Завершенные сессии»;

3) в меню над таблицей нажать на кнопку «Обновить» (Рисунок 121);

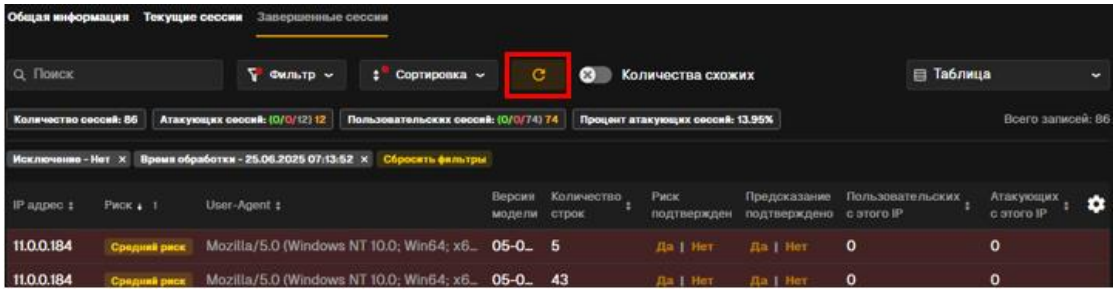

Рисунок 121 – Ручное обновление списка текущих и завершенных сессий

4) попытка обновления не означает, что в логах появились новые строки и информация в таблице может не обновиться. Тем не менее после нажатия кнопки попытка обновления информации будет выполнена.

6.9 Изменение частоты обновления при потоковой обработке

Для потоковой обработки можно изменить параметр частоты обновления – время, через которое «AML» обращается к логу журнала для получения новых добавленных строк. Изменить частоту обновления можно с помощью следующих действий:

1) перейти к просмотру журнала;

2) перейти к просмотру сессии:

– для пакетного режима – переключиться на вкладку «Сессии»;

– для потокового режима – переключиться на вкладку «Текущие сессии»/«Завершенные сессии»;

3) в меню над таблицей нажать на кнопку с изображением шестеренки (Рисунок 122);

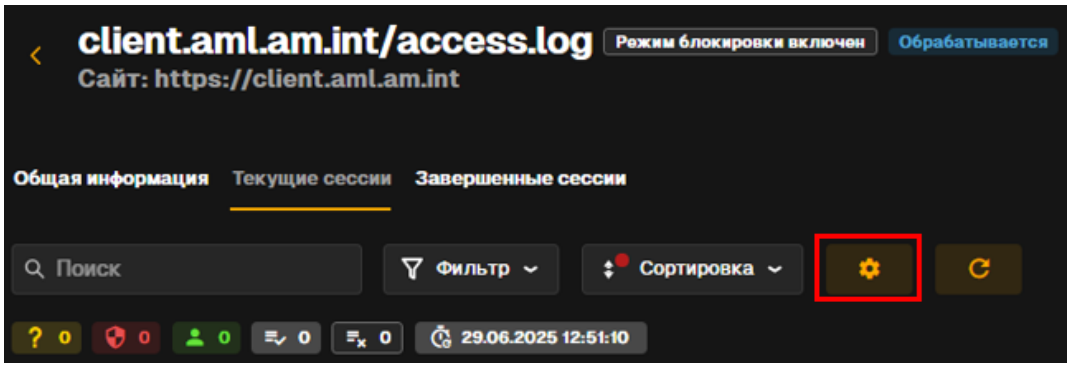

Рисунок 122 – Изменение частоты обновления при потоковой обработке

4) в открывшемся модальном окне «Частота обновления» из выпадающего списка выбрать необходимое значение частоты (Рисунок 123);

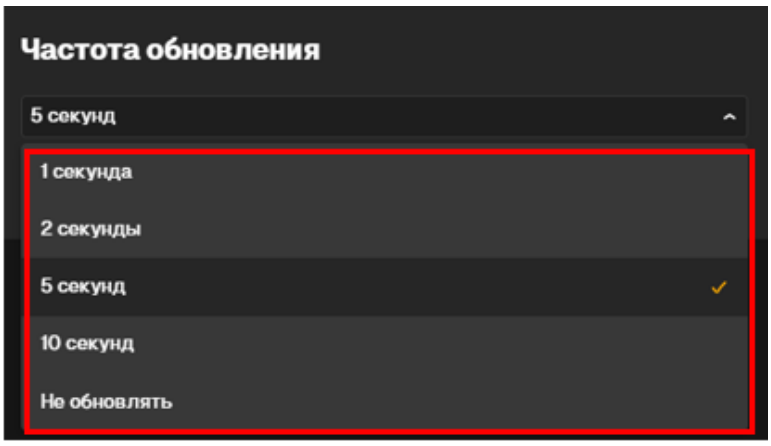

Рисунок 123 – Выбор необходимой частоты обновления

5) после выбора значения нажать на кнопку «Применить» (Рисунок 124);

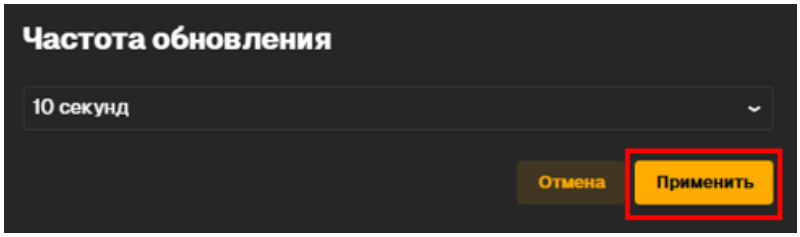

Рисунок 124 – Применение настроек частоты обновления

6) изменения сохранятся, а запросы к журналу лога будут выполняться с указанной при изменении частотой.

6.10 Просмотр статистики сессии

При работе с сессиями пользователь имеет возможность ознакомиться не только с таблицей/блоками, содержащими подробные данные, но и с краткой статистической информацией по всем зафиксированным сессиям. Просмотреть статистику сессии можно с помощью следующих действий:

1) перейти к просмотру журнала;

2) перейти к просмотру сессии (Рисунок 125):

– для пакетного режима – переключиться на вкладку «Сессии»;

– для потокового режима – переключиться на вкладку «Текущие сессии»/«Завершенные сессии»;

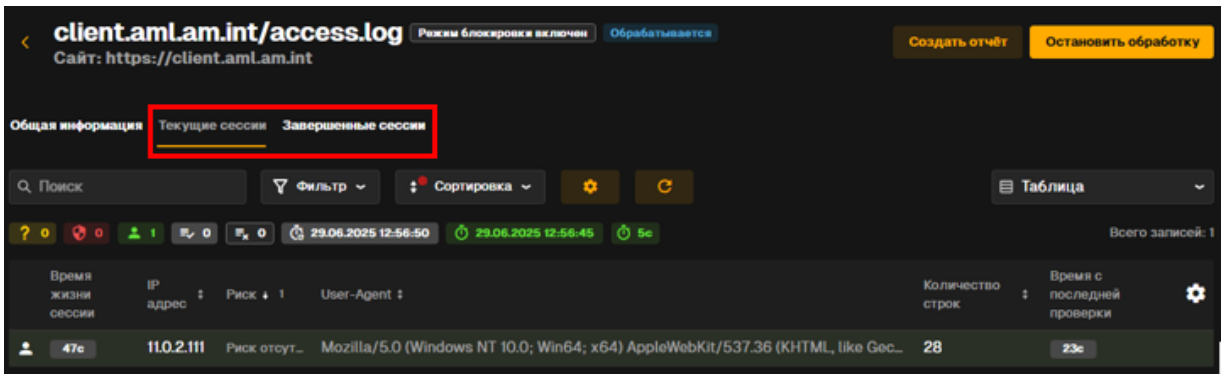

Рисунок 125 – Переход к сессиям журнала

3) над шапкой таблицы будут отображены информационные элементы интерфейса (Рисунок 126):

– количество непредсказанных сессий (желтый блок с иконкой «Знак вопроса»);

– количество атакующих сессий (красный блок с иконкой «Щит»);

– количество пользовательских сессий (зеленый блок с иконкой «Пользователь»);

– количество сессий с ресурсами из списка исключений (серый блок с иконкой «Список с галочкой»);

– количество заблокированных сессий – только в потоковом режиме (серый блок с иконкой «Список с крестиком»);

– время последней синхронизации с журналом логов – только в потоковом режиме;

– время последней записи в журнале.

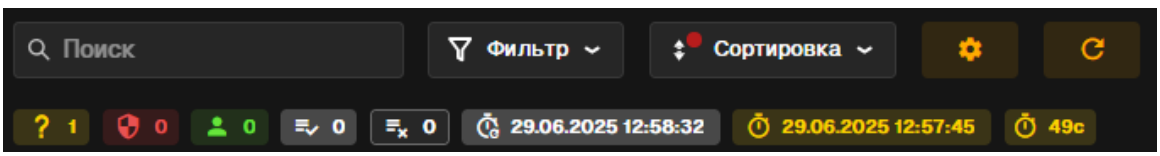

Рисунок 126 – Просмотр статистики сессии

6.11 Сортировка сессий

При необходимости для удобства работы сессий значения в таблице можно отсортировать по полям:

– «Дата и время начала/окончания»;

– «IP-адрес»;

– «Риск»;

– «User-Agent»;

– «Количество строк».

Для сортировки необходимо выполнить следующие действия:

1) перейти к просмотру журнала;

2) перейти к просмотру сессии:

– для пакетного режима – переключиться на вкладку «Сессии»;

– для потокового режима – переключиться на вкладку «Текущие сессии»/«Завершенные сессии»;

3) далее нажать на элемент управления «Сортировка» (Рисунок 127);

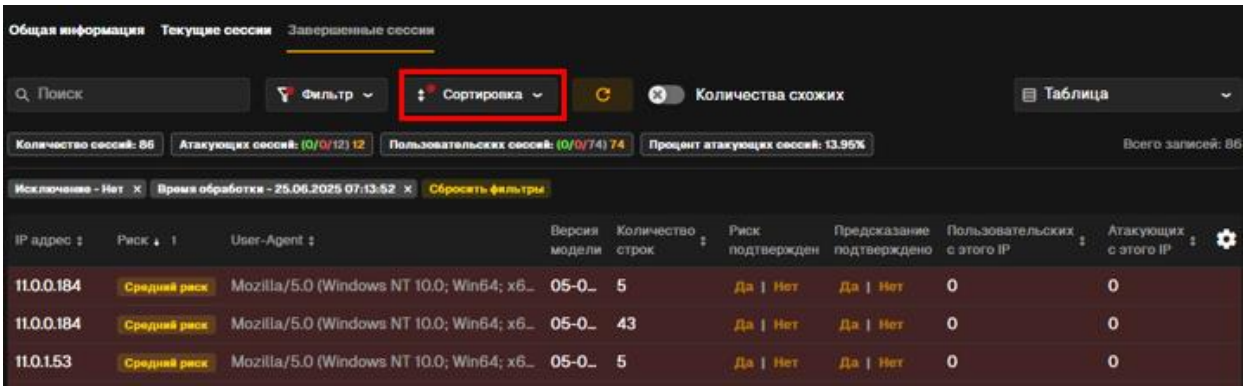

Рисунок 127 – Сортировка сессий

4) в появившемся окне нажать на название поля, по которому необходимо выполнить сортировку (Рисунок 128);

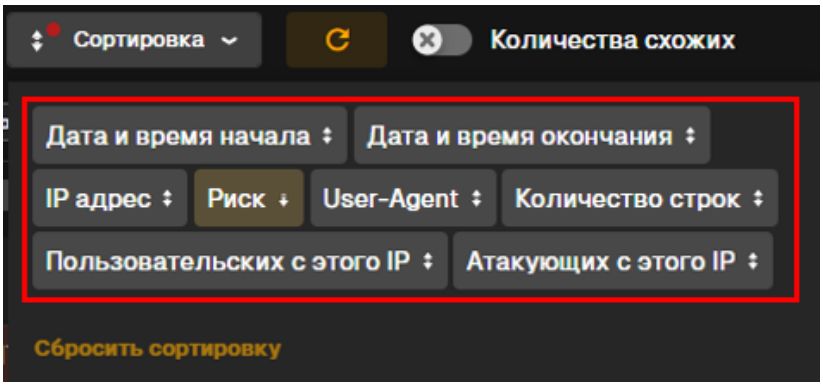

Рисунок 128 – Выбор полей для осуществления сортировки

5) по первому нажатию выполнится сортировка по возрастанию, по второму нажатию – по убыванию, третье нажатие сбросит сортировку по столбцу (Рисунок 129);

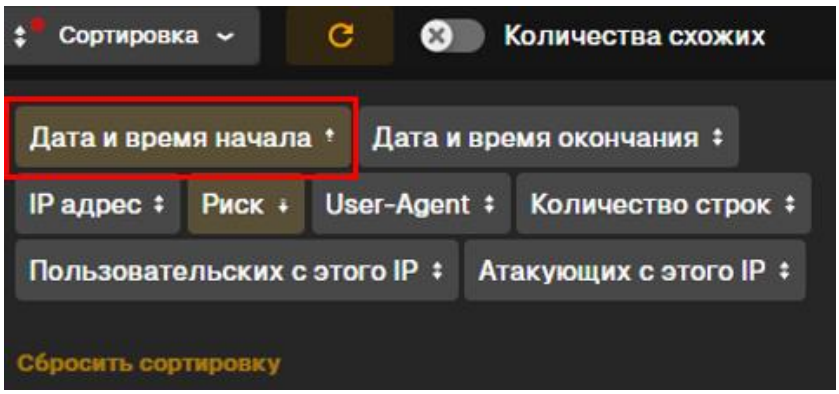

Рисунок 129 – Настройка порядка сортировки

6) сортировать можно одновременно по нескольким столбцам. Приоритет сортировки определяется последовательностью выбора сортируемых столбцов и указывается возле иконки сортировки в шапке таблицы (Рисунок 130);

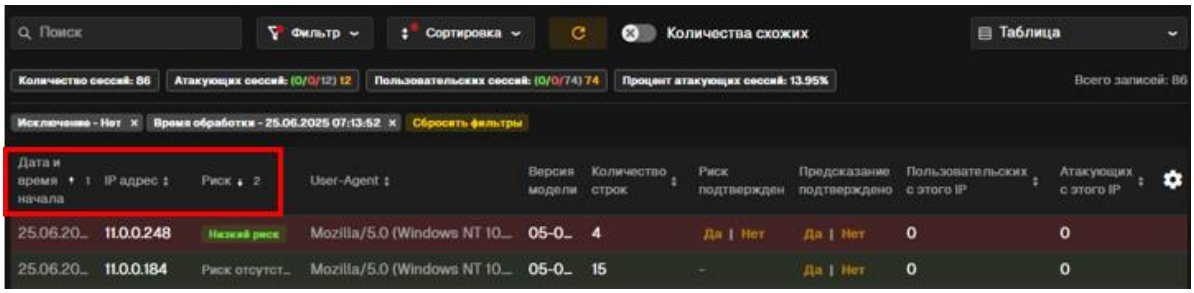

Рисунок 130 – Сортировка сессий в шапке таблицы

7) в табличном представлении также можно нажать на столбец для сортировки значений по столбцу. Сортировка будет работать по логике, описанной в предыдущих пунктах.

6.12 Фильтрация сессий

Для удобства работы с таблицей сессий значения в таблице можно отфильтровать с помощью следующих действий:

1) перейти к просмотру журнала;

2) перейти к просмотру сессии:

– для пакетного режима – переключиться на вкладку «Сессии»;

– для потокового режима – переключиться на вкладку «Текущие сессии»/«Завершенные сессии»;

3) далее нажать на элемент управления «Фильтр» (Рисунок 131);

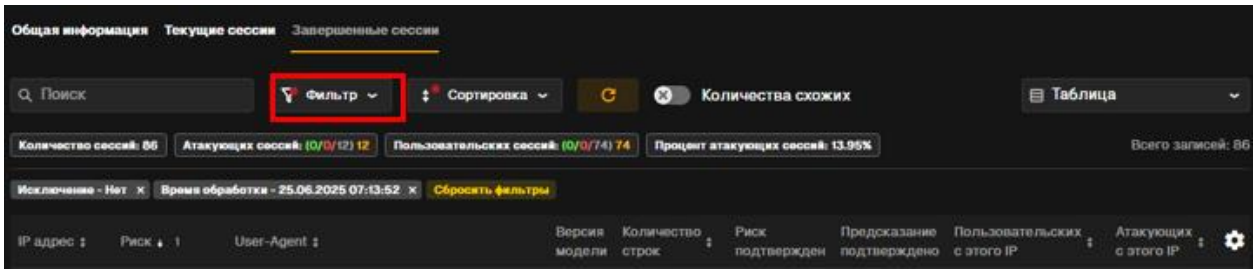

Рисунок 131 – Фильтрация сессий

4) в выпадающих списках по наименованию полей выбрать значения, по которым необходимо выполнить фильтрацию (Рисунок 132);

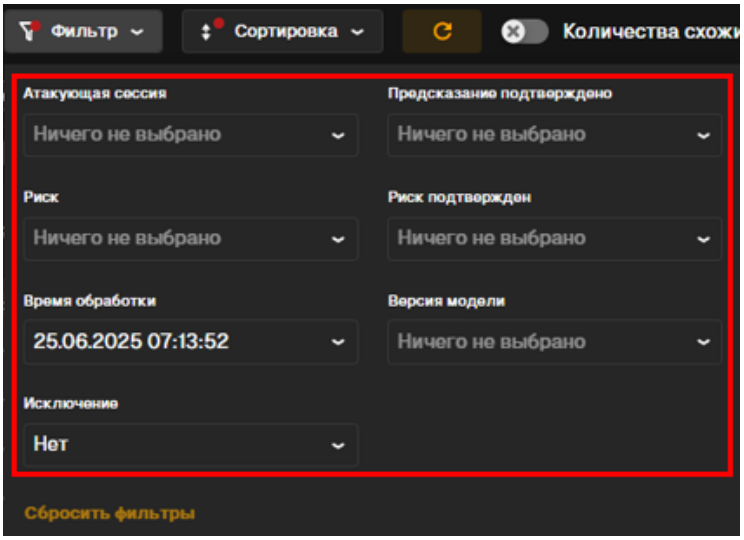

Рисунок 132 – Настройка фильтра

5) фильтры применяются автоматически (Рисунок 133);

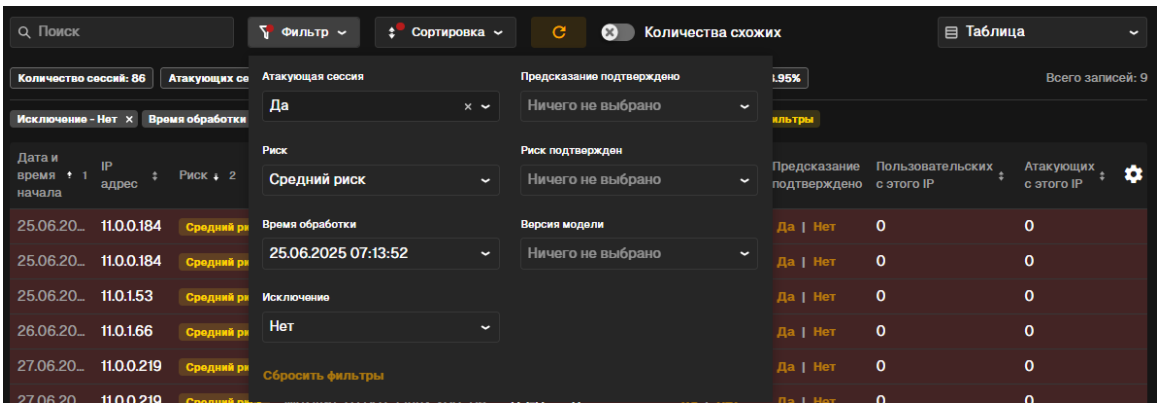

Рисунок 133 – Результат работы фильтра

6) при необходимости можно сбросить все значения для установленных фильтров с помощью кнопки «Сбросить фильтры» (Рисунок 134).

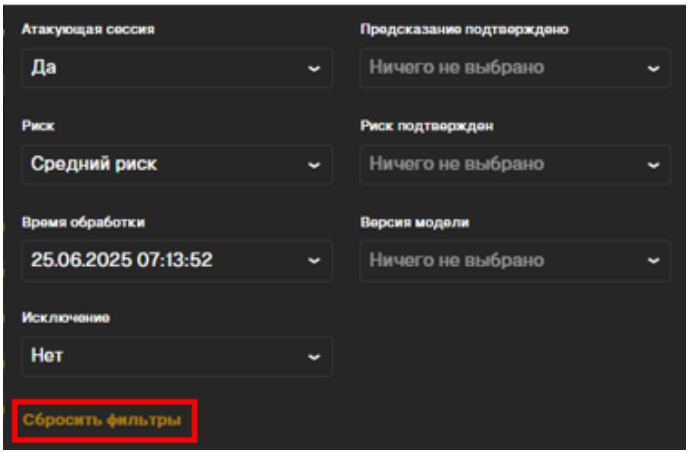

Рисунок 134 – Сброс фильтра

6.13 Поиск по списку сессий

Для ускорения работы со списком сессий и удобного процесса работы с информацией можно использовать поиск по списку сессий с помощью следующих действий:

1) перейти к просмотру журнала;

2) перейти к просмотру сессии:

– для пакетного режима – переключиться на вкладку «Сессии»;

– для потокового режима – переключиться на вкладку «Текущие сессии»/«Завершенные сессии»;

3) в левом верхнем углу над таблицей ввести значение в поле поиска, который выполняется по полям «IP-адрес» и «User-Agent» (Рисунок 135);

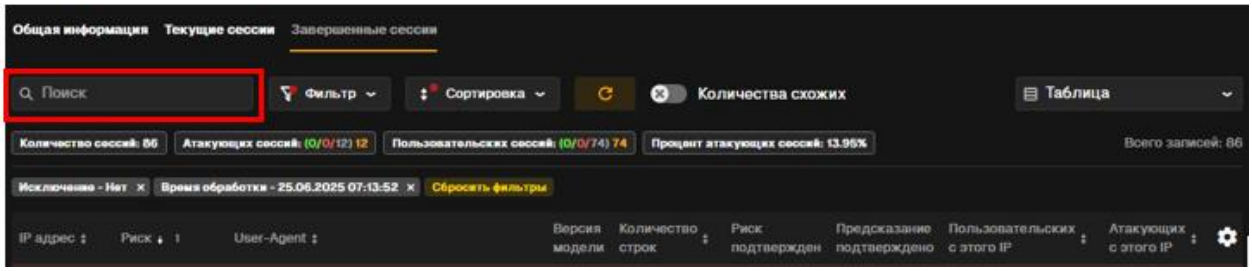

Рисунок 135 – Поиск по списку сессий

4) в таблице будут отображены строки, которые удовлетворяют введенному в поле поиска значению, поиск выполняется на вхождение (Рисунок 136).

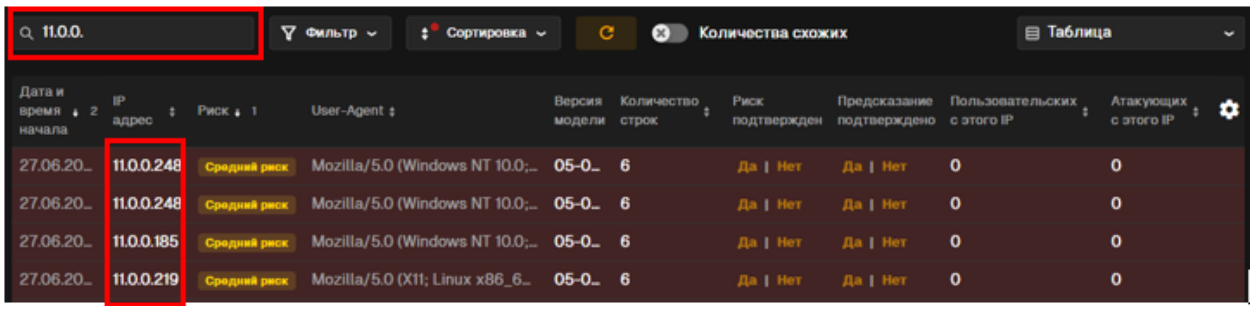

Рисунок 136 – Результат работы поиска по списку сессий

7 Работа с исключениями

В разделе «Исключения» могут быть настроены параметры сессий, которые считаются «доверенными» и не будут восприниматься моделью как атакующие. Пользователь с помощью данного раздела может управлять перечнями исключений в доступных сайтах.

7.1 Просмотр списка исключений

В разделе «Исключения» пользователь может ознакомиться со списком исключений, добавленных на доступные ресурсы, с помощью следующих действий:

1) перейти в раздел «Список исключений» (Рисунок 137);

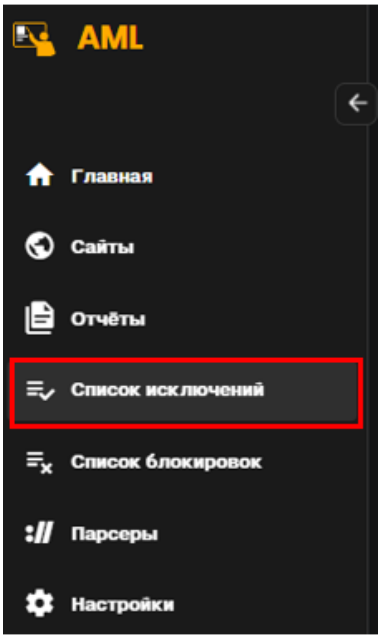

Рисунок 137 – Переход к разделу «Список исключений»

2) далее Система отобразит в данном разделе информацию, по имеющимся на данный момент исключениям, к относящимся сайтам, их типу, а также текущий статус активности исключения (Рисунок 138);

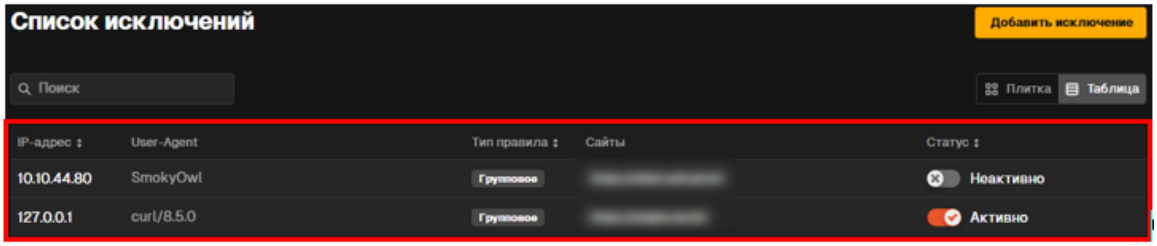

Рисунок 138 – Просмотр списка исключений

3) визуализация раздела может быть изменена с табличного представления на формат «Плитка». Для изменения нужно нажать на соответствующий вид визуализации в правом верхнем углу (Рисунок 139).

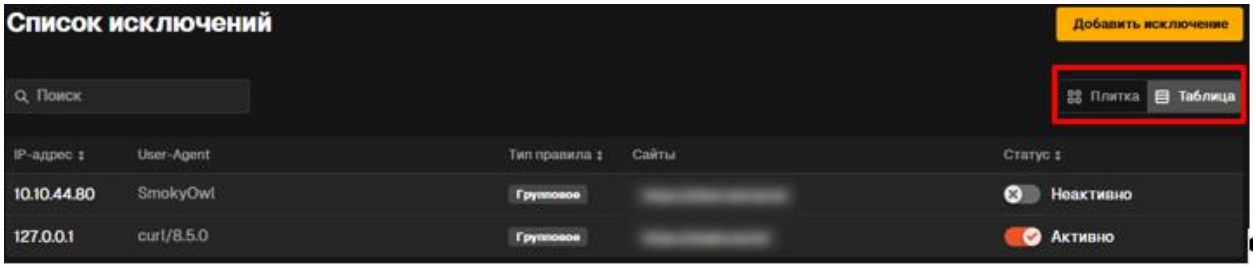

Рисунок 139 – Настройка отображения списка исключений

7.2 Поиск по списку исключений

Для удобства и ускорения взаимодействия со списком исключений можно осуществлять поиск с помощью следующих действий:

1) перейти к разделу «Список исключений»;

2) в поле поиска в верхнем левом углу ввести искомое значение (Рисунок 140);

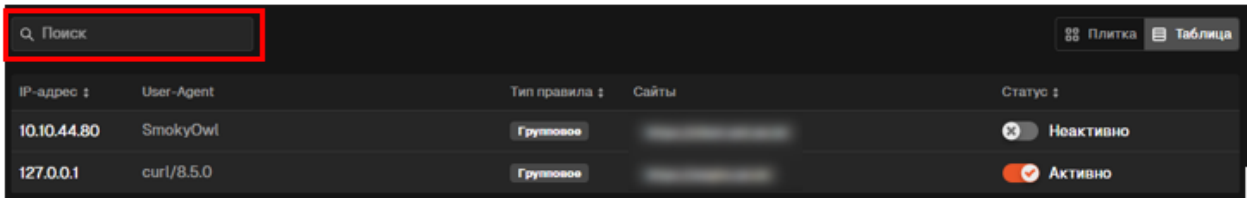

Рисунок 140 – Поиск по списку исключений

3) для введенного значения выполнится поиск на вхождение среди списка исключений, поиск выполняется по полям «IP-адрес» и «User-Agent» (Рисунок 141).

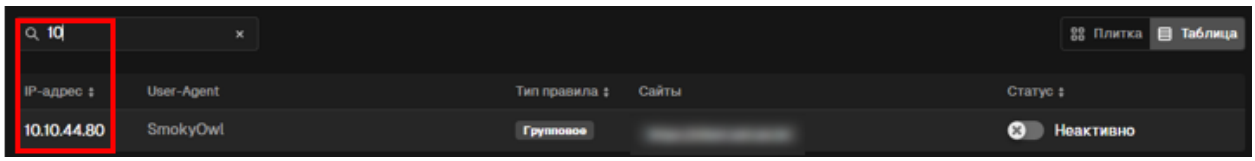

Рисунок 141 – Результат работы поиска по списку исключений

7.3 Создание нового исключения

В разделе «Исключения» пользователь может указать «IP-адрес» и «User-Agent» как доверенные для одного или нескольких ресурсов, создав исключение. Создать исключение можно с помощью следующих действий:

1) перейти в раздел «Список исключений»;

2) нажать на кнопку «Добавить исключение» в правом верхнем углу страницы (Рисунок 142);

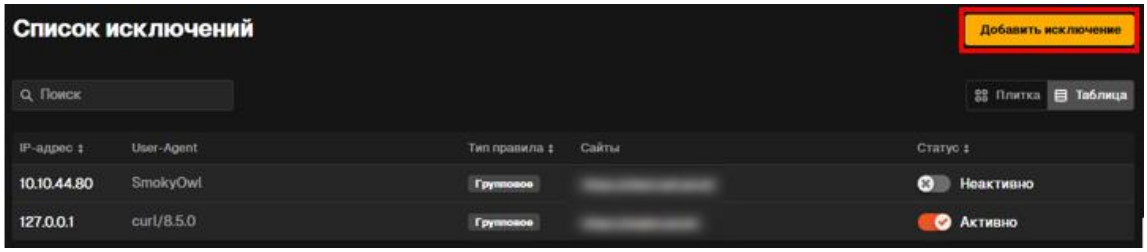

Рисунок 142 – Создание нового исключения

3) в открывшемся окне в блоке «Добавление параметров» указать параметры исключения «IP», «User-Agent», выбрав из выпадающего списка, ввести значения для них (Рисунок 143);

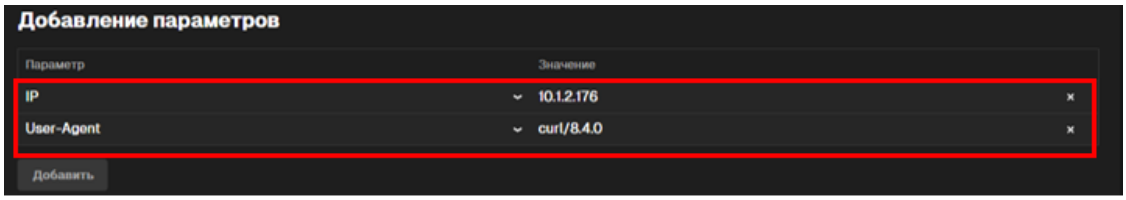

Рисунок 143 – Добавление параметров исключения

4) в блоке «Настройки» следует указать необходимость применения исключения для всех пользователей, отметив чекбокс. Если чекбокс проставлен, то исключение будет добавлено в списки исключений всех пользователей, кому доступен ресурс. Если чекбокс не проставлен, то

исключение добавится индивидуально для создающего пользователя (Рисунок 144);

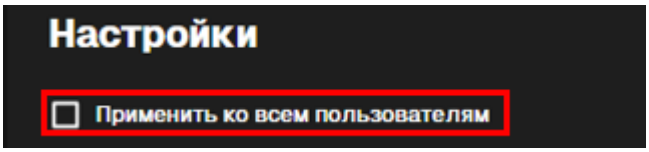

Рисунок 144 – Настройка видимости исключения

5) после нажатия кнопки «Далее» осуществится переход к шагу 2 создания исключения «Выбор сайтов» (Рисунок 145);

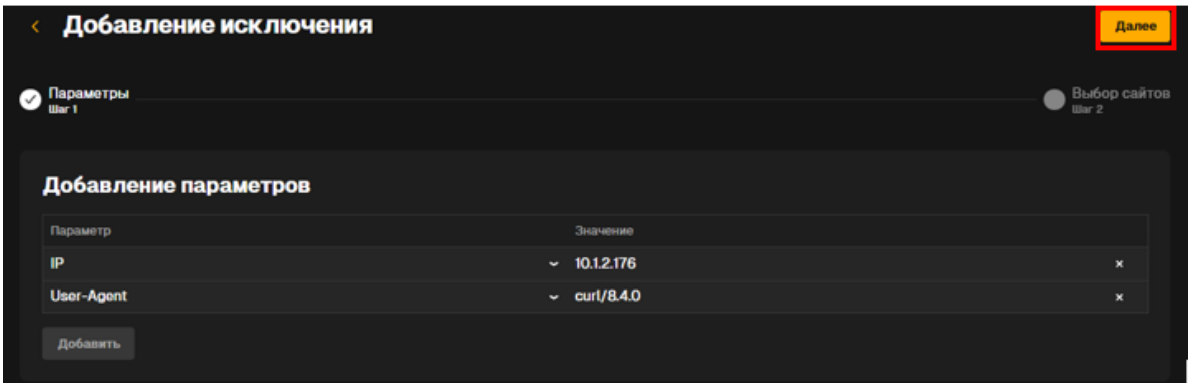

Рисунок 145 – Переход к выбору сайтов

6) в таблице с перечнем сайтов выбрать те, для которых должно быть активно создаваемое исключение, отметив чекбоксы. Если отметить чекбокс в шапке таблицы, то исключение будет добавлено для всех доступных пользователю сайтов (Рисунок 146);

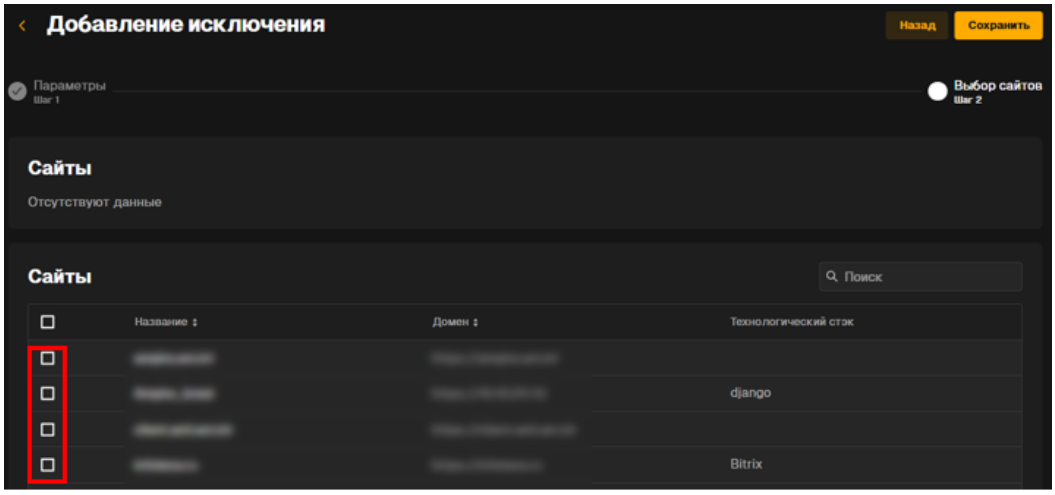

Рисунок 146 – Выбор сайтов для исключения

7) выбранные сайты отобразятся в верхнем блоке «Сайты» (Рисунок 147);

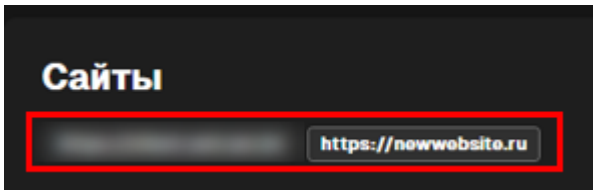

Рисунок 147 – Отображение выбранных сайтов

8) после выбора необходимых сайтов следует нажать на кнопку «Сохранить» (Рисунок 148);

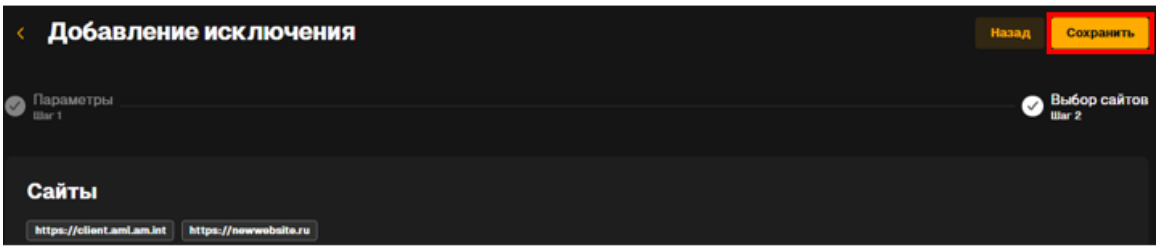

Рисунок 148 – Сохранение созданного исключения

9) новое исключение будет добавлено в список исключений (Рисунок 149).

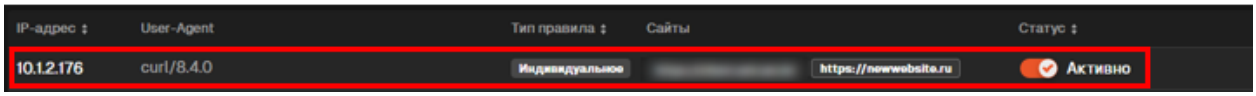

Рисунок 149 – Отображение созданного исключения

7.4 Создание нового исключения из лога сессии

Исключения можно создавать не только в разделе «Исключения», но и в логах сессии с помощью следующих действий:

1) перейти к просмотру сессии из текущих или завершенных сессий конкретного журнала;

2) в правом верхнем углу нажать на кнопку «Добавить в исключения» (Рисунок 150);

Рисунок 150 – Создание нового исключения из лога сессии

3) процесс создания исключения аналогичен описанному в предыдущем подразделе, нет необходимости вводить значения в поля «IP-адрес» и «User-Agent» вручную, указанные значения автоматически добавятся из выбранного лога сессии. На шаге 2 создания исключения также автоматически будет добавлен сайт, которому принадлежат логи сессии.

7.5 Отображение статистики исключений в результатах анализа

При просмотре информации по журналу в результатах анализа можно ознакомиться с отдельной сводкой статистики для полей «IP-адрес»/«User-Agent», которые являются доверенными, с помощью следующих действий:

1) перейти к просмотру журнала;

2) в блоке «Результаты анализа» в правом столбце будут отображены результаты анализа, касающиеся только списка исключений (Рисунок 151).

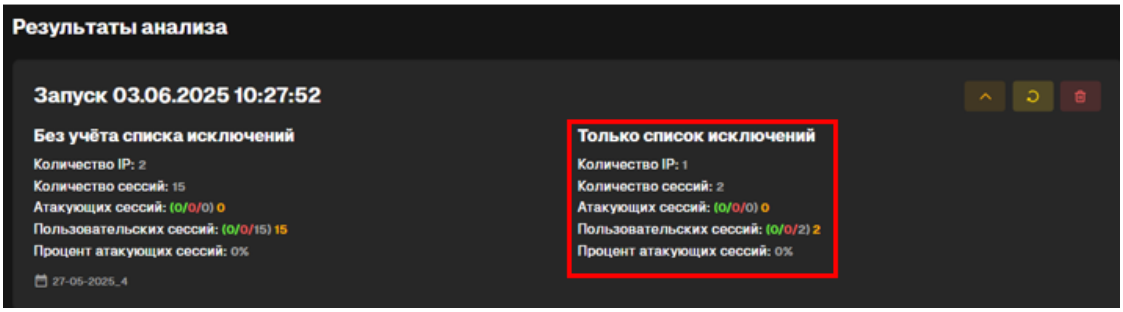

Рисунок 151 – Отображение статистики исключений в результатах анализа

7.6 Отключение исключения

При необходимости временно удалить поля «IP-адрес»/«User-Agent» из списка доверенных – это можно выполнить с помощью отключения исключения и следующих действий:

1) перейти в раздел «Список исключений»;

2) навести курсор мыши на строку (или блок в формате «Плитка») с исключением, которое необходимо отключить;

3) нажать на иконку меню выбора действий (Рисунок 152);

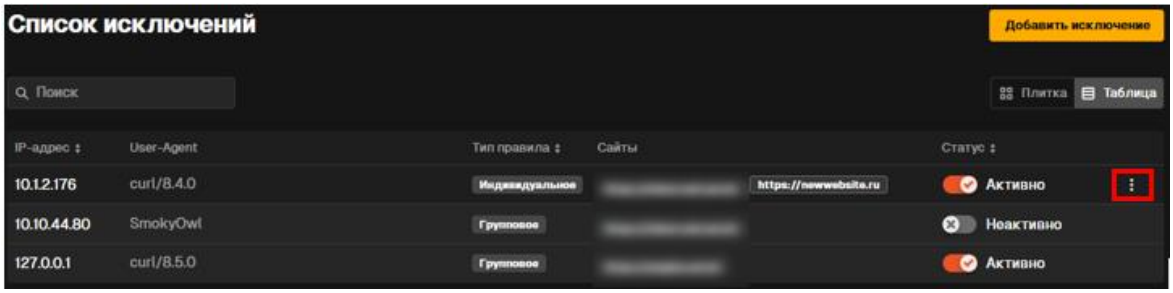

Рисунок 152 – Открытие меню действий над исключениями

4) в появившемся меню выбрать пункт «Отключить» (Рисунок 153);

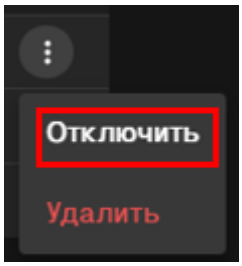

Рисунок 153 – Отключение исключения

5) положение переключателя в поле «Статус» изменится на «Неактивно» (Рисунок 154);

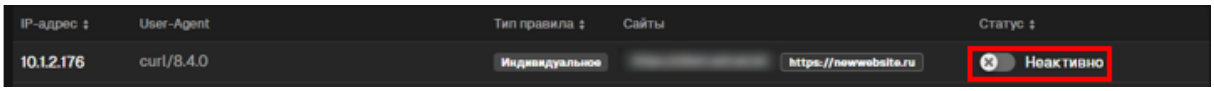

Рисунок 154 – Отображение неактивного исключения в таблице исключений

6) аналогично через меню действий можно включить исключение.

7.7 Удаление исключения

Если поля «IP-адрес»/«User-Agent» не являются доверенными, то можно их удалить из списка исключений с помощью следующих действий:

1) перейти в раздел «Список исключений»;

2) навести курсор мыши на строку (или блок в формате «Плитка») с исключением, которое необходимо удалить;

3) нажать на иконку меню выбора действий (Рисунок 155);

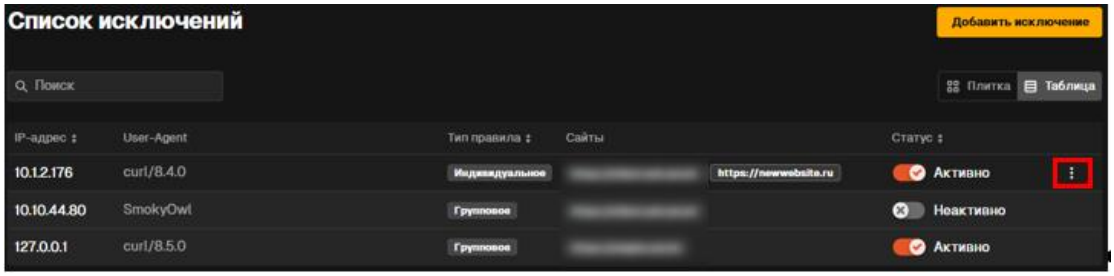

Рисунок 155 – Открытие меню действий над исключениями

4) в появившемся меню выбрать пункт «Удалить» (Рисунок 156);

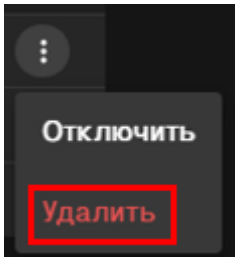

Рисунок 156 – Удаление исключения

5) в появившемся меню подтвердить удаление с помощью кнопки «Удалить» (Рисунок 157);

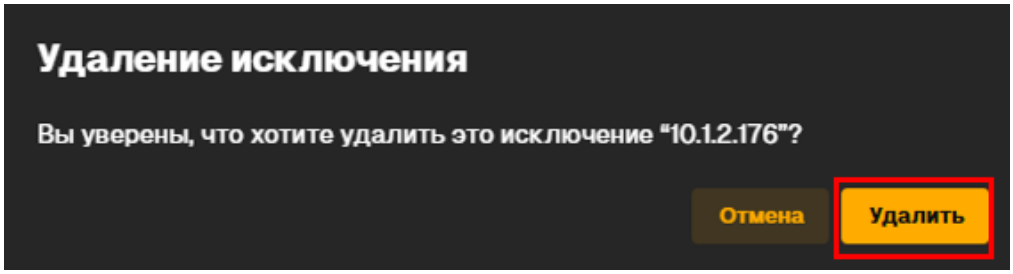

Рисунок 157 – Подтверждение удаления исключения

6) исключение будет удалено из списка.

8 Работа с блокировками

В разделе «Блокировки» пользователь может настроить автоматическую блокировку атакующих сессий на доступных ресурсах. Работа с блокировками доступна только в том случае, если в панели администратора заполнены данные о сервере и реализован доступ к серверу.

8.1 Просмотр ресурсов, для которых может быть настроена блокировка

При внесении администратором Системы информации о сервере ресурса в панели администратора в «AML» появляется возможность работать с блокировкой сессий для данного ресурса, при условии, что в данный момент логи указанного сервера обрабатываются в потоковом режиме.

Ознакомиться со списком ресурсов, для которых можно включить блокировку, можно с помощью следующих действий:

1) перейти в раздел «Список блокировок» (Рисунок 158);

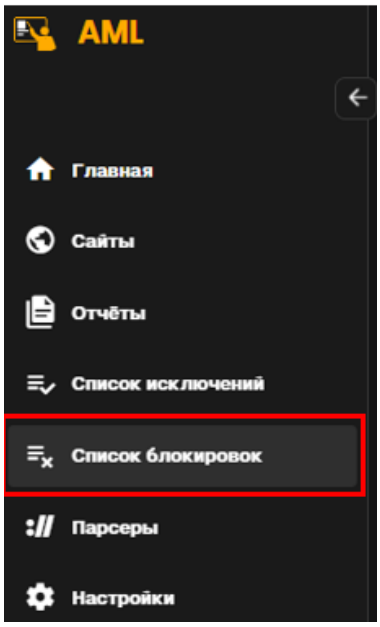

Рисунок 158 – Переход к разделу «Список блокировок»

2) в указанном разделе можно ознакомится с информацией о ресурсах, для которых может быть активна блокировка, а также с настройками блокировки: «Минимальный уровень риска», учет поля «User-Agent» при

блокировке, «Время блокировки». Также в данном разделе отображается статус активности блокировки на данный момент (Рисунок 159);

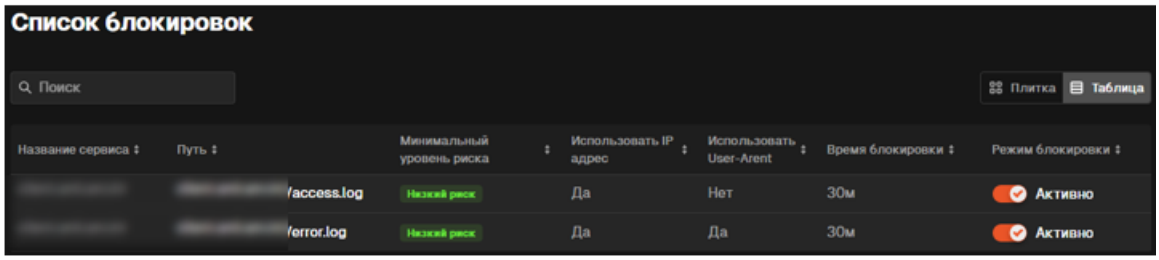

Рисунок 159 – Просмотр ресурсов, для которых может быть настроена блокировка

3) при необходимости можно изменить визуализацию раздела – в правом верхнем углу выбрать необходимый формат «Плитка»/«Таблица» (Рисунок 160).

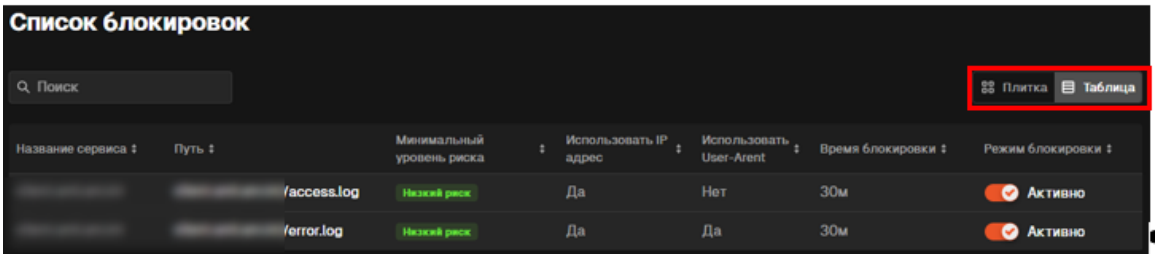

Рисунок 160 – Настройка отображения ресурсов, для которых может быть настроена блокировка

8.2 Включение и выключение блокировки для ресурса

При работе с ресурсами может возникнуть необходимость выключить или включить созданное правило по блокировке на определенном ресурсе, что можно выполнить с помощью следующих действий:

1) перейти в раздел «Список блокировок»;

2) в строке (или блоке в формате «Плитка») изменить положение переключателя в столбце «Режим блокировки» для ресурса, на котором нужно включить/выключить блокировку (Рисунок 161);

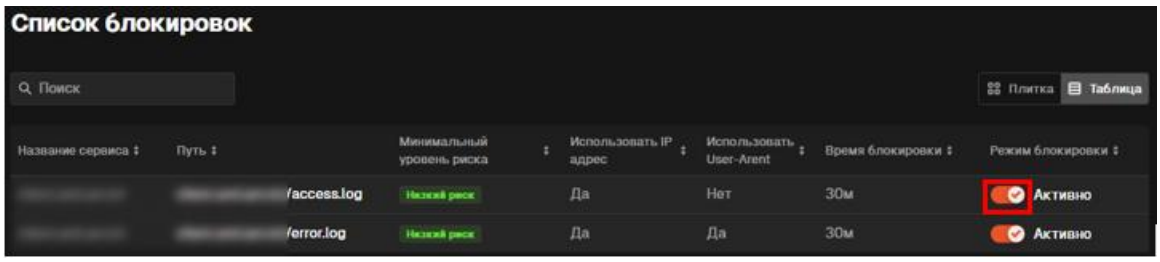

Рисунок 161 – Включение и выключение блокировки для ресурса

3) статус активности режима блокировки для ресурса изменится на противоположный (Рисунок 162).

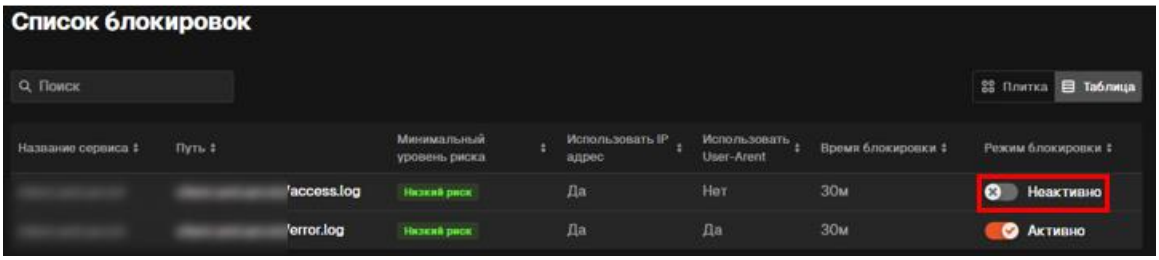

Рисунок 162 – Отображение выключенной блокировки для ресурса

8.3 Переход к списку заблокированных сессий ресурса

В разделе «Список блокировок» имеется возможность ознакомиться с сессиями, заблокированными для данного ресурса, с помощью следующих действий:

1) перейти к разделу «Список блокировок»;

2) нажать на строку/блок ресурса, для которого необходимо перейти к списку заблокированных сессий (Рисунок 163);

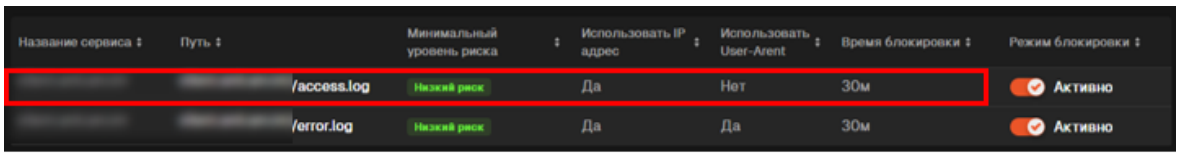

Рисунок 163 – Переход к списку заблокированных сессий ресурса

3) будет осуществлен переход к списку заблокированных сессий выбранного ресурса (Рисунок 164);

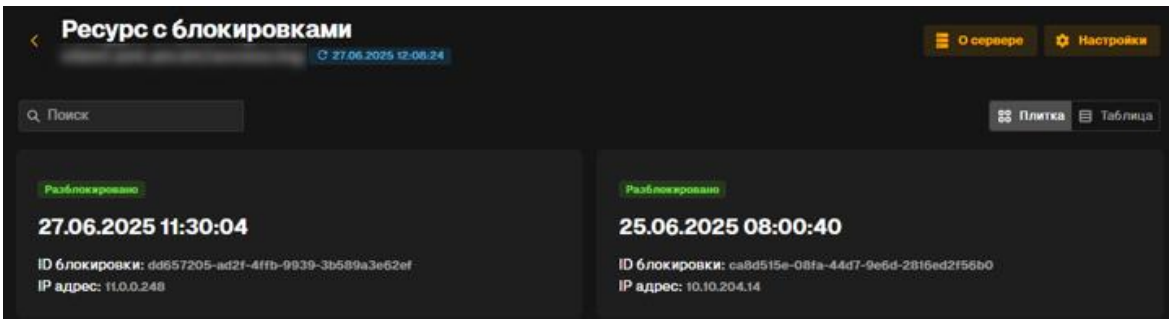

Рисунок 164 – Просмотр заблокированных сессий ресурса

4) при необходимости можно изменить отображение заблокированных сессий на странице – в правом верхнем углу выбрать необходимый формат «Плитка»/«Таблица» (Рисунок 165).

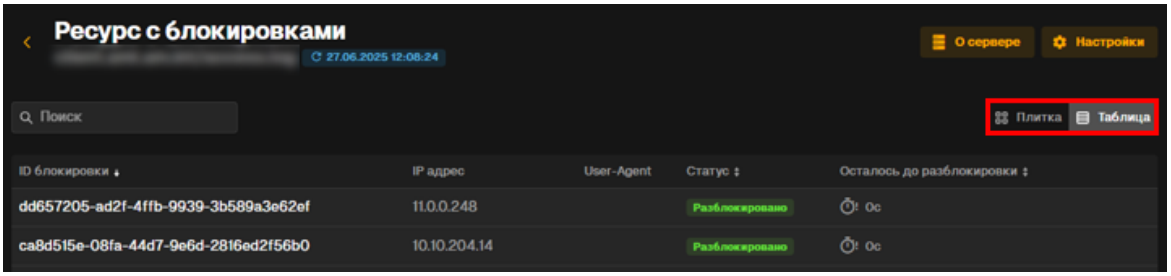

Рисунок 165 – Изменение отображения заблокированных сессий ресурса

8.4 Просмотр информации о сервере на странице ресурса

На странице заблокированных сессий можно подробнее ознакомиться с информацией о сервере с помощью следующих действий:

1) перейти к списку заблокированных сессий ресурса;

2) в правом верхнем углу нажать кнопку «О сервере» (Рисунок 166);

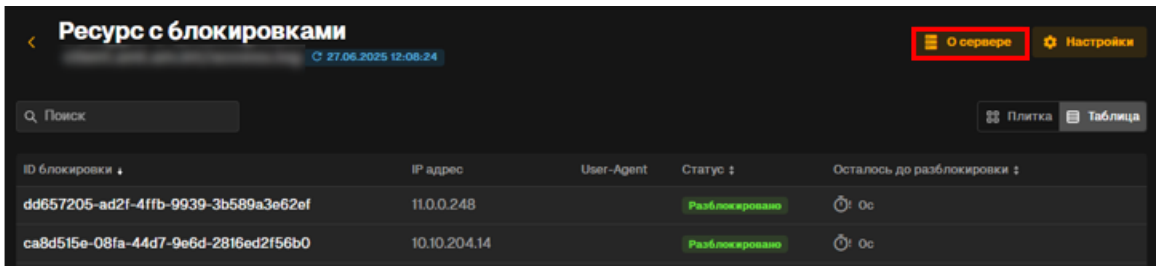

Рисунок 166 – Просмотр информации о сервере на странице ресурса

3) в модальном окне будет представлена информация о ресурсе, которая в Системе доступна только для ознакомления (Рисунок 167);

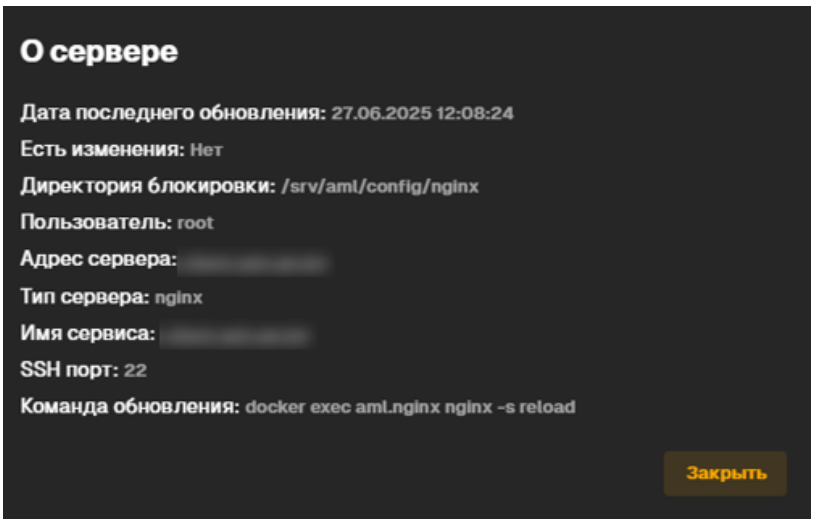

Рисунок 167 – Просмотр информации о сервере на странице ресурса

8.5 Просмотр и изменение настроек блокировки на странице ресурса

Если возникает необходимость внести изменения в ранее добавленные блокировки, то на странице заблокированных сессий можно ознакомиться и изменить настройки блокировки с помощью следующих действий:

1) перейти к списку заблокированных сессий ресурса;
2) в правом верхнем углу нажать кнопку «Настройки» (Рисунок 168);

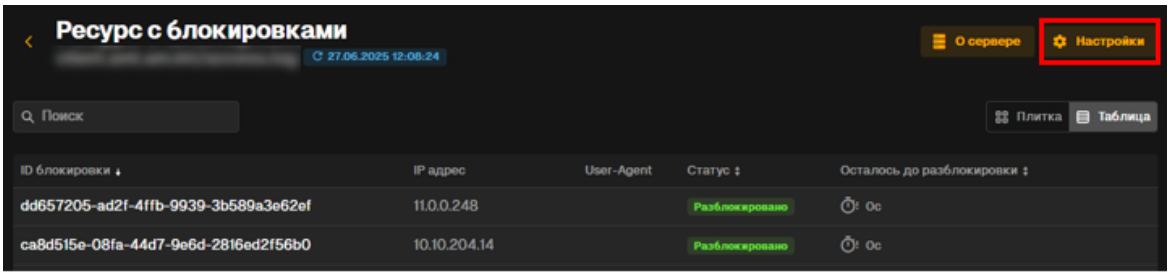

Рисунок 168 – Переход к настройке блокировок на ресурсе

3) при настройке блокировки можно изменить «Минимальный уровень риска», «Время блокировки», а также учет поля «User-Agent» при блокировке сессии (Рисунок 169);

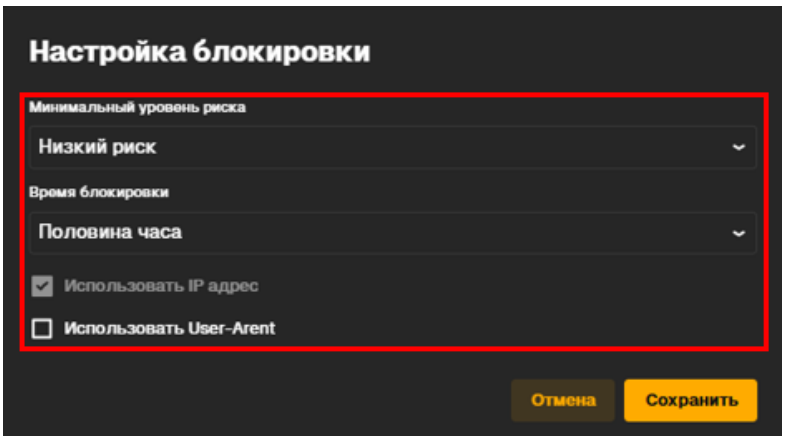

Рисунок 169 – Изменение настроек блокировок на ресурсе

4) после внесения изменений в настройки блокировки нажать кнопку «Сохранить» (Рисунок 170).

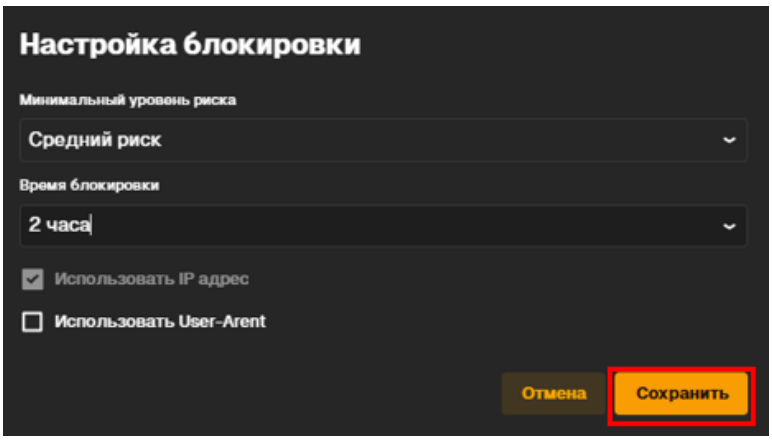

Рисунок 170 – Сохранение измененных настроек блокировок

8.6 Ручное включение и выключение блокировки сессии

На странице заблокированных сессий можно ознакомиться с тем, какие сессии на данный момент заблокированы. Если в списке заблокированных сессий отображена та, что не должна быть заблокирована по тем или иным причинам, то можно вручную снять блокировку ранее настроенного срока с помощью следующих действий:

1) перейти к списку заблокированных сессий;

2) навести курсор мыши на блокировку, которую необходимо включить/выключить, нажать на иконку меню выбора действий (Рисунок 171);

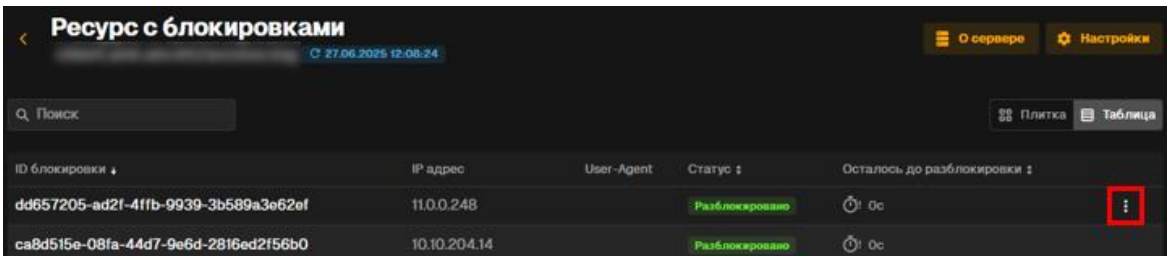

Рисунок 171 – Открытие меню выбора действий

3) в меню выбора действий выбрать пункт «Включить»/«Выключить» (Рисунок 172);

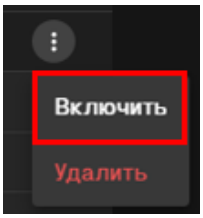

Рисунок 172 – Ручное включение и выключение блокировки сессии

4) статус для данной блокировки будет изменен. Если изменить статус на «Заблокировано», то запустится таймер времени до разблокировки в соответствии с настройками блокировки на данном ресурсе (Рисунок 173).

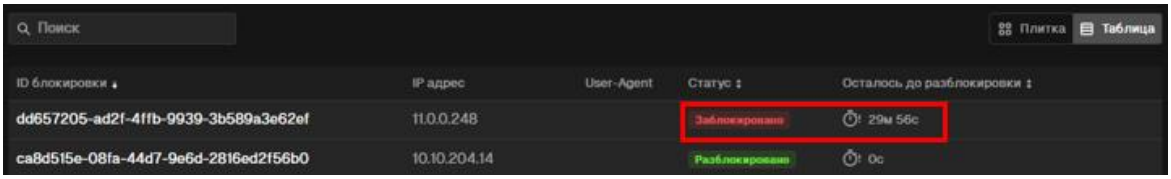

Рисунок 173 – Изменение состояния блокировки сессии

8.7 Поиск по заблокированным сессиям

Для ускорения работы с разделом по списку заблокированных сессий для ресурса можно осуществлять поиск с помощью следующих действий:

1) перейти к странице заблокированных ресурсов;

2) в поле поиска в верхнем левом углу ввести искомое значение (Рисунок 174);

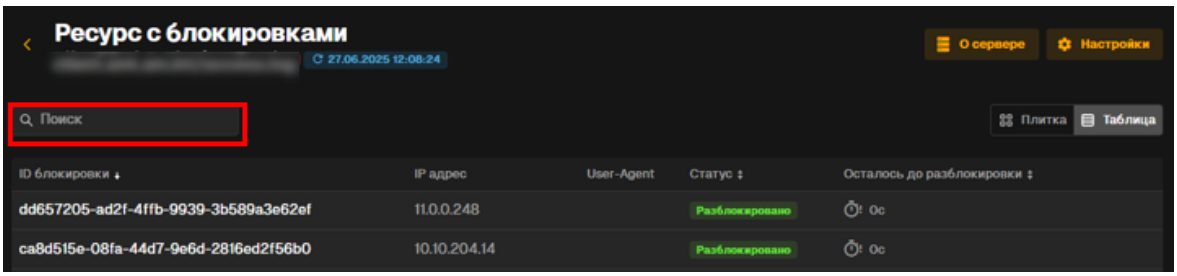

Рисунок 174 – Поиск по заблокированным сессиям

3) поиск осуществляется по полям «ID блокировки», «IP-адрес» и «User-Agent» на вхождение (Рисунок 175).

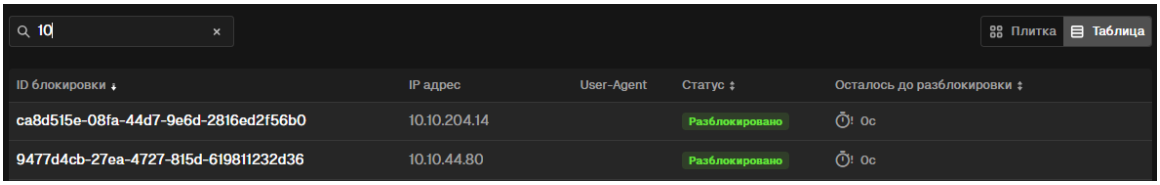

Рисунок 175 – Результат поиска по заблокированным сессиям

8.8 Удаление блокировки сессии

При отсутствии необходимости в хранении блокировку сессии можно удалить из Системы с помощью следующих действий:

1) перейти к странице заблокированных сессий;

2) навести курсор мыши на блокировку, которую необходимо удалить. Нажать на иконку меню выбора действий (Рисунок 176);

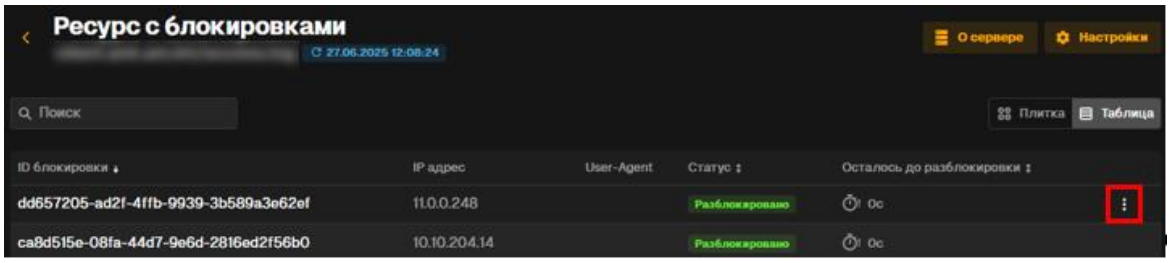

Рисунок 176 – Открытие меню выбора действий

3) в меню выбора действий выбрать пункт «Удалить» (Рисунок 177);

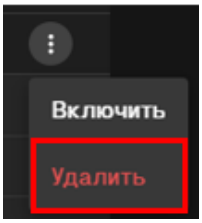

Рисунок 177 – Удаление блокировки сессии

4) подтвердить удаление с помощью кнопки «Удалить» (Рисунок 178).

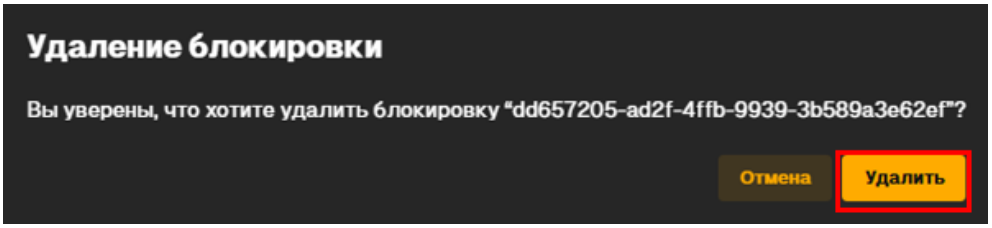

Рисунок 178 – Подтверждение удаления блокировки

9 Работа с разделом «Парсеры»

В разделе «Парсеры» пользователь может изучить предустановленные парсеры журналов сайтов или добавить свои, если логи используемого сервера имеют иной формат.

9.1 Создание парсера

Если планируется подключать к «AML» для анализа нестандартные источники логов, то может потребоваться добавить в Систему новые парсеры для журналов. Добавление нового парсера можно выполнить с помощью следующих действий:

1) перейти в раздел «Парсеры» (Рисунок 179);

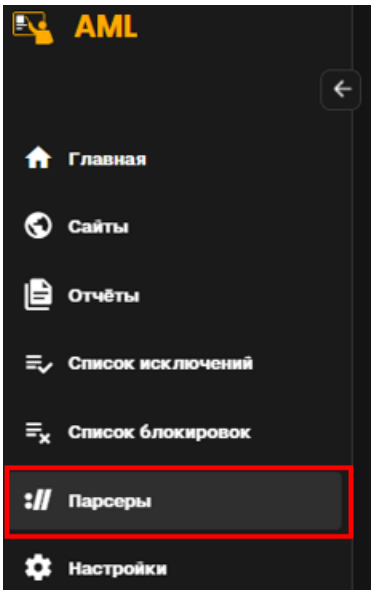

Рисунок 179 – Переход к разделу «Парсеры»

2) нажать на кнопку «Добавить парсер» (Рисунок 180);

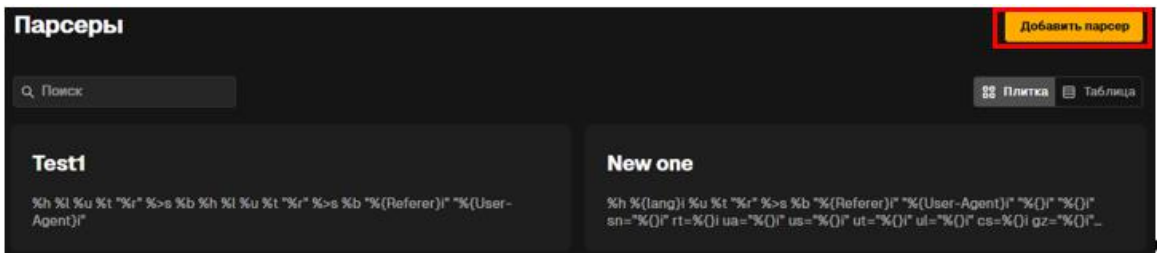

Рисунок 180 – Создание парсера

3) далее откроется страница создания нового парсера: в блоке «Общая информация» ввести «Название», «Формат», используемый в журналах лога, для которых будет использован данный парсер (Рисунок 181);

Рисунок 181 – Заполнение общей информации о парсере

4) в блоке «Проверка» можно вставить пример строки из журнала лога для проверки корректность работы парсера (Рисунок 182);

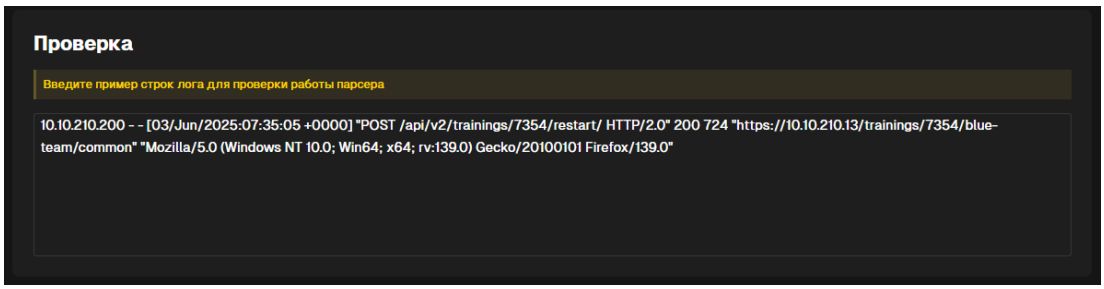

Рисунок 182 – Проверка корректности работы парсера

5) если парсер корректно работает на введенном примере, то в блоке «Проверка» будет выведен визуализированный для пользователя результат работы парсера (Рисунок 183);

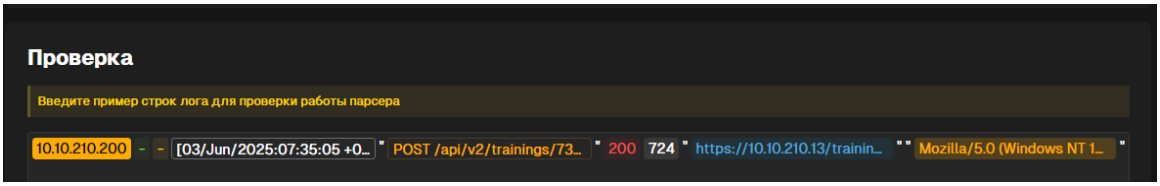

Рисунок 183 – Результат успешной проверки корректности работы парсера

6) при успешной проверке парсер можно загрузить в Систему после нажатия кнопки «Сохранить» в правом верхнем углу страницы (Рисунок 184);

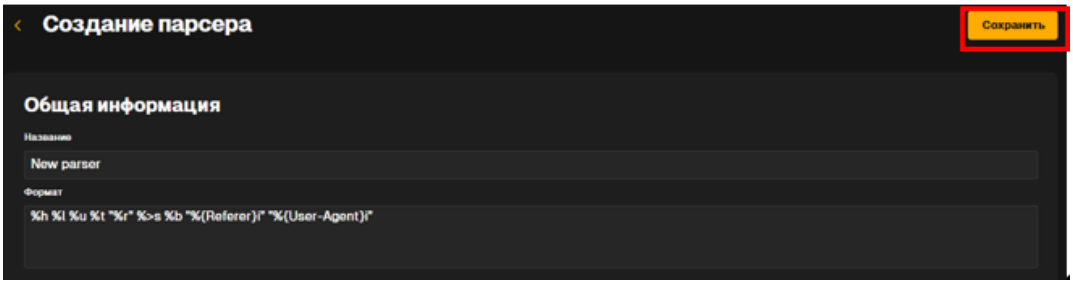

Рисунок 184 – Сохранение созданного парсера

7) новый парсер будет добавлен к списку парсеров в разделе (Рисунок 185).

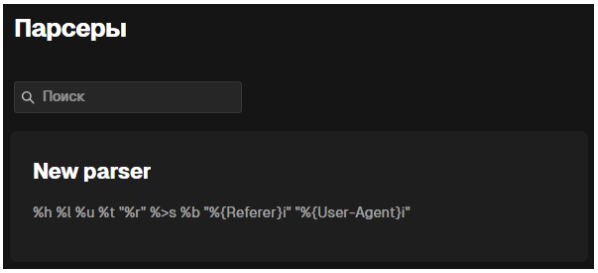

Рисунок 185 – Добавленный парсер

9.2 Редактирование парсера

Если при работе с Системой возникает необходимость внести изменения в парсер, ранее добавленный в Систему, то его можно отредактировать с помощью следующих действий:

1) перейти в раздел «Парсеры»;

2) нажать на парсер, который необходимо отредактировать (Рисунок 186);

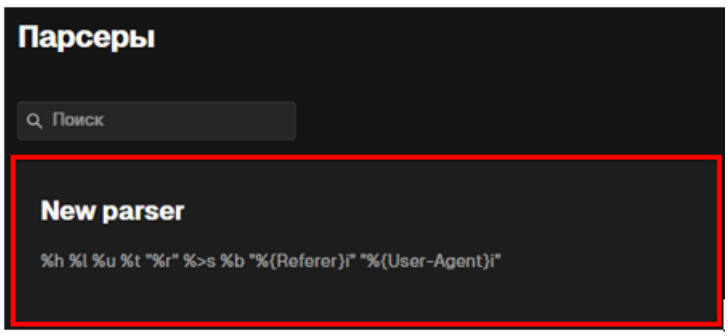

Рисунок 186 – Переход к редактированию парсера

3) далее откроется страница редактирования парсера (Рисунок 187);

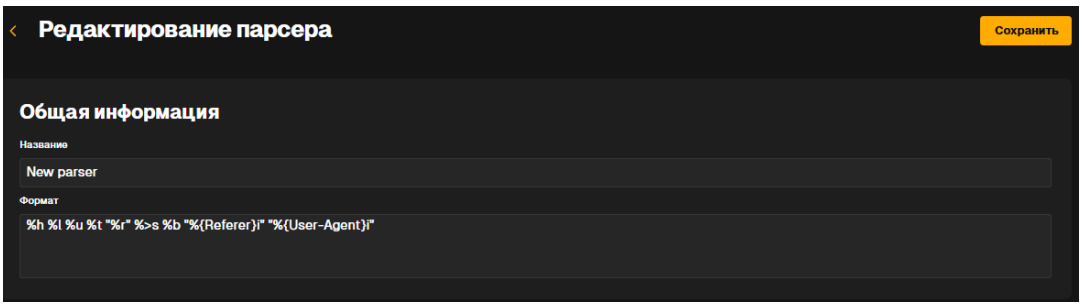

Рисунок 187 – Редактирование парсера

4) внести изменения в «Название», «Формат». При редактировании можно также осуществить проверку, которая выполняется аналогично предыдущим пунктам (Рисунок 188).

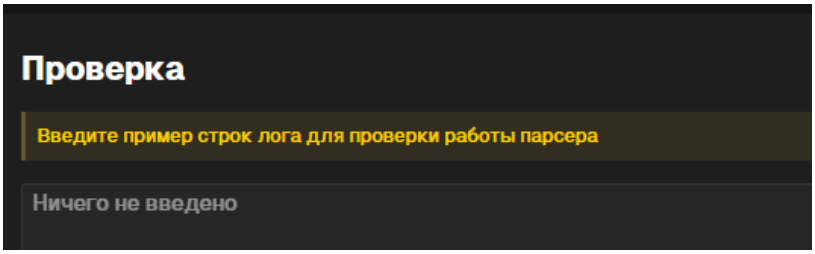

Рисунок 188 – Проверка корректности работы парсера

9.3 Удаление парсера

Добавленные в Систему парсеры можно удалить при необходимости. В Системе имеются предустановленные парсеры, которые поставляются вместе с Системой и удалить их невозможно. Удалить парсер можно с помощью следующих действий:

1) перейти в раздел «Парсеры»;

2) навести курсор мыши на тот парсер, который необходимо удалить. Нажать в правом верхнем углу на иконку меню выбора действий (Рисунок 189);

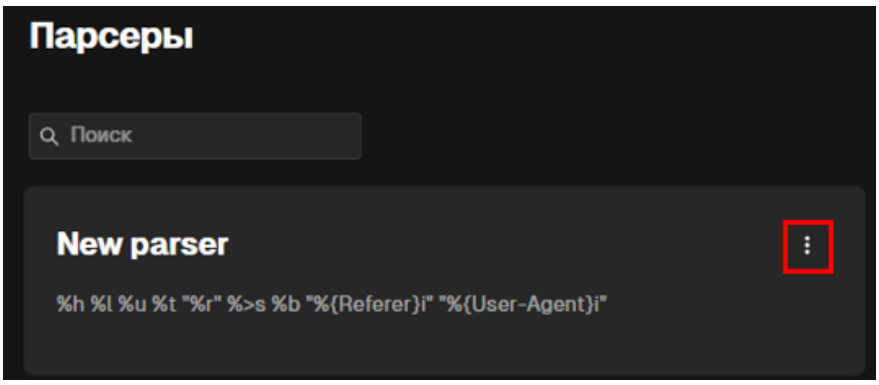

Рисунок 189 – Открытие меню выбора действий с парсером

3) выбрать в контекстном меню «Удалить» (Рисунок 190);

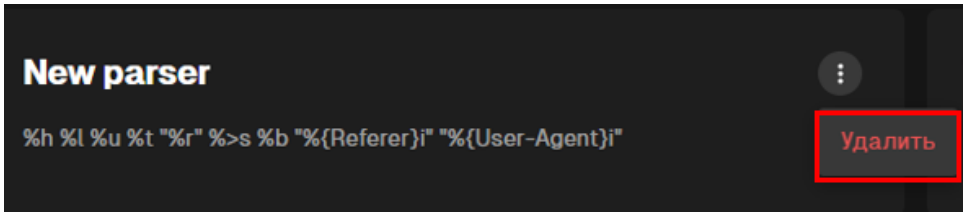

Рисунок 190 – Удаление парсера

4) подтвердить удаление в открывшемся модальном окне (Рисунок 191);

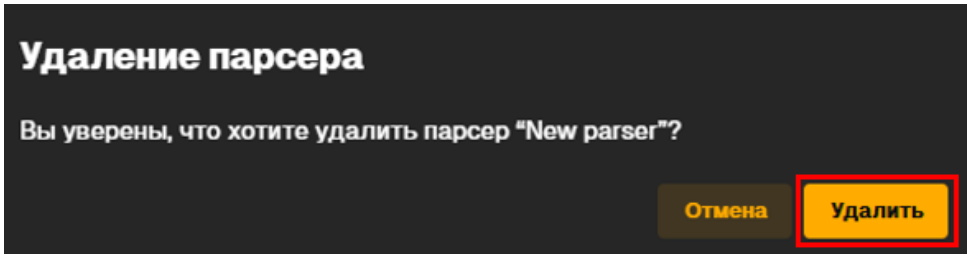

Рисунок 191 – Подтверждение удаления парсера

5) выбранный парсер будет удален из Системы.

10 Работа с панелью администратора

10.1 Авторизация в панели администратора

Для начала работы с панелью администратора в «AML» у пользователя должен быть доступ к серверу, а также логин или пароль, задаваемый при первом запуске Системы или выданный другим администратором. Логин и пароль для доступа к панели администратора и для доступа к веб-интерфейсу Системы одинаковы для пользователя. Имея данную информацию можно авторизоваться в панели администратора с помощью следующих действий:

1) в окне браузера перейти к панели администратора по адресу или домену сервера, на котором развернута Система https://<ip_or_domain>/admin/. Далее отобразится форма авторизации (Рисунок 192);

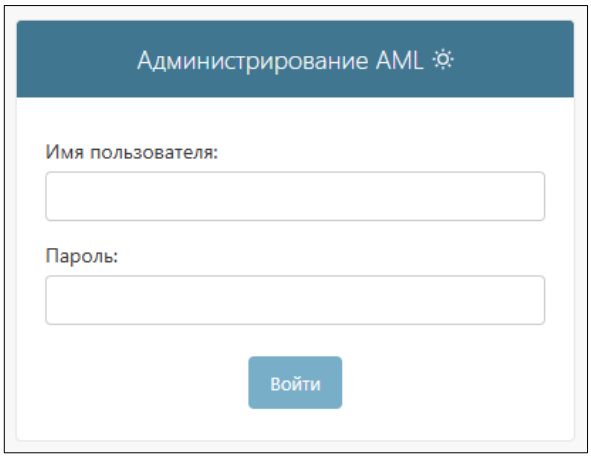

Рисунок 192 – Авторизация в панели администратора

2) в соответствующие поля ввести «Имя пользователя» и «Пароль» от учетной записи администратора и нажать кнопку «Войти» (Рисунок 193);

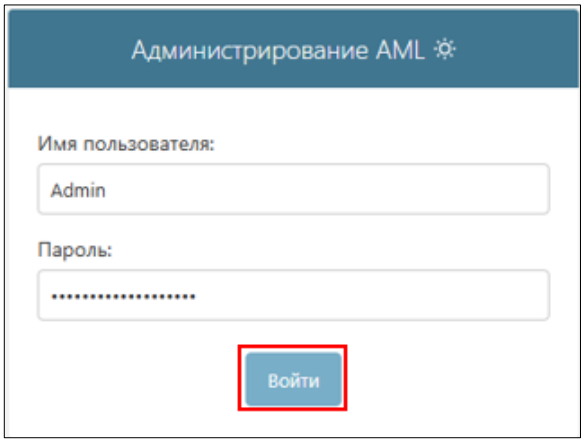

Рисунок 193 – Кнопка входа в панель администратора

3) пользователь будет перенаправлен в панель администратора (Рисунок 194);

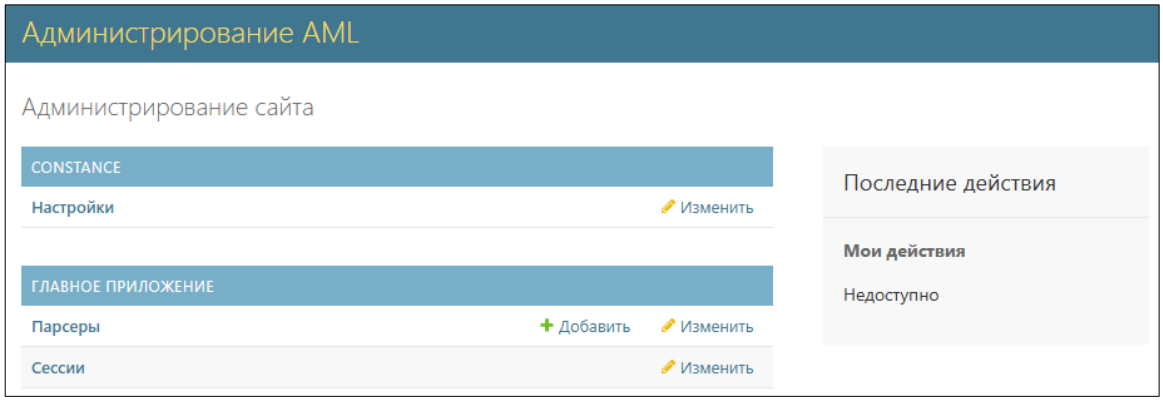

Рисунок 194 – Внешний вид панели администратора

10.2 Смена пароля

При необходимости из панели администратора можно сменить пароль для доступа к Системе (пароль будет изменен как для доступа к панели администратора, так и к веб-интерфейсу «AML»). Смену пароля можно выполнить с помощью следующих действий:

1) в правом верхнем углу интерфейса панели администратора нажать на кнопку «Смена пароля». Пользователь будет перенаправлен на страницу смены пароля (Рисунок 195);

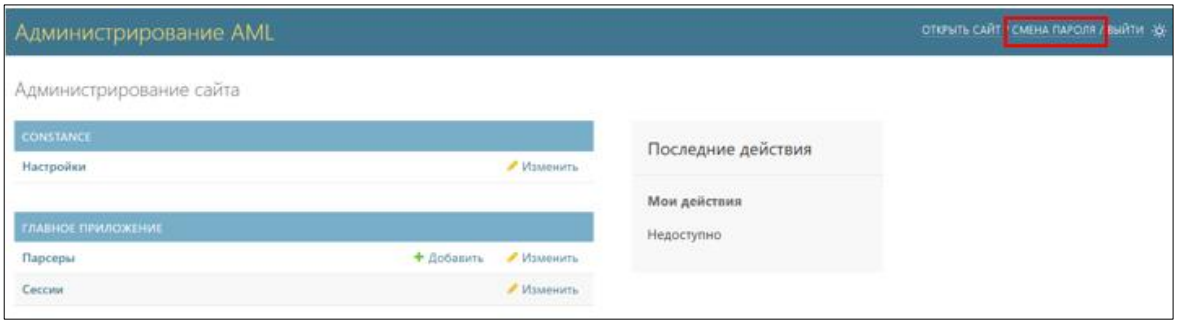

Рисунок 195 – Переход на страницу смены пароля

2) на странице смены пароля необходимо ввести старый пароль от аккаунта, новый пароль и подтверждение нового пароля. Новый пароль должен удовлетворять указанным условиям:

– пароль не должен быть слишком похож на другую личную информацию;

– пароль должен содержать как минимум 8 символов;

– пароль не должен быть слишком простым и распространенным;

– пароль не может состоять только из цифр.

После заполнения всех полей нажать на кнопку «Изменить мой пароль» (Рисунок 196);

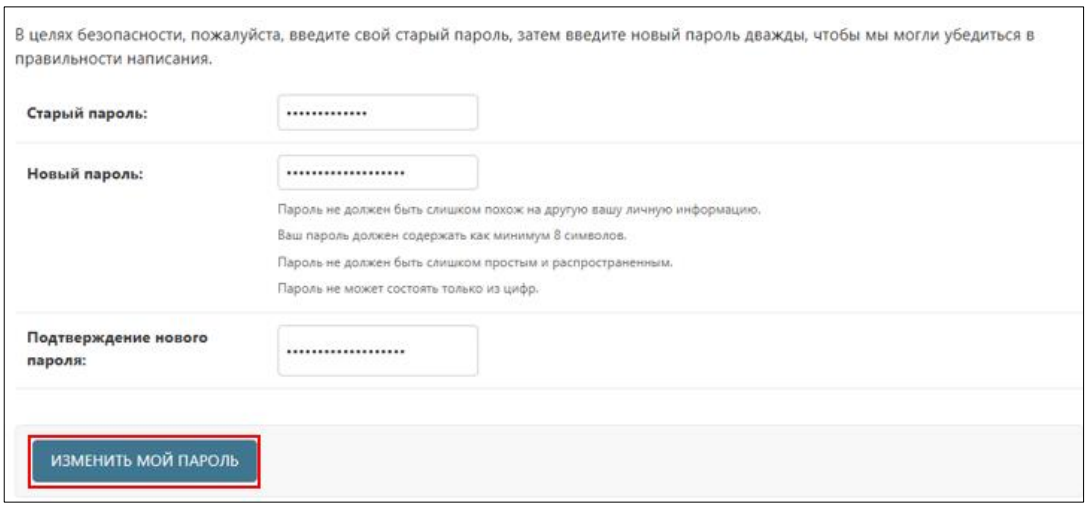

Рисунок 196 – Смена пароля

3) далее Система оповестит об успешном изменении пароля (Рисунок 197).

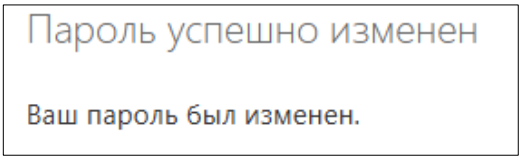

Рисунок 197 – Оповещение Системы об успешном изменении пароля

10.3 Возвращение к веб-интерфейсу и выход из Системы

По завершении работы с панелью администратора пользователь может вернуться к веб-интерфейсу Системы или совершить выход из своего аккаунта с помощью следующих действий:

1) в правом верхнем углу интерфейса нажать на кнопку «Открыть сайт» для возвращения к интерфейсу Системы или на кнопку «Выйти» для выхода из Системы (Рисунок 198);

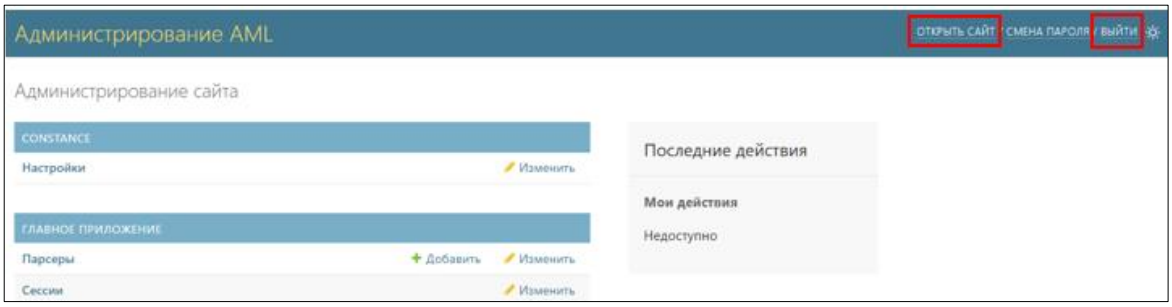

Рисунок 198 – Возвращение к веб-интерфейсу и выход из Системы

2) после нажатия на кнопку «Открыть сайт» пользователь останется авторизованным и будет перенаправлен на страницу «Главная» (Рисунок 199);

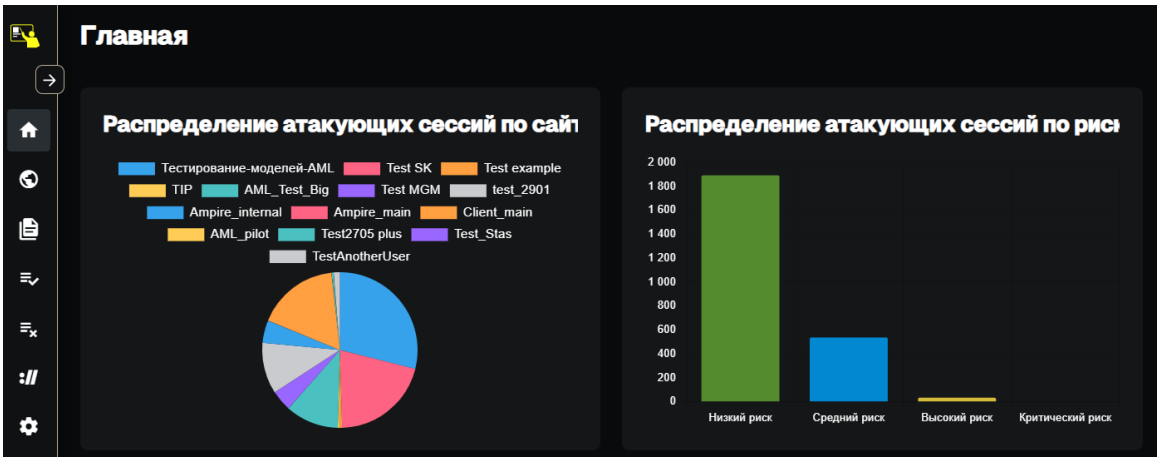

Рисунок 199 – Возвращение к веб-интерфейсу

3) после нажатия на кнопку «Выйти» пользователь будет перенаправлен на страницу авторизации веб-интерфейса Системы (Рисунок 200);

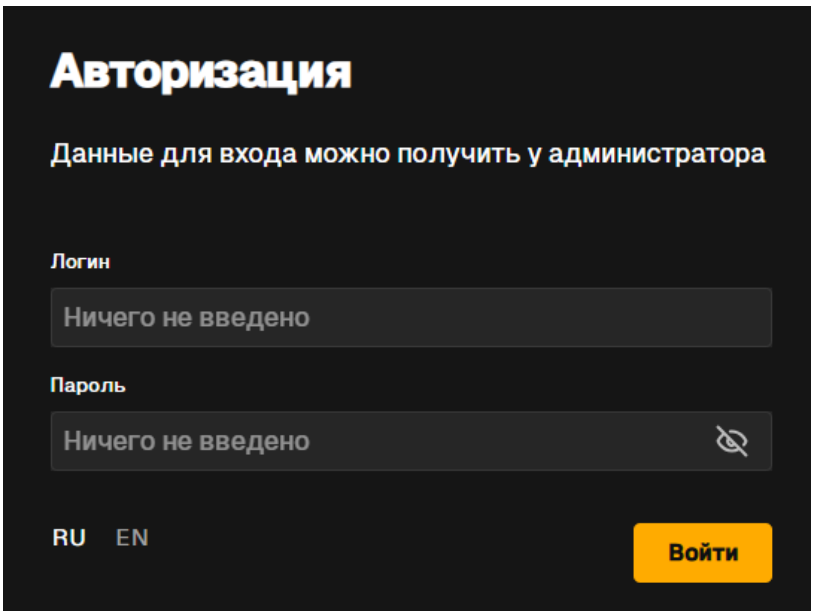

Рисунок 200 – Выход из Системы

11 Работа с пользователями и группами

11.1 Создание пользователя

В панели администратора «AML» пользователь может создать нового пользователя для работы в Системе с помощью следующих действий:

1) перейти в раздел «Пользователи» в блоке «Пользователи и группы» (Рисунок 201);

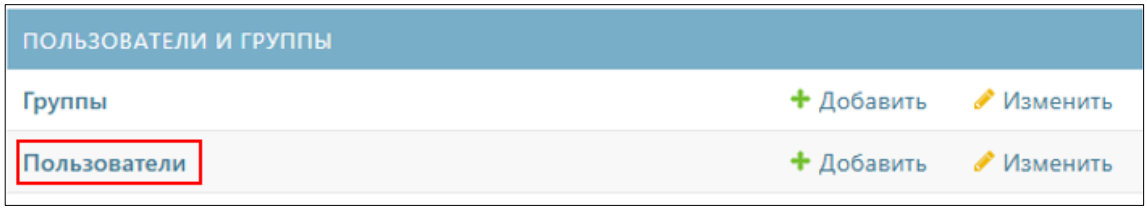

Рисунок 201 – Переход к странице создания пользователя

2) далее Система отобразит список созданных пользователей, даст возможность отфильтровать значения по полю «Статус персонала/суперпользователя», по активности пользователя и принадлежности к группам. Для определенного отображения нужно нажать в блоке справа на необходимое значение фильтра (Рисунок 202);

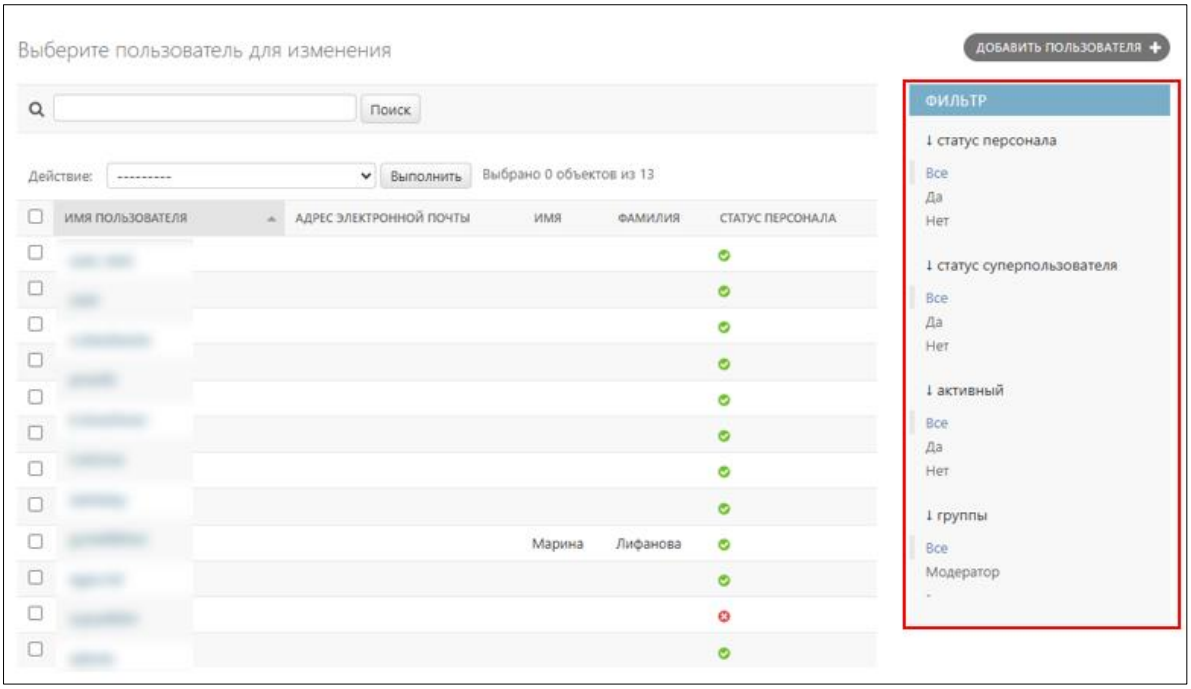

Рисунок 202 – Фильтр по пользователям Системы

3) для создания пользователя нужно нажать кнопку «Добавить пользователя» (Рисунок 203);

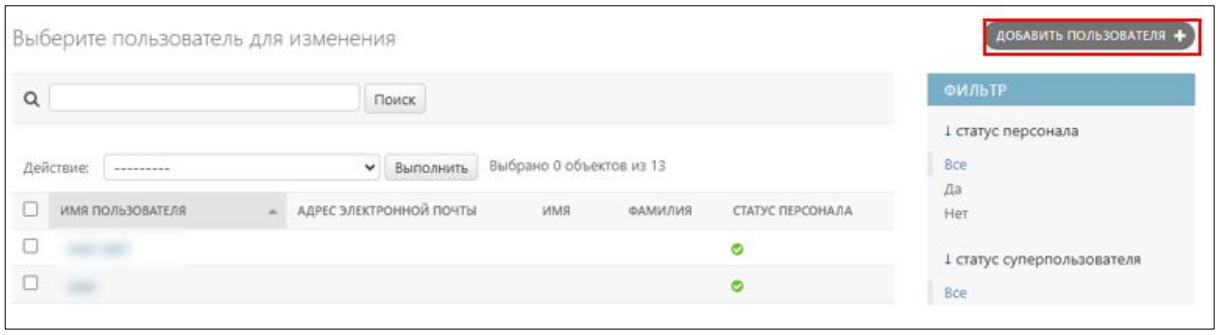

Рисунок 203 – Создание пользователя

4) на открывшейся странице необходимо указать «Имя пользователя», «Пароль» для доступа в Систему и подтверждение пароля. После заполнения нажать на одну из трех кнопок сохранения (Рисунок 204):

– по кнопке «Сохранить» можно после сохранения вернуться в раздел «Пользователи»;

– по кнопке «Сохранить и добавить другой объект» пользователь будет сохранен, далее повторно откроется форма создания пользователя;

– по кнопке «Сохранить и продолжить редактирование» пользователь будет сохранен, далее карточка откроется для редактирования;

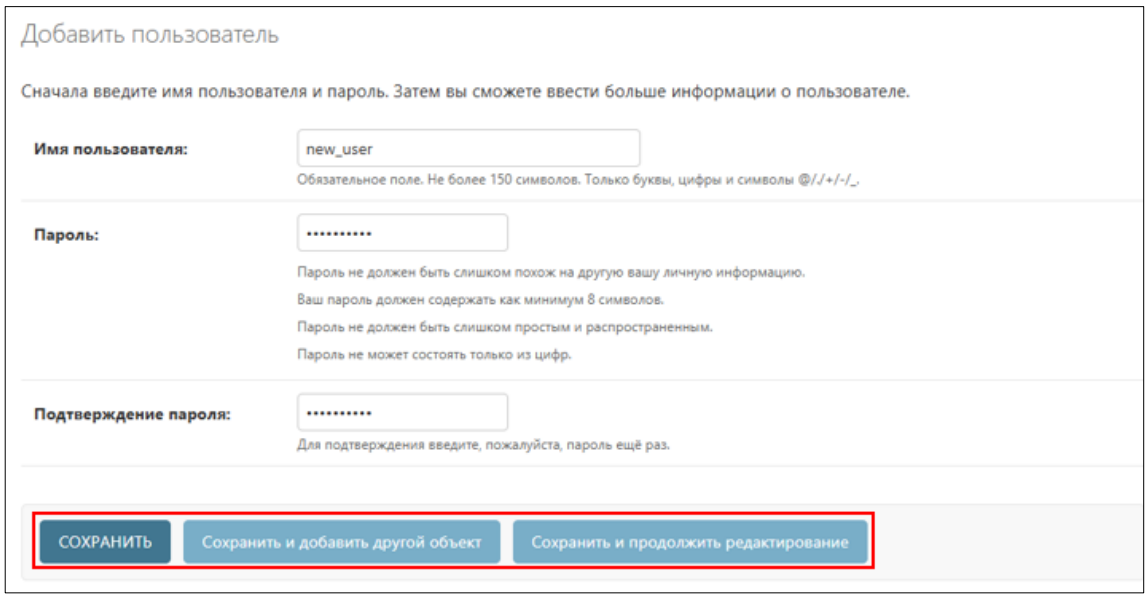

Рисунок 204 – Заполнение информации о новом пользователе

5) после сохранения Система оповестит об успешном создании пользователя (Рисунок 205).

Рисунок 205 – Системное оповещение об успешном создании пользователя

11.2 Изменение профиля пользователя

Если в учетную запись пользователя необходимо внести изменения, то можно выполнить изменения с помощью перехода в карточку с информацией данного пользователя. Редактирование пользователя можно выполнить с помощью следующих действий:

1) перейти в раздел «Пользователи»;

2) выбрать пользователя, в учетную запись которого нужно внести изменения (Рисунок 206);

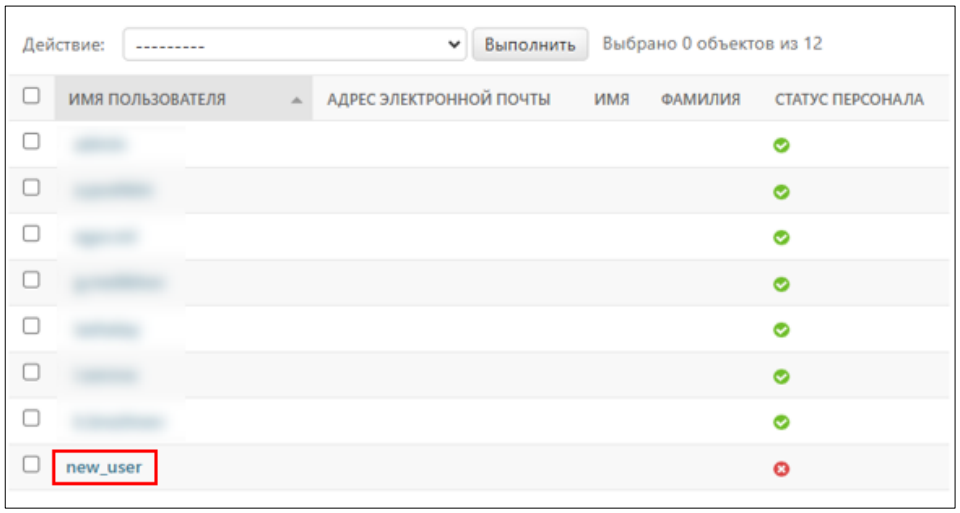

Рисунок 206 – Выбор пользователя для изменения

3) на открывшейся странице изменения данных можно сменить пароль пользователя, заполнив форму (Рисунок 207);

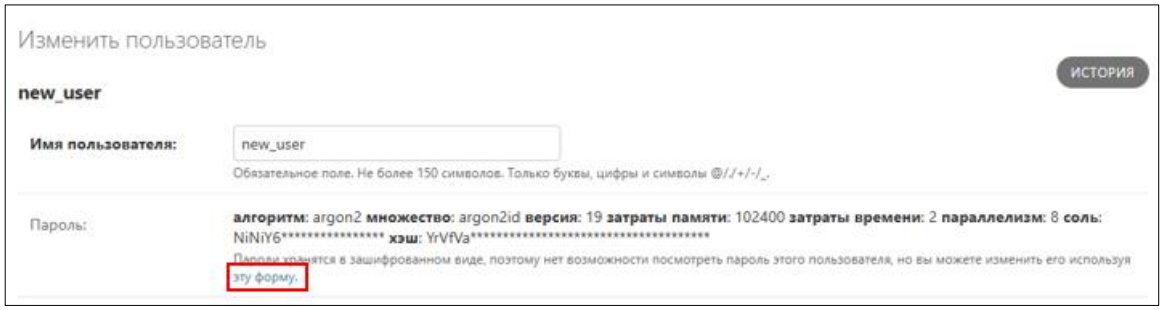

Рисунок 207 – Форма смены пароля пользователя

4) в блоке «Персональная информация» можно внести информацию о пользователе в поля «Имя», «Фамилия» и «Адрес электронной почты» (Рисунок 208);

Рисунок 208 – Добавление персональной информации пользователя

5) в блоке «Права» можно изменить (Рисунок 209):

– «Статус Активности» – может ли пользователь авторизоваться и выполнять действия в Системе;

– «Статус Персонала» – имеет ли пользователь доступ к панели администратора;

– «Статус Суперпользователя» – проставляется в случае, если у пользователя имеются все доступные права на работу в Системе без явного их назначения;

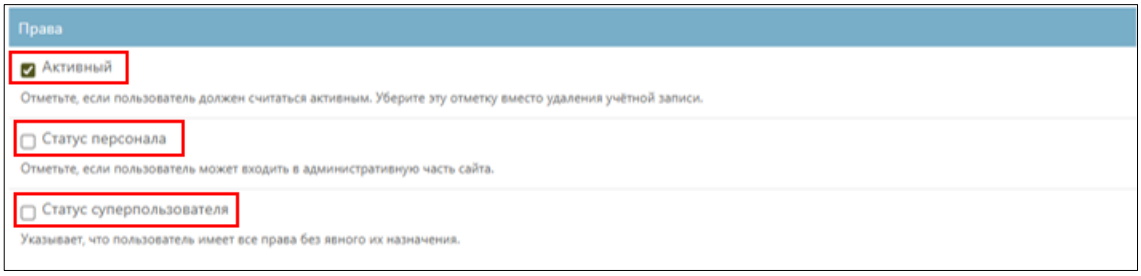

Рисунок 209 – Изменение статусов пользователя

6) далее в блоке «Права» можно указать группы, к которым относится пользователь. Можно выбрать и добавить из списка конкретную группу или выбрать все доступные (Рисунок 210);

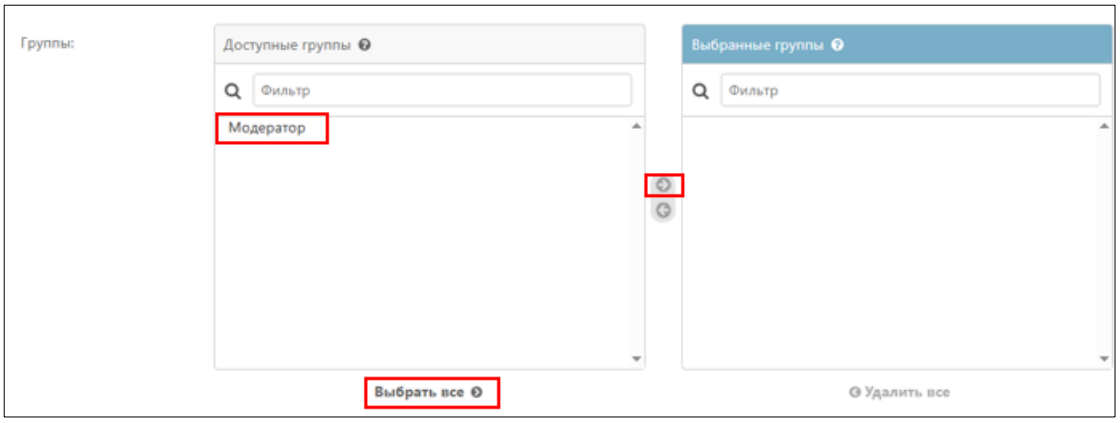

Рисунок 210 – Выбор групп, к которым относится пользователь

7) помимо добавления пользователя в группы, обладающие набором прав, можно выделить определенные личные права пользователю. Выделение прав можно выполнить в блоке «Права» в пункте «Права пользователя», для выполнения необходимо выбрать необходимые права в таблице «Доступные права пользователя» и перенести их в таблицу «Выбранные права пользователя» с помощью стрелки. Также можно использовать кнопку «Выбрать все», если нужно выдать пользователю полный набор прав для работы с Системой (Рисунок 211);

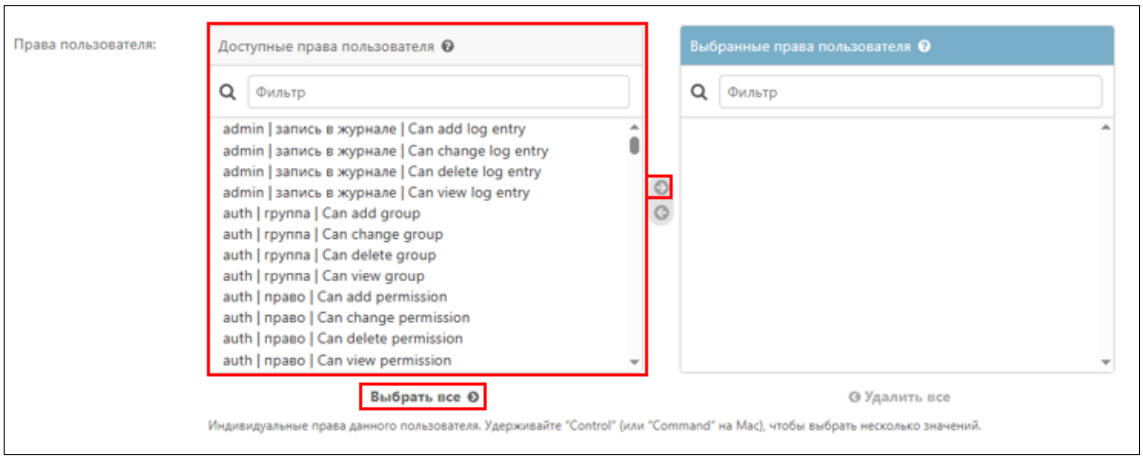

Рисунок 211 – Изменение прав доступа

8) после завершения редактирования пользователя в нижней части страницы сохранить изменения, нажав на одну из кнопок – «Сохранить», «Сохранить и добавить другой объект» или «Сохранить и продолжить редактирование» (Рисунок 212);

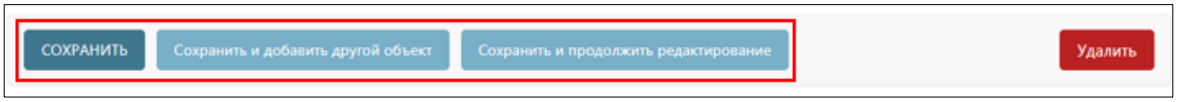

Рисунок 212 – Сохранение изменений

9) после сохранения изменений Система оповестит об успешном изменении профиля пользователя (Рисунок 213).

Рисунок 213 – Системное оповещение об успешном изменении профиля пользователя

11.3 Удаление пользователя

Помимо того, что пользователя, которому больше не нужен доступ к Системе можно деактивировать, также можно удалить пользователя из Системы. Из раздела «Пользователи» доступно массовое удаление учетных записей, а из карточки пользователя можно удалить конкретную учетную запись. Для этого нужно выполнить следующие действия:

1) перейти в раздел «Пользователи»;

2) в выпадающем списке «Действие» выбрать «Удалить выбранные пользователи» (Рисунок 214);

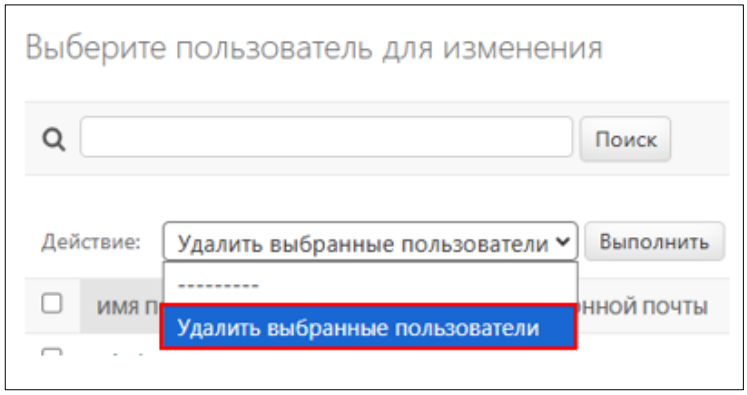

Рисунок 214 – Выбор действия удаления

3) отметить чекбоксы с теми пользователями, которых нужно удалить. При выделении чекбокса в шапке таблицы будут выбраны/сброшены все строки (Рисунок 215);

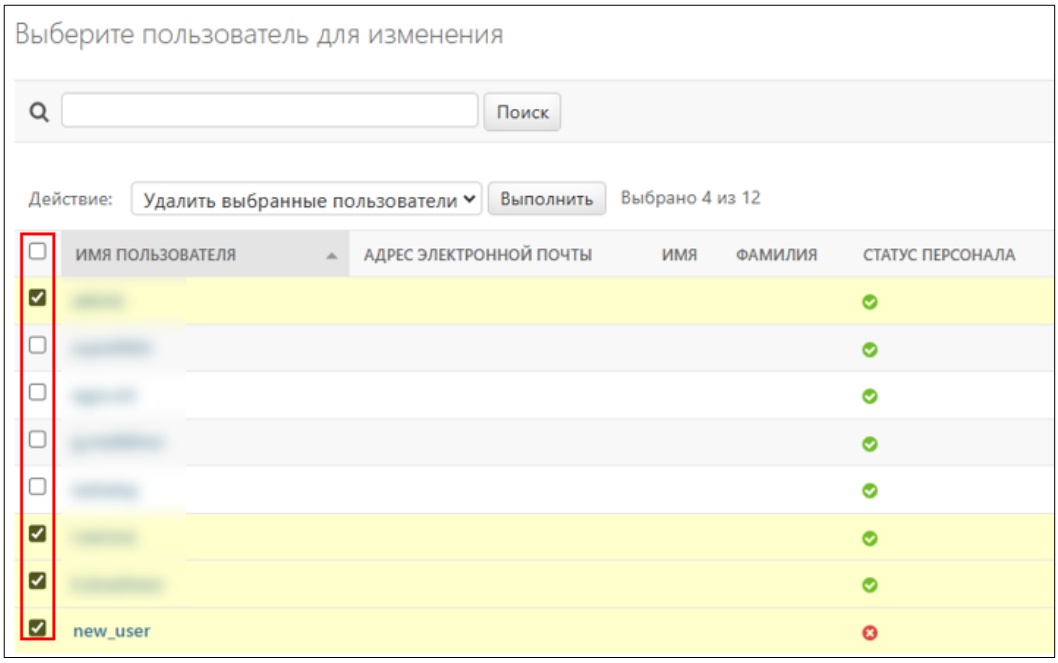

Рисунок 215 – Выбор пользователей для удаления

4) нажать кнопку «Выполнить» (Рисунок 216);

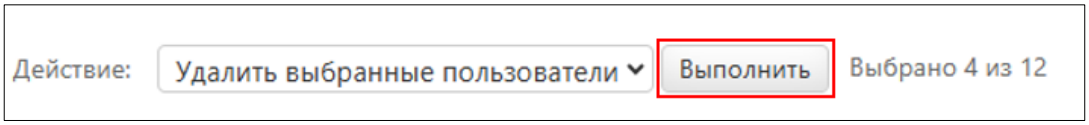

Рисунок 216 – Удаление пользователя

5) после подтверждения удаления в следующем окне выполнится удаление выбранных учетных записей (Рисунок 217);

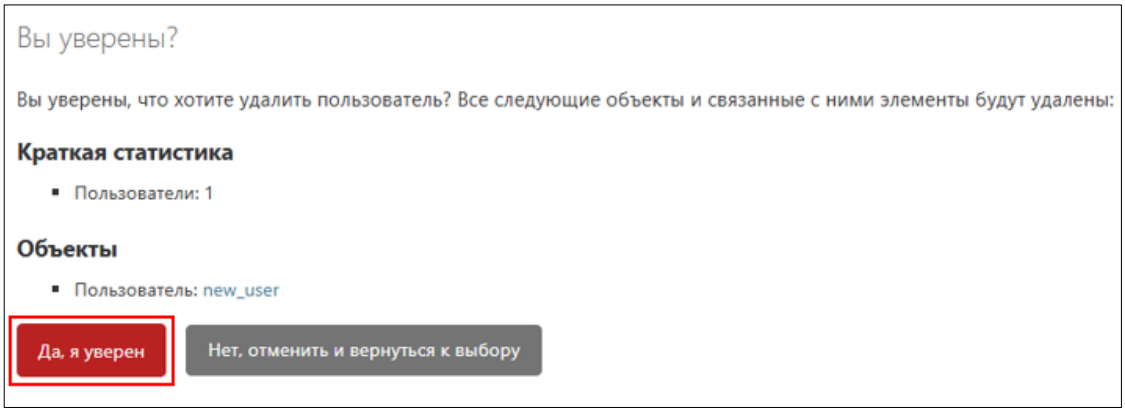

Рисунок 217 – Подтверждение удаления пользователя

6) для удаления одного пользователя нужно перейти к странице редактирования и в правом нижнем углу страницы нажать на кнопку «Удалить» (Рисунок 218);

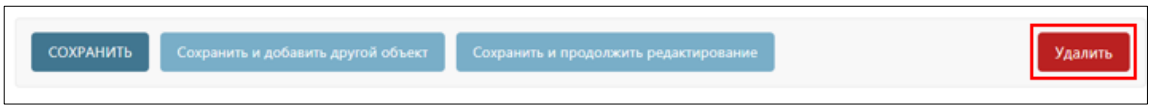

Рисунок 218 – Удаление пользователя из карточки пользователя

7) после подтверждения удаления в следующем окне выполнится удаление выбранных учетных записей.

11.4 Создание группы

Для ускорения выдачи прав для пользователей при работе с Системой можно использовать функциональность по созданию групп. Группа в панели администратора – это набор пользователей и прав доступа, который определяет возможности панели администратора, которыми могут пользоваться пользователи, добавленные в данную группу.

Создать новую группу можно с помощью следующих действий:

1) перейти в раздел «Группы» блока «Пользователи и группы» (Рисунок 219);

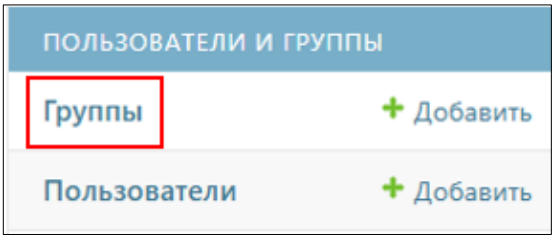

Рисунок 219 – Переход к разделу «Группы»

2) нажать на кнопку «Добавить группу +» (Рисунок 220);

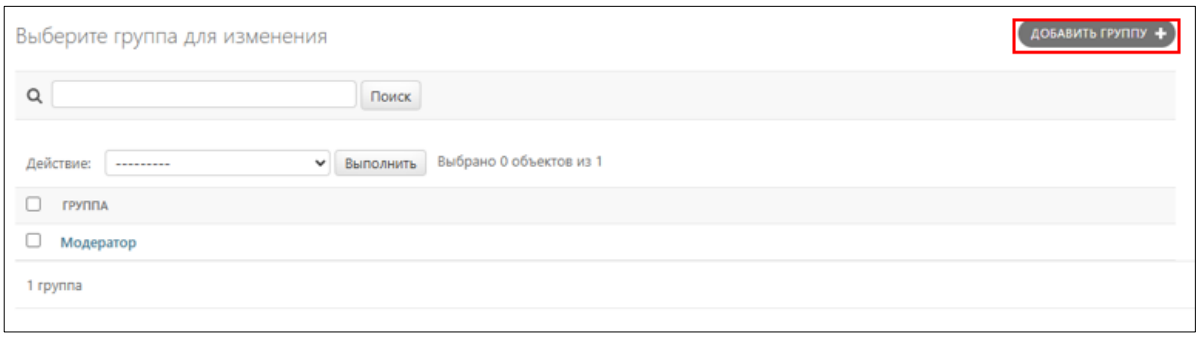

Рисунок 220 – Создание группы

3) на странице создания группы необходимо указать «Название» и выбрать права, которыми будут наделены пользователи данной группы. Для выбора прав нужно отметить их в списке «Доступные права» и перенести после нажатия стрелки в список «Выбранные права» (Рисунок 221);

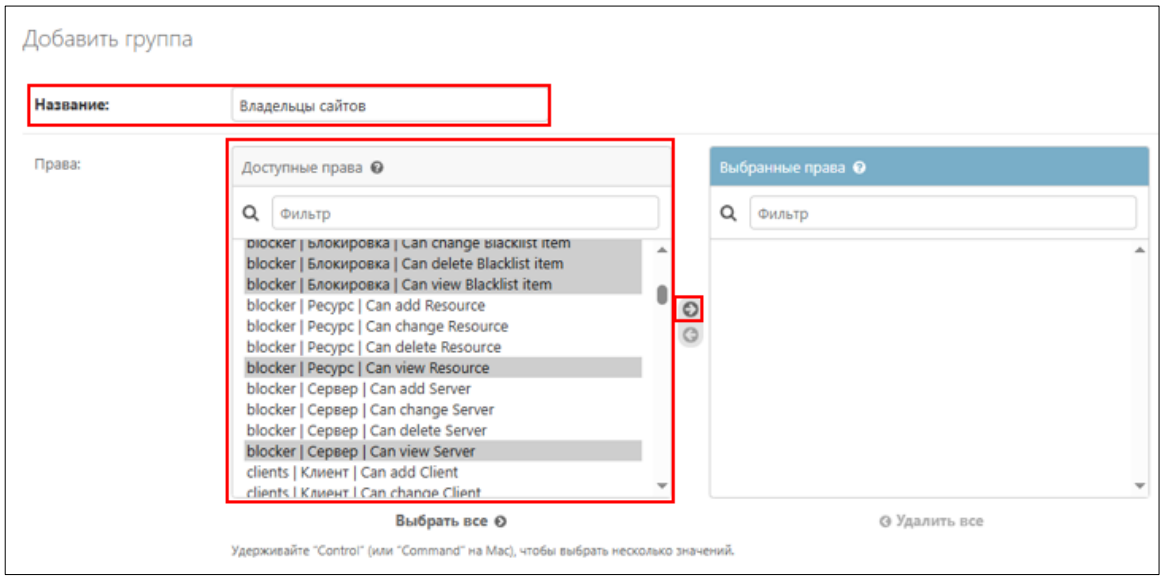

Рисунок 221 – Выбор названия и прав доступа для группы

4) после записи названия и выбора необходимых прав нажать на одну из кнопок сохранения:

– по кнопке «Сохранить» можно после сохранения вернуться в раздел «Группы»;

– по кнопке «Сохранить и добавить другой объект» группа будет сохранена, далее повторно откроется форма создания группы;

– по кнопке «Сохранить и продолжить редактирование» группа будет сохранена, далее карточка данной группы откроется для редактирования.

После сохранения Система оповестит об успешном создании группы (Рисунок 222).

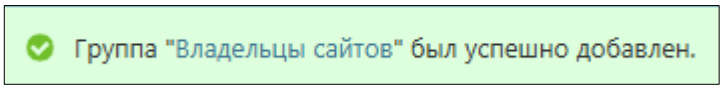

Рисунок 222 – Системное оповещение об успешном создании группы

11.5 Изменение группы

При необходимости в созданную группу можно внести изменения с помощью следующих действий:

1) перейти в раздел «Группы»;

2) выбрать из списка ту группу, которую необходимо отредактировать (Рисунок 223);

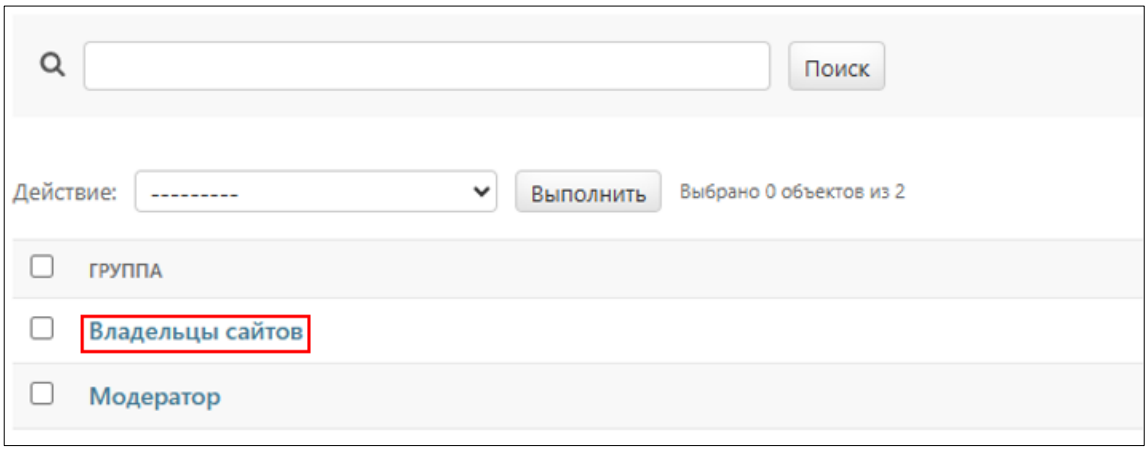

Рисунок 223 – Выбор группы для изменения

3) внести изменения в название и права группы (Рисунок 224);

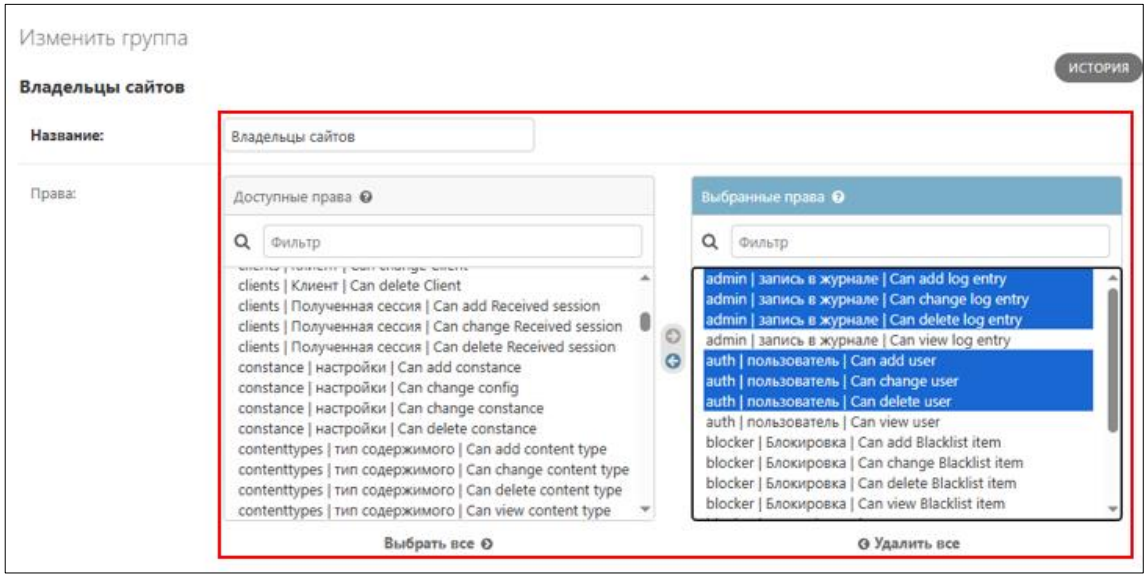

Рисунок 224 – Изменение группы

4) нажать на одну из кнопок сохранения, Система оповестит об успешных изменениях.

11.6 Удаление группы

Если в группе нет необходимости, то данную группу можно удалить из Системы. Удаление групп можно выполнить массово через страницу раздела «Группы» или можно удалить конкретную группу через карточку группы с помощью следующих действий:

1) перейти в раздел «Группы»;

2) в выпадающем списке «Действие» выбрать «Удалить выбранные группы» (Рисунок 225);

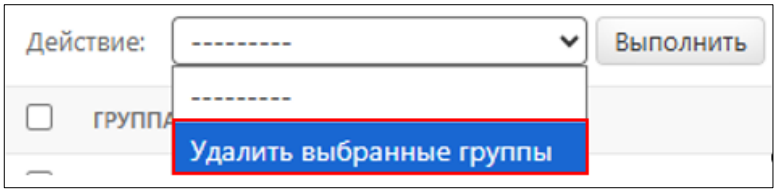

Рисунок 225 – Выбор действия удаления

3) отметить чекбоксы с теми группами, которые нужно удалить. При выделении чекбокса в шапке таблицы будут выбраны все строки, далее нажать кнопку «Выполнить» (Рисунок 226);

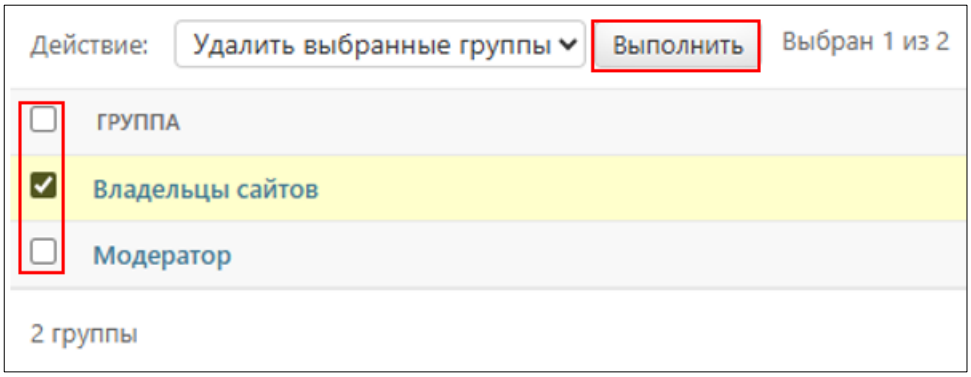

Рисунок 226 – Выбор групп для удаления

4) подтвердить удаление группы и выданных для данной группы прав (Рисунок 227);

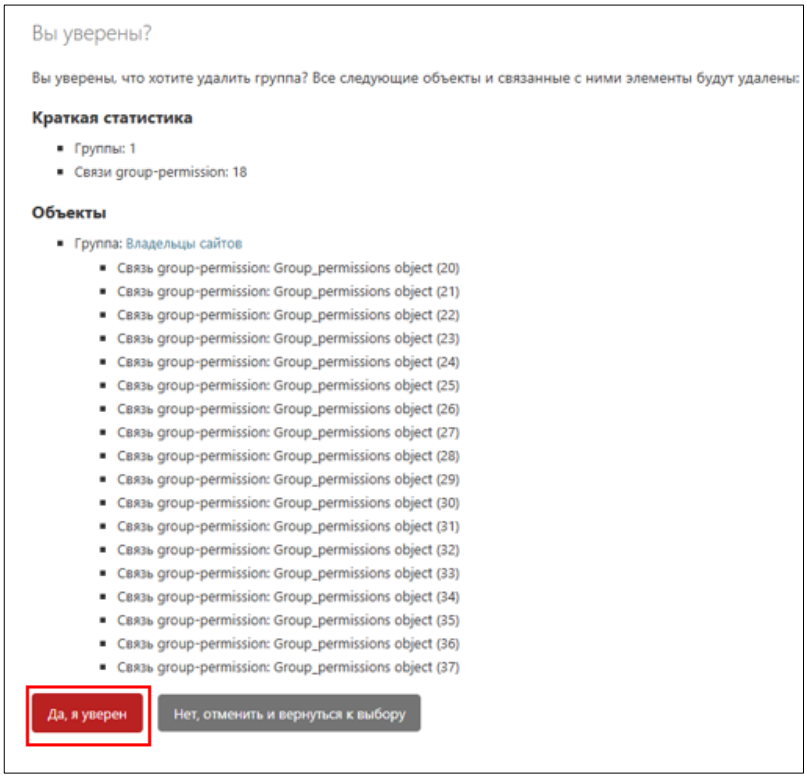

Рисунок 227 – Подтверждение удаления группы

5) далее Система оповестит об успешном удалении группы (Рисунок 228);

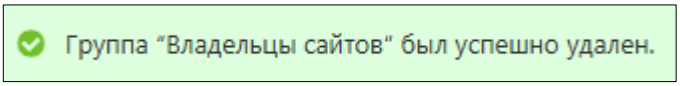

Рисунок 228 – Системное оповещение об успешном удалении группы

6) при необходимости удаления только одной группы можно выполнить удаление с помощью перехода к странице редактирования группы. На странице группы нужно нажать кнопку «Удалить» (Рисунок 229);

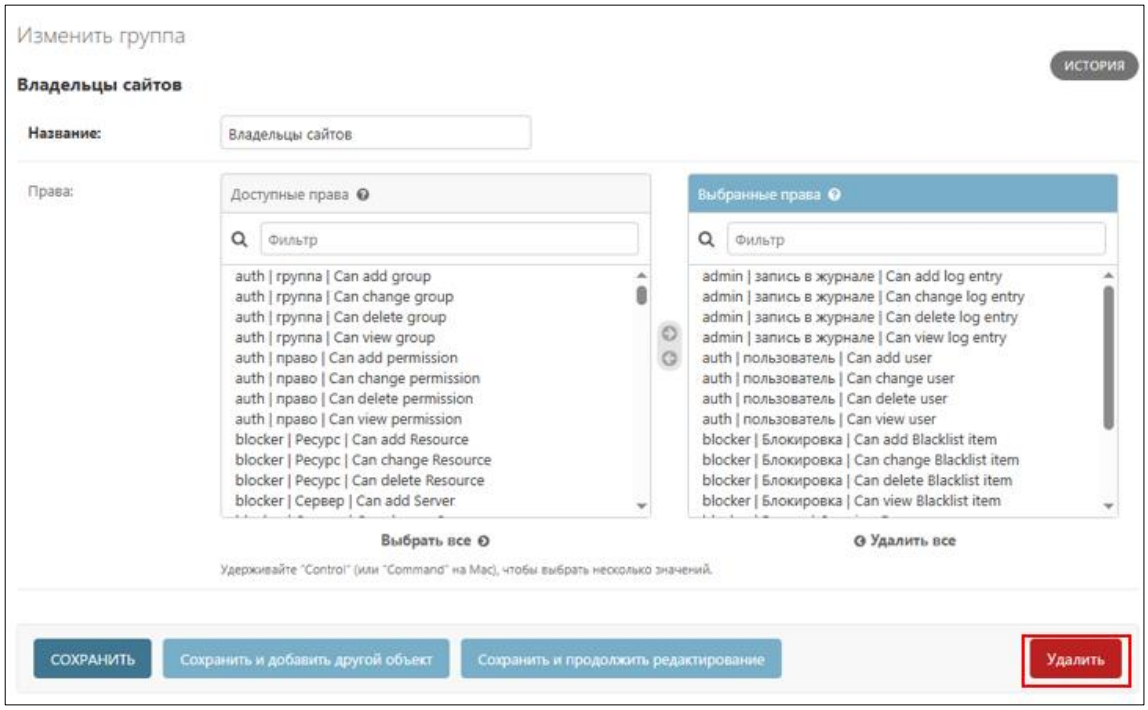

Рисунок 229 – Удаление группы из карточки группы

7) подтвердить удаление группы и выданных для группы прав, Система оповестит об успешном удалении группы.

12 Настройка значений и периодических задач

12.1 Настройка значений по умолчанию

В различных разделах Системы используются значения по умолчанию:

– «Максимальное количество запросов внутри сессии»;

– «Интервал обновления журнала при потоковой обработке»;

– «Базовое время блокировки» и т.д.

В панели администратора можно настроить используемые значения по умолчанию. Рекомендуется выполнять настройку только при особой необходимости, так как изменение значений по умолчанию может повлиять на работу Системы. Изменение настроек можно выполнить с помощью следующих действий:

1) перейти в раздел «CONSTANCE – Настройки» (Рисунок 230);

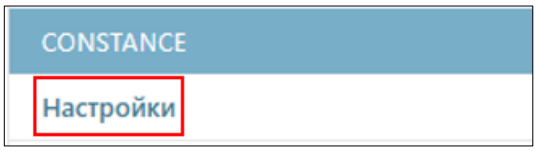

Рисунок 230 – Переход к разделу «CONSTANCE – Настройки»

2) в блоке «General options» можно изменить значения по умолчанию для журналов событий и разбиения их на сессии:

– «Минимальное количество запросов внутри сессии для обработки»;

– «Максимальное количество запросов внутри сессии»;

– «Максимальное количество строк файла журнала»;

– «Необходимость использования препроцессора».

В случае изменения исходных значений в столбце «Было изменено» для данного значения иконка изменится на галочку зеленого цвета. Каждое из значений можно сбросить до значения по умолчанию после нажатия кнопки «Reset to default» (Рисунок 231).

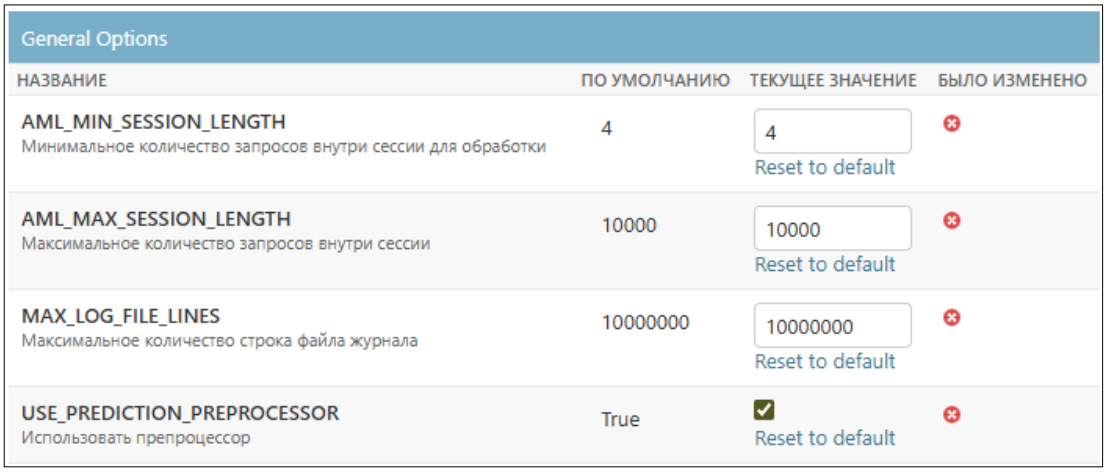

Рисунок 231 – Настройка значений по умолчанию

3) в блоке «Watch options» можно изменить значения по умолчанию для временных интервалов при потоковой обработке, а также смежные значения (Рисунок 232):

– «Интервал обновления статистики журнала потоковой обработки, сек»;

– «Интервал перепроверки сессий потоковой обработки, сек»;

– «Интервал перезагрузки списков исключений (потоковый режим), сек»;

– «Завершить потоковую обработку при запуске»;

– «Проверять сессию при сохранении, если она была изменена»;

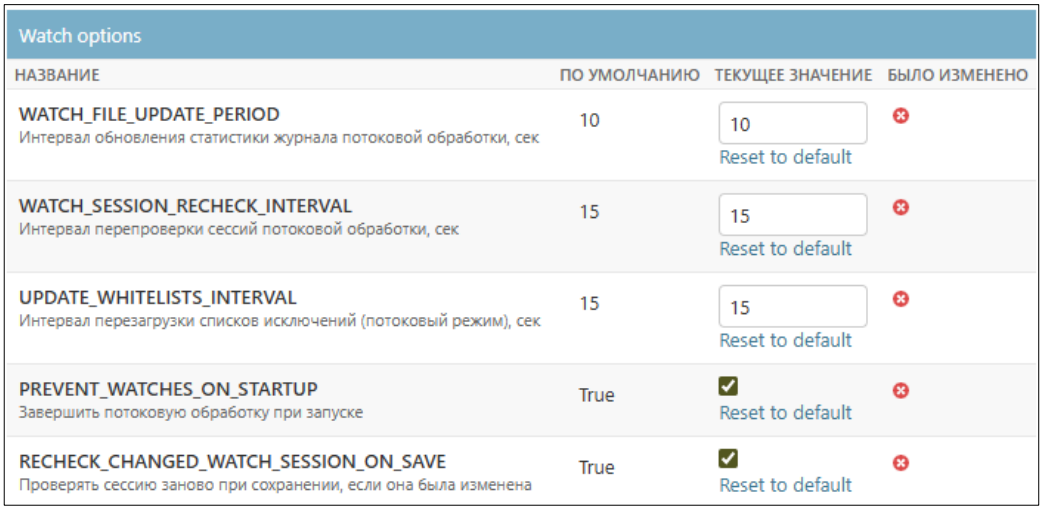

Рисунок 232 – Настройка значений по умолчанию

4) в блоке «Watch session bloking» можно изменить параметры, связанные с режимом блокировки (Рисунок 233):

– «Блокировка по ip/useragent»;

– «Базовое время блокировки, сек»;

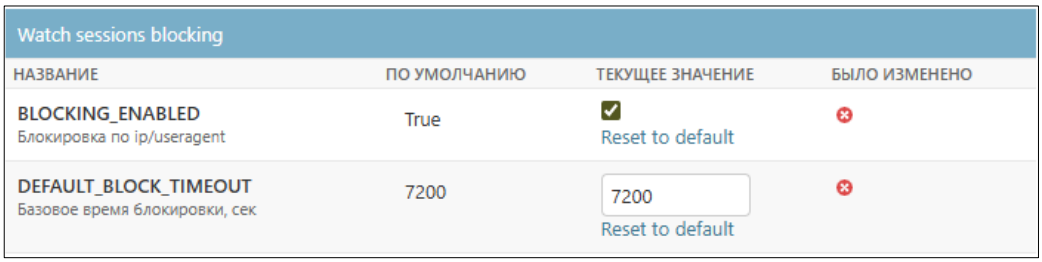

Рисунок 233 – Настройка значений по умолчанию

5) после внесения изменений в значения раздела нажать кнопку «Сохранить» в правом нижнем углу страницы (Рисунок 234);

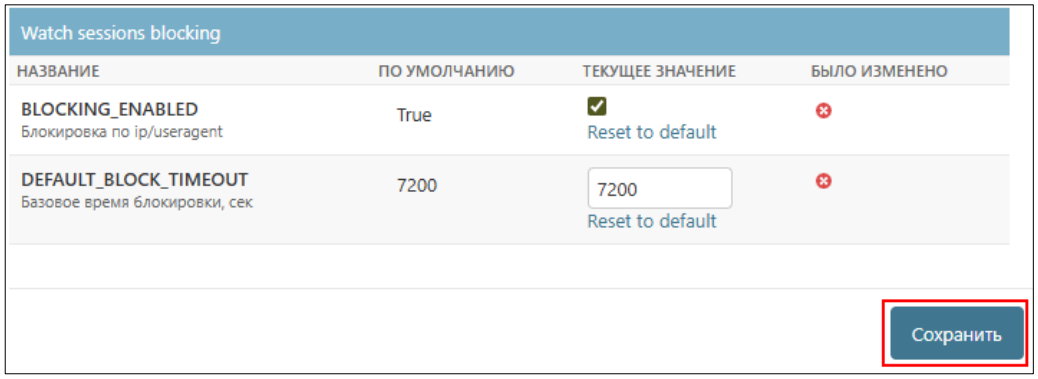

Рисунок 234 – Сохранение измененных настроек

12.2 Периодические задачи

В Системе имеются задачи, которые предназначены для автоматизации регулярных процессов и запускаются Системой по расписанию. В панели администратора можно управлять выполнением данных задач – включать и выключать их, запускать вручную при необходимости, переключать активность и удалять.

Не рекомендуется производить критичных действий с периодическими задачами во избежание нарушений в работе Системы. Настройку периодических задач можно выполнить с помощью следующих действий:

1) перейти в раздел «Периодические задачи» (Рисунок 235);

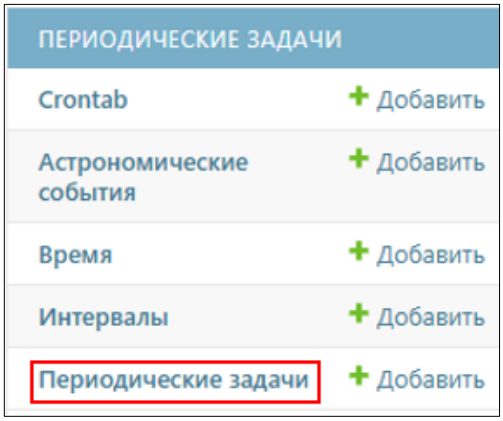

Рисунок 235 – Переход к разделу «Периодические задачи»

2) далее отобразится список созданных в Системе периодических задач с указанием их наименования, статуса активности, расписания, даты и времени последнего запуска и признака одноразовой задачи. Из списка задач следует выбрать и отметить чекбоксами те, для которых необходимо выполнить действие (Рисунок 236);

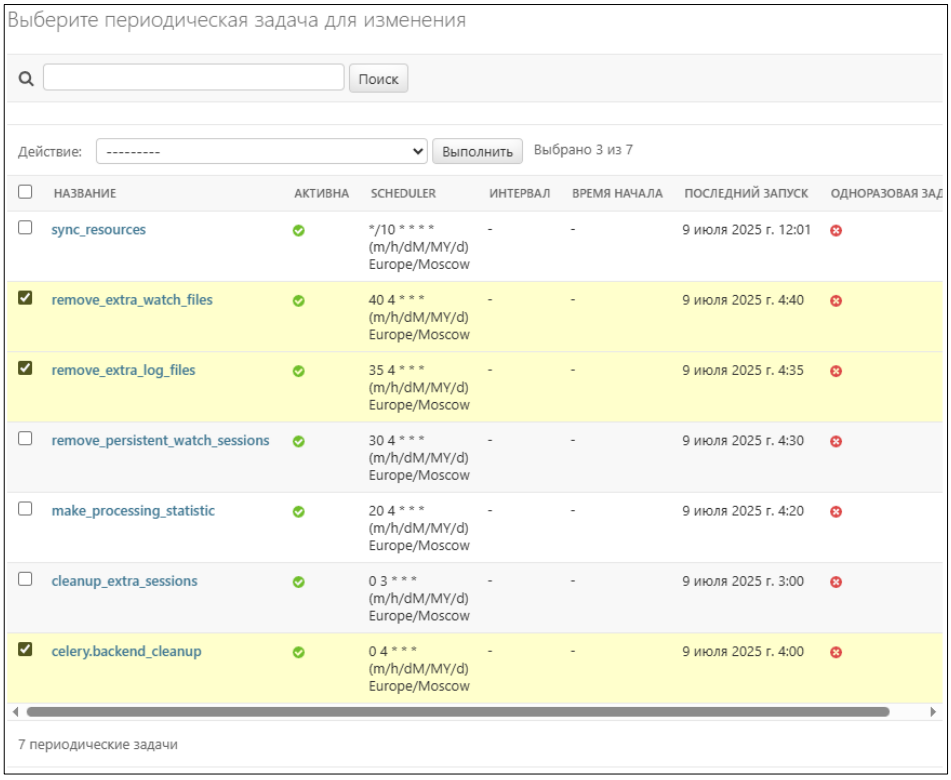

Рисунок 236 – Выбор периодических задач для выполнения действия

3) выбрать нужное действие из выпадающего списка над шапкой таблицы (Рисунок 237);

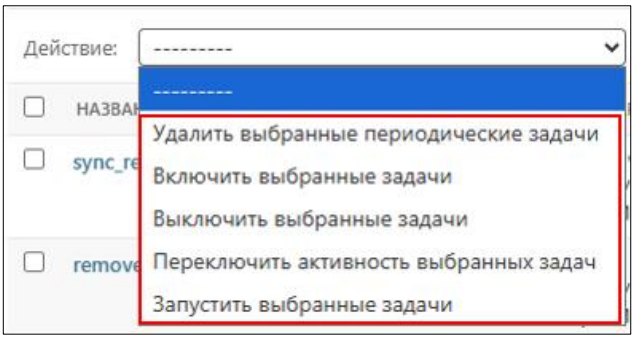

Рисунок 237 – Выбор действия с периодическими задачами

4) нажать кнопку «Выполнить» (Рисунок 238);

Рисунок 238 – Запуск выполнения выбранного действия

5) с выбранными периодическими задачами будет выполнено необходимое действие.

13 Потоковый режим и блокировки

13.1 Настройка сервера для потокового режима

«AML» позволяет обрабатывать журналы веб-ресурсов в потоковом режиме – после выбора журнала пользователем Система автоматически отслеживает изменения, анализирует их «в потоке», определяет атакующие и пользовательские сессии. Для этого необходимо настроить процесс доставки журналов событий в Систему. Для настройки доставки журналов до сервера «AML» необходимо выполнение двух обязательных требований:

1) с сервера «AML» имеется сетевой доступ до источника журналов;

2) на источнике журналов существует пользователь с правами на чтение директории с журналами событий и их содержанием, а также возможностью подключения по SSH с помощью пароля (требуется только один раз для доставки SSH-ключей).

Если выполняются два условия, то для сервера можно настроить доставку журналов с помощью следующих действий:

1) перейти в раздел «Сервисы доставки журналов» (Рисунок 239);

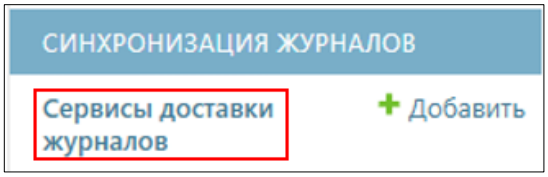

Рисунок 239 – Переход к разделу «Сервисы доставки журналов»

2) нажать кнопку «Добавить сервис доставки журналов +» (Рисунок 240);

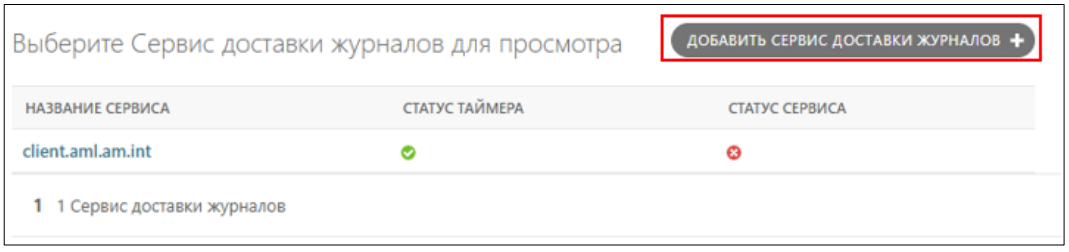

Рисунок 240 – Добавление нового сервиса доставки журнала

3) на открывшейся странице создания указать параметры:

– «Название сервиса» – наименование, предназначенное для идентификации сервиса в Системе, может принимать любое удобное значение, является обязательным;

– «Адрес сервера» – IP-адрес или доменное имя источника журналов, является обязательным;

– «SSH порт» – используемый для подключения порт. Значение в этом поле является обязательным, если используется нестандартный SSH порт;

– «Удаленный пользователь» – имя пользователя учетной записи пользователя с правами на чтение директории с журналами для подключения по SSH, является обязательным;

– «Удаленный пароль» – пароль от указанной учетной записи пользователя для подключения по SSH, является обязательным;

– «Директория на сервере» – абсолютный путь до директории, в которой хранятся необходимые журналы, является обязательным;

– «Интервал синхронизации» – частота, с которой будет осуществляться запрос на обновление информации о событиях в журнале. Если оставить поле пустым, то по умолчанию будет записан интервал таймера синхронизации в 20 секунд.

По завершении заполнения формы создания нажать кнопку «Сохранить» (Рисунок 241).

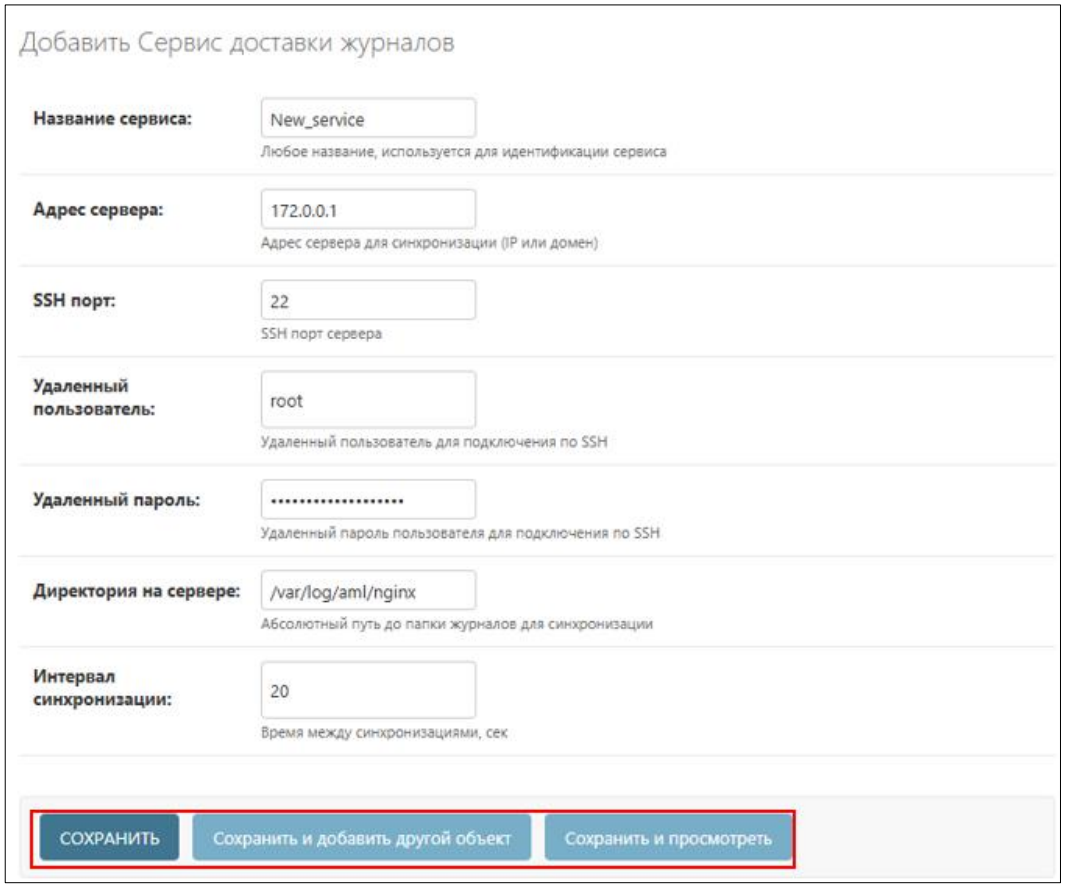

Рисунок 241 – Добавление параметров нового сервиса

После сохранения и проверки корректности данных для подключения будут созданы таймер и сервис systemd, отвечающие за синхронизацию данных с сервера для своевременного получения новых записей журнала. Добавленный сервер и путь до него появятся в списке при добавлении потоковой обработки в Системе.

13.2 Подготовка веб-сервера к блокировкам сессий для Nginx

Если журнал событий в «AML» обрабатывается в потоковом режиме, то для него можно настроить блокировку атакующих сессий – механизм, ограничивающий доступ к веб-ресурсу для IP-адресов или пар «IP-адрес» и «User-Agent», инициировавших атакующую сессию, путем отправки команды на веб-сервер. Для синхронизации работы сервера «AML» и веб-сервера, на котором необходимо блокировать сессии, нужно внести изменения в

конфигурационные файлы. Для подготовки сервера Nginx к блокировкам сессий необходимо выполнить следующие настройки:

1) создать файл blacklist.conf в директории с конфигурационными файлами или в любом удобном месте, например в /etc/nginx/;

2) в основную конфигурацию веб-сервера в раздел http помещается блок, который проверяет наличие соответствующих запросу «IP-адрес» и «User-Agent» в файле blacklist.conf, и при успехе возвращает переменную block_token, содержащую токен блокировки:

```
map "$remote_addr:$http_user_agent" $block_token {
  default "";
  include /etc/nginx/blacklist.conf;
}
```

3) также в блоке http необходимо указать значение параметра map_hash_bucket_size не меньше 256:

```
map_hash_bucket_size 256;
```

4) в раздел server для необходимого веб-сайта помещается блок, блокирующий запрос, если переменная block_token не пустая:

```
if ($block_token) {
  return 403;
}
```

5) пример файла blacklist.conf – переменная $block_token содержит код блокировки, по которому можно отследить заблокированную сессию и управлять ее блокировкой:

```
    # Для юзер агента требуется экранировать двоеточие и двойные кавычки
    "<IP>:<UA>" "block_token";         # В общем виде
    "10.0.1.1:badbot" "block_token";   # Блокировка по IP-адресу и юзер агенту
    "10.0.1.1:" "block_token";         # Блокировка по IP-адресу и пустому юзер агенту
```

6) для вывода кода блокировки нужно добавить в раздел server код, подменяющий 403 ответ на html-документ, содержащийся прямо в конфигурации Nginx:

```
# Пример:
error_page 403 @403error;
location @403error {
  default_type "text/html; charset=utf-8";
  return 403 "<h3><style>
  html { color-scheme: light dark; }
  body { width: 35em; margin: 0 auto;
  font-family: Tahoma, Verdana, Arial, sans-serif; }
  </style>Вы заблокированы, обратитесь к администратору.</h3>
  <h3>Ваш код блокировки - $block_token</h3>";
```

7) для подключения внешнего файла, подменяющего страницу блокировки, требуется доставить на сервер файл block.html (находится на сервере «AML» по пути /srv/aml/blocker/block.html) и в раздел server добавить код:

```
error_page 403 @blocked;
location @blocked {
  rewrite ^ /block.html break;
  allow all;
  internal;
  ssi on;
  root    /var/www; # здесь содержится путь до директории с файлом "block.html"
}
```

8) после внесения конфигурации на веб-сервер на хосте «AML» выпускаются SSH ключи для доставки файла списка и отправки команды на обновление конфигурации. Далее на портале «AML» создается сервис, следящий за актуальностью списка блокировок. Команда обновления конфигурации задается при создании сервиса:

```
nginx -s reload
```

13.3 Подготовка веб-сервера к блокировкам сессий для Apache

Для синхронизации работы сервера «AML» и веб-сервера, на котором необходимо блокировать сессии, нужно внести изменения в конфигурационные файлы. Для подготовки сервера Apache к блокировкам сессий необходимо выполнить следующие настройки:

1) создать файл blacklist.conf в директории с конфигурационными файлами или в любом удобном месте, например в /usr/local/apache2/conf;

2) в файл основной конфигурации веб-сервера htdocs (apache2.conf) в блок с расположением содержимого сайта добавить строку, содержащую обращение к файлу черного списка. В нем проверяется соответствие полей «IP-адрес» и «User-Agent» из запроса с заблокированными комбинациями и при нахождении переменной block_token присваивается значение. В конце файла стоит условие – если переменная block_token не пустая, запретить доступ:

```
Include conf/blacklist.conf
Require all granted
Deny from env=block_token
```

3) пример файла blacklist.conf – переменная $block_token содержит код блокировки, по которому можно отследить заблокированную сессию и управлять ее блокировкой:

```
    # Для юзер агента требуется экранировать одинарные кавычки
    SetEnvIfExpr "%{REMOTE_ADDR} == '<IP>' && %{HTTP_USER_AGENT}
== '<UA>'" block_token="block_token"       # В общем виде
    SetEnvIfExpr     "%{REMOTE_ADDR}     ==     '10.0.1.1'     &&
%{HTTP_USER_AGENT}  ==  'badbot'"  block_token="block_token"  #
Блокировка по IP-адресу и юзер агенту
    SetEnvIfExpr     "%{REMOTE_ADDR}     ==     '10.0.1.1'     &&
%{HTTP_USER_AGENT} == ''" block_token="block_token"           #
Блокировка по IP-адресу и пустому юзер агенту
    SetEnvIfExpr      "%{REMOTE_ADDR}      ==      '10.0.1.1'"
block_token="block_token"
```

4) после включения черного списка можно добавить код, подменяющий 403 ответ на html-документ, содержащий для информации токен блокировки:

```
SetEnvIf Host ^ suppress-error-charset
ErrorDocument 403 "<head><meta http-equiv='Content-Type' content='text/html; charset=utf-8'></head><h3><style>html { color-scheme: light dark; } body { width: 35em; margin: 0 auto; font-family: Tahoma, Verdana, Arial, sans-serif; } </style>Вы заблокированы, обратитесь к администратору.</h3> <h3>Ваш кот ^__^
```

5) для подключения внешнего файла, подменяющего страницу блокировки, требуется доставить на сервер файл block.html (находится на сервере «AML» по пути /srv/aml/blocker/block.html), изменить его разрешение на .shtml, и добавить код:

```
Options +Includes
AddType text/html .shtml
AddOutputFilter INCLUDES .shtml
ErrorDocument 403 /block.shtml
```

6) после внесения конфигурации на веб-сервер на хосте «AML» выпускаются SSH ключи для доставки файла списка, и отправки команды на обновление конфигурации. Далее на портале «AML» создается сервис, следящий за актуальностью списка блокировок. Команда обновления конфигурации задается при создании сервиса:

```
apachectl -k graceful
```

13.4 Настройка сервера для блокировок

Для настройки блокировки событий необходимо выполнение трех обязательных требований:

– настроена потоковая обработка журналов;

– имеется сетевой доступ до сервера;

– на веб-сервере существует пользователь с правами, достаточными для выполнения команды обновления конфигурации и правами на запись файла blacklist.conf, а также возможностью подключения по SSH по паролю (требуется только один раз, для доставки SSH-ключей).

Если данные условия выполняются, то для сервера можно настроить блокировку атакующих сессий с помощью следующих действий:

1) настроить конфигурации веб-сервера, что представлено в соответствующем описании (Подраздел 13.2 – для сервера Nginx, Подраздел 13.3 – для сервера Apache);

2) в панели администратора перейти в раздел «Серверы» в блоке «Приложение блокировок» (Рисунок 242);

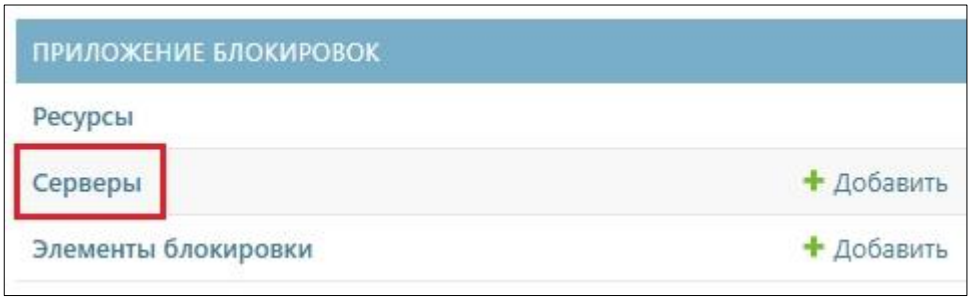

Рисунок 242 – Переход к разделу «Серверы»

3) нажать на кнопку «Добавить сервер +» (Рисунок 243);

Рисунок 243 – Добавление нового сервера

4) на открывшейся странице добавления сервера указать параметры:

– «Название сервиса» – наименование, предназначенное для идентификации сервиса в Системе, аналогичное сервису потоковой обработки, является обязательным;

– «Адрес сервера» – IP-адрес или доменное имя веб-сервера, на которые будет отправляться черный список, является обязательным;

– «SSH порт» – используемый для подключения порт. Значение в данном поле является обязательным, если используется нестандартный SSH порт;

– «Удаленный пользователь» – имя пользователя учетной записи пользователя для подключения по SSH, является обязательным;

– «Удаленный пароль» – пароль от указанной учетной записи пользователя для подключения по SSH, является обязательным;

– «Remote blacklists dir» – абсолютный путь до директории с blacklist.conf на веб-сервере, является обязательным;

– «Update command» – команда которой будет обновляться конфигурация, является обязательным;

– «Тип сервера» – Nginx или Apache. По завершении заполнения формы создания нажать кнопку «Сохранить» (Рисунок 244);

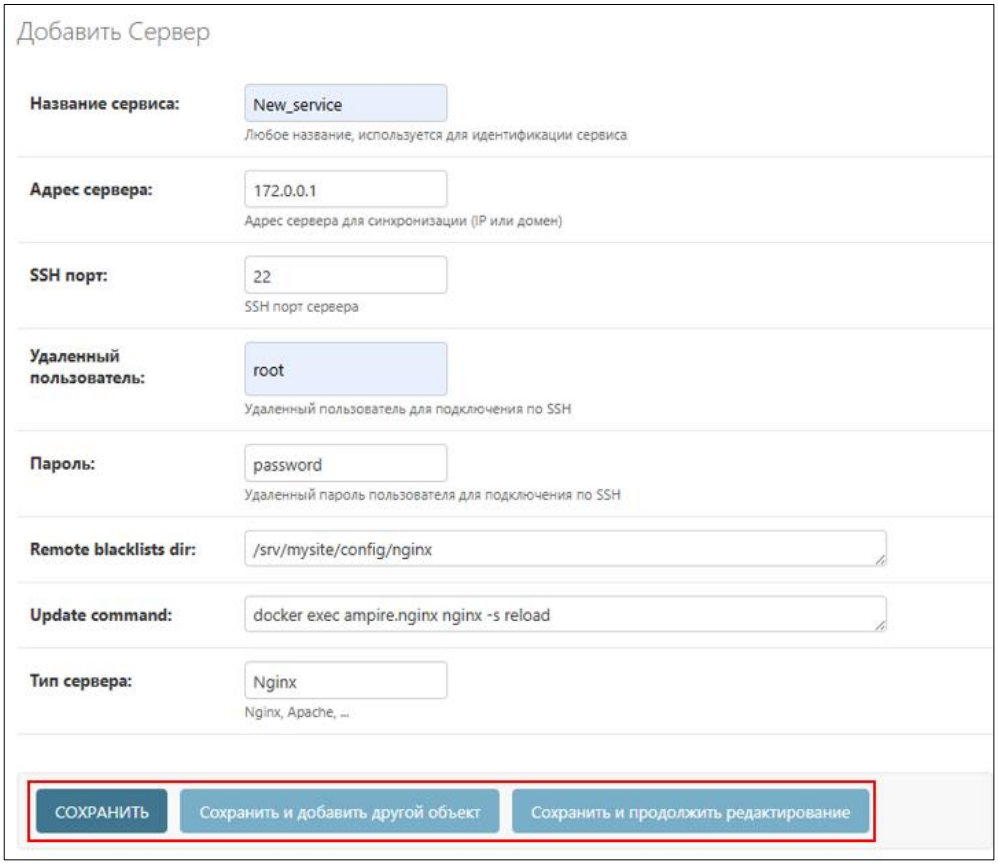

Рисунок 244 – Добавление информации о новом сервере

5) перейти в раздел «Ресурсы» в блоке «Приложение блокировок» (Рисунок 245);

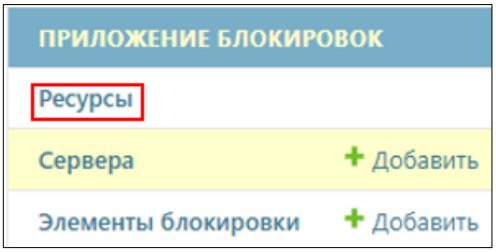

Рисунок 245 – Переход к разделу «Ресурсы»

6) выбрать из списка ресурс, на котором необходимо настроить блокировку (Рисунок 246);

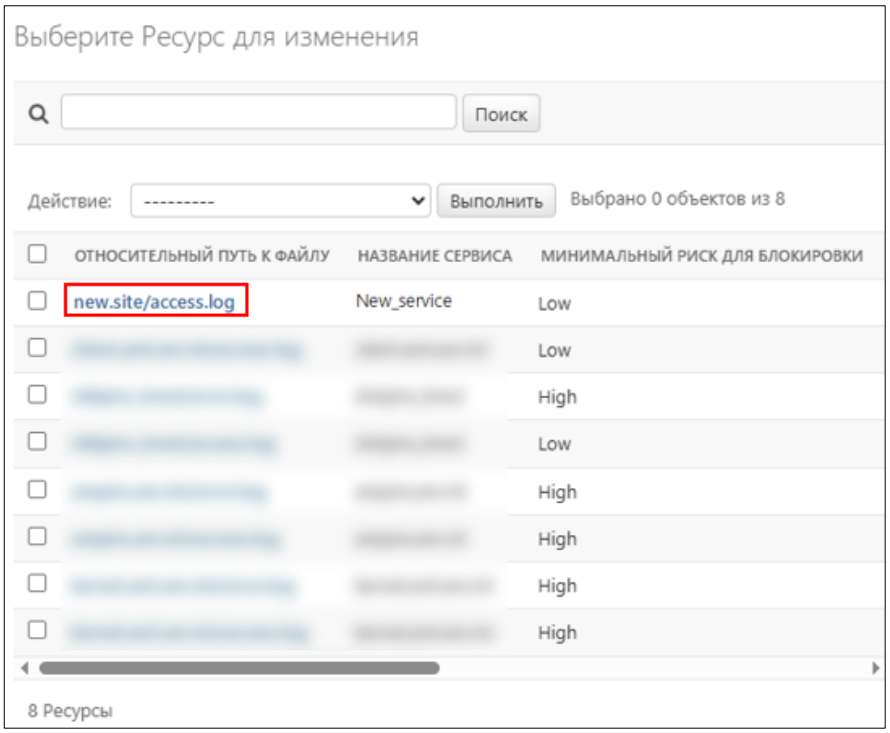

Рисунок 246 – Выбор ресурса для настройки блокировок

7) на странице ресурса в блоке «Конфигурация» настроить параметры блокировки (Рисунок 247):

– «Минимальный риск блокировки»;

– «Время блокировки»;

– «Использование «User-Agent»»;

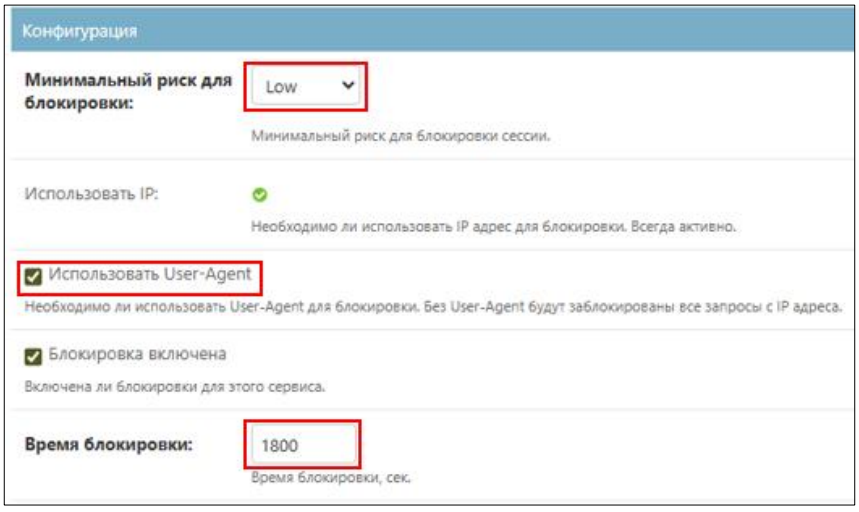

Рисунок 247 – Настройка сервера для блокировок

8) включить блокировку, активировав чекбокс (Рисунок 248);

Рисунок 248 – Включение блокировки

9) сохранить настройки (Рисунок 249);

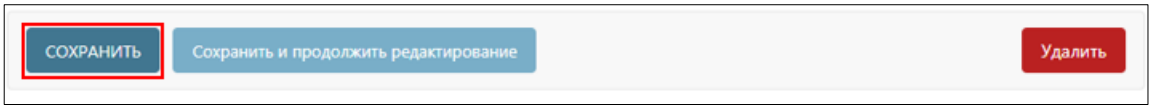

Рисунок 249 – Сохранение настроек сервера

10) после выбора и сохранения всех указанных настроек блокировка атакующих сессий на веб-сервере будет активирована и начнет работать с указанными параметрами.