NTechnology | SIEM

Руководство пользователя

НЦОТ

Содержание

1.Общая информация о системе

1.1 О документе

Этот документ содержит справочную информацию и инструкции по настройке и администрированию системы, предназначенной для сбора и анализа событий информационной безопасности (Security Information and Event Management system) «NTechnology SIEM» (далее – NT SIEM). Содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности.

Комплект документации NT SIEM включает в себя следующие документы:

- Этот документ;
- Руководство по созданию запросов – содержит описание наборов запросов и результаты применения этих запросов;
- Руководство по установке – содержит информацию для внедрения продукта в инфраструктуру организации: инструкции по установке, первоначальной настройке и удалению продукта;
- Руководство по написанию правил – содержит рекомендации по созданию правил нормализации, агрегации, корреляции и обогащения событий.

1.2 Краткое описание возможностей системы

Система NT SIEM предоставляет следующие функциональные возможности:

- Активный и пассивный сбор журналов событий с различных источников;
- Мониторинг событий и инцидентов, а также агентов и состояния системы;
- Визуализация данных в форме дашбордов;
- Анализ журналов событий в соответствии с правилами нормализации, корреляции, агрегации и обогащения;
- Формирование инцидентов на основе процессов агрегации, обогащения и корреляции;
- Реагирование на инциденты информационной безопасности;
- Хранение событий и инцидентов информационной безопасности;
- Фильтрация по различным параметрам событий и инцидентов, в том числе с использованием избранных запросов для быстрого доступа к фильтрам по событиям;

- Использование готовой базы правил с возможностью дополнительно загрузить системные правила, а также создать пользовательские правила и табличные списки;
- Отправка уведомлений пользователям в рамках веб-приложения и по электронной почте;
- Выгрузка отчетов за настраиваемый период времени;
- Интеграция с SOAR-системами.

2.Основные элементы интерфейса системы

В данном разделе описаны основные элементы интерфейса NT SIEM, доступные после успешного входа в систему. Работа с NT SIEM осуществляется через графический пользовательский интерфейс на основе ролевой модели (Приложение А).

2.1 Главное меню

Главное меню расположено в левой части страницы и обеспечивает доступ к основным функциям системы. Главное меню содержит название системы, логотип, страницы и группы страниц:

- «Панель мониторинга»;
- «События»;
- «Инциденты»;
- «Агенты»;
- «Отчеты»;
- «База правил»;
- «Настройки системы».

Следует обратить внимание, что в стандартной ролевой модели доступ к группам страниц «База знаний» и «Настройки системы» ограничен (см. Приложение А).

По умолчанию главное меню отображается в свернутом виде. Разворачивается при нажатии на иконку < и сворачивается при нажатии на иконку >.

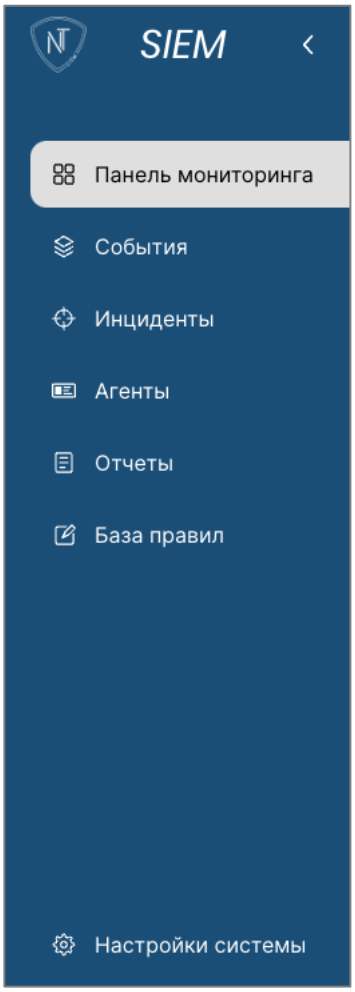


Рисунок 1– Главное меню в развернутом виде

Рисунок 2 – Главное меню в свернутом виде

2.2 Верхняя навигационная панель

В верхней навигационной панели (рис. 3) расположены названия доступных на выбранной странице категории.

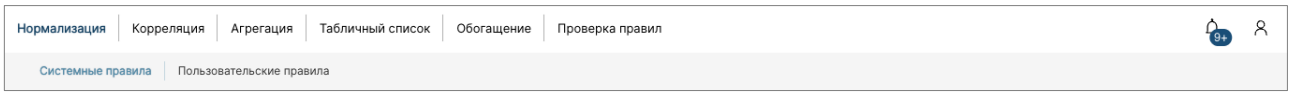


Рисунок 3 – Верхняя навигационная панель

В верхней навигационной панели также размещены статичные кнопки:

– Профиль. При нажатии на кнопку профиля появляется выпадающий список с кнопками: Профиль для просмотра информации о пользователе, Справка для скачивания эксплуатационной документации и Выйти для выхода из учетной записи и возврата на страницу авторизации.

– Уведомления. При нажатии на кнопку открывается список уведомлений. Рядом с иконкой уведомлений после действий пользователя в системе всплывают напоминания о состоянии лицензии, ответы системы об успешности или неуспешности операций, а также другие информационные сообщения. Можно удалить одно уведомление нажав на иконку , которая находится рядом с выбранным уведомлением, а также очистить список уведомлений, нажав кнопку Очистить все внизу списка уведомлений.

2.3 Панель инструментов

Панель инструментов (рис.4) расположена под верхней навигационной панелью. Состав кнопок на панели инструментов зависит от страницы.

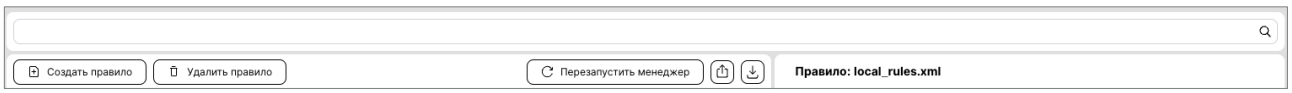


Рисунок 4 – Панель инструментов

Следует обратить внимание, что при нажатии на определенные кнопки, например, «Удалить», будет появляться уведомление для подтверждения действия.

2.4 Рабочая область

Под панелью инструментов расположена рабочая область (рис.5), наполнение которой различается от страницы к странице. Она может содержать текстовую информацию и поля для ее ввода, а также таблицы и графики. По умолчанию отображаемые данные в списках отсортированы от новых к более старым записям. На некоторых страницах может быть поисковая строка для настройки фильтрации отображаемых данных на странице.

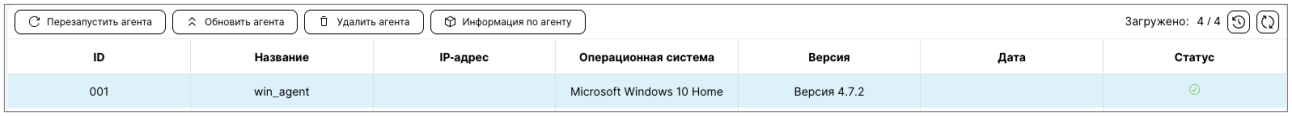


Рисунок 5 – Рабочая область

Рабочая область может быть разделена на несколько частей (рис.6), а также иметь кнопки для выполнения определенных функций.

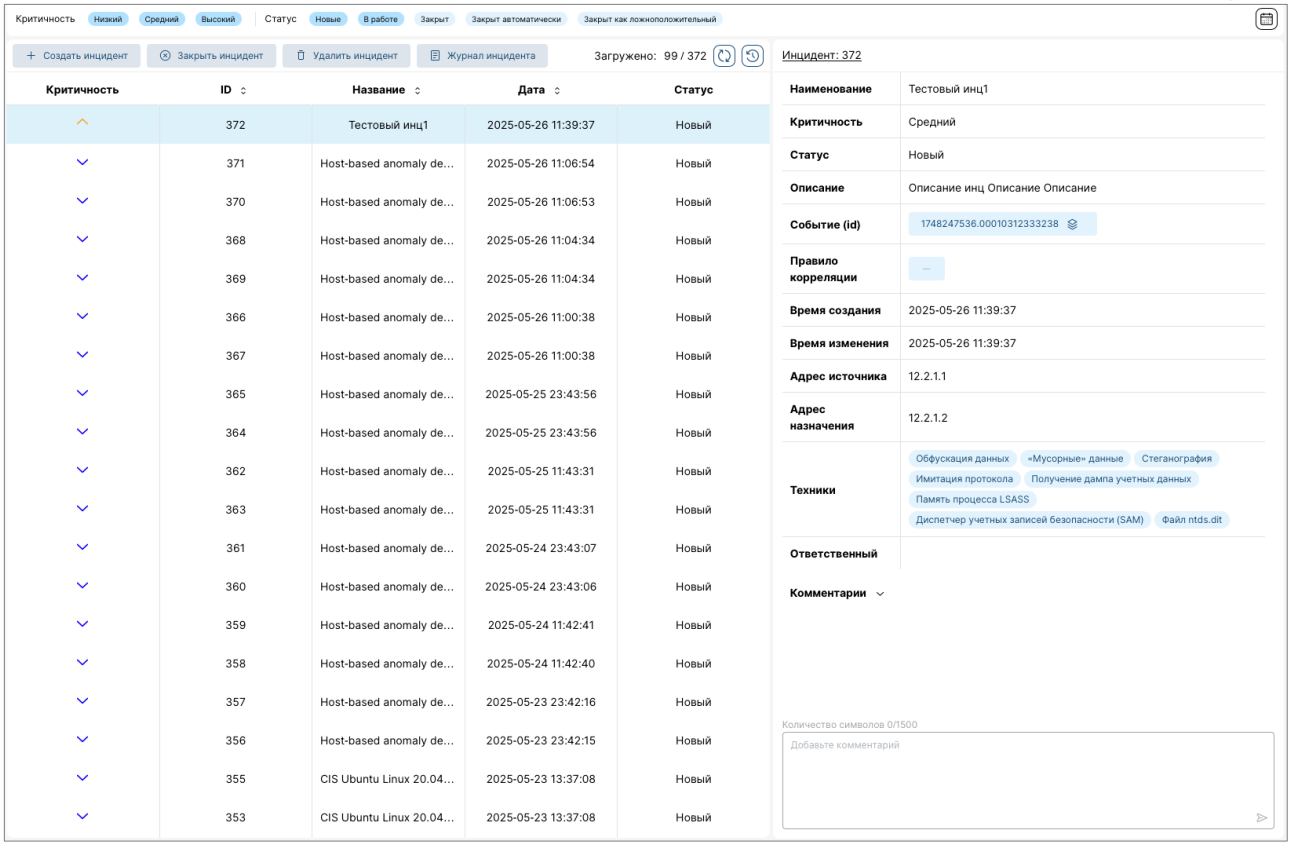


Рисунок 6 – Рабочая область с боковой панелью

При разделении рабочей области в правой части экрана располагается боковая панель для просмотра выбранного элемента таблицы.

3.Основные процессы в системе

3.1 Интерфейс раздела «Панель мониторинга»

При входе в NT SIEM по умолчанию открывается страница «Панель мониторинга». На данной странице можно просмотреть информацию в виде виджетов, настраивать период времени для фильтрации отображаемой информации, а также настраивать состав виджетов, представленных на странице.

В рабочей области страницы расположены преднастроенные виджеты:

- Круговая диаграмма с информацией об агентах, разделенных по статусам (подключен, отключен, в ожидании);
- Круговая диаграмма с информацией об инцидентах, разделенных по статусам (новый, в работе, закрыт, закрыт как ложноположительный, закрыт автоматически);

- Круговая диаграмма с информацией об инцидентах, разделенных по уровню критичности (низкий, средний, высокий);
- Виджет с информацией о количестве ненормализованных событий;
- Линейный график с информацией о количестве событий в секунду, поступающих в систему, и их среднее значение за выбранный период времени;
- Комбинированный виджет, представленный текстом и диаграммой, с информацией о системе: операционная система, процессор, память, IP-адрес, серверное время, время работы, соотношение занятой и свободной памяти (как внутренней, так и внешней).

Следует обратить внимание, что при первом входе в систему после установки NT SIEM некоторые виджеты будут пустыми, вследствие отсутствия зарегистрированных агентов в системе, информации о собранных событиях и выявленных инцидентах.

3.2 Работа с дашбордами и виджетами

Информация на виджетах обновляется автоматически (по умолчанию каждые 60 секунд). Для обновления виджета вручную необходимо нажать на кнопку – виджет обновится без дополнительных настроек и подтверждений.

При необходимости, можно отфильтровать информацию, представленную на виджетах, по определенному временному периоду. Для этого необходимо нажать на кнопку «Календарь», после чего открывается окно с возможностью выбора временного интервала (рис.7).

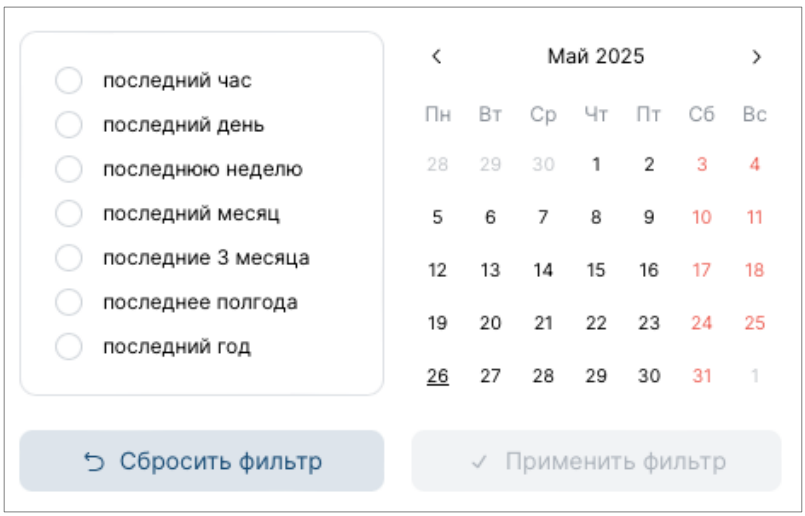


Рисунок 7 – Фильтрация

Для применения выбранных параметров необходимо нажать на кнопку «Применить фильтр» в окне. В свою очередь, при нажатии на кнопку «Сбросить

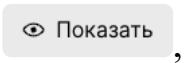
фильтр» происходит очистка выбранных параметров и возвращение виджета в исходное состояние (по умолчанию). Закрыть фильтр можно путем нажатия на любую область вне. Обратите внимание, что подчеркнутое число – сегодняшняя дата.

Для виджетов с информацией о ненормализованных событиях и с информацией об инцидентах по умолчанию установлен фильтр, отображающий данные за весь период, а для линейного графика с информацией о количестве событий в секунду – один день. Также для виджета с информацией о количестве событий в секунду настроено автообновление раз в 3 минуты, а для остальных – раз в минуту.

Следует обратить внимание, что при переходе на другую страницу фильтры не будет сохраняться.

Для настройки отображения виджетов на панели мониторинга, а именно возможности изменения их количества и порядка, в правом верхнем углу страницы предусмотрена кнопка 

. При нажатии на нее открывается боковое модальное окно, в котором отображается текущее состояние виджетов (рис.8). При нажатии на кнопку 

виджет станет недоступен для просмотра, и кнопка изменится на кнопку 

, при нажатии на которую виджет будет доступен для просмотра.

Можно также изменить порядок элементов на странице, для этого необходимо зажать элемент и перетащить его в любое место в списке. Порядок виджетов моментально изменится в соответствии со списком в модальном окне.

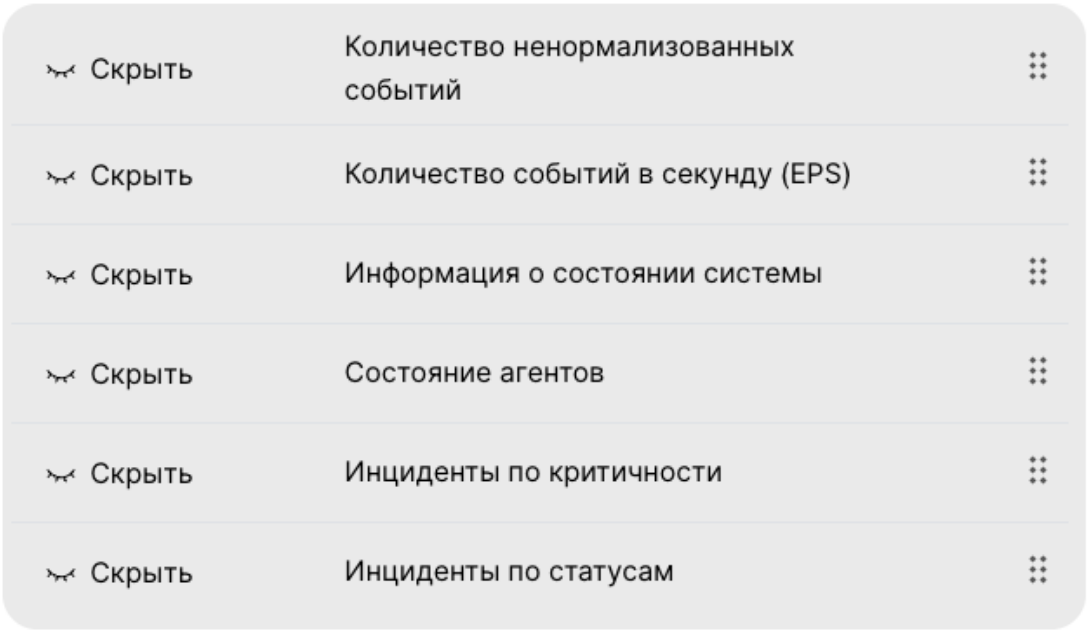


Рисунок 8 – Отображение виджетов

3.3 Интерфейс раздела «События»

3.3.1 Страница «События»

Группа страниц предназначена для работы с событиями и представлена страницами: «События» и «Списки запросов». На странице «Списки запросов» можно просматривать, создавать, редактировать, пополнять и удалять списки с запросами, а также выполнять экспорт и импорт списков.

На странице «События» в таблице представлена информация как по нормализованным, так и ненормализованным событиям. На странице «События» можно просматривать перечень событий и информацию о них, выполнять фильтрацию и привязку событий к инциденту, а также выгружать события в файл в формате `.csv`.

Нормализованным считается то событие, которое прошло процесс приведения данных к нормализованному виду и имеет уровень критичности (см. Руководство по написанию правил). Уровень критичности можно посмотреть в поле `level`. Событию может быть присвоен уровень от 0 до 15. При уровне критичности события 7 и выше создается инцидент.

Панель инструментов страницы «События» представлена поисковой строкой для ввода запросов (см. Руководство по написанию запросов) и кнопками для работы с событиями:

 – для фильтрации элементов в таблице по временному периоду;

 – для создания и сохранения нового поискового запроса;

 – для работы со списками запросов;

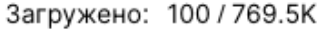
 – для обновления таблицы;

 – для настройки периодичности обновления таблицы;

 – для экспорта событий;

– для связи выделенного в таблице события с существующим инцидентом. Для работы с кнопкой необходимо выбрать элемент из списка;

–для фильтрации данных в таблице по категориям: все события, нормализованные или ненормализованные события;



– счетчик событий, показывающий количество отображаемых событий из числа всех событий.

Рабочая область страницы разделена на две части: левая часть представляет собой таблицу с перечнем событий, правая – боковую панель с подробной информацией о выбранном событии, разбитой по категориям.

3.3.2 Страница «Списки запросов»

На странице «Списки запросов» представлена информация по спискам запросов. Панель инструментов на странице «Списки запросов» представлена совокупностью кнопок:

– для регистрации нового списка запросов;

– для удаления списка запросов. Для работы с кнопкой на панели инструментов необходимо выбрать элемент из перечня;


– для экспорта списков запросов. Для работы с кнопкой на панели инструментов необходимо выбрать элемент(-ы) из перечня;


– для импорта списков запросов.

Рабочая область страницы разделена на две части: левая часть представляет собой перечень списков запросов, правая – боковую панель с подробной информацией о выбранном списке и кнопками для дополнительных действий.

3.4 Работа с событиями

3.4.1 Фильтрация данных на странице «События»

По умолчанию отображаемые данные в таблице отсортированы от новых к более старым записям. При необходимости, можно отфильтровать информацию по определенному временному периоду. Для этого необходимо нажать на кнопку «Календарь»  , после чего откроется окно с возможностью выбора временного интервала (рис.9). Закрыть фильтр также можно путем нажатия на любую область вне.

Для применения выбранных параметров необходимо нажать на кнопку «Применить фильтр» в окне. В свою очередь, при нажатии на кнопку «Сбросить фильтр» происходит очистка выбранных параметров и обновление данных в соответствии с установленным параметром по умолчанию (за весь период).

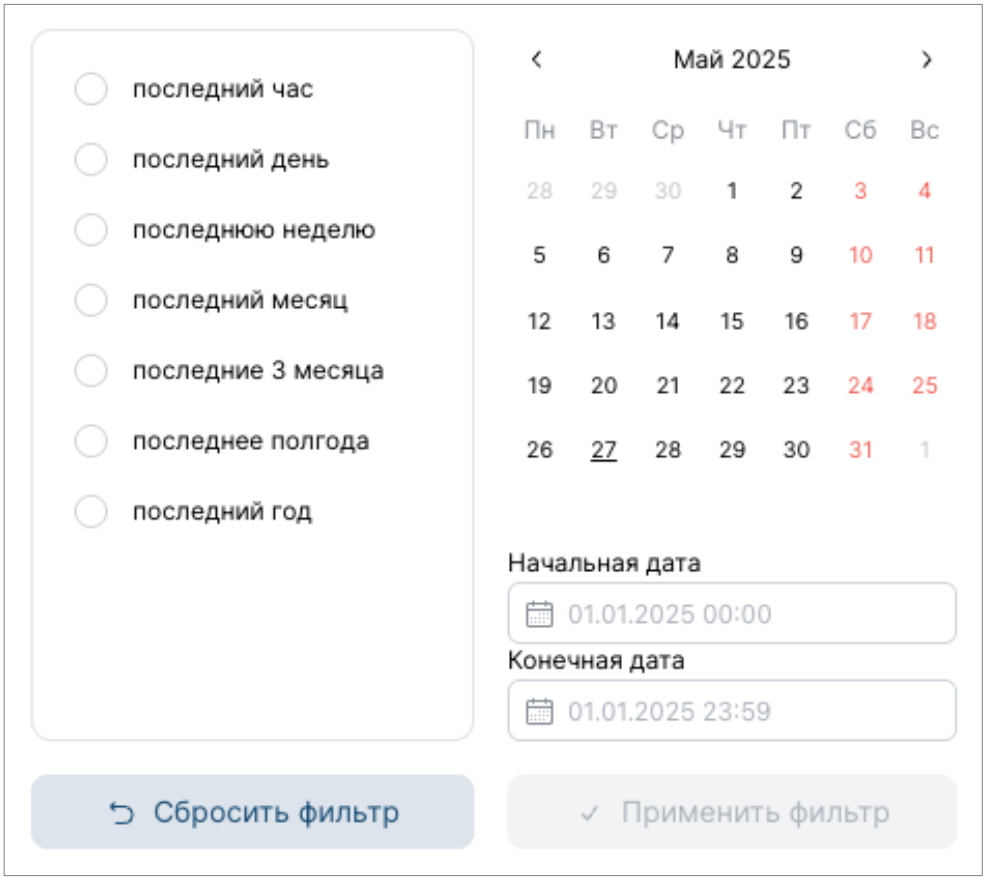


Рисунок 9 – Компонент «Календарь» для фильтраци по дате и времени

Для обновления данных в таблице необходимо нажать на кнопку , настроить период автоматического обновления данных в меню, открывающемся при нажатии на (по умолчанию – пятнадцать минут).

Для фильтрации событий по определенным критериям можно использовать поисковую строку и язык запросов (см. Руководство по созданию запросов).

Информация о событии в левой части рабочей области разделена по полям (например, `location`, `agent.name` и т.п.), при нажатии на значение которых появляется выбор оператора (`OR`, `AND` или `NOT`), который, соответственно, будет добавлен в поисковую строку для быстрой навигации по событиям (рис.10). А для поля корреляции `id` предусмотрена возможность просмотра правила, по которому было обработано событие.

В свою очередь поля событий распределены по категориям: служебные, поля нормализации и поля корреляции.

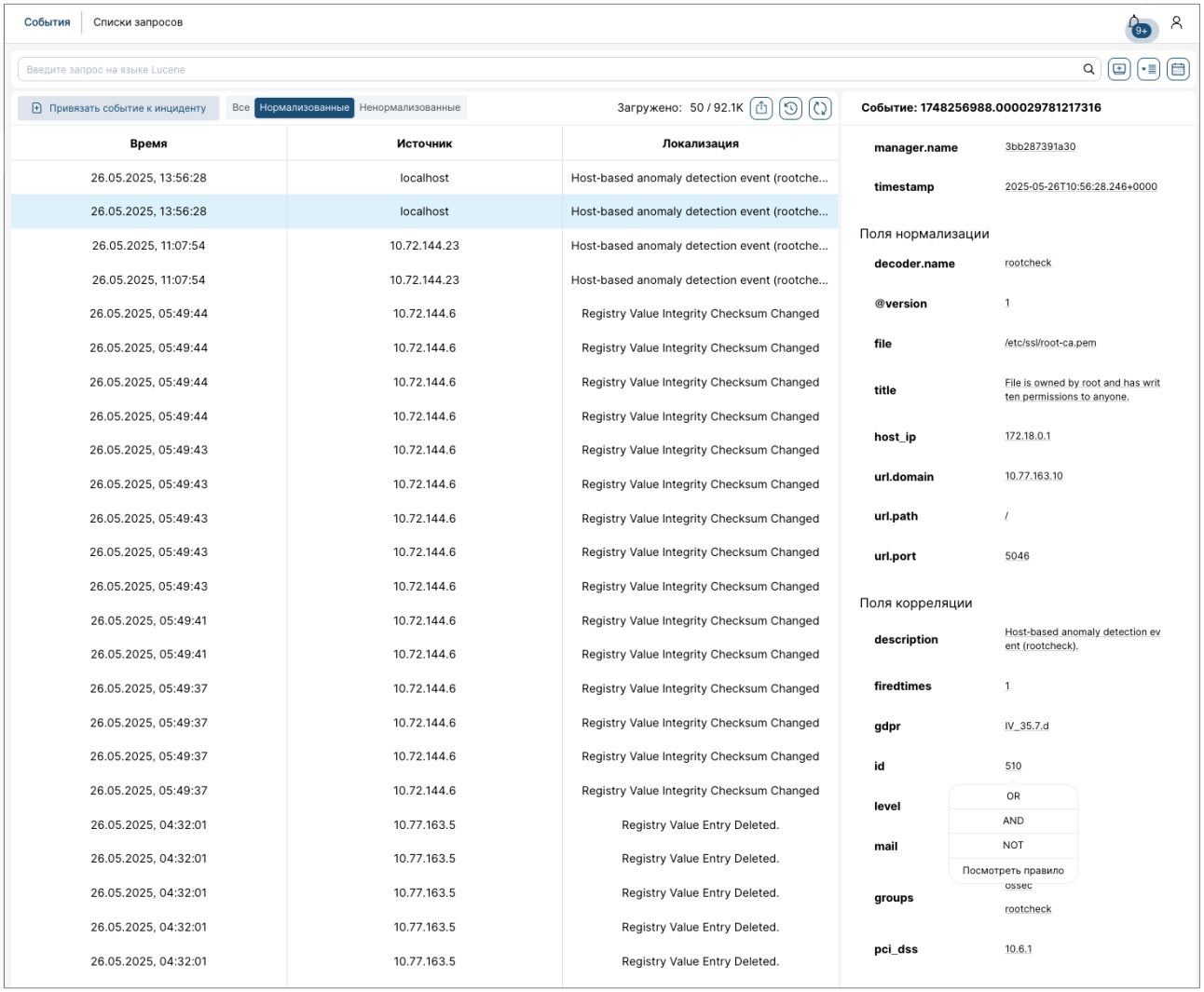


Рисунок 10 – Быстрый поиск по событиям

Следует обратить внимание, что можно скопировать `full_log` (событие). Для этого следует навести курсов мыши на данное поле и нажать на элемент .

3.4.2 Привязка события к инциденту

Для установки связи события и инцидента необходимо выделить событие и нажать на кнопку Привязать событие к инциденту. Далее откроется список с доступными для связи инцидентами (рис. 11).

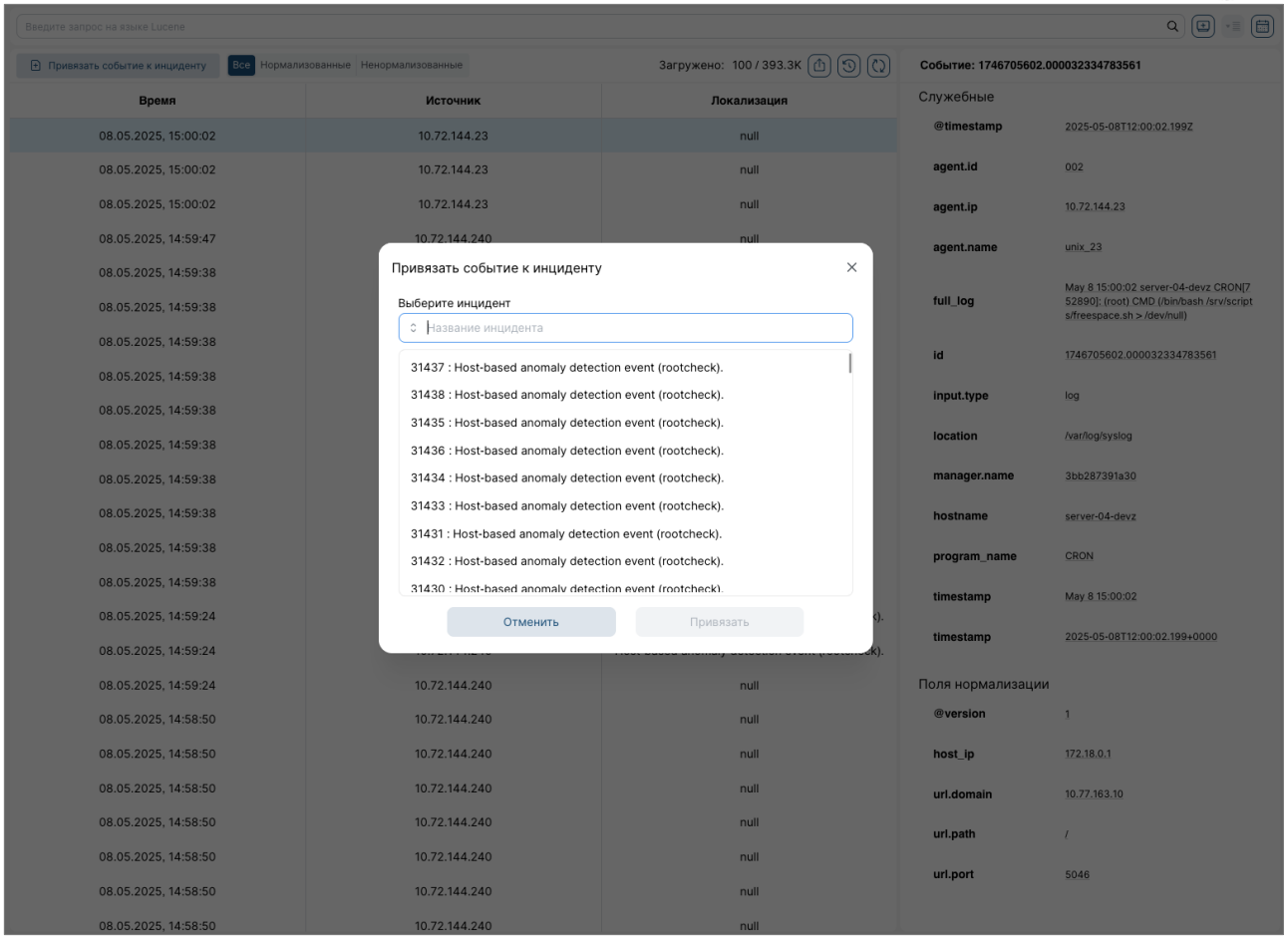


Рисунок 11 – Функция привязки события к инциденту

Следует выбрать существующий инцидент из списка и нажать на кнопку «Привязать». Для закрытия окна необходимо нажать на кнопку ✕ или на кнопку «Отменить». Обратите внимание, что к одному инциденту можно привязать несколько событий.

3.4.3 Выгрузка событий

Для того, чтобы выгрузить события, необходимо на элементе управления выбрать необходимую вкладку, например Все | Нормализованные **Ненормализованные**. Далее выбрать период времени или отфильтровать список событий и нажать на кнопку  . По умолчанию, установлен лимит выгрузки за весь период с ограничение в 100 тысяч строк.

3.4.4 Работа с пользовательскими запросами

Для сохранения пользовательских запросов для последующего быстрого доступа к ним необходимо нажать на кнопку  : откроется модальное окно (рис.12) с полями для заполнения. Следует обратить внимание, что если был

заранее введен запрос в поисковую строку, а затем нажата кнопка , то поле «Запрос» (рис. 12) будет заполнено введённым в поисковую строку запросом.

Следует ввести данные во все поля, а в поле «Список запросов» выбрать к какому списку запросов отнести создаваемых запрос. Поля «Наименование», «Запрос» и «Список запросов» являются обязательными.

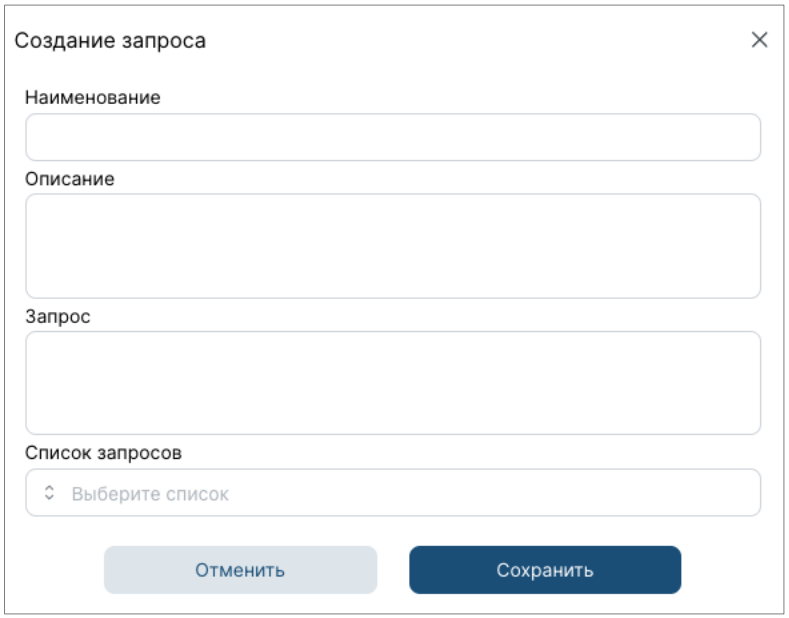


Рисунок 12 – Сохранение запроса

Для сохранения запроса нужно нажать на кнопку «Сохранить», а для отмены – «Отменить». Следует обратить внимание, что при нажатии на кнопку процесс сохранения будет прерван и все введенные данные будут потеряны. Результат операции отобразится в уведомлениях.

Для того, чтобы использовать сохраненный запрос, необходимо нажать на кнопку . После нажатия откроется информация с доступными списками запросов (рис.13). Следует выбрать список запросов, где находится интересующий запрос, нажать на и выбрать запрос из предложенных. После нажатия на запрос, он отобразится в поисковой строке. Далее следует произвести поиск.

Если в списке запросов пустой, то есть относящихся к нему запросов нет, то список будет выделен тусклым серым цветом и элемент будет неактивным (рис. 13)

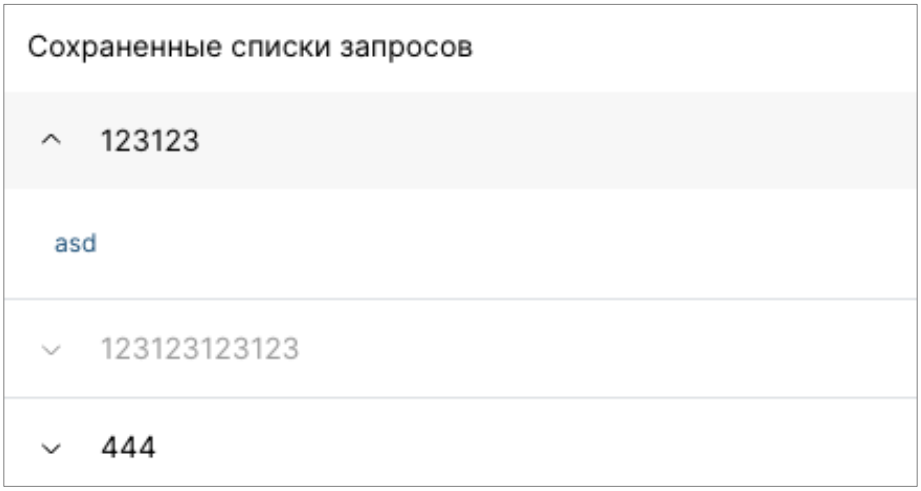


Рисунок 13 – Сохраненные списки запросов

3.4.5 Работа с пользовательскими списками запросов

Для того, чтобы создать новый список запросов следует перейти на страницу «Списки запросов» и нажать на кнопку Создать список. Далее откроется модальное окно (рис.14), где необходимо заполнить поля. Поле «Наименование» является обязательным.

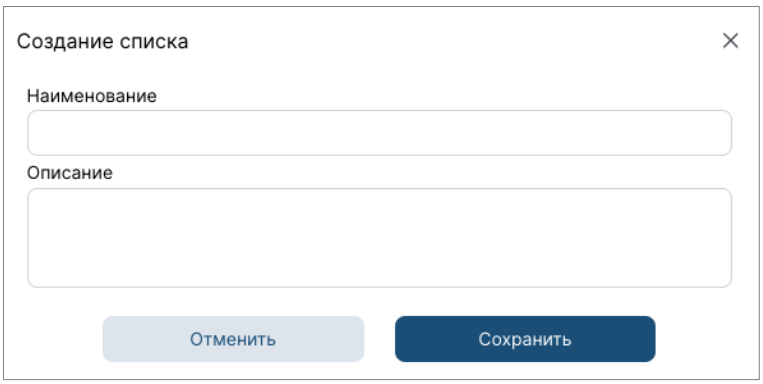


Рисунок 14 – Создание списка запросов

Для сохранения запроса нужно нажать на кнопку «Сохранить», а для отмены – «Отменить». Следует обратить внимание, что при нажатии на кнопку ✕ процесс создания будет прерван и все введенные данные будут потеряны.

Рабочая область страницы разделена на две части: левая часть представляет собой перечень списков запросов, правая – боковую панель с подробной информацией о выбранном списке и кнопками для дополнительных действий (рис15).

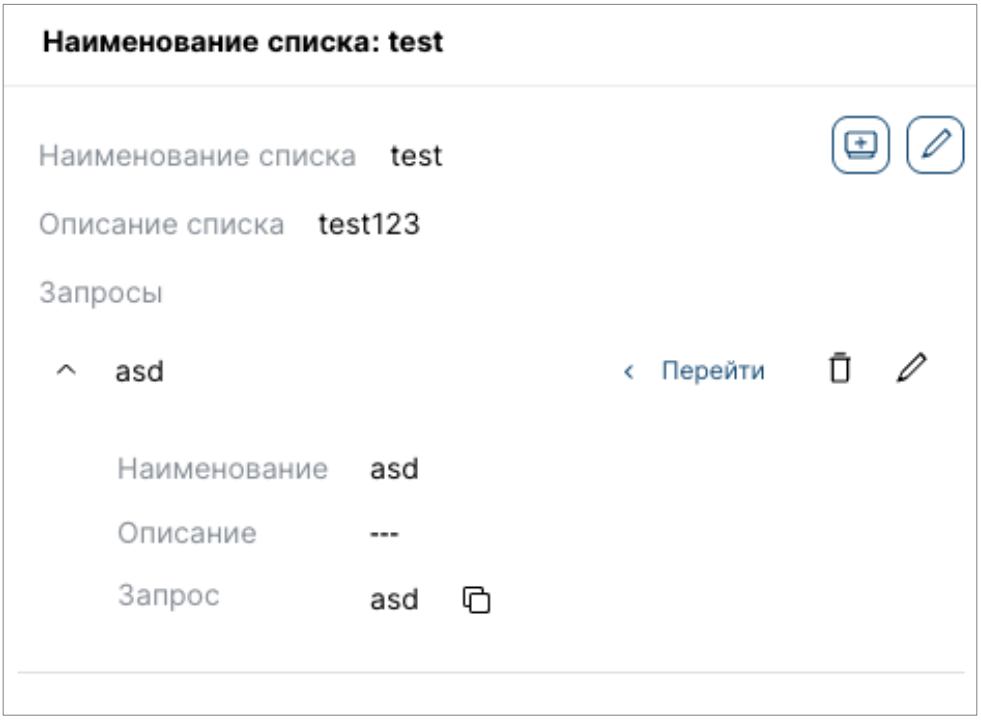


Рисунок 15 – Список пользовательских запросов

В целях управления наполнением списка запросов можно:

- просмотреть подробнее запрос, нажав на кнопку ^.
- добавить запрос в список, нажав на кнопку . Откроется модальное окно (рис.12) с возможностью заполнения полей. Обратите внимание, поле «Список запросов» будет заполнено выбранным списком, однако поле можно редактировать.
- отредактировать запрос, нажав на кнопку . Откроется модальное окно (рис.12) с заполненными полями в соответствии с выбранным запросом. Все поля будут доступны для редактирования.
- удалить запрос из списка, нажав на кнопку . В случае успешности появится соответствующее уведомление.
- Нажав на кнопку Перейти (рис.16), произойдет переход на страницу «События», где данные будут сразу отфильтрованы по выбранному запросу, а текст запроса введен в поисковой строке;
- Скопировать запрос нажатием на элемент . В случае успешности, система уведомит пользователя и элемент изменится на .

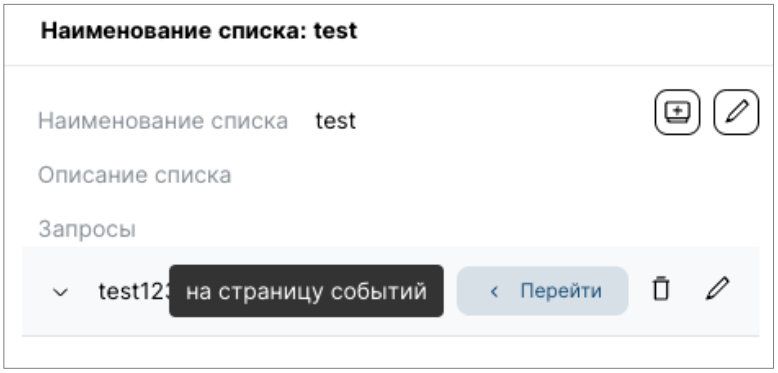


Рисунок 16 – Переход на страницу для быстрой фильтрации данных

Для того чтобы отредактировать список запросов следует нажать на кнопку . После чего появляется модальное окно (рис.17), в котором поля «Название» и «Описание» становятся доступны для изменения.

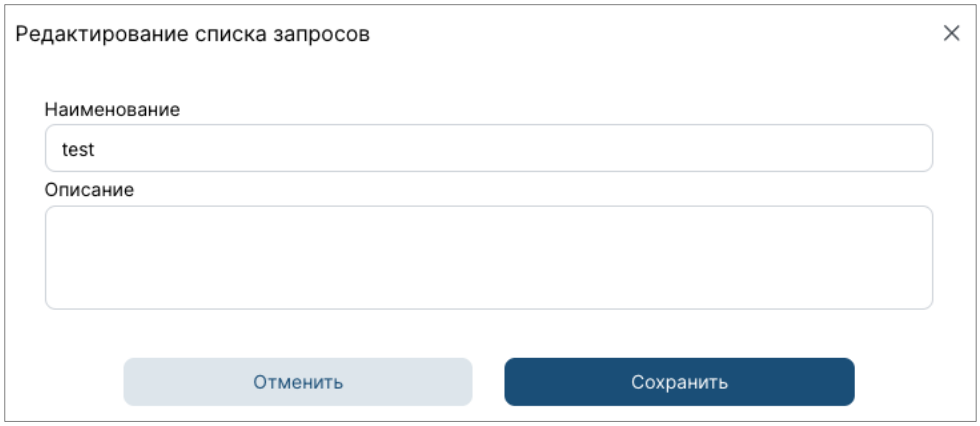


Рисунок 17 – Редактирование списка запросов

Для того, чтобы экспортировать список запросов необходимо выбрать его в перечне и нажать на кнопку . Список запросов будет сохранен в формате json.

Для того, чтобы импортировать список запросов, следует нажать на кнопку и в открывшемся проводнике выбрать загружаемый файл. Результат загрузки отобразится в уведомлениях.

Для того, чтобы удалить список запросов необходимо выбрать элемент в перечне и нажать на кнопку Удалить список, подтвердить действие в всплывающем уведомлении. Результат операции отобразится в уведомлениях.

3.5 Интерфейс раздела «Инциденты»

Страница предназначена для работы с инцидентами. На странице представлены функции просмотра, создания, редактирования, удаления

инцидентов, их фильтрации по нескольким категориям, а также просмотра истории изменения инцидента.

Панель инструментов представлена группой фильтров и совокупностью кнопок:

– для регистрации нового инцидента вручную;

– для закрытия инцидента вручную;

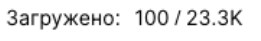
– для удаления инцидента;

– для просмотра истории изменения инцидента;


– для фильтрации элементов в таблице по временному периоду;


– для обновления данных вручную;


– настройка периодичности обновления таблицы;



– счетчик инцидентов, показывающий количество отображаемых инцидентов на странице из числа всех инцидентов.

Для работы с кнопками на панели инструментов необходимо выбрать инцидент из списка.

Рабочая область страницы разделена на две части: левая часть представляет собой список с инцидентами, правая – боковую панель с подробной информацией о выбранном инциденте.

Для каждого инцидента в таблице указан набор параметров:

- Критичность – уровень критичности инцидента. Показатели критичности: низкий  , средний  и высокий  ;
- ID – идентификационный номер инцидента;
- Название – наименование инцидента;
- Дата – дата и время создания инцидента;
- Статус – статус инцидента. Показатели статуса: новый, в работе, закрыт, закрыт автоматически, закрыт как ложноположительный.

Следует обратить внимание, что инциденту присваивается качественный уровень критичности, в зависимости от уровня события, на основе которого он был создан:

- Низкий  уровень критичности (из событий уровня 7-9);
- Средний  уровень критичности (из событий уровня 10-12);
- Высокий  уровень критичности (из событий уровня 13-15).

3.6 Работа с инцидентами

3.6.1 Фильтрация данных на странице «Инциденты»

По умолчанию отображаемые данные в таблице отсортированы от новых к более старым записям. При необходимости, можно отфильтровать информацию по определенному временному периоду. Для этого необходимо нажать на кнопку «Календарь»  , после чего откроется окно с возможностью выбора временного интервала (рис.9). Закрыть фильтр также можно путем нажатия на любую область вне.

Для применения выбранных параметров необходимо нажать на кнопку «Применить фильтр» в окне. В свою очередь, при нажатии на кнопку «Сбросить фильтр» происходит очистка выбранных параметров и обновление данных в соответствии с установленным параметром по умолчанию (за весь период).

Над панелью инструментов представлен набор фильтров инцидентов по критичности и статусу. Для установки фильтрации можно выбирать несколько маркеров критичности и статусов (рис.18).

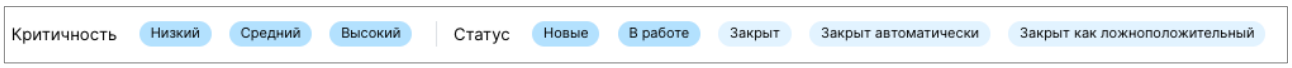


Рисунок 18 – Фильтры по статусу и критичности

Так же отфильтровать инциденты можно в таблице, при нажатии на поля «ID», «Дата» и «Название». При первом нажатии будет фильтрация по возрастанию, а при повторном нажатии меняется на противоположную.

Процесс фильтрации может быть осуществлен одновременно по нескольким параметрам.

3.6.2 Создание инцидента вручную

Для создания инцидента вручную следует нажать на кнопку на панели инструментов

. Далее появится модальное окно с полями (рис.19) для заполнения.

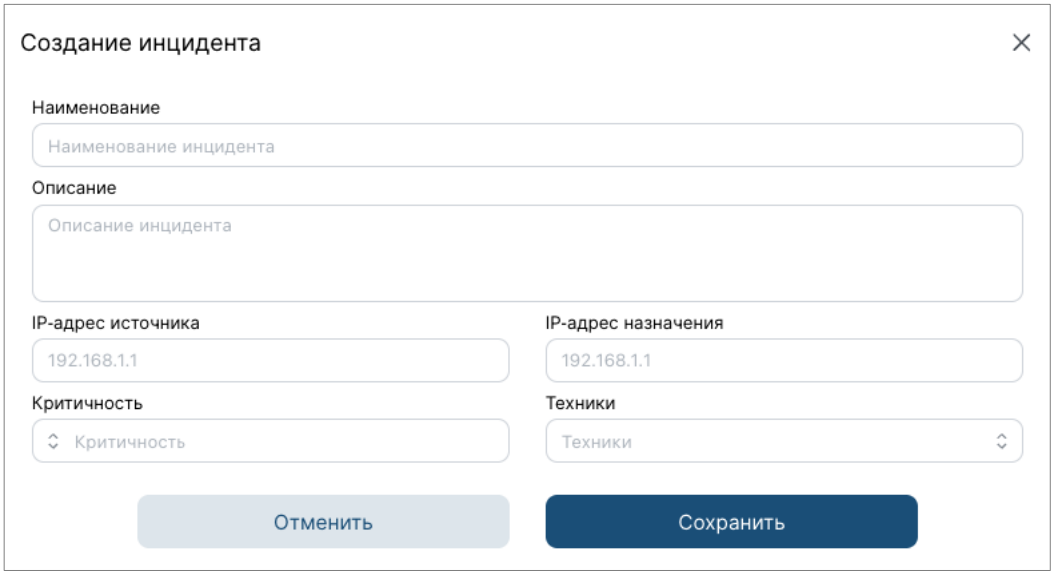


Рисунок 19 – Создание инцидента вручную

Следует обратить внимание, что в поле «Описание» есть ограничение в 60 символов, а в полях, содержащих IP-адреса, следует указывать данные в формате IPv4. В раскрывающемся списке «Критичность» необходимо выбрать уровень: высокий, средний, низкий, а в раскрывающемся списке «Техники» – техники MITRE ATT&CK.

Для сохранения инцидента необходимо нажать на кнопку «Сохранить». Далее происходит возврат на ранее активную страницу, добавление нового инцидента в систему и, соответственно, в таблицу, а также появляется уведомление «Инцидент успешно создан» (в случае неуспешности – уведомление «Не удалось создать инцидент»).

В случае если необходимо выйти из режима создания, следует нажать на кнопку «Отменить» или ✕, однако все введенные данные будут утеряны.

3.6.3 Отображение информации о конкретном инциденте, просмотр истории инцидента, комментарии

Для отображения полной информации в правой части рабочей области нужно выбрать инцидент в таблице (рис.20).

Для просмотра комментариев следует нажать на ⌄ и раскроется список со всеми комментариями, а для того, чтобы скрыть нажать на ^. Для того, чтобы оставить комментарий, необходимо в окне для ввода комментария ввести текст и нажать на ➢. Доступное количество символов для ввода – 1500.

Для перехода к дополнительной информации используются поля «Событие» и «Правило корреляции».

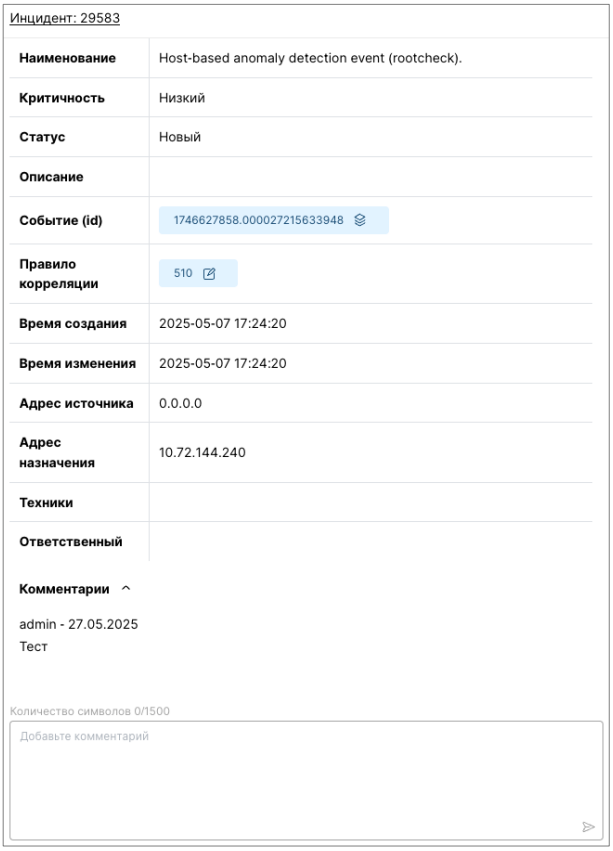


Рисунок 20 – Просмотр инцидента

Для просмотра информации о событии следует нажать на кнопку идентификатора события вида 1745394747.000154580280040, после чего появится модальное окно (рис.21) с подробной информацией о событии, где все поля разделены на категории.

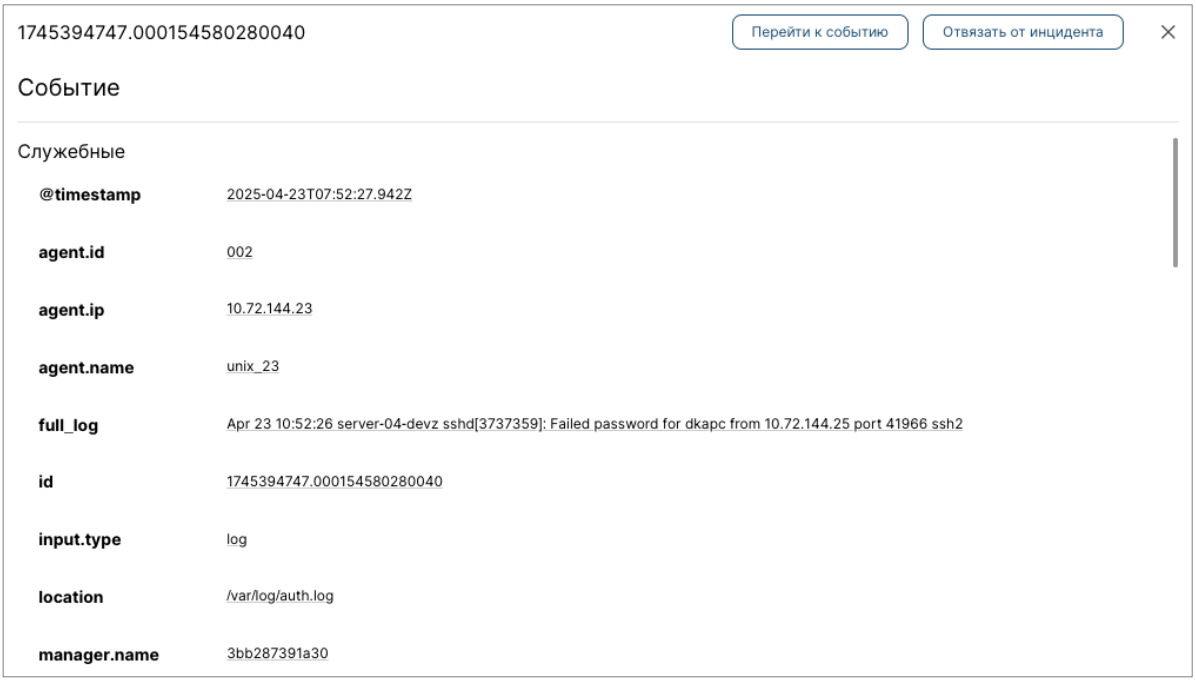


Рисунок 21 – Просмотр события через страницу «Инциденты»

При нажатии на кнопку Перейти к событию произойдет переход на страницу «События» и фильтр в соответствии с `id` события.

Также можно удалить связь выбранного события с инцидентом, нажав на кнопку Отвязать от инцидента.

Можно также скопировать `full_log` (событие), для этого надо навести на значение поля и нажать на появившийся элемент.

Для того, чтобы закрыть окно с информацией о событии следует нажать на ×.

Для просмотра информации о правиле корреляции необходимо нажать на кнопку идентификатора правила вида 533. Появится модальное окно с возможностью просмотра текста правила. Если на момент просмотра правило отсутствует в системе, модальное окно не будет содержать текст, а вместо этого появится соответствующее уведомление.

Для того, чтобы просмотреть историю изменения инцидента необходимо выбрать элемент в таблице и нажать на кнопку Журнал инцидента. Далее появится боковое модальное окно, в котором можно раскрыть подробную информацию о выбранном состоянии инцидента (рис.22), при этому элемент ⌄ измениться на ⌃. Вернуться на страницу «Инциденты» можно при нажатии на ← или по нажатию вне модального окна.

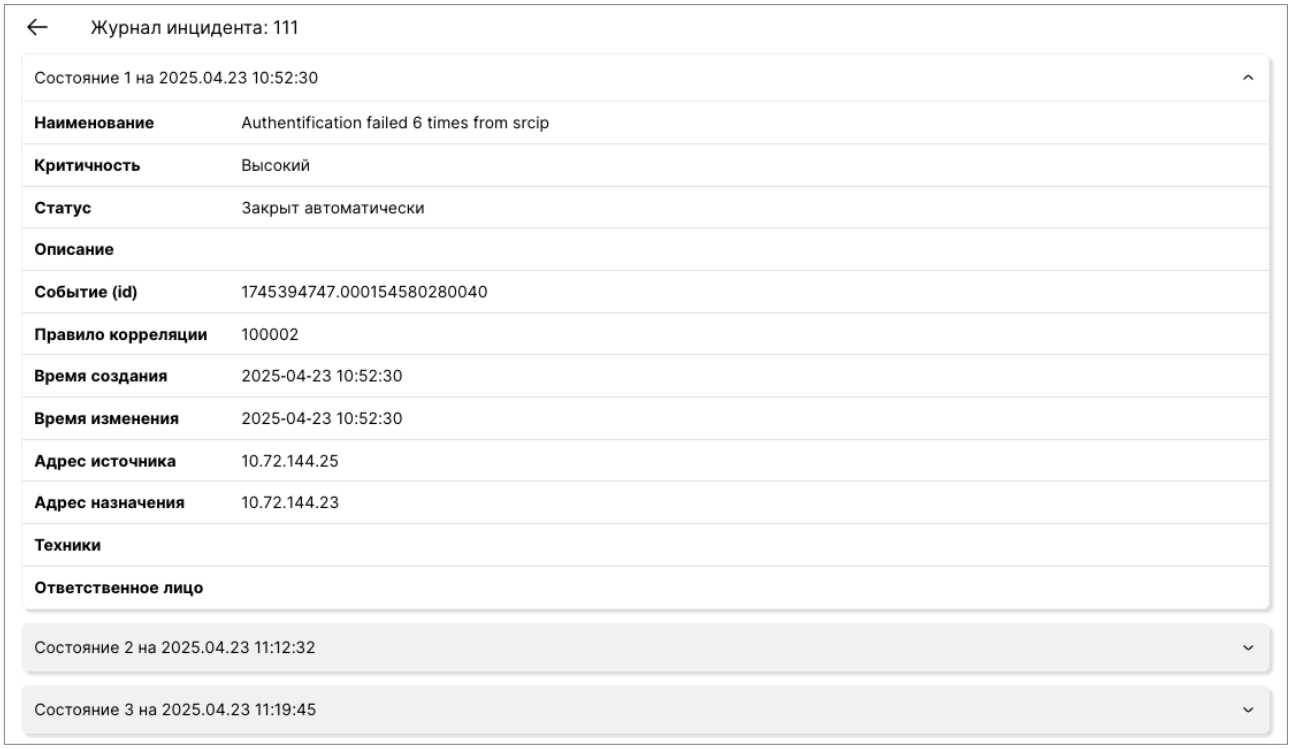


Рисунок 22 – Журнал инцидента

3.6.4 Редактирование информации о конкретном инциденте

Для того, чтобы отредактировать инцидент необходимо перейти на сущность «Карточка инцидента». Для этого в правой части рабочей области страницы «Инциденты» (рис. 20) нажать на название инцидента Инцидент: 29583 . Система откроет новую страницу, где появится возможность внесения изменений (рис. 23).

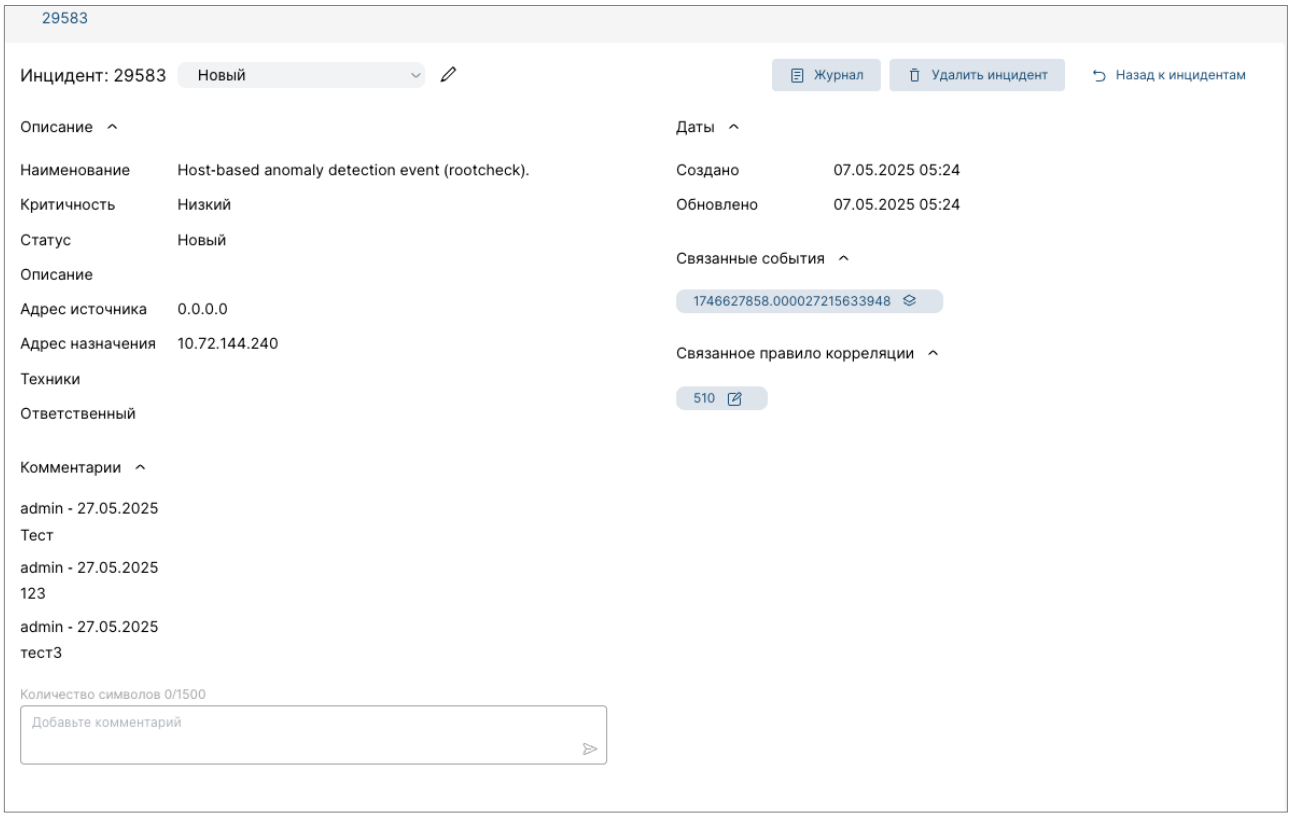


Рисунок 23 – Карточка инцидента

Для редактирования полей с описанием необходимо нажать на ✎ и все значения полей в блоке «Описание» станут доступны для изменения (рис. 24).

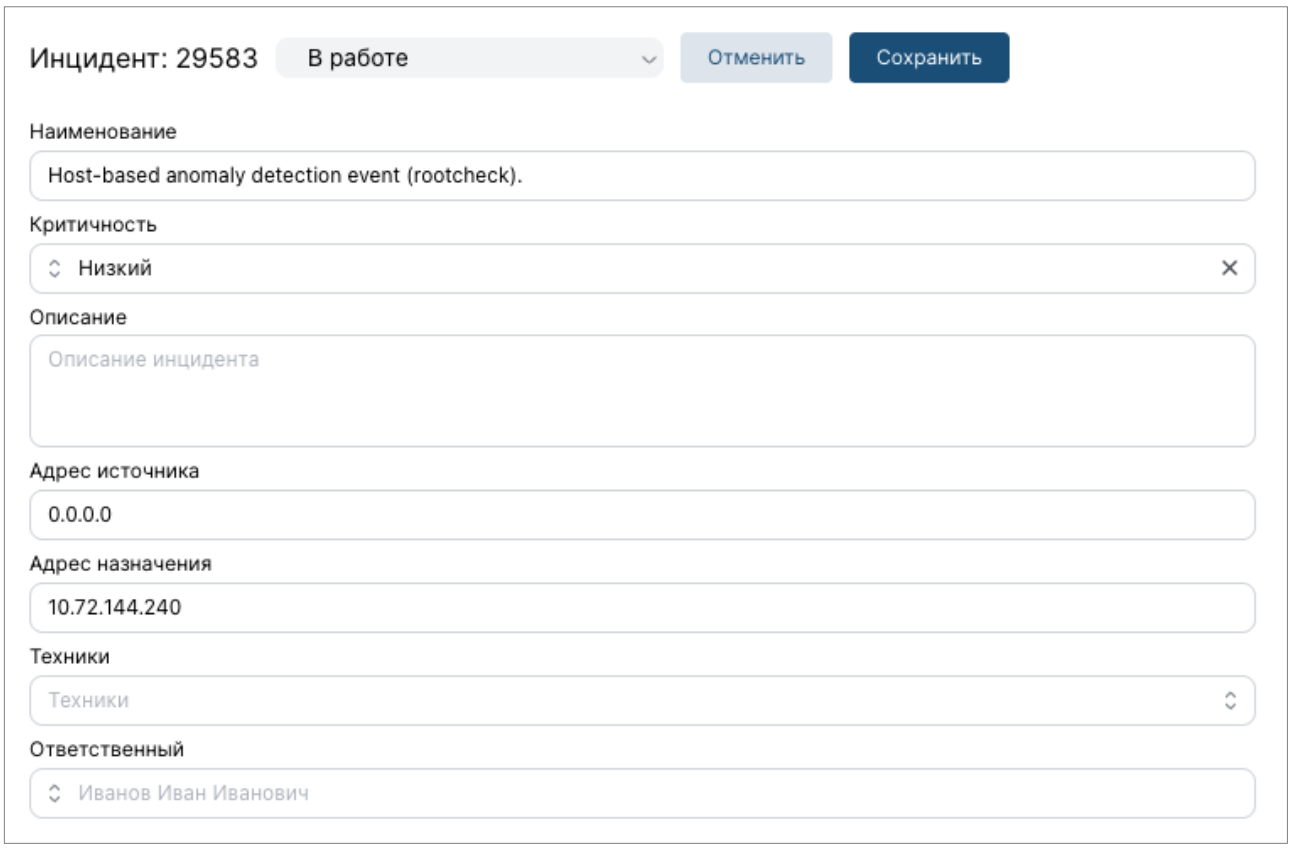


Рисунок 24 – Редактирование инцидента

Следует обратить внимание, что в поле «Описание» есть ограничение в 60 символов, а в полях, содержащих IP-адреса, следует указывать данные в формате IPv4. В поле «Критичность» можно изменить уровень инцидента (высокий, средний, низкий), в «Техники» – выбрать техники MITRE ATT&CK, а в поле «Ответственный» выбрать ответственного пользователя. Для сохранения внесенных изменений нужно нажать на кнопку «Сохранить», а для отмены – «Отменить».

Для изменения статуса инцидента нужно открыть раскрывающий список

, который находится рядом с названием инцидента, и выбрать нужный вариант.

Через страницу «Карточка инцидента» доступны возможности:

- создания комментариев, в также просмотр их истории (алгоритм аналогичен пункту 3.6.3);
- просмотр журнала инцидента (алгоритм аналогичен пункту 3.6.3);
- просмотра связанного события, его отвязка от инцидента и переход на страницу «События» для его подробного изучения (алгоритм аналогичен пункту 3.6.3);

- просмотра связанного правила корреляции (алгоритм аналогичен пункту 3.6.3);
- удаления инцидента;
- возврат назад к станице «Инциденты».

Для того, чтобы вернуться на страницу «Инциденты» следует нажать на кнопку 

. Обратите внимание, что страница будет обновлена, следовательно все фильтры, выделенный инцидент не сохранятся.

Для того, чтобы удалить инцидент необходимо нажать на кнопку 

, подтвердить действие в всплывающем уведомлении. Результат операции отобразится в уведомлениях и произойдет возврат на страницу «Инциденты». В случае если необходимо выйти из режима удаления, следует нажать на кнопку «Отменить» или ✕.

Обратите внимание, что можно скрывать и раскрывать блоки на странице «Карточка инцидента» с помощью элементов ^ и ⌄ соответственно.

3.6.5 Закрытие и удаление инцидента

Для того, чтобы присвоить инциденту статус «Закрыт», достаточно выбрать элемент в таблице на странице «Инциденты» и нажать на кнопку 

. Появится окно с вариантами выбора статуса «Закрыт как ложноположительный» или «Закрыт», как только выбор будет сделан, то кнопка «Закрыть» станет активной. При нажатии на нее инциденту присвоится выбранный статус, и он будет закрыт.

В случае если необходимо выйти из режима закрытия, следует нажать на кнопку «Отменить» или ✕.

Для того, чтобы удалить инцидент необходимо выбрать элемент в таблице и нажать на кнопку 

, подтвердить действие в всплывающем уведомлении. Результат операции отобразится в уведомлениях.

В случае если необходимо выйти из режима удаления, следует нажать на кнопку «Отменить» или ✕.

3.7 Интерфейс раздела «Агенты»

3.7.1 Страница «Агенты»

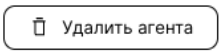
Группа страниц предназначена для работы с агентами. На странице «Агенты» можно просматривать список существующих агентов и установленного на них программного обеспечения (далее – ПО), перезапускать,

обновлять и удалять агента, а на странице «Новый агент» – осуществлять развертывание нового агента.

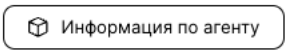
Панель инструментов содержит следующие кнопки:

– для переподключения агента, установленного на ОС Windows;

– для обновления версии агента;



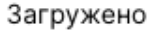
– для ручного удаления неактуального агента;



– для просмотра сведений о составе ПО агента.


– для обновления данных таблицы вручную;


– настройка периодичности обновления страницы. По умолчанию – раз в 15 минут;



– счетчик агентов, показывающий количество отображаемых агентов на странице из числа всех агентов.

Для каждого агента в списке указан набор параметров:

- ID;
- Название;
- IP-адрес;
- Операционная система;
- Версия;
- Дата;
- Статус. Показатели статуса: подключен  , отключен  , подключается/в ожидании  и не подключался.

3.7.2 Страница «Новый агент»

Страница «Новый агент» представляет собой последовательность из шагов для реализации функции развертывания нового агента:

- Выбор пакета для загрузки и установки в систему;
- Ввод IP-адреса сервера или полного доменного имени;
- Ввод названия агента;

Выполнение загрузки, установки и запуска агента: на экране появятся команды, которые необходимо будет выполнить в командном сроке подключаемого устройства.

Для подключения нового агента необходимо следовать инструкциям на странице «Новый агент» и в Руководстве по установке.

3.8 Работа с агентами

Для реализации функций перезапуска и обновления агента нужно выбрать агент из списка и нажать соответствующую кнопку.

Следует обратить внимание, что, если установлена последняя версия агента, обновление не будет происходить и на экране всплывет соответствующее уведомление. Кроме того, перезапуск возможен только для ОС Windows, но не для UNIX-подобных систем агента.

Для просмотра состава программного обеспечения агента, следует нажать на кнопку Информация по агенту, появится боковое модальное окно, в котором можно раскрыть список ПО (рис.25), при это элемент ⌄ изменить на ⌃.

Вернуться на страницу «Агенты» можно при нажатии на ← или по нажатию вне модального окна.

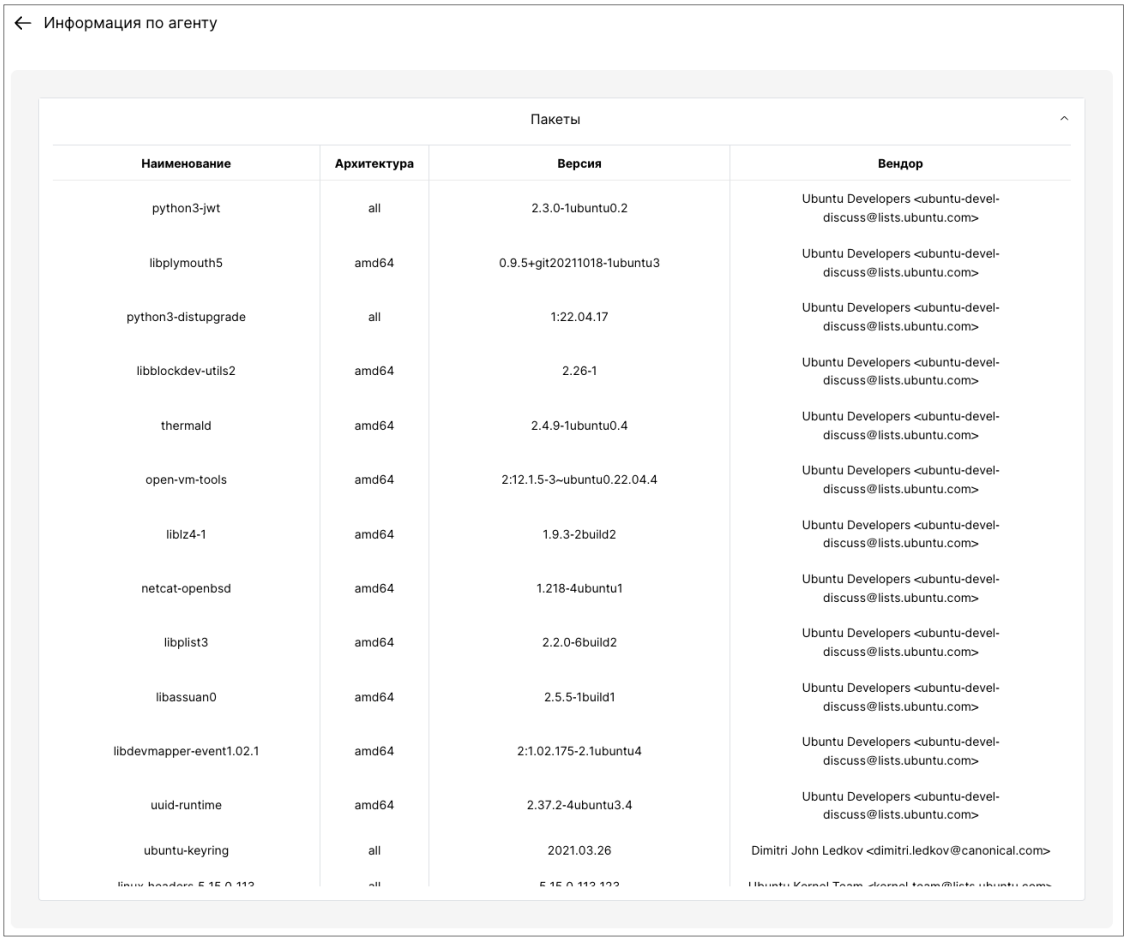


Рисунок 25 – Просмотр информации по агенту

Для реализации функции удаления агента из пользовательского интерфейса необходимо выбрать агент из списка и нажать на кнопку «Удалить».

Следует обратить внимание, что агент должен быть неактивен минимум 1 день, иначе функция удаления недоступна. Появится модальное окно для подтверждения действия. В случае, если пользователь не подтверждает свое действие, все данные остаются неизменными. Если пользователь подтвердил свое действие, агент удаляется.

Для удаления агента с конечного устройства следует воспользоваться инструкцией в Руководстве по установке.

3.9 Интерфейс раздела «Отчеты»

На странице «Отчеты» представлен функционал для генерации отчетом. Данные в отчет выгружаются за определенный период времени. Шаблон отчета будет сформирован с указанием:

- Периода, за который предоставляются данные;
- Информации в табличном виде о событиях;
- Информации в виде диаграмм об инцидентах;
- Информации в табличном виде об инцидентах;
- Данных об агентах и инцидентах, связанных с каждым агентом.

3.10 Работа с отчетами

Для формирования и сохранения отчета необходимо выбрать временной период (рис.26).

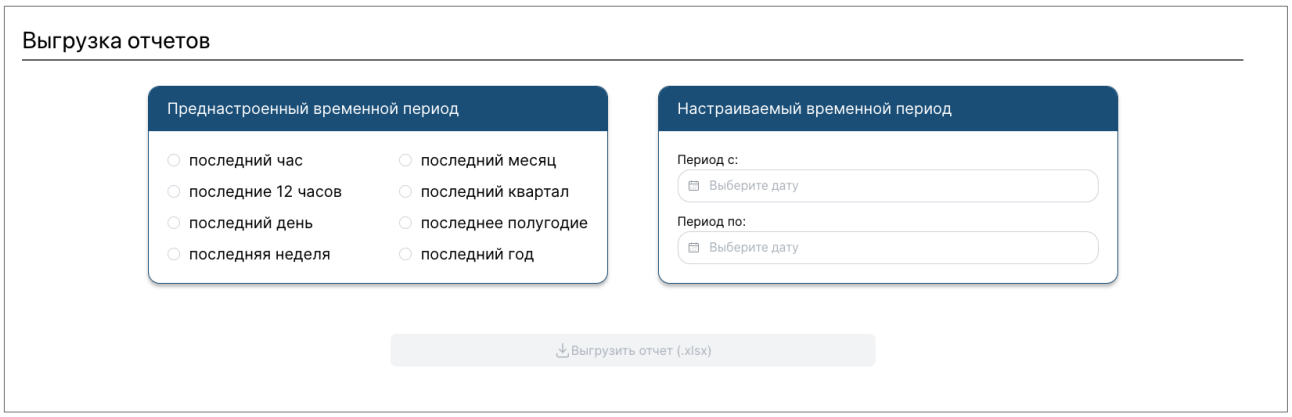


Рисунок 26 – Выгрузка отчета

По преднастроенным параметрам можно выбрать период получения данных (рис.26). Кроме того, есть возможность задать временной промежуток вручную, заполнив поля «Период с» и «Период по».

По нажатию на кнопку «Выгрузить отчет», начинается процесс выгрузки отчета. Отчет будет представлен в формате xlsx.

3.11 Интерфейс раздела «База правил»

Страница предназначена для работы с правилами нормализации, корреляции, агрегации, обогащения, табличными списками, а также их проверку, при условии, что у Пользователя есть соответствующие привилегии (Приложение А).

В группе страниц «База правил» над панелью инструментов (при наличии) располагается строка для поиска отображаемых на странице данных (см. Руководство по созданию запросов).

В группе страниц «База правил» под строкой поиска располагается рабочая область, которая делится на две части: таблицу с перечнем правил или табличных списков и боковую панель для просмотра и редактирования выбранного элемента таблицы. Количество колонок таблицы и их содержание, в том числе тип данных, зависит от вида правил на странице. Интерфейс страницы «Проверка» будет описан ниже в соответствующем подпункте.

3.11.1 Страницы «Нормализация», «Корреляция», Агрегация» и «Обогащение»

Страницы «Нормализация» и «Корреляция» имеют категории:

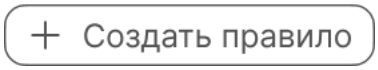
- Системные правила – для просмотра и работы с преднастроенными правилами;
- Пользовательские правила – для просмотра и работы с правилами, созданными пользователем;

Страницы «Агрегация» и «Обогащение» имеют категорию:

- Пользовательские правила – для просмотра и работы с правилами агрегации, созданными пользователем.

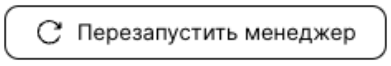
В категории «Системные правила» представлен функционал просмотра общего списка правил и конкретного правила.

В категории «Пользовательские правила» представлен функционал для просмотра, создания, удаления, а также импорта и экспорта правил. Для этого под строкой поиска расположена панель инструментов со следующими кнопками:



– для создания нового пользовательского правила;

– для удаления пользовательского правила;



– для перезапуска ядра системы для применения внесенных изменений;

 – для экспорта пользовательских правил;

 – для импорта пользовательских правил.

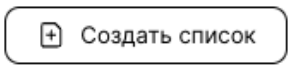
3.11.2 Страница «Табличный список»

Страница «Табличный список» имеет категорию:

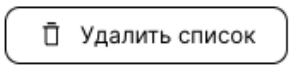
- Пользовательский список – это массив данных, которые используются для хранения списков значений.

В категории «Пользовательский список» страницы «Табличный список» под строкой для настройки фильтрации располагается рабочая область, которая делится на две части: перечень табличных списков и боковую панель для просмотра и редактирования выбранного списка и его элементов (справа).

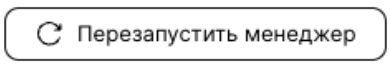
Под строкой для настройки фильтрации табличных списков расположена панель инструментов со следующими кнопками:



– для создания нового пользовательского табличного списка;



– для удаления пользовательского табличного списка;



– для перезапуска ядра системы для применения внесенных изменений;

 – для экпорта пользовательских списков;

 – для импорта пользовательских списков.

Для написания правил и табличных списков следует обращаться к Руководству по написанию правил.

3.11.3 Страница «Проверка правил»

На странице «Проверка правил» рабочая область, которая разделена на две части: одна с полем для ввода события(-ий), а другая для получения результата обработки введенного события(-ий).

На странице панель инструментов представлена следующими кнопками:

– для закрытия уникальной сессии.

– для запуска процесса проверки введенного события на основе базы правил.

3.12 Работа с базой правил

3.12.1 Создание правила

Для создания пользовательского правила необходимо нажать на одноименную кнопку в панели инструментов, после чего откроется модальное окно с редактируемыми полями: название файла и текст правила (рис.27).

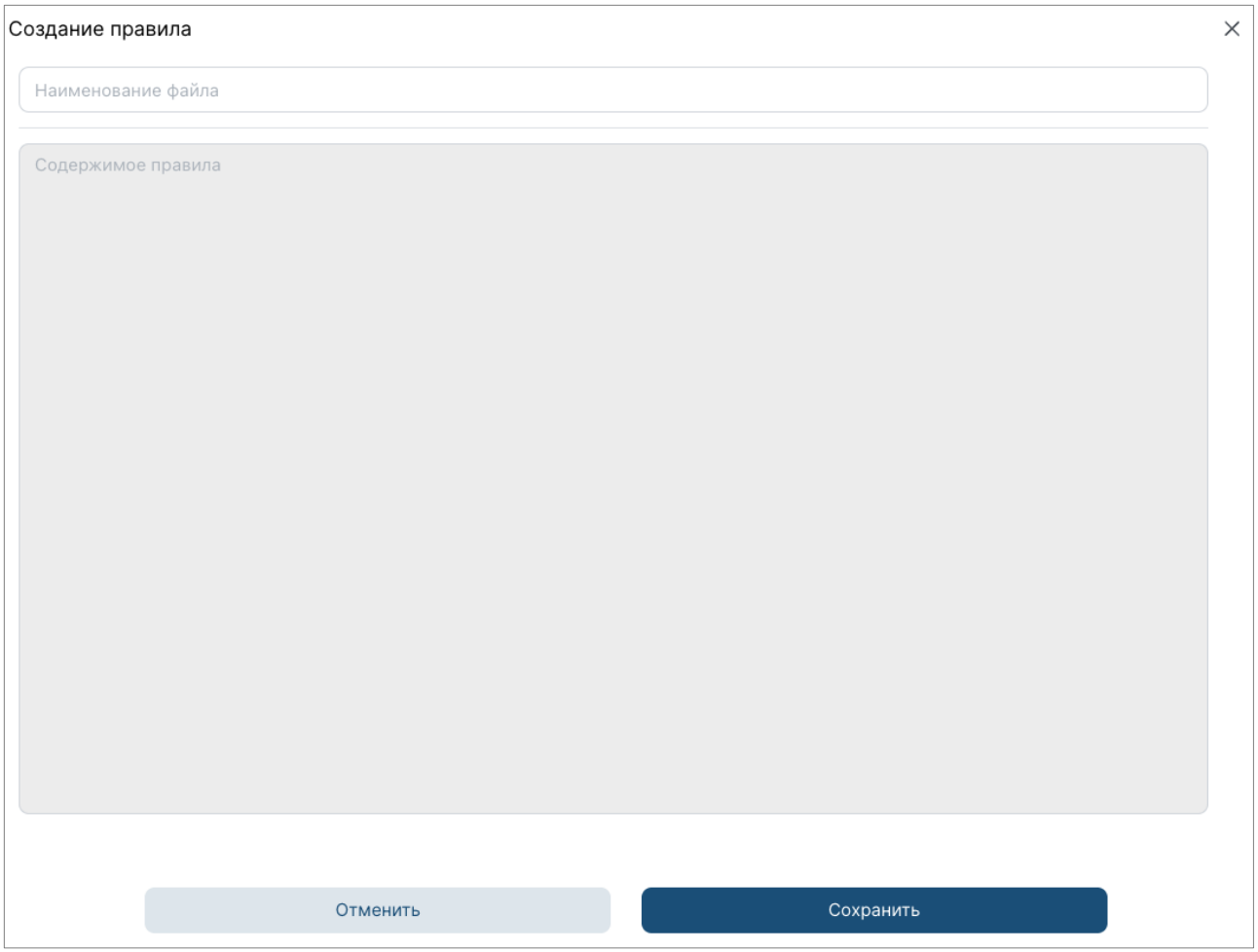


Рисунок 27 – Создание правила

После того, как введен текст правила, и ему присвоено имя, правило следует сохранить нажатием на кнопку «Сохранить». В целях корректной работы с базой правил следует обратиться к Руководству по написанию правил.

Далее происходит возврат на ранее активную страницу из группы страниц «База правил», добавление нового правила в систему и, соответственно, в таблицу, а также появляется соответствующее уведомление «Правило создано успешно» (в случае неуспешности – уведомление «Не удалось создать правило»).

Следует обратить внимание, что после сохранения нового правила необходим перезапуск ядра системы для применения внесенных изменений. Для этого необходимо нажать на кнопку Перезапустить менеджер на панели инструментов.

В случае, если необходимо выйти из режима создания, следует нажать на кнопку «Отменить» или ×, однако все введенные данные будут утеряны.

3.12.2 Редактирование правила

Для того, чтобы отредактировать пользовательское правило, его нужно выбрать в таблице и нажать на соответствующую кнопку. После нажатия на кнопку «Редактировать» открывается боковое модальное окно (рис.28), в котором текст правила доступен для изменения, в то время как название правила остается неизменным.

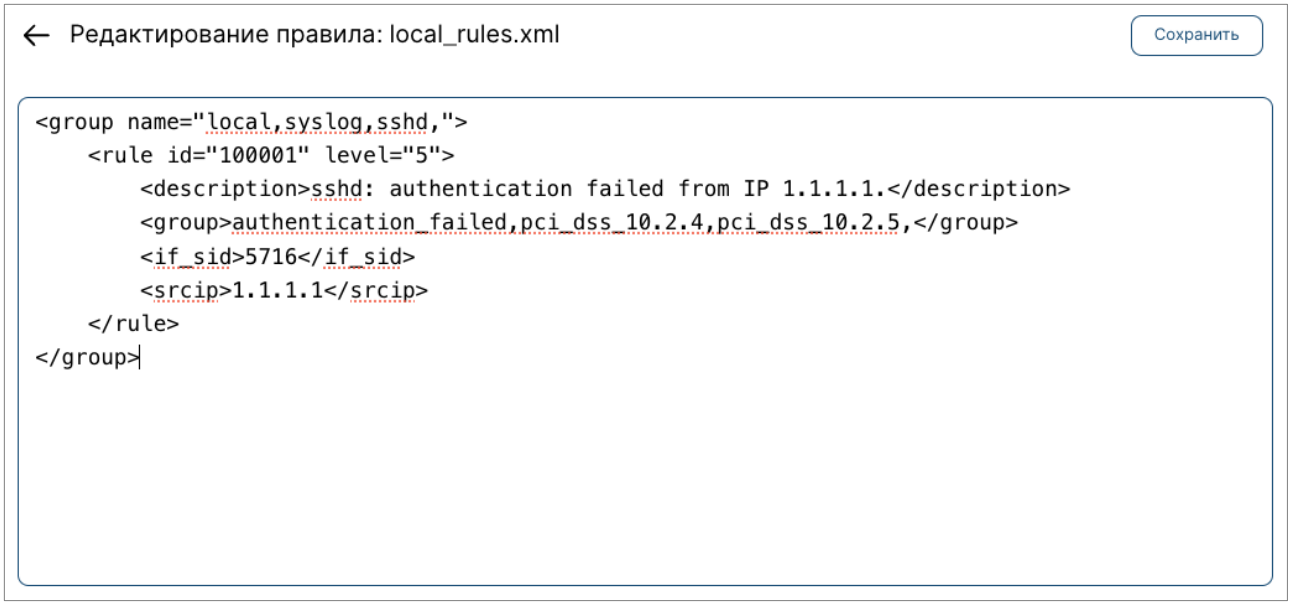


Рисунок 28 – Режим редактирования правила

Вернуться на страницу с общим списком правил без сохранения изменений можно при нажатии на ← .

Для сохранения изменений необходимо нажать на кнопку «Сохранить», после чего появится уведомление «Правило успешно отредактировано» (в случае неуспешности – уведомление «Не удалось отредактировать правило»).

Следует обратить внимание, что после сохранения отредактированного правила необходим перезапуск ядра системы для применения внесенных изменений. Для этого необходимо нажать на кнопку Перезапустить менеджер на панели инструментов.

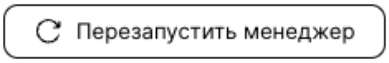
3.12.3 Удаление, экспортирование и импортирование правила

Для того, чтобы удалить пользовательское правило необходимо выбрать правило в таблице и нажать на кнопку 

. Результат операции отобразится в уведомлениях: «Правило успешно удалено» или «Не удалось удалить правило» соответственно. Аналогично процессу созданию и редактированию правило, необходимо будет перезапустить менеджер.

Для того, чтобы экспортировать пользовательское правило необходимо выбрать его в списке правил и нажать на кнопку  . Правило будет сохранено в формате xml.

Для того, чтобы импортировать правило, следует нажать на кнопку  , в открывшемся проводнике выбрать загружаемый файл. Результат загрузки отобразится в уведомлениях: «Правило успешно загружено» или «Не удалось загрузить правило».

Следует обратить внимание, что после импортирования нового правила необходим перезапуск ядра системы для применения внесенных изменений. Для этого необходимо нажать на кнопку 

на панели инструментов.

3.12.4 Создание пользовательского списка

Для создания пользовательского списка необходимо нажать на одноименную кнопку в панели инструментов, после чего откроется модальное окно с редактируемыми полями для названия файла и ввода значений (рис.29).

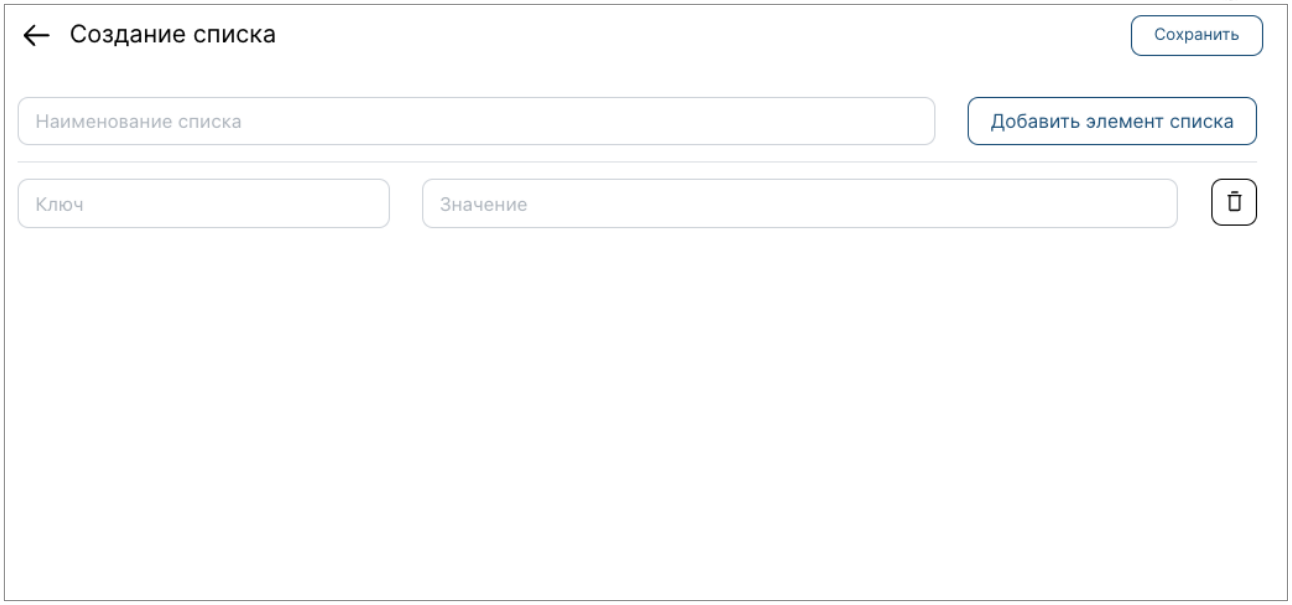


Рисунок 29 – Создание списка

Для того, чтобы добавить новые элементы в список необходимо нажать на кнопку Добавить элемент списка и ввести данные в поля «Ключ» и «Значение».

Для того, чтобы удалить элементы из списка необходимо нажать на кнопку в поле, которое необходимо удалить (рис.30).

Рисунок 30 – Элемент в табличном списке

Для сохранения изменений необходимо нажать на кнопку «Сохранить». Далее происходит возврат на ранее активную страницу из группы страниц «База правил», добавление нового списка в систему и, соответственно, в таблицу, а также появляется соответствующее уведомление «Список создан успешно» (в случае неуспешности – уведомление «Не удалось создать список»).

Следует обратить внимание, что после сохранения нового списка необходим перезапуск ядра системы для применения внесенных изменений. Для этого необходимо нажать на кнопку Перезапустить менеджер на панели инструментов.

В случае, если необходимо выйти из режима создания, следует нажать на кнопку «Отменить» или ×, однако все введенные данные будут утеряны.

3.12.5 Редактирование пользовательского списка

Для того, чтобы отредактировать табличный список, его нужно выбрать и нажать на соответствующую кнопку в боковой панели. После нажатия на кнопку

«Редактировать» открывается боковое модальное окно (рис.31), в котором можно добавить или удалить элемент списка, отредактировать пару «Ключ» и «Значение». Однако название списка остается неизменным.

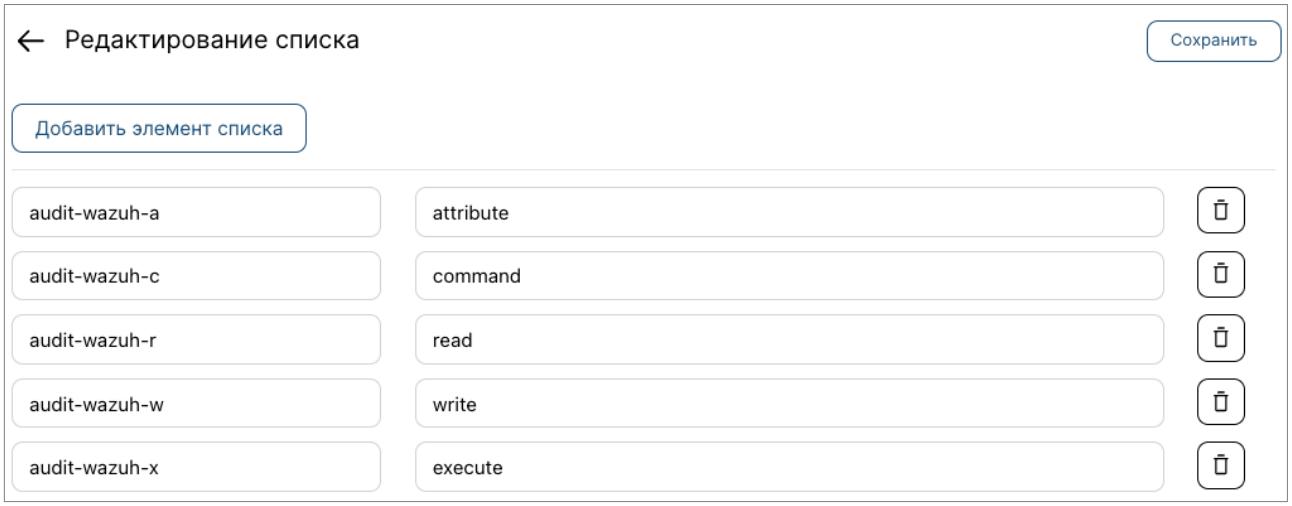


Рисунок 31 – Режим редактирования табличного списка

Вернуться на страницу «Табличный список» без сохранения изменений можно при нажатии на ← .

Для сохранения изменений необходимо нажать на кнопку «Сохранить», после чего появится уведомление «Список успешно отредактирован» (в случае неуспешности – уведомление «Не удалось отредактировать список»).

Следует обратить внимание, что после сохранения отредактированного списка необходим перезапуск ядра системы для применения внесенных изменений. Для этого необходимо нажать на кнопку Перезапустить менеджер на панели инструментов.

3.12.6 Удаление, экспортирование и импортирование пользовательского списка

Процессы удаления, а также экспортирование и импортирование табличного списка аналогичны соответствующим процессам по работе с правилами. Выгрузка и загрузка табличных списков происходит в формате txt.

3.12.7 Создание правила обогащения

Для того, чтобы добавить правило обогащения необходимо перейти на страницу «Обогащение» и нажать на кнопку Добавить правило, после чего откроется модальное окно (рис.32) с полями для заполнения. Поля «Поле события» и «Новое поле события» являются обязательными для заполнения.

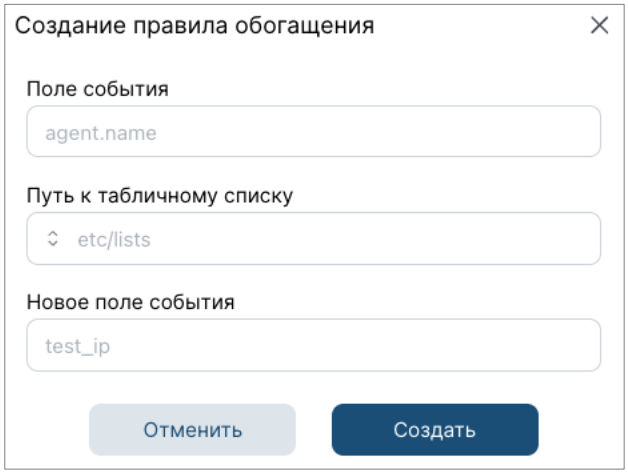
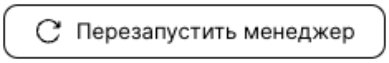


Рисунок 32 – Добавление нового правила обогащения

Для сохранения правила необходимо нажать на кнопку «Сохранить». Далее происходит возврат на ранее активную страницу из группы страниц «База правил», добавление нового списка в систему и, соответственно, в таблицу, а также появляется уведомление «Правило создано успешно» (в случае неуспешности – уведомление «Не удалось создать правило»).

В случае, если необходимо выйти из режима создания, следует нажать на кнопку «Отменить» или ✕, однако все введенные данные будут утеряны.

Следует обратить внимание, что после сохранения нового правила необходим перезапуск ядра системы для применения внесенных изменений. Для этого необходимо нажать на кнопку 

на панели инструментов.

3.12.8 Редактирование правила обогащения

Для того, чтобы отредактировать правило обогащения, его нужно выбрать и нажать на соответствующую кнопку в боковой панели. После нажатия на кнопку 

открывается боковое модальное окно (рис.33), в котором можно отредактировать «Путь к табличному списку» и «Новое поле события». Однако, «Поле события» является неизменным текстовым блоком.

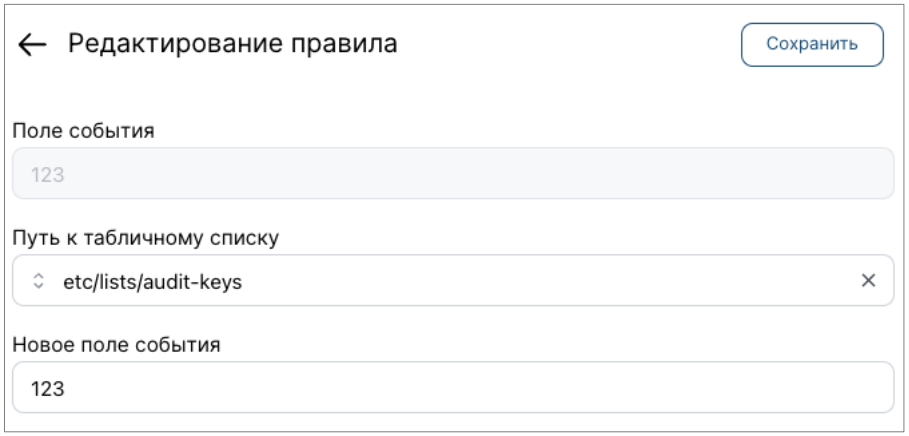


Рисунок 33 – Редактирование правила обогащения

Следует обратить внимание, что после сохранения нового правила необходим перезапуск ядра системы для применения внесенных изменений. Для этого необходимо нажать на кнопку Перезапустить менеджер на панели инструментов.

3.12.9 Удаление правила обогащения

Для того, чтобы удалить правило обогащения необходимо выбрать его в таблице и нажать на кнопку Удалить правило. Результат операции отобразится в уведомлениях: «Правило успешно удалено» или «Не удалось удалить правило» соответственно. Аналогично процессу созданию и редактированию, необходимо будет перезапустить менеджер.

3.12.10 Проверка правил

Для того, чтобы проверить набор правил, существующий в системе, можно воспользоваться страницей «Проверка правил» (рис.34).

Для этого в поле событие ввести событие (набор событий), которое будет проанализировано на основе существующего набора правил в системе. Далее необходимо нажать на кнопку Проверить. Система обработает события построчно.

В блоке «Результат» появятся итоги обработки введенного события (-ий). Можно очистить блок «События» с помощью элемента , а также скопировать результат анализа с помощью элемента .

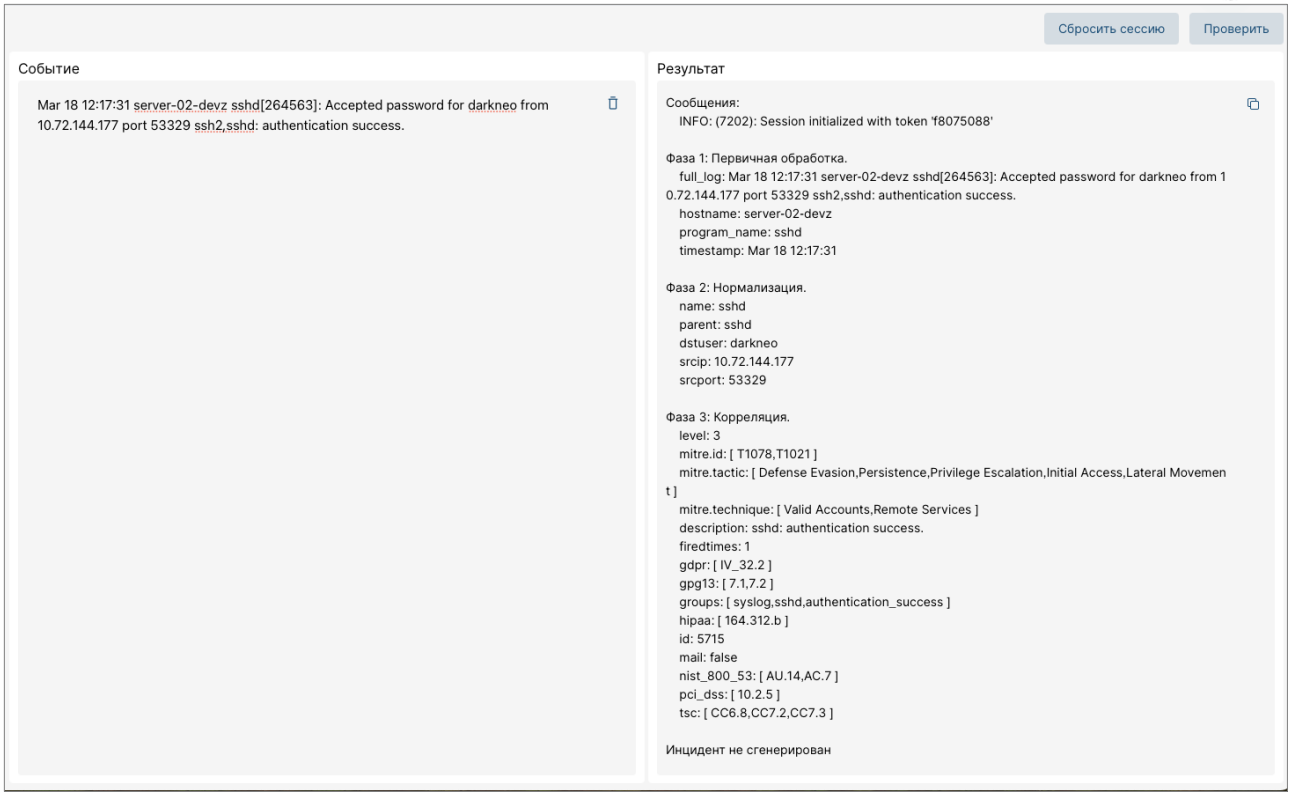


Рисунок 34 – Страница «Проверка правил»

Обратите внимание, что при первом запросе на обработку события создается сессия. Сессии – это изолированные среды для тестирования элементов базы правил. В рамках одной сессии сохраняется история событий и количество срабатываний правил, что обеспечивает корреляцию событий и, соответственно, проверку валидности правил корреляции.

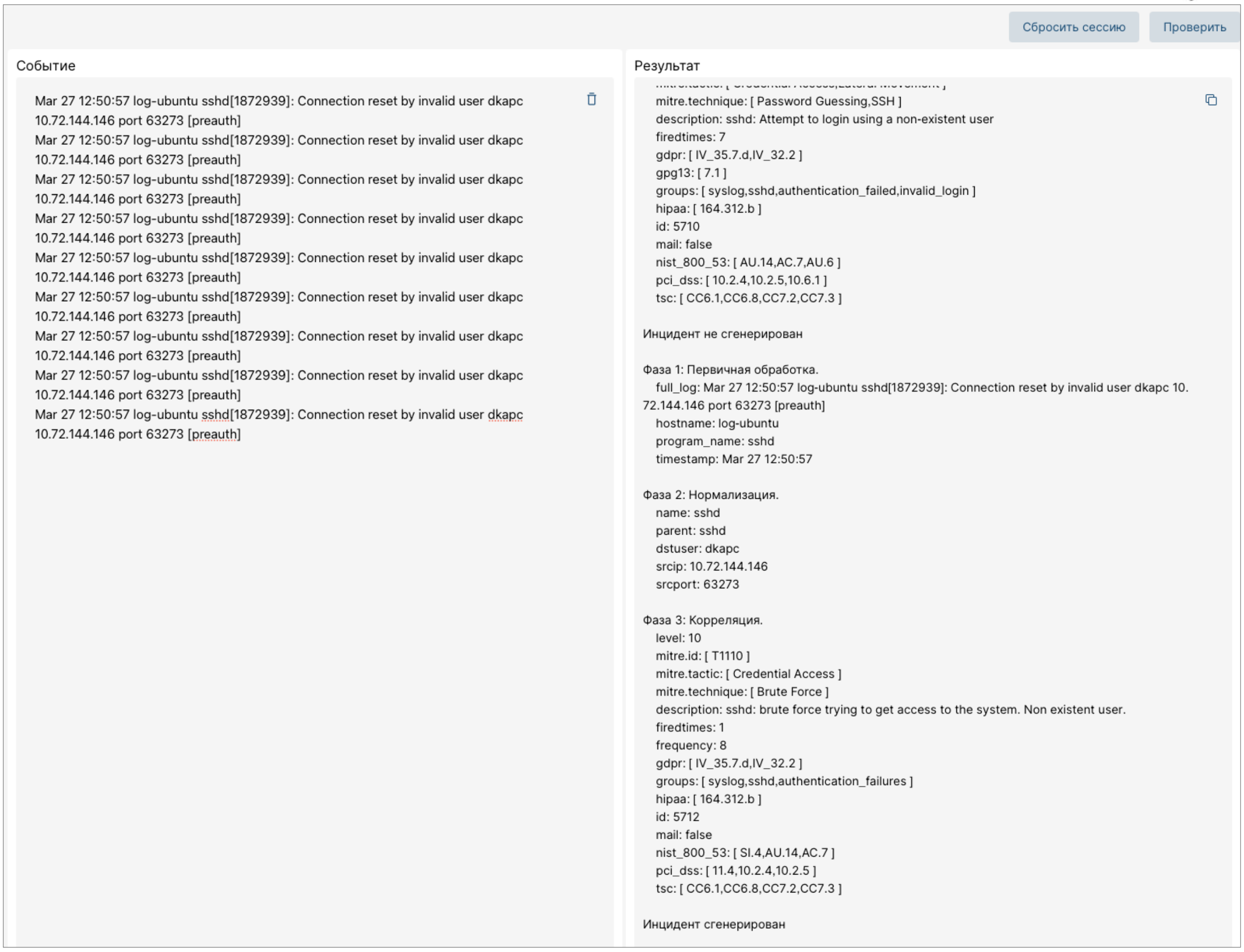


Рисунок 35 – Проверка правил с корреляцией событий

Как видно из рисунка 35, было зафиксировано определенное количество неудачных попыток входа в систему под одним пользователем, и на основе проведенной корреляции событий система сформировала инцидент типа [Brute Force].

Для того, чтобы сбросить сессию необходимо нажать кнопку 

либо она закроется автоматически по прошествию 15 минут бездействия.

3.13 Интерфейс раздела «Настройки системы»

Для группы страниц «Настройки системы» представлен функционал для работы с Пользователями, Ролями, лицензированием, а также настройки интеграции с SOAR-системой, почтовой рассылки и загрузки системных правил, при условии наличия соответствующих привилегий.

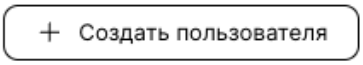
3.13.1 Страница «Пользователи»

Рабочая область страницы «Пользователи» разделена на две части: левая часть представляет собой список с пользователями, правая – таблицу с подробной информацией о выбранном пользователе.

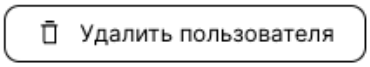
Для каждого пользователя в списке указан набор параметров:

- Статус;
- Имя пользователя;
- ФИО;
- Электронная почта;
- Роль.

Панель инструментов содержит кнопки:



– для регистрации нового пользователя вручную;



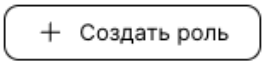
– для удаления пользователя вручную.

3.13.2 Страница «Роли»

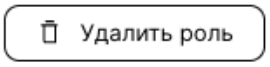
Рабочая область страницы «Роли» так же разделена на две части: левая часть представляет собой список с Ролями, правая – таблицу с подробной информацией о выбранной Роли. Для каждой Роли в списке указан набор параметров:

- Название;
- Описание;
- Привилегии.

Панель инструментов содержит кнопки:



– для регистрации новой роли пользователем;



– для удаления роли.

3.13.3 Страница «Лицензирование»

На странице «Лицензирование» представлен функционал, позволяющий просматривать информацию о лицензии (рис.36). Инструкция по добавлению лицензии описана в Руководстве по установке.

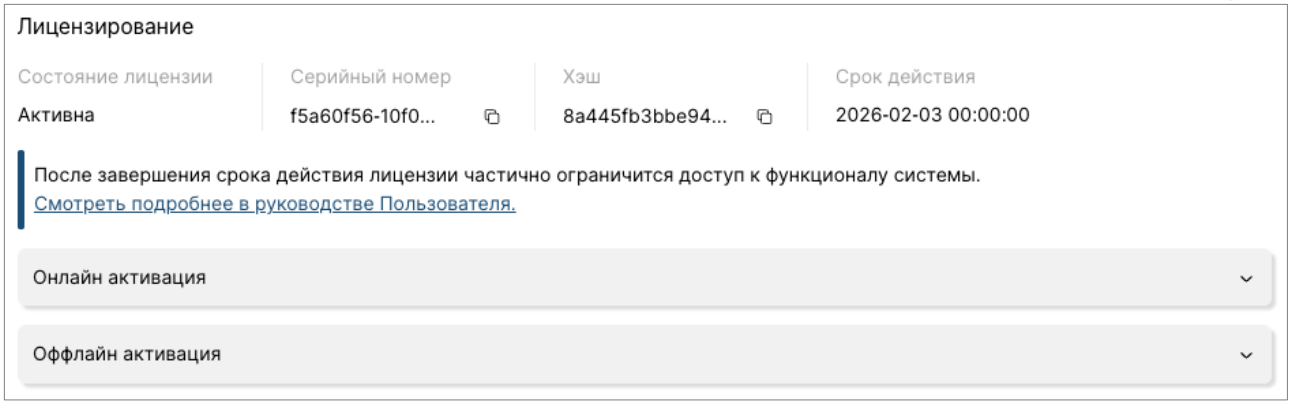


Рисунок 36 – Страница «Лицензирование»

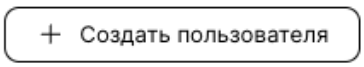
3.13.4 Страница «Дополнительные настройки»

На странице «Дополнительные настройки» представлен функционал по настройкам системы, выходящий за рамки работы с пользователями и ролями, а также лицензирования продукта: настройка интеграции с SOAR-системой и почтовой рассылки, а также загрузка системных правил (рис. 37).

Рисунок 37 – Блоки для дополнительных настроек

3.14 Работа с настройками системы

3.14.1 Создание пользователя

Для создания нового пользователя нажать на кнопку 

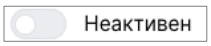
на странице «Пользователи». После этого появится модальное окно с полями для ввода информации (рис.38). «Имя пользователя», «Пароль», «Фамилия», «Имя», «Отчество» и «Электронная почта» являются обязательными полями для заполнения.

Минимальное количество символов в поле «Пароль» 10, включая латинские заглавные и строчные буквы, цифры и специальные символы !@#$%^&*()_+. Можно воспользоваться функцией для генерации пароля, для этого необходимо нажать на элемент Генерация пароля. По умолчанию значение поля «Пароль» видно, но его можно скрыть нажатием на элемент .

Поле «Имя пользователя» может содержать цифры, заглавные, прописные буквы и символы «_», «-».

Можно присвоить статус активности Пользователю 

. Если задан статус 

, пользователь может авторизоваться в системе и иметь доступ к интерфейсу в соответствии с выданными ему привилегиями. В случае если задан статус 

, у пользователя отсутствует доступ к системе.

Следует обратить внимание, что нельзя деактивировать системного пользователя – роль «Супер администратор».

Для сохранения нового пользователя нужно нажать на кнопку «Сохранить». Если пользователь не подтверждает свое действие, нажимает кнопку «Отменить» или закрывает окно ✕, несохраненные данные будут утеряны.

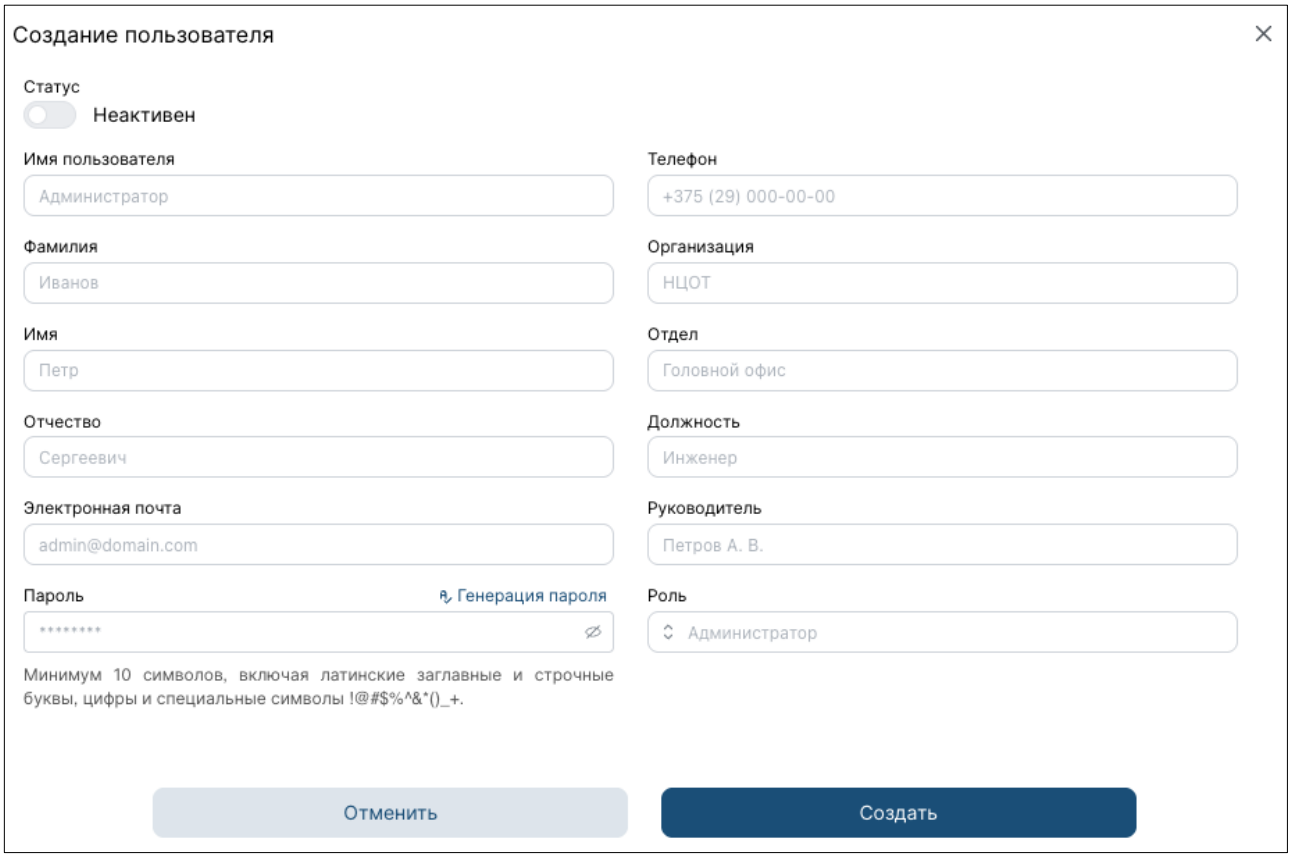


Рисунок 38 – Создание нового пользователя

3.14.2 Редактирование пользователя

Для редактирования информации о пользователе необходимо нажать на кнопку «Редактировать» в таблице с подробной информацией о пользователе, в таком случае поля с текстовой информацией станут доступными для изменения (рис. 39).

Для сохранения изменений нужно нажать на кнопку «Сохранить». Если пользователь не подтверждает свое действие или при нажатии на кнопку «Отменить», все данные остаются неизменными.

Следует обратить внимание, что можно изменить пароль учетной записи, для этого следует ввести или сгенерировать новый набор символов в поле «Пароль» и сохранить внесенные изменения.

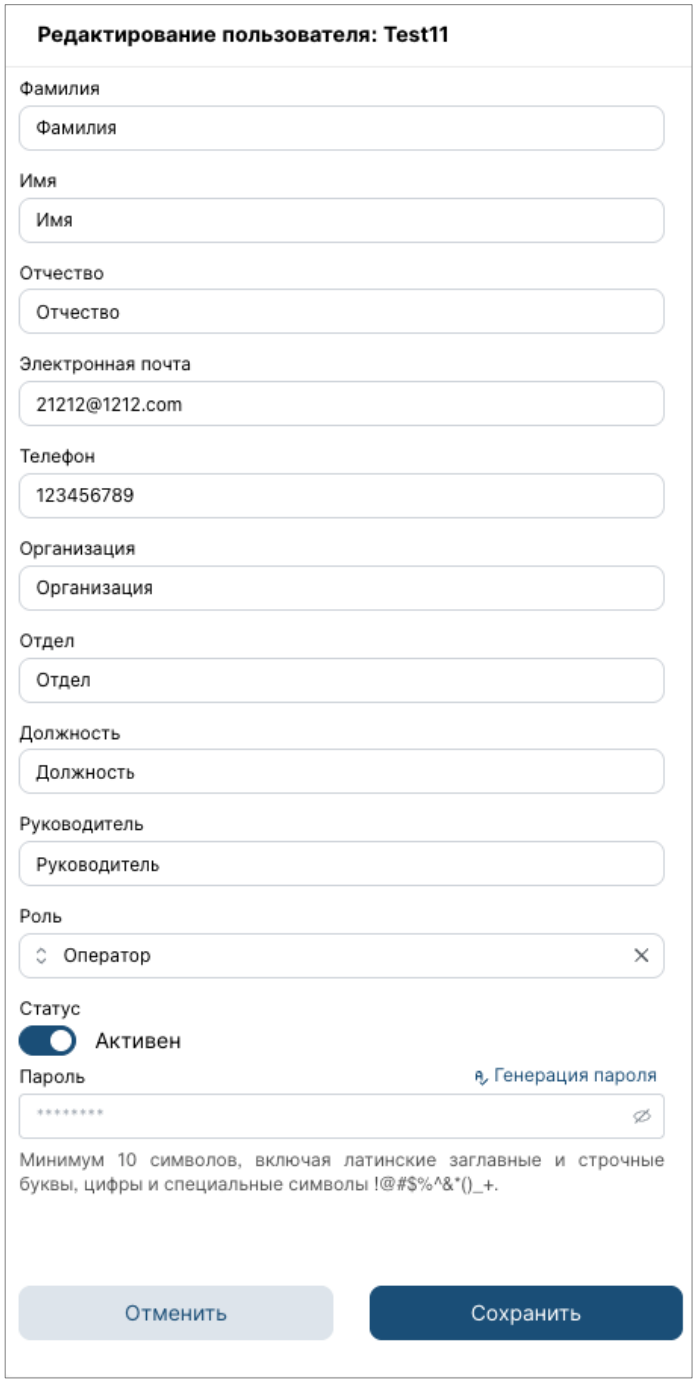
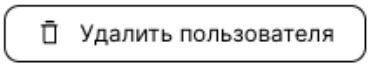


Рисунок 39 – Редактирование пользователя

3.14.3 Удаление пользователя

Для удаления пользователя необходимо выбрать пользователя из списка и нажать на кнопку с соответствующим названием. При нажатии на кнопку 

всплывает модальное окно для подтверждения действия. В случае подтверждения действия выбранный пользователь удаляется, в противном случае – все данные остаются неизменными.

Следует обратить внимание что, если пользователь хоть раз заходил в систему, его нельзя удалить.

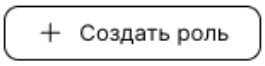
3.14.4 Создание роли

При развертывании NT SIEM (см. Руководство по установке) автоматически создается учетная запись, имеющая все возможные привилегии. Эту учетную запись невозможно заблокировать или удалить (Приложение 1).

В системе реализована ролевая модель управления доступом с набором стандартных ролей «Администратор» и «Оператор» (Приложение 1). Каждая роль содержит набор привилегий, которые определяют доступные для Пользователя разделы интерфейса и операции в системе.

Стандартная роль «Администратор» имеет набор привилегий: работа с инцидентами, событиями, агентами, базой правил, выгрузка отчета, просмотр личного профиля и загрузка эксплуатационной документации.

Стандартная роль «Оператор» имеет набор привилегий: работа с инцидентами, событиями, агентами, выгрузка отчета, просмотр личного профиля и загрузка эксплуатационной документации.

В случае, если стандартных ролей недостаточно для выполнения рабочих задач, можно создать новую роль. Для создания новой роли необходимо нажать на кнопку 

на странице «Роли». Далее появится модальное окно (рис.40), в котором необходимо ввести данные в поля «Наименование» и «Описание», а также в раскрывающемся списке «Привилегии» выбрать набор прав для создаваемой роли (Приложение 1). Поле «Наименование» и «Выбор привилегий» не могут быть пустыми.

Рисунок 40 – Создание роли

Для сохранения новой роли нужно нажать на кнопку «Сохранить». Если пользователь не подтверждает свое действие, нажимает кнопку «Отменить» или закрывает окно ✕, несохраненные данные будут утеряны.

3.14.5 Редактирование роли

Для редактирования информации о роли необходимо нажать на кнопку «Редактировать» в таблице с подробной информацией, и поля станут доступными для изменения (рис.41).

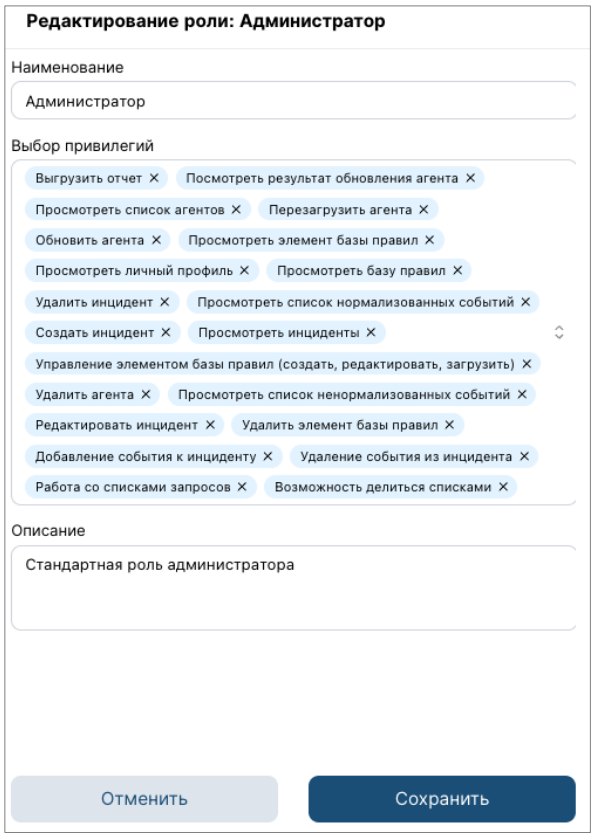
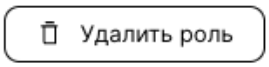


Рисунок 41 – Редактировае роли

Для сохранения изменений нужно нажать на кнопку «Сохранить». Если пользователь не подтверждает свое действие или при нажатии на кнопку «Отменить», все данные остаются неизменными.

3.14.6 Удаление роли

Для удаления роли необходимо выбрать роль из списка и нажать на кнопку с соответствующим названием. При нажатии на кнопку 

всплывает модальное окно для подтверждения действия. В случае подтверждения действия выбранная роль удаляется, в противном случае – все данные остаются неизменными.

3.14.7 Работа с лицензией

При развертывании NT SIEM, Пользователь должен активировать лицензию для получения доступа к системе (см. Руководство по установке):

- В случае положительного результата, пользователю становится доступен весь функционал системы в соответствии с его ролью;
- В случае отрицательного результата, пользователь получает ограниченный доступ к системе.

В случае, когда срок лицензии вышел и лицензия не была продлена, разработчик оставляет за собой право ограничить функциональность NT SIEM при отсутствии у пользователя активной лицензии.

В случае, когда лицензия была продлена, весь функционал системы будет доступен пользователям в соответствии с их ролями.

Следует обратить внимание, что при изменении конфигурации, необходимо обновление лицензии, для этого следует обратиться к поставщику программного обеспечения.

3.14.8 Интеграция с SOAR-системой

Для интеграции с SOAR-системой в соответствующем блоке (рис.42) на странице представлены поля, которые доступны для редактирования.

В поле «URL» следует ввести IP-адрес SOAR-системы, в которую будут передаваться данные. В поле «Токен» ввести токен, получаемый от владельца SOAR-системы соответственно.

В поле «Наименование организации» ввести название предприятия, в котором установлена система. В поле «Группа» присвоить группу, для получаемых значений, например, инциденты ООО «Компания1».

Заполнение полей «URL», «Токен», «Наименование организации» и «Группа» являются обязательными.

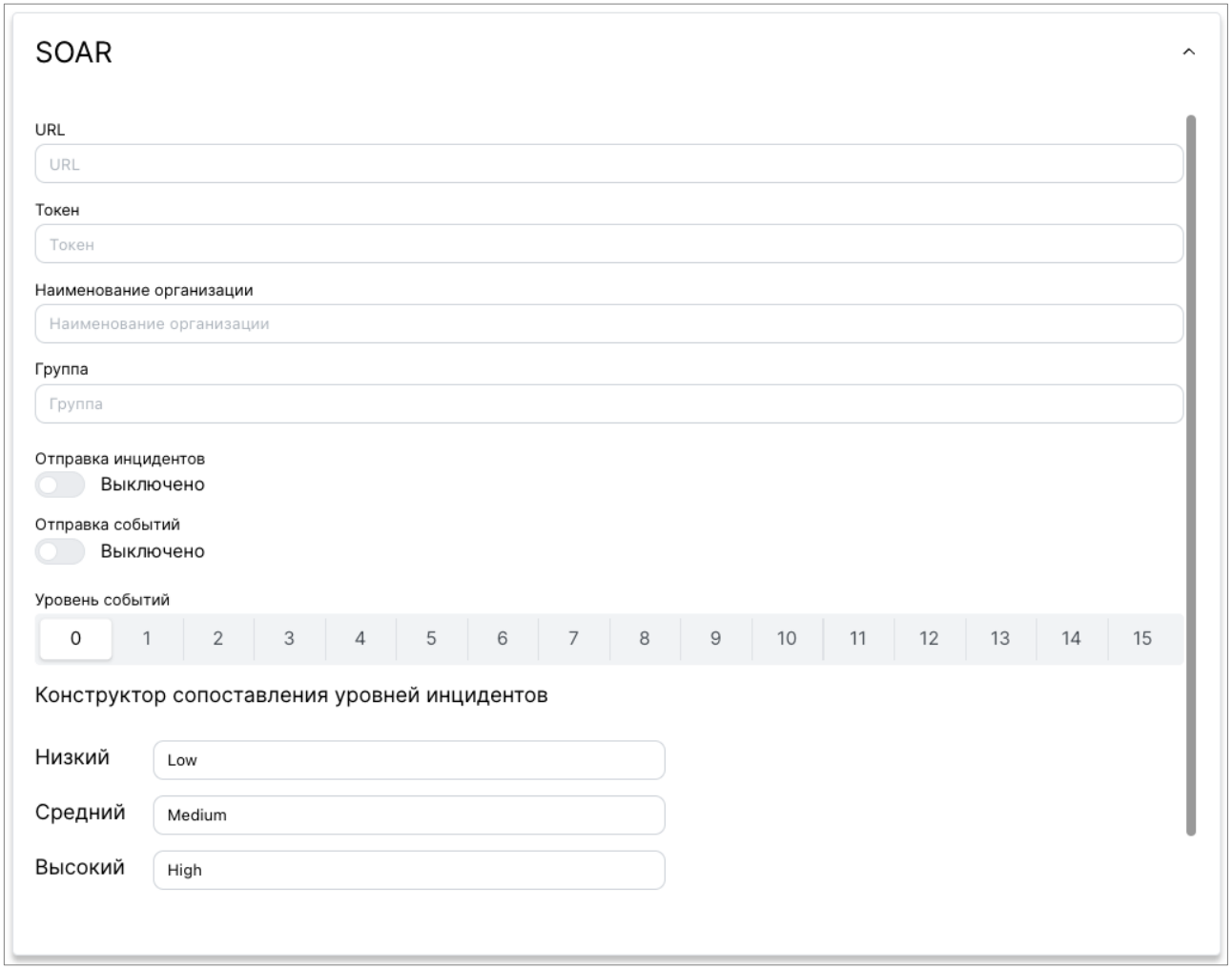


Рисунок 42 – Блок «SOAR»

Для того, чтобы настроить какие данные передавать, следует использовать переключатели «Отправка инцидентов» и «Отправка событий». Например, если необходимо передавать только инциденты, то следует поменять состояние на переключателе на «Включено»:

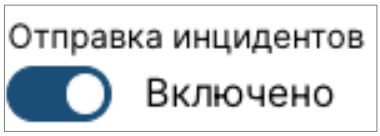


Рисунок 43 – Активный переключатель «Отправка инцидентов»

В системе NT SIEM есть 3 уровня инцидента: низкий, средний и высокий, а в SOAR-системе может использоваться другая система классификации инцидентов. Для сопоставления уровней инцидентов NT SIEM и SOAR-системы, следует воспользоваться блоком «Конструктор сопоставления уровней инцидентов», где необходимо ввести релевантные значения уровней инцидентов

SOAR-системы. Информацию необходимо получить у владельца SOAR-системы.

Пример. Если необходимо передавать инциденты и события, то следует поменять состояния на двух переключателях, а также задать начальный уровень критичности событий, которые будут передаваться в SOAR-систему. Например, если выбрано число 10, то будут передаваться все события уровня критичности 10 и выше.

Для сохранения изменений необходимо нажать на кнопку «Сохранить». Все изменения принимаются системой единовременно.

3.14.9 Загрузка системных правил

Для загрузки системных правил в NT SIEM используется отдельный элемент (рис.44). Следует обратить внимание, что архив с системными правилами должен быть с расширением .tar, весом не более 5 Мб и иметь определенную структуру.

Внутри архива должна лежать папка pack, содержащая:

1. Папку decoders с вложенным минимум одним .xml-файлом. В файлах в сумме должно содержаться более 30 валидных системных правил нормализации.

2. Папку rules с вложенным минимум одним .xml- файлом, содержащим минимум 1 валидное системное правило корреляции. Зарезервированная системой нумерация системных правил корреляции – с 1 до 99999.

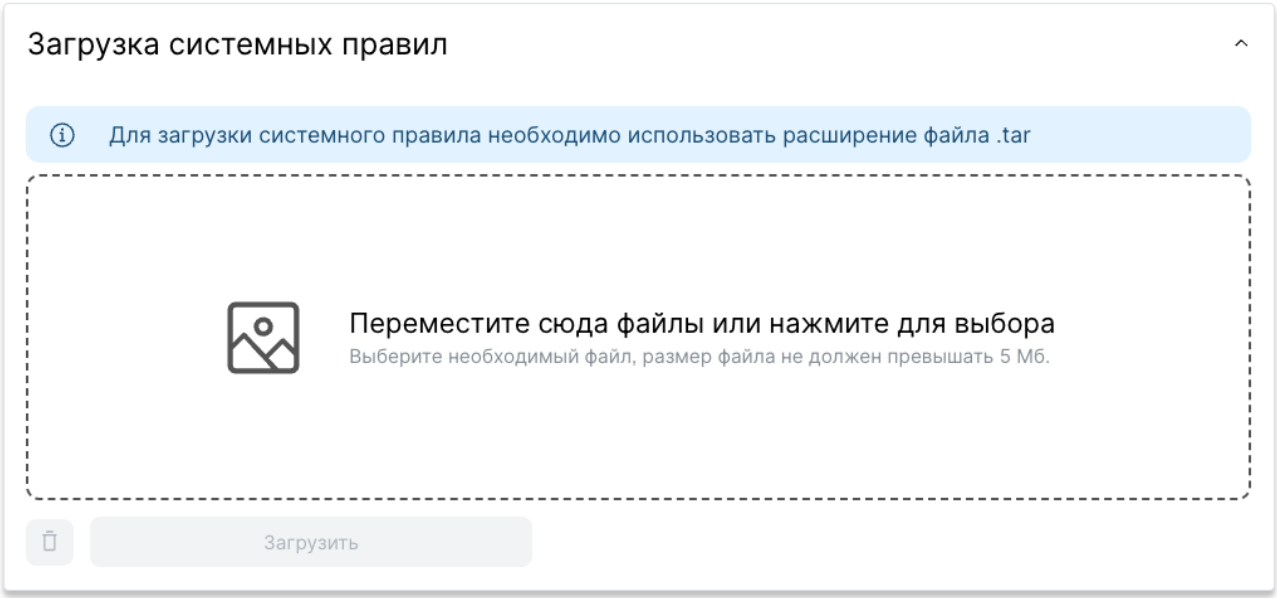


Рисунок 44 – Блок «Загрузка системных правил»

Выбор файла для загрузки может быть осуществлен как после нажатия на блок загрузки, так и путем перемещения файла в соответствующую область (рис.45).

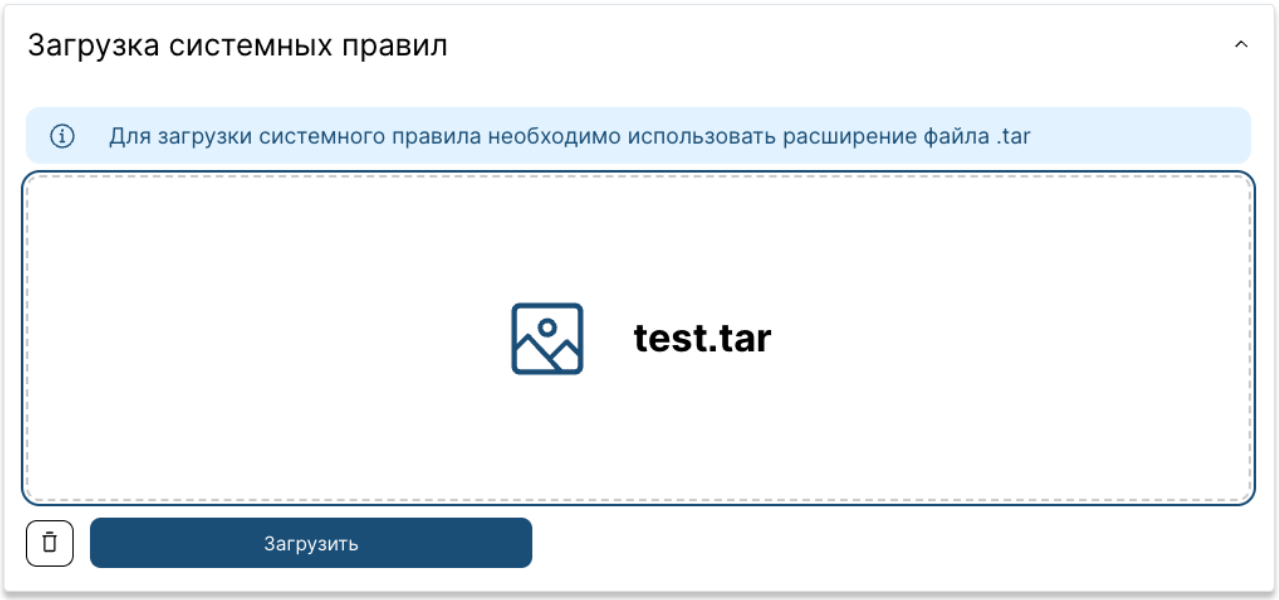


Рисунок 45 – Блок «Загрузка системных правил» с загруженным архивом

После выбора файла следует нажать на кнопку Загрузить, после чего начнется загрузка файла в систему. Результат загрузки отобразится соответствующими уведомлениями. Для того чтобы сбросить выбранный файл, следует нажать на кнопку .

3.14.10 Реализация почтовой рассылки

Для реализации почтовой рассылки в соответствующем блоке на странице представлены поля, которые доступны для редактирования (рис. 46).

В поле «Исходящая почта» вводится почта отправителя, а в «Логин исходящей почты» указывается логин для авторизации на исходящую почту.

Следует обратить внимание, что заполнение поля «Логин исходящей почты» зависит от вида почтового сервера. Например, если почтовый сервис Mail.ru, то в логине необходимо указать имя электронного ящика, значок «@» собачки и домен: somebody@mail.ru. А если почтовый сервис Яндекс, то в логине необходимо указать имя электронного ящика без значка «@» и домен: somebody (без «@yandex.ru»).

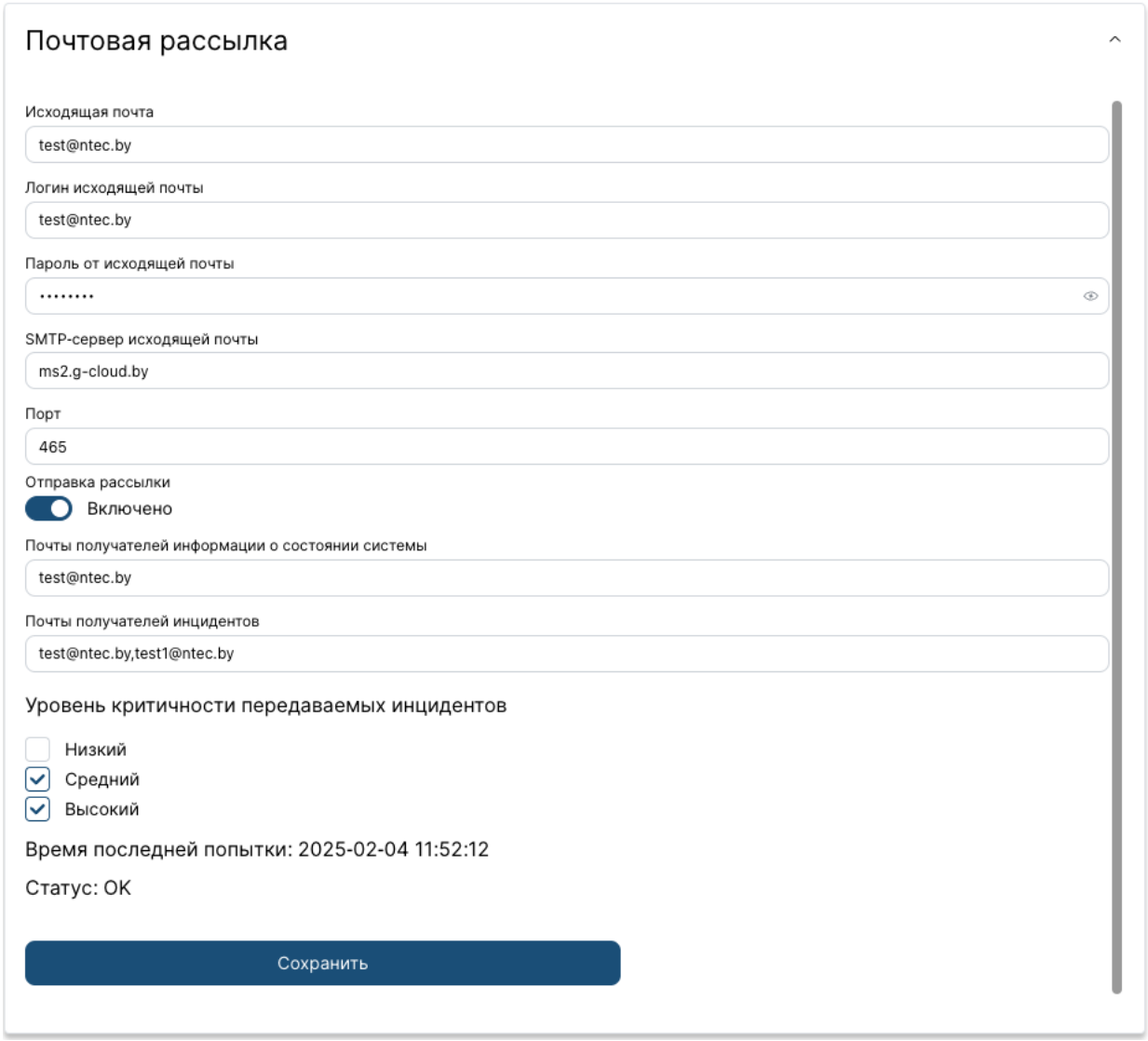


Рисунок 46 – Блок «Почтовая рассылка»

В поле «Пароль от исходящей почты» вводится пароль от почты отправителя, а в полях «SMTP-сервер исходящей почты» и «Порт» указывается адрес или имя SMTP-сервера и порт, который будет использоваться для подключения к серверу и отправки электронных писем соответственно.

В поле «Почты получателей информации о состоянии системы» вводятся электронные адреса получателей, которых необходимо уведомить о состоянии системы, а в поле «Почты получателей инцидентов» – о инцидентах. Почты в этих полях могут дублироваться. Проверка состояния системы производится раз в 60 секунд, в случае возникновения неполадок, отправится письмо на указанные в поле «Почты получателей информации о состоянии системы» адреса. Следует обратить внимание, что в полях «Почты получателей…» перечисление электронных почт получателей происходит через запятую.

Переключатель «Отправка рассылки» по умолчанию находится в состоянии «Включено». Для того, чтобы дезактивировать почтовую рассылку необходимо изменить состояние переключателя на «Выключено» (рис.47):

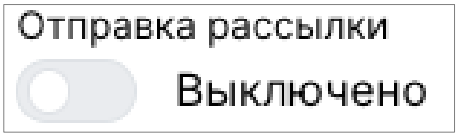


Рисунок 47 – Переключатель «Отправка рассылки»

Также необходимо выбрать «Уровень критичности передаваемых инцидентов», которые будут рассылаться на электронные адреса, указанные в поле «Почты получателей инцидентов». По умолчанию выбраны все уровни.

Следует обратить внимание, что поля, представленные на рисунке 48, являются обязательными для заполнения.

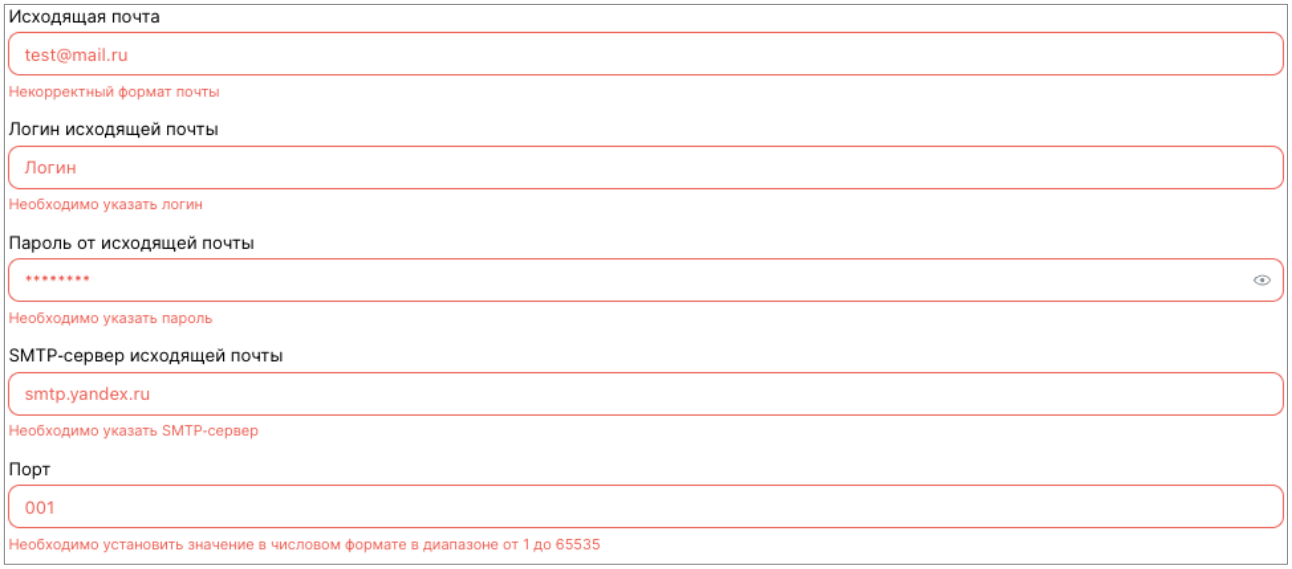


Рисунок 48 – Часть блока «Почтовая рассылка»

Для сохранения изменений необходимо нажать на кнопку «Сохранить». Все изменения принимаются системой единовременно. Несохраненные данные будут утеряны и потребуют повторного ввода.

3.15 Администрирование NTechnology SIEM

Иногда возникает необходимость удостовериться в том, что исполняемый файл приложения не был изменен, для этого необходимо настроить мониторинг целостности файлов.

Мониторинг целостности файлов – это процесс безопасности, используемый для контроля целостности системных и прикладных файлов. Он сравнивает базовую информацию с информацией последней версии файла. Это сравнение обеспечивает прозрачность изменений и обновлений критических файлов. Модуль мониторинга целостности файлов выполняет сканирование в режиме реального времени или по расписанию.

3.15.1 Алгоритм настройки мониторинга целостности файлов

Для того, чтобы настроить возможность мониторинга целостности файлов необходимо модифицировать конфигурационные файлы на конечных устройствах. В зависимости от системы, где стоят агенты, будут разные пути доступа к конфигурационным файлам:

1. Linux: `nano /var/ossec/etc/ossec.conf`
2. Windows:
    a. `C:\Program Files (x86)\ossec-agent\ossec.conf`
    b. `C:\Program Files (x86)\win32ui. Нажмите View> View Config.`

Все внесенные параметры для мониторинга целостности файлов в конфигурационные файлы должны располагаться в разделе `syscheck`:

```
<syscheck>
…
</syscheck>
```

Пример:

```
<!-- File integrity monitoring -->
      <syscheck>
       <disabled>no</disabled>
 <!-- Frequency that syscheck is executed default every 12 hours -->
       <frequency>43200</frequency>
       <scan_on_start>yes</scan_on_start>
<!-- Directories to check  (perform all possible verifications) -->
       <directories>/etc,/usr/bin,/usr/sbin</directories>
       <directories>/bin,/sbin,/boot</directories>
<!-- Files/directories to ignore -->
       <ignore>/etc/mtab</ignore>
       <ignore>/etc/hosts.deny</ignore>
```

```
      <ignore>/etc/mail/statistics</ignore>
      <ignore>/etc/random-seed</ignore>
      <ignore>/etc/random.seed</ignore>
      <ignore>/etc/adjtime</ignore>
      <ignore>/etc/httpd/logs</ignore>
      <ignore>/etc/utmpx</ignore>
      <ignore>/etc/wtmpx</ignore>
      <ignore>/etc/cups/certs</ignore>
      <ignore>/etc/dumpdates</ignore>
      <ignore>/etc/svc/volatile</ignore>
<!-- File types to ignore -->
      <ignore type="sregex">.log$|.swp$</ignore>
<!-- Check the file, but never compute the diff -->
      <nodiff>/etc/ssl/private.key</nodiff>
      <skip_nfs>yes</skip_nfs>
      <skip_dev>yes</skip_dev>
      <skip_proc>yes</skip_proc>
      <skip_sys>yes</skip_sys>
<!-- Nice value for Syscheck process -->
      <process_priority>10</process_priority>
<!-- Maximum output throughput -->
      <max_eps>50</max_eps>
<!-- Database synchronization settings -->
      <synchronization>
        <enabled>yes</enabled>
        <interval>5m</interval>
        <max_eps>10</max_eps>
      </synchronization>
    </syscheck>
```

После того, как все необходимые параметры были добавлены, следует перезапустить Siem Agent с привилегиями администратора, чтобы применить любые изменения конфигурации:

1. Linux:
    a. `systemctl stop siem-agent && sudo systemctl start siem-agent`
    b. `systemctl restart siem-agent`
2. Windows:

```
Restart-Service -Name siem
```

3.15.2 Параметры для настройки мониторинга целостности файлов

Таблица 1 – Поддерживаемые параметры

Параметр	Значение по умолчанию	Допустимые значения	Описание
allow_remote_prefilter_cmd	no	yes, no	Позволяет применить опцию `prefilter_cmd`. Пример: `<allow_remote_prefilter_cmd>yes</allow_remote_prefilter_cmd>`
database	disk	disk, memory	Указывает, где будет храниться база данных.
directories	/etc,/usr/bin,/usr /sbin,/bin,/sbin	Любой каталог Любая переменная среды	Список подлежащих мониторингу каталогов. Каталоги могут быть разделены запятыми или несколькими строками, чтобы включить несколько каталогов. Существует ограничение в 64 каталога, разделённых запятой, которые могут быть записаны в одну строку. Может включать различные атрибуты (табл.2). Пример: `<directories check_all="no" check_sha256="yes">/etc</directories>`
disabled	no	yes, no	Указывает, включен ли мониторинг. Пример: `<disabled>no</disabled>`
frequency	43200	Любое положительное число	Период проверки в секундах. `<frequency>43200</frequency>`

ignore		Любое имя каталога	Список файлов или каталогов, которые должны игнорироваться.
			Игнорируемые файлы и каталоги все еще сканируются, но результаты не сообщаются. Имеет атрибут `type` с значениями `sregex`.
			Примеры:
			`<ignore>/etc/mtab</ignore>`
			`<ignore type="sregex">.log$|.swp$</ignore>`

max_eps	50	От 0 до 1000000	Устанавливает максимальную скорость для отчёта событий. Значение 0 означает, что параметр выключен. Пример: `<max_eps>50</max_eps>`
max_files_per_second	0	Любое целое положительное число	Устанавливает максимальное количество сканируемых файлов в секунду. Если параметр установлен на 0, то ограничений на количество

Параметр	Значение по умолчанию	Допустимые значения	Описание
			просматриваемых файлов в секунду не будет. Пример: `<max_files_per_second>100</max_files_per_second>`
prefilter_cmd	N/A	Команда для предотвращения предварительной компановки	Для предотвращения создания ложных положительных результатов при предварительном подключении. Пример: `<prefilter_cmd>/usr/sbin/prelink -y</prefilter_cmd>`
process_priority	10	От -20 до 19	Устанавливает приоритет процессу мониторинга, где -20 – максимальный приоритет, 19 – минимальный. Пример: `<process_priority>10</process_priority>`
registry_ignore		Любые записи рееста	Список записей в реестре, которые будут проигнорированы. Одна запись на одну строку. Имеет атрибуты `arch` (доступные значения 32bit, 64bit, оба) и `type` с значениями `sregex`. `<registry_ignore>HKEY_LOCAL_MACHINE\Security\Policy\Secrets</registry_ignore>` `<registry_ignore type="sregex">\Enum$</registry_ignore>`
scan_day	N/A	День недели	День недели для мониторинга. Пример: `<scan_day>thursday</scan_day>`
scan_time	N/A	Время в течении дня.	Время начала мониторинга. Пример: `<scan_time>8:30</scan_time>` `<scan_time> 9pm </scan_time>`
skip_dev	yes	yes, no	Указывается, следует ли проводить мониторинг в каталогах /dev. Пример: `<skip_dev>yes</skip_dev>`
skip_nfs	yes	yes, no	Указывается, следует ли проводить мониторинг в сетевых файловых системах. Пример: `<skip_nfs>yes</skip_nfs>`
skip_proc	yes	yes, no	Указывается, следует ли проводить мониторинг в каталогах /proc. Пример: `<skip_proc>yes</skip_proc>`
skip_sys	yes	yes, no	Указывается, следует ли проводить мониторинг в каталогах /sys. Пример: `<skip_sys>yes</skip_sys>`
file_limit	yes	yes, no	Указывается ограничение на количество файлов, которые должны быть на

Параметр	Значение по умолчанию	Допустимые значения	Описание

			мониторинге. Имеет атрибуты `enabled` (доступные значения yes, no) и `entries` (доступны значения с 1 по 2147483647).
			Пример:
			`<!-- Maximum number of files to be monitored -->`
			`<file_limit>`
			`<enabled>yes</enabled>`
			`<entries>100000</entries>`
			`</file_limit>>`

registry_limit	yes	yes, no	Указывается ограничение на количество записей реестра, которые должны быть на мониторинге. Имеет атрибуты `enabled` (доступные значения yes, no) и `entries` (доступные значения с 1 до 2147483647).
			`<!-- Maximum number of registries to be monitored -->`
			`<registry_limit>`
			`<enabled>yes</enabled>`
			`<entries>100000</entries>`
			`</registry_limit>`

synchronization			Параметры синхронизации базы данных. Может включать различные атрибуты (табл.3).
			`<!-- Database synchronization settings -->`
			`<synchronization>`
			`<enabled>yes</enabled>`
			`<interval>5m</interval>`
			
			`<max_interval>1h</max_interval>`
			`<response_timeout>30</response_timeout>`
			
			`<queue_size>16384</queue_size>`
			`<thread_pool>1</thread_pool>`
			`<max_eps>10</max_eps>`
			`</synchronization>`

windows_audit_interval	300 секунд	Любое время от 1 до 9999	Устанавливается частота проверки агентом Windows. Пример: `<windows_audit_interval>300</windows_audit_interval>`

diff			Настройка дифференциальных параметров. Может включать различные атрибуты (табл.4). Пример:
			`<diff>`
			`<disk_quota>`
			`<enabled>yes</enabled>`

Параметр	Значение по умолчанию	Допустимые значения	Описание
			<limit>1GB</limit> </disk_quota> <file_size> <enabled>yes</enabled> <limit>50MB</limit> </file_size> <nodiff>/etc/ssl/private.key</nodiff> </diff>
whodata			Имеет атрибуты restart_audit (доступные значения yes, no), audit_key (любая строка, разделенная запятой), startup_healthcheck (доступные значения yes, no). Пример: <!-- Whodata options --> <whodata> <restart_audit>yes</restart_audit> <audit_key>auditkey1,auditkey2</audit_key> <startup_healthcheck>yes</startup_healthcheck> </whodata>
windows_registry			Список записей в реестре, подлежащих мониторингу. Может включать различные атрибуты (табл.5). Пример: <windows_registry arch="both">HKEY_LOCAL_MACHINE\Software\Classes\Protocols</windows_registry> <windows_registry arch="both" restrict_value="^some_value_name$">HKEY_LOCAL_MACHINE\Software\Policies</windows_registry> <windows_registry arch="both" check_sum="no">HKEY_LOCAL_MACHINE\SOFTWARE\test_key</windows_registry> <windows_registry arch="64bit" recursion_level="3">HKEY_LOCAL_

Параметр	Значение по умолчанию	Допустимые значения	Описание
			MACHINE\SYSTEM\Setup</windows_registry>

Например, мониторинг в режиме реального времени:

```
<syscheck>
    <directories
    realtime="yes"><FILEPATH_OF_MONITORED_DIRECTORY></directories>
</syscheck>
```

Таблица 2 – Поддерживаемые атрибуты параметра `directories`

Атрибут	Значение по умолчанию	Допустимые значения	Описание
realtime	no	yes, no	Для мониторинга в реальном времени. Работа в реальном времени только с каталогами, но не с отдельными файлами.
whodata	no	yes, no	Отслеживание данных.
report_changes	no	yes, no	Отслеживание изменений в файле (только текстовые файлы).
diff_size_limit	50MB	Любое число в формате KB/MB/GB	Ограничение максимального размера файла, который будет сообщать сведения о различии при включении `report_changes`. Файлы, превышающие это значение, не будут сообщать информацию о различии.
check_all	yes	yes, no	Записывает значения всех атрибутов ниже.
check_sum	yes	yes, no	Записывает хэш запущенных файлов с заранее посчитанными значениями (MD5, SHA1, и SHA256). Аналогичен следующим атрибутам: `check_md5sum="yes", check_sha1sum="yes", check_sha256sum="yes.`
check_sha1sum	yes	yes, no	Записывает хеш файлов (SHA-1).
check_md5sum	yes	yes, no	Записывает хеш файлов (MD5).
check_sha256sum	yes	yes, no	Записывает хэш файлов (SHA-256).

Атрибут	Значение по умолчанию	Допустимые значения	Описание
check_size	yes	yes, no	Записывает размер файлов.
check_owner	yes	yes, no	Записывает владельца файлов в Linux.
check_group	yes	yes, no	Записывает группу владельцев файлов или директориев. В ОС Windows, Group ID всегда 0 и имя группы пустое значение.
Атрибут	Значение по умолчанию	Допустимые значения	Описание
check_perm	yes	yes, no	Записывает разрешение файлов/каталогов. В Windows для каждого пользователя или группы записывается список запрещенных и разрешенных файлов/каталогов. Он работает на Linux и Windows с разделами NTFS.
check_attrs	yes	yes, no	Записывает атрибуты файлов в Windows.
check_mtime	yes	yes, no	Записывает время изменения файла.
check_inode	yes	yes, no	Записывает файл `inode` в Linux.
restrict	N/A	sregex	Ограничение проверки файлов, содержащих введенную строку в имени файла. Любой путь к каталогу или файлу разрешен.
tags	N/A	Список тегов, разделенный запятыми	Для добавления тегов в уведомления для каталогов, находящихся на мониторинге.
recursion_level	256	Число от 0 до 320	Ограничение максимального уровня рекурсии.

Например, когда существует конфликт между вариантами, изменяющими один и тот же атрибут, последний из них отменяет все действия:

```
<directories check_all="no" check_sha256="yes">/etc</directories>
```

Если существует конфликт между блоком с подстановочными знаками и другим без них, то для конкретного случая будет использоваться блок без подстановочных знаков. В качестве примера:

```
<directories>C:\Users\*\Downloads</directories>
```

Таблица 3 – Поддерживаемые атрибуты параметра `synchronization`

Атрибут	Значение по умолчанию	Допустимые значения	Описание
enabled	yes	yes, no	Указывается, что периодические синхронизации инвентаризации выполняются.
registry_enabled	yes	yes, no	На агентах Windows, позволяет делать синхронизацию инвентаризации для записей в реестре.
interval	5 m (s, m, h, d).	Любое число больше или равное 0.	Указывается начальный промежуток времени между синхронизациями инвентаризации.
max_interval	1 h	Любое число больше или равное interval (s, m, h, d).	Максимальный интервал времени для запуска синхронизации.
response_timeout	30	Любое число от 0 до interval.	Время ожидания в секундах после отправки или получения сообщения синхронизации для следующей операции синхронизации. Если агент не отправляет или не получает сообщение в этом интервале, синхронизация отмечена как успешная.
queue_size	16384	Целое число в промежутке от 2 до 1000000	Указывается размер очереди ответов менеджера на синхронизацию.
thread_pool	1	Любое целое число, больше 0.	Указывается количество потоков, используемых для синхронизации базы данных.
max_eps	10	Целое число в промежутке от 0 до 1000000	Устанавливается максимальная скорость передачи сообщений синхронизации.

Таблица 4 – Поддерживаемые атрибуты параметра `diff`

Атрибут	Значение по умолчанию	Допустимые значения	Описание
disk_quota			Этот атрибут может быть использован для ограничения размера папки *queue/diff/local*, где SIEM хранит сжатые файлы, используемые для выполнения операции *diff*, когда *report_changes* включена. Имеет атрибуты *enabled* (доступные значения yes, no) и *limit*

Атрибут	Значение по умолчанию	Допустимые значения	Описание
			(любое положительное число KB/MB/GB).
file_size			Эта опция может быть использована для ограничения размера файла, который будет сообщать информацию о различиях при включении `report_changes`. Имеет атрибуты `enabled` (доступные значения yes, no) и `limit` (любое положительное число KB/MB/GB).
nodiff		Любое имя файла	Список файлов, не подлежащих вычислению (один файл на строку). Пример: `/etc/ssl/private.key`
registry_nodiff		Любой путь реестра, с добавленным value_name	Список значений, не подлежащих вычислению (один элемент на строку). Пример: `HKEY_LOCAL_MACHINE\SOFTWARE\test_key\value_name`

Таблица 5 – Поддерживаемые атрибуты параметра `windows_registry`

Атрибут	Значение по умолчанию	Допустимые значения	Описание
arch	32bit	32bit, 64bit, оба	Выбор `Registry view` в зависимости от архитектуры.
tags	N/A	Список тегов, разделенный запятыми	Для добавления тегов в уведомления для каталогов, находящихся на мониторинге.
report_changes	no	yes, no	Отслеживание изменений в файле (только текстовые файлы).
diff_size_limit	50MB	Любое число в формате KB/MB/GB	Ограничение максимального размера файла, который будет сообщать сведения о различии при включении `report_changes`. Файлы, превышающие это значение, не будут сообщать информацию о различии.
check_all	yes	yes, no	Записывает значения всех атрибутов ниже.

Атрибут	Значение по умолчанию	Допустимые значения	Описание
check_sum	yes	yes, no	Записывает хэш запущенных файлов с заранее посчитанными значениями (MD5, SHA1, и SHA256). Аналогичен следующим атрибутам: `check_md5sum="yes"`, `check_sha1sum="yes"`, `check_sha256sum="yes.`
check_sha1sum	yes	yes, no	Записывает хеш файлов (SHA-1).
check_md5sum	yes	yes, no	Записывает хеш файлов (MD5).
check_sha256sum	yes	yes, no	Записывает хэш файлов (SHA-256).
check_size	yes	yes, no	Записывает размер файлов.
check_owner	yes	yes, no	Записывает владельца файлов в Linux.
check_group	yes	yes, no	Записывает группу владельцев файлов или директориев. В ОС Windows, Group ID всегда 0 и имя группы пустое значение.
check_perm	yes	yes, no	Записывает разрешение файлов/каталогов. В Windows для каждого пользователя или группы записывается список запрещенных и разрешений. Он работает на Linux и Windows с разделами NTFS.
check_mtime	yes	yes, no	Записывает время изменения файла.
check_type	yes	yes, no	Записывает файл `inode` в Linux.
restrict_key	N/A	sregex	Ограничивается проверка реестрами, содержащими в имени реестра введенные `sregex`. Допускается любое значение реестра.
restrict_value	N/A	sregex	Ограничивается проверка значений реестра, содержащие введенное значение `sregex` в имени значения. Допускается любое значение реестра.
recursion_level	256	Число от 0 до 320	Ограничение максимального уровня рекурсии.

Уведомления в системе будут выглядеть следующим образом:

Источник	Локализация	Сырое событие
10.72.144.42	File deleted.	File '/home/darkneo/test_fim123.txt' deleted\nMode: realtime\n
10.72.144.42	File deleted.	File '/home/darkneo/test_fim.txt' deleted\nMode: realtime\n
10.72.144.42	Integrity checksum changed.	File '/home/darkneo/script.sh' modified\nMode: realtime\nChanged
10.72.144.42	Integrity checksum changed.	File '/home/darkneo/script.sh' modified\nMode: realtime\nChanged
10.72.144.42	Integrity checksum changed.	File '/home/darkneo/script.sh' modified\nMode: realtime\nChanged
10.72.144.42	File added to the system.	File '/home/darkneo/script.sh' added\nMode: realtime\n
10.72.144.42	Integrity checksum changed.	File '/home/darkneo/denis_milodec.txt' modified\nMode: realtime\n.
10.72.144.42	Integrity checksum changed.	File '/home/darkneo/denis_milodec.txt' modified\nMode: realtime\n.
10.72.144.42	Integrity checksum changed.	File '/home/darkneo/denis_milodec.txt' modified\nMode: realtime\n.

Рисунок 49 – Страница «События»

Кроме того, в системе будут созданы инциденты:

ID	Критичность	Дата	Название	Статус
393	⌄	30.08.2024, 11:12:13	File deleted.	Новые
392	⌄	30.08.2024, 11:10:37	File deleted.	Новые
391	⌄	30.08.2024, 09:51:26	Integrity checksum changed.	Новые
390	⌄	30.08.2024, 09:48:21	Integrity checksum changed.	Новые
389	⌄	30.08.2024, 09:47:35	Integrity checksum changed.	Новые
388	⌄	30.08.2024, 09:08:26	Integrity checksum changed.	Новые
387	⌄	30.08.2024, 09:08:12	Integrity checksum changed.	Новые
386	⌄	30.08.2024, 09:00:55	Integrity checksum changed.	Новые

Рисунок 50 – Страница «Инциденты»

Приложение А

Таблица 6 – Таблица привилегий ролей в системе NT SIEM

№ п/п	Привилегия	Суперадминистратор	Администратор	Оператор
Пользователи				
1.1	Просмотреть всех пользователей	✓		
1.2	Просмотреть пользователя	✓		
1.3	Создать пользователя	✓		
1.4	Обновить пользователя	✓		
1.5	Удалить пользователя	✓		
1.6	Присвоить роль пользователю	✓		
1.7	Удалить роль пользователя	✓		
1.8	Просмотреть роль пользователя	✓		
Роли				
2.1	Просмотреть роли	✓		
2.2	Создать роль	✓		
2.3	Редактировать роль	✓		
2.4	Удалить роль	✓		
Инциденты				
3.1	Просмотреть инциденты	✓	✓	✓
3.2	Просмотр истории инцидента	✓	✓	✓
3.3	Создать инцидент	✓	✓	✓
3.4	Редактировать инцидент	✓	✓	✓
3.5	Удалить инцидент	✓	✓	✓

№ п/п	Привилегия	Суперадминистратор	Администратор	Оператор
3.6	Добавление события к инциденту	✓	✓	✓
3.7	Удаление события из инцидента	✓	✓	
	События			
4.1	Просмотреть список событий	✓	✓	✓
4.2	Работа со списками запросов	✓	✓	✓
4.3	Возможность делиться списками	✓	✓	
	Агенты			
5.1	Просмотреть список агентов	✓	✓	✓
5.2	Перезагрузить агента	✓	✓	✓
5.3	Обновить агента	✓	✓	✓
5.4	Удалить агента	✓	✓	✓
5.5	Посмотреть результат обновления агента	✓	✓	✓
5.6	Добавить агента	✓	✓	
	База правил			
6.1	Просмотреть базу правил	✓	✓	
6.2	Просмотреть элемент базы правил	✓	✓	
6.3	Управление элементом базы правил (создать, редактировать, загрузить)	✓	✓	
6.4	Удалить элемент базы правил	✓	✓	
6.5	Перезагрузка менеджера	✓	✓	
	Отчеты			
7.1	Выгрузить отчет	✓	✓	✓

№ п/п	Привилегия	Суперадминистратор	Администратор	Оператор
Профиль пользователя				
8.1	Просмотреть личный профиль	✓	✓	✓
Лицензирование				
9.1	Просмотреть информацию о лицензии	✓		
9.2	Загрузить ключ лицензирования	✓		
Настройки системы				
10.1	Обновить системные правила	✓		
10.2	Просмотреть настройки SOAR	✓		
10.3	Обновить настройки SOAR	✓		
10.4	Просмотреть настройки почты	✓		
10.5	Обновить настройки почты	✓		