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 основные функциональные возможности:

- Сбор журналов событий с различных источников;
- Визуализация данных в виде графиков, диаграмм в форме дашбордов;
- Анализ журналов событий в соответствии с правилами нормализации, корреляции, агрегации и обогащения;
- Формирование инцидентов на основе процессов агрегации, обогащения и корреляции;
- Управление инцидентами 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, а также возможность создания собственных правил и табличных списков;
- Мониторинг состояния системы;
- Отправка уведомлений пользователям в рамках веб-приложения и по электронной почте;

- Формирование и выгрузка отчетов за определенный период времени;
- Осуществление интеграций, в том числе и с SOAR-системами;
- Мониторинг активов.

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»;
- «Активы»;
- «Отчеты»;
- «База правил»;
- «Настройки системы».

Следует обратить внимание, что в стандартной ролевой модели доступ к группам страниц «База правил» 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 <.

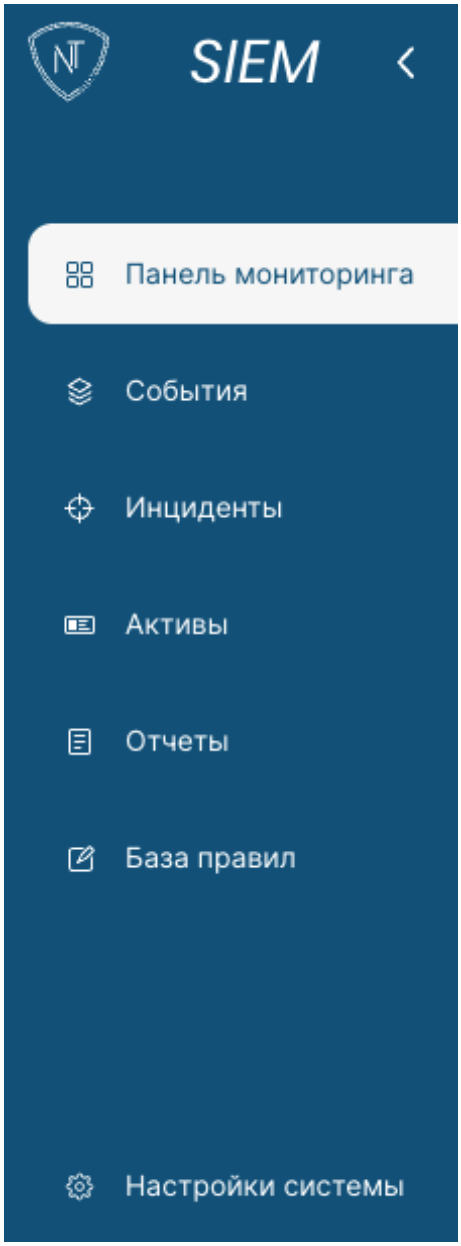


Рисунок 1 - Главное меню в развернутом виде

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.

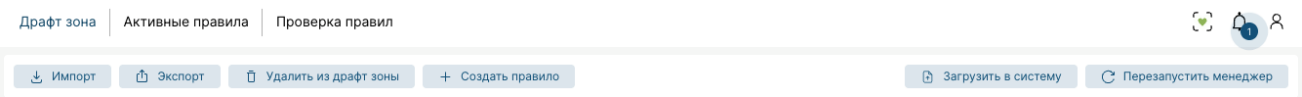


Рисунок 3 - Верхняя навигационная панель

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 и возможности сменить пароль;

Справка для скачивания эксплуатационной документации;

О системе для просмотра информации о системе (версия и дата выпуска ПО);

Выйти для выхода из учетной записи и возврата на страницу авторизации.

– Уведомления об инцидентах и активах. При нажатии на кнопку открывается список уведомлений об инцидентах и о состоянии актива. Можно удалить одно уведомление, нажав на иконку , которая находится рядом с выбранным уведомлением, а также очистить весь список уведомлений, нажав на кнопку вверху списка Удалить все . Для перехода на страницу с подробной информацией об инциденте или активе необходимо нажать на выделенную синим цветом ссылку Перейти к инциденту.

– Системные уведомления. При нажатии на кнопку открывается список с системными уведомлениями: о состоянии лицензии, о доступности свободного пространства на жестком диске Системы и о сбоях работы системы. Для перехода на страницу с подробной информацией необходимо нажать на выделенную синим цветом ссылку Перейти к настройкам.

Уведомления имеют свои цвета, отражающие степень критичности содержащейся в них информации для системы: светло-зеленый – удовлетворительное состояние системы, желтый цвет – низкая критичность, оранжевый цвет – требуется повышенное внимание, красный – предупреждение о серьезной проблеме.

Следует обратить внимание, что цвет на иконке может меняться, в зависимости от того, какие уведомления содержатся в списке. Например, если есть хоть одно критическое уведомление, то цвет изменится на красный.

Рядом с иконками уведомлений после действий пользователя в системе всплывают ответы системы об успешности или неуспешности операций, а также другие информационные сообщения.

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.

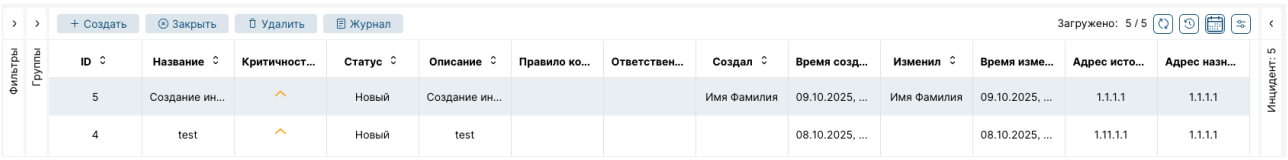


Рисунок 5 – Рабочая область

Рабочая область может быть разделена на несколько частей, которые можно на некоторых страницах скрывать (рис.6), а также иметь кнопки для выполнения определенных функций. Для удобства отображения можно вручную изменить ширину частей рабочей области.

Рисунок 6 – Рабочая область с боковой панелью

2.5 Гибкие таблицы, множественный выбор

На некоторых станицах рабочая область содержит таблицы с данными. При первом переходе на страницу данные в таблице представлены со стандартным набором столбцов, однако при необходимости их можно добавить или убрать. Данные сохранятся для данного пользователя. Для того, чтобы изменить набор следует нажать кнопку  , и далее появится список с возможными вариантами столбцов (рис.7), где следует поставить или убрать галочку 

. Как следствие, таблица будет изменена согласно выбранным столбцам. Для того, чтобы изменения были сохранены,

необходимо нажать кнопку Сохранить , после чего конфигурация таблицы применится и сохранится. Минимально в таблице должен быть один столбец.

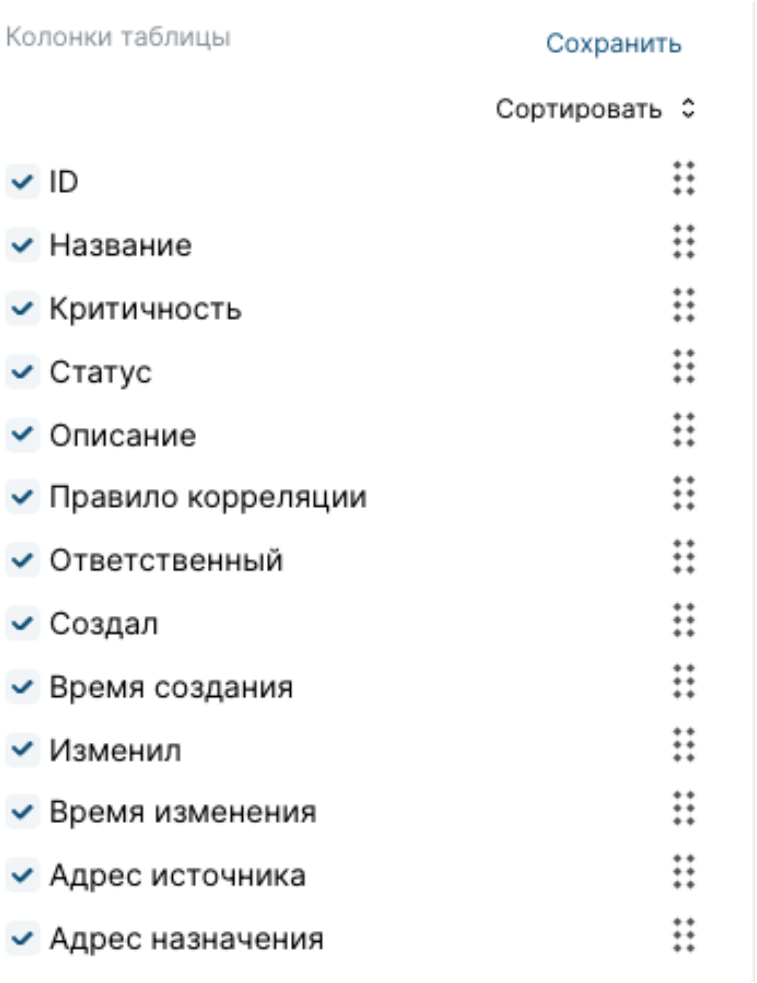


Рисунок 7– Список с возможными вариантами столбцов

Можно изменить порядок отображения столбцов: для этого следует зажать строку в списке со столбцами и перетянуть на нужное место. Также можно отсортировать столбцы в алфавитном порядке с помощью элемента Сортировать , после чего соответствующие изменения отобразятся в таблице (рис. 8).

Для удобства отображения данных можно так же вручную изменить ширину столбцов в таблице. Для сохранения ширины колонок необходимо нажать кнопку «Сохранить», необходимо нажать кнопку Сохранить , после чего конфигурация таблицы применится и сохранится.

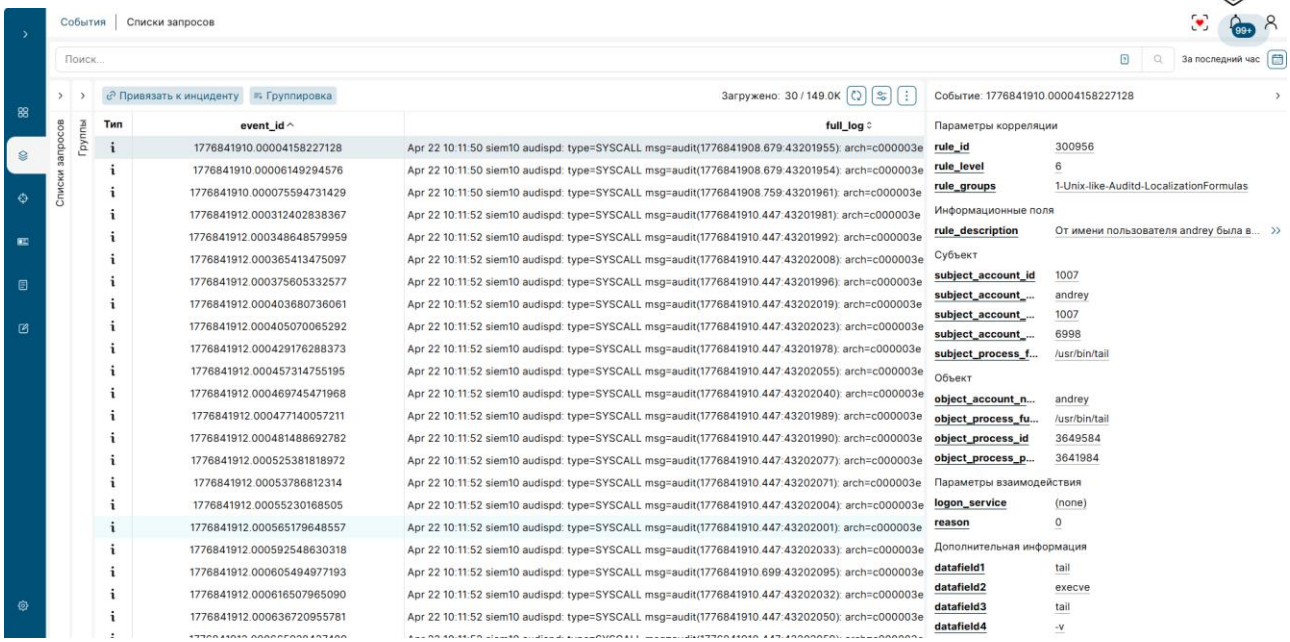


Рисунок 8 – Сортировка столбцов в гибких таблицах

В таблицах поддерживается множественный выбор элементов. При этом будет предоставляться подробная информация по первому выделенному элементу (рис.9).

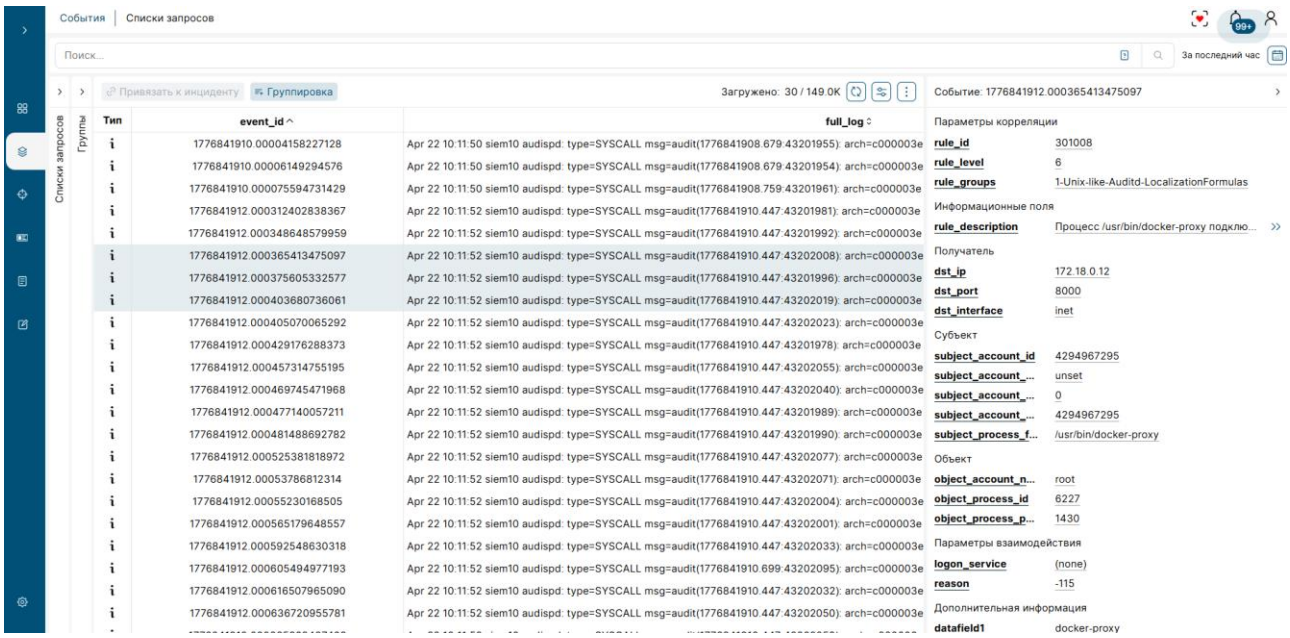


Рисунок 9 – Множественный выбор элементов таблицы

3.Основные процессы в системе

3.1 Интерфейс раздела «Панель мониторинга»

При входе в NT SIEM по умолчанию открывается группа страниц «Панель мониторинга» со стандартным дашбордом. Следует обратить внимание, что при первом входе в систему после установки NT SIEM некоторые виджеты будут пустыми, вследствие отсутствия информации о собранных событиях и выявленных инцидентах.

На предустановленном дашборде можно просмотреть информацию в виде виджетов и настраивать период времени для фильтрации отображаемой информации. Кроме того, можно настраивать автоматическое обновление, как виджетов по отдельности, так и всего дашборда в целом. При этом настройка отдельного виджета имеет более высокий приоритет, чем настройка всего дашборда.

Предустановленный дашборд содержит в себе преднастроенные виджеты:

- Круговая диаграмма с информацией об инцидентах, разделенных по статусам (новый, в работе, закрыт, закрыт как ложноположительный);
- Полукруговая диаграмма с информацией об инцидентах, разделенных по критичности (низкая, средняя, высокая);
- Полукруговая диаграмма с событиями по категориям (нормализованные, ненормализованные);
- Линейный график с информацией о количестве событий в секунду, поступающих в систему;
- Столбчатая диаграмма с информацией об активах, разделенных по значимости (низкая, средняя, высокая);
- Столбчатая диаграмма с информацией об активах по состоянию (актуальные, неактуальные, неподключенные).

Если необходимо, можно скрыть параметры, отображаемые на виджете. Для этого следует нажать на соответствующий параметр, после чего виджет будет обновлен.

Виджеты являются кликабельными. При нажатии на какой-либо участок диаграммы осуществляется переход на страницу с детализацией (активы, события или инциденты), где отфильтрована информация именно по выбранному фрагменту.

Помимо предустановленного дашборда, система также обеспечивает возможность создания пользовательских – с расширенным набором виджетов и дополнительными возможностями по их настройке.

3.2 Работа с дашбордами и виджетами

3.2.1 Работа с преднастроенным дашбордом

Информация на виджетах обновляется автоматически по умолчанию каждые 60 секунд, за исключением виджета с количеством событий в секунду, для которого настроено автообновление раз в 5 минут. Для обновления виджета вручную необходимо нажать кнопку  и выбрать опцию «Обновление» – 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.10).

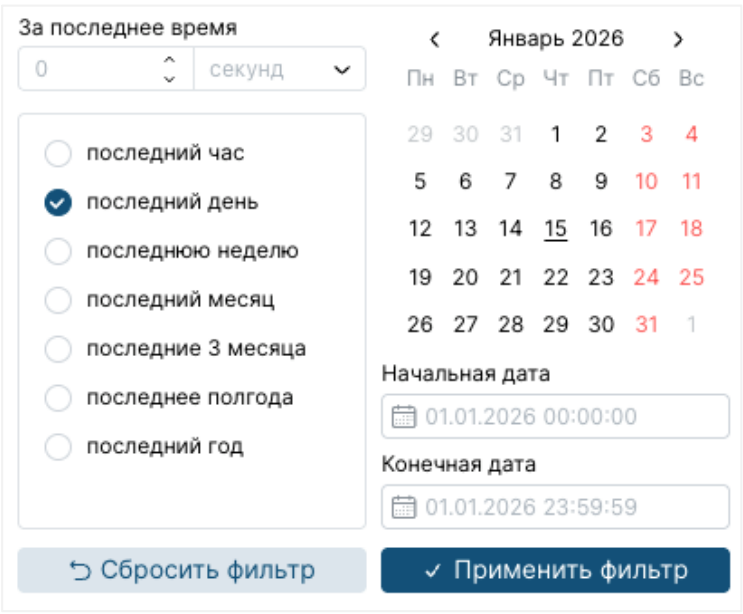


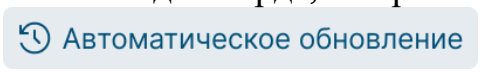
Рисунок 10 – Фильтрация по временному периоду для виджета

Для применения выбранных параметров необходимо нажать на кнопку «Применить фильтр» в модальном окне. В свою очередь, при нажатии на кнопку «Сбросить фильтр» происходит очистка выбранных параметров и возвращение виджета в исходное состояние (по умолчанию). Закрыть календарь можно путем нажатия на любую область вне модального окна. Следует обратить внимание, что подчеркнутое число – дата, установлена в операционной системе как сегодняшний день.

Для виджетов предусмотрены следующие настройки по умолчанию:

Название виджета	Фильтр по времени	Автоматическое обновление
События по категориям	За последний час	Каждую минуту

Название виджета	Фильтр по времени	Автоматическое обновление
Инциденты по критичности	За последний день	Каждую минуту
Инциденты по статусам	За последний день	Каждую минуту
Активы по значимости	Нет, отображаются данные за все время	Каждую минуту
Состояние активов	Нет, отображаются данные за все время	Каждую минуту
Количество событий в секунду (EPS)	За последний день	Каждые 5 минут.

Для установки автоматического обновления всего дашборда, в правом верхнем углу страницы предусмотрена кнопка 

. При нажатии на нее открывается окно с возможностью выбора периода автоматического обновления (рис.11).

При этом настройка отдельного виджета имеет более высокий приоритет, чем настройка всего дашборда.

Для настройки автоматического обновления виджета необходимо нажать кнопку  и в появившемся окне выбрать необходимый параметр.

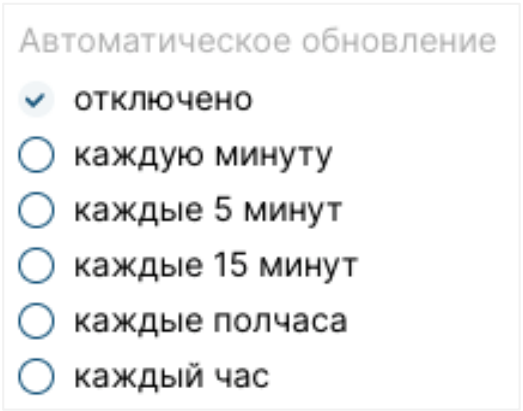


Рисунок 11 – Выбор периода автоматического обновления дашборда

3.2.2 Работа с пользовательским дашбордом

Для создания пользовательского дашборда следует нажать кнопку + на панели инструментов рядом с наименованием системного дашборда. Далее новые дашборды создаются в режиме редактирования (рис. 12).

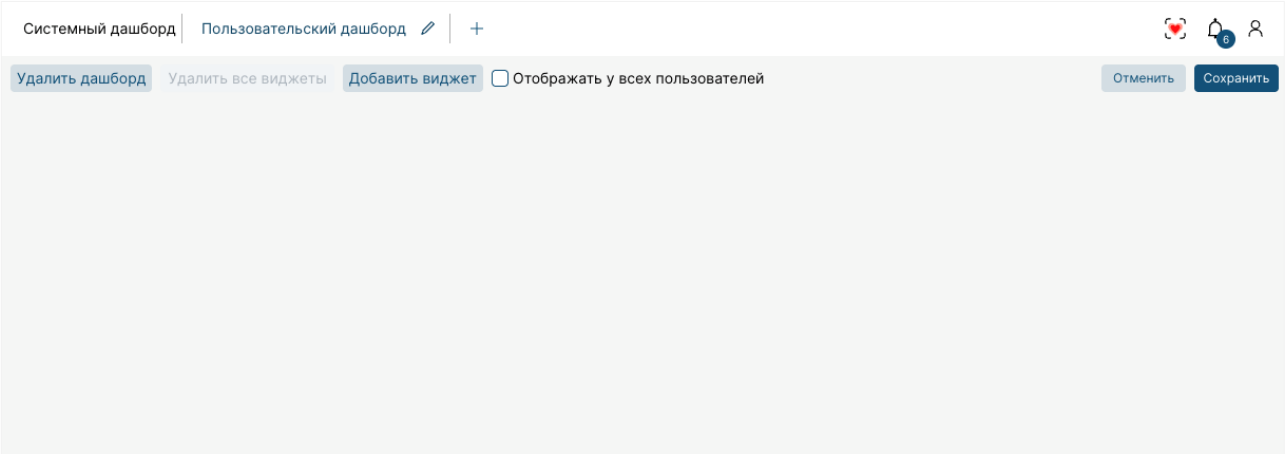


Рисунок 12 – Пользовательский дашборд в режиме редактирования

Для того, чтобы переименовать дашборд нужно нажать , после чего поле с наименование будет доступным для изменения Пользовательский дашборд 24/50 . Новые изменения сохраняются после нажатия на галочку . Переименовать дашборд можно как в режиме редактирования, так и в режиме просмотра. Следует обратить внимание на наличие ограничения количества символов (максимум - 50).

Для того, чтобы распространить дашборд среди пользователей системы в рамках одной установки, необходимо поставить соответствующую галочку Отображать у всех пользователей , после чего дашборд станет доступен для просмотра тем пользователям, которые обладают правами на просмотр пользовательских дашбордов. Следует обратить внимание, что редактировать и удалять дашборд может только его автор.

Для сохранения дашборда и всех внесенных изменений следует нажать кнопку Сохранить. Однако, при нажатии на Отменить или при выходе из режима редактирования без сохранения, все внесенные изменения будут утеряны без возможности восстановления. Для того, чтобы вернуть в режим редактирования следует нажать кнопку Редактировать.

Для удаления дашборда следует воспользоваться режимом редактирования (рис. 12), далее нажать кнопку Удалить дашборд и во всплывающем уведомлении подтвердить действие. Результат операции отобразится в уведомлениях.

3.2.3 Работа с виджетами на пользовательском дашборде

Для добавления виджета на пользовательский дашборд необходимо нажать на кнопку Добавить виджет, после чего откроется модальное окно со списком доступных виджетов (рис. 13). При необходимости можно воспользоваться поисковой строкой для быстрого поиска нужного виджета. В открывшемся окне следует выбрать виджет, при необходимости изменить тип

его визуализации и нажать на кнопку «Добавить», после чего виджет будет добавлен на дашборд.

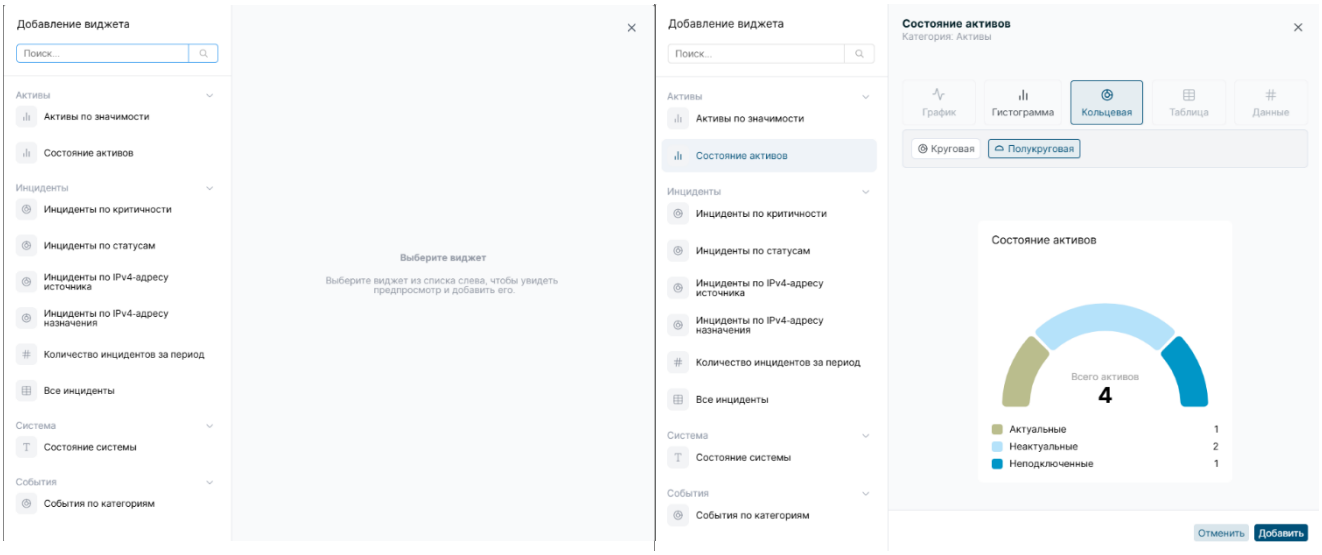


Рисунок 13 – Выбор и добавление виджета

После того, как виджет был добавлен на дашборд необходимо закрыть модальное окно нажав на ✕ или на область вне модального окна.

Положение виджета на дашборде можно изменить. Для этого необходимо зажать левой кнопкой мыши элемент ✥ и перетащить виджет в желаемое место. Остальные элементы на дашборде автоматически изменят положение в соответствии с внесенными изменениями.

При необходимости можно изменить и размер виджета. Для этого необходимо потянуть за правый нижний уголок виджета и, удерживая его, растянуть или сжать виджет до нужных размеров.

Для настройки виджета необходимо нажать на кнопку ⋮ и выбрать опцию «Настроить». Откроется модальное окно, в котором можно изменить наименование виджета, а также выбрать доступный тип визуализации диаграммы (рис. 14).

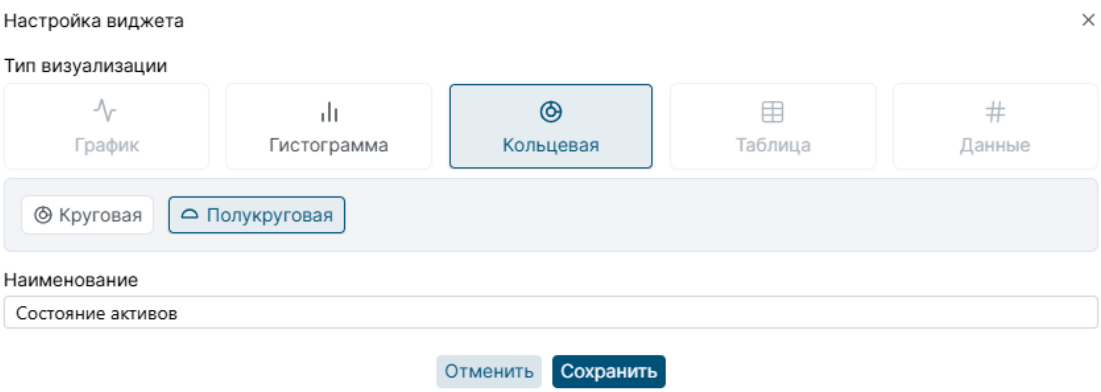


Рисунок 14 – Настройка виджета

Для виджета «EPS указанных источников» в окне настроек также предусмотрен блок для управления IP – адресами:

- **Добавление адреса.** В поле «IP-адрес источника» необходимо ввести адрес и сохранить изменение. Следует обратить внимание, что без заполненного адреса отображение актуального графика невозможно.
- **Редактирование.** Добавленные адреса отображаются в списке. Для изменения адреса можно воспользоваться редактированием.
- **Включение и отключение.** Предусмотрена возможность не удалять адрес, а временно отключить его. Это позволяет при необходимости быстро включить адрес обратно, не вводя его заново.
- **Удаление**. Ненужные адреса можно удалить из списка.
- **Защита от повторов.** При попытке добавить уже существующий в списке адрес действие блокируется с информационным уведомлением «Такой адрес уже добавлен».
- **Отмена изменений.** Чтобы отменить изменения в поле ввода адреса и выйти из режима редактирования, необходимо нажать на крестик в поле ввода. Для сохранения всех изменений необходимо нажать кнопку Сохранить, для отмены — кнопку Отменить.

Для удаления виджета можно нажать на кнопку ⋮ и выбрать опцию «Удалить виджет» или использовать кнопку Удалить все виджеты для удаления сразу всех виджетов на дашборде. Результат операции отобразится в уведомлениях.

После сохранения дашборда система выходит из режима редактирования. В режиме просмотра доступны следующие возможности:

- **Обновление виджетов.** Можно обновлять данные в виджетах вручную.
- **Фильтрация по времени.** Для большинства виджетов доступна настройка временного диапазона (исключение составляют виджеты «Активы по значимости», «Состояние активов», «Состояние системы»).
- **Автоматическое обновление.** Можно настроить автообновление как для отдельного виджета, так и для всего дашборда целиком. Работа с данными настройками аналогична работе с системным дашбордом (см. п. 3.2.1).

Следует обратить внимание, что настройка отдельного виджета имеет более высокий приоритет, чем настройка всего дашборда.

При создании большого количества пользовательских дашбордов верхняя навигационная панель может заполниться. В таком случае необходимо воспользоваться колесом прокрутки компьютерной мыши.

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» можно просматривать перечень событий и информацию о них, выполнять фильтрацию и привязку событий к инциденту, группировать и выгружать события в файл в формате `.csv`.

В таблице на странице «События» отображается информация по всем событиям: как нормализованным, так и ненормализованным.

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 `rule_level`. Событию может быть присвоен уровень от 0 до 15. При уровне критичности события 7 и выше создается инцидент.

Ненормализованным считается событие, не прошедшее нормализацию. Уровень критичности не присваивается.

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

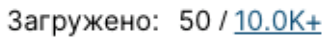
 – для фильтрации элементов в таблице по временному периоду;

 – для обновления таблицы;

 – для настройки периодичности обновления таблицы и экспорта событий;

 – для работы с гибкими таблицами (п. 2.5);

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



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

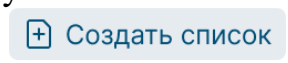
Рабочая область страницы разделена на части: в центре расположена таблица с перечнем событий, слева – список доступных запросов и группы событий, а справа – боковая панель с подробной информацией о выбранном событии, структурированной по категориям. По умолчанию левые боковые панели отображаются в свернутом виде, правая панель – в развернутом. Для раскрытия левых панелей или закрытия правой необходимо нажать на кнопку раскрытия `>` или кнопку закрытия `<` соответственно.

Следует обратить внимание, что событию в зависимости от уровня (поле `rule_level`) присваивается тип:

- Информативное событие  (уровень 0-6);
- Низкая критичность  (уровень 7-9);
- Средняя критичность  (уровень 10-12);
- Высокая критичность  (уровень 13-15).

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 загрузки списков запросов в систему. Для работы с кнопкой на панели инструментов необходимо выбрать элементы из перечня;

 – для скачивания 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.15). 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. Данные в таблице по умолчанию показаны за последний час.

Также можно сортировать события в таблице при нажатии на наименование поля. При первом нажатии будет произведена сортировка по возрастанию, а при повторном нажатии меняется на противоположную.

Процесс фильтрации может быть осуществлен одновременно по периоду и по поисковым запросам.

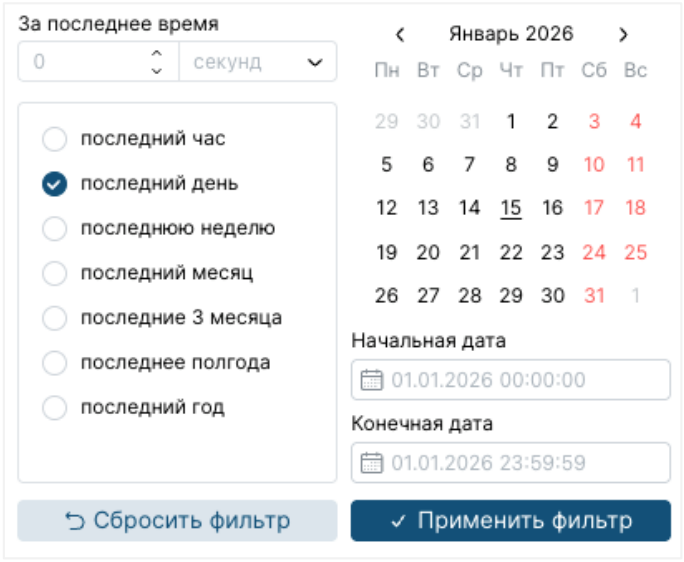


Рисунок 15 – Компонент «Календарь» для фильтрации по дате и времени

Для обновления данных в таблице необходимо нажать на кнопку . Для настройки периода автоматического обновления данных следует нажать , в открывшемся списке выбрать вариант «Автоматическое обновление» и настроить временной интервал (по умолчанию – пятнадцать минут).

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

Для удобства ввода запросов в строке поиска предусмотрена функция подсказок. Система предлагает два типа подсказок:

- подсказки по полям (ключам);
- подсказки по логическим операторам.

Подсказки по ключам содержат названия доступных полей для поиска, (например, `rule_level`, `rule_id`, `rule_groups`). Список полей соответствует настройкам отображения таблицы на странице «События» (за исключением поля `full_log`).

Подсказки по логическим операторам содержат операторы AND, OR, NOT для построения сложных поисковых запросов.

Подсказки отображаются в виде выпадающего списка с возможностью прокрутки. Выбор осуществляется стрелками ↓↑ и клавишей Enter или кликом мыши по необходимому элементу.

В поисковой строке доступна кнопка (по умолчанию активна), которая позволяет:

- временно отключить отображение подсказок;
- включить подсказки обратно.

Состояние кнопки (включено/ выключено) сохраняется при переходе между страницами.

Информация о событии в правой части рабочей области разделена по полям (например, `location`, `dst_ip` 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.16). А для поля корреляции `rule_id`, `decoder_name` предусмотрена возможность просмотра правила, по которому было обработано событие.

В свою очередь поля событий распределены по категориям: параметры корреляции, информационные поля, дополнительная информация, точка сбора, служебные данные.

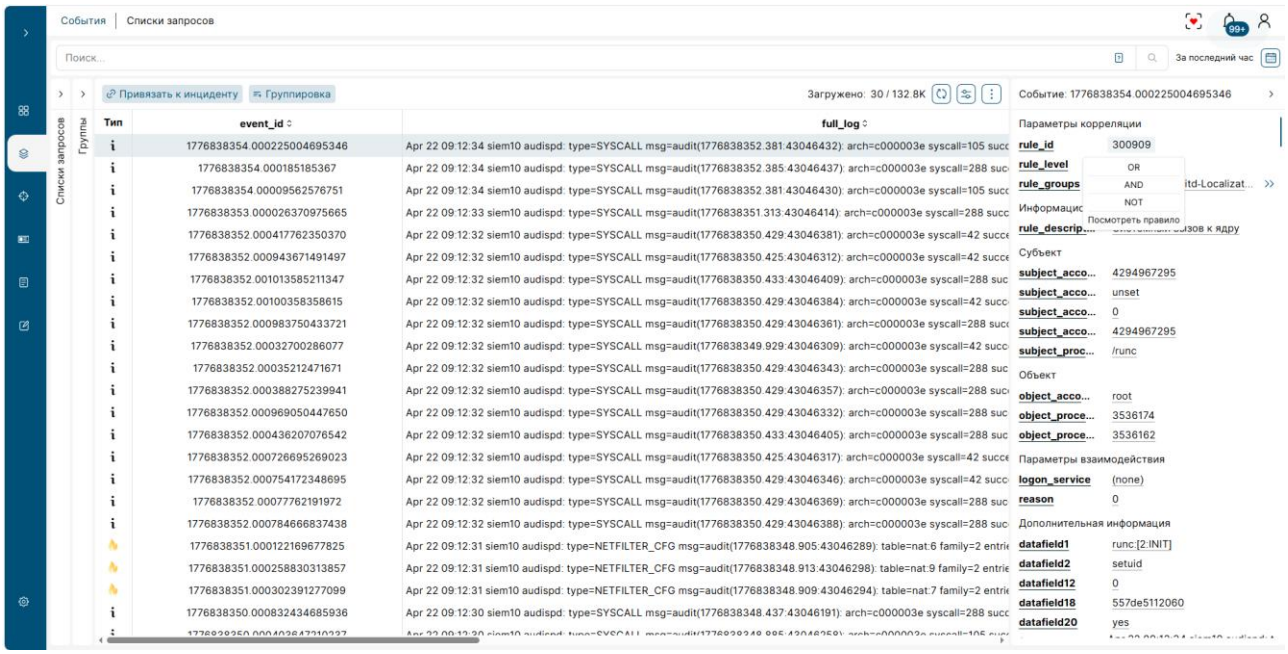


Рисунок 16 – Быстрый поиск по событиям

Следует обратить внимание, что поле `full_log` можно скопировать. Для этого следует навести курсор 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 к инциденту. Далее откроется список с доступными для связи инцидентами (рис. 17). Можно воспользоваться поисковой строкой для поиска инцидента, для этого следует ввести валидный запрос (см. Руководство по запросам).

Далее следует выбрать существующий инцидент из списка и нажать на кнопку «Привязать». Для закрытия окна необходимо нажать на кнопку ✕ или

на кнопку «Отменить». Следует обратить внимание, что к одному инциденту можно привязать несколько событий.

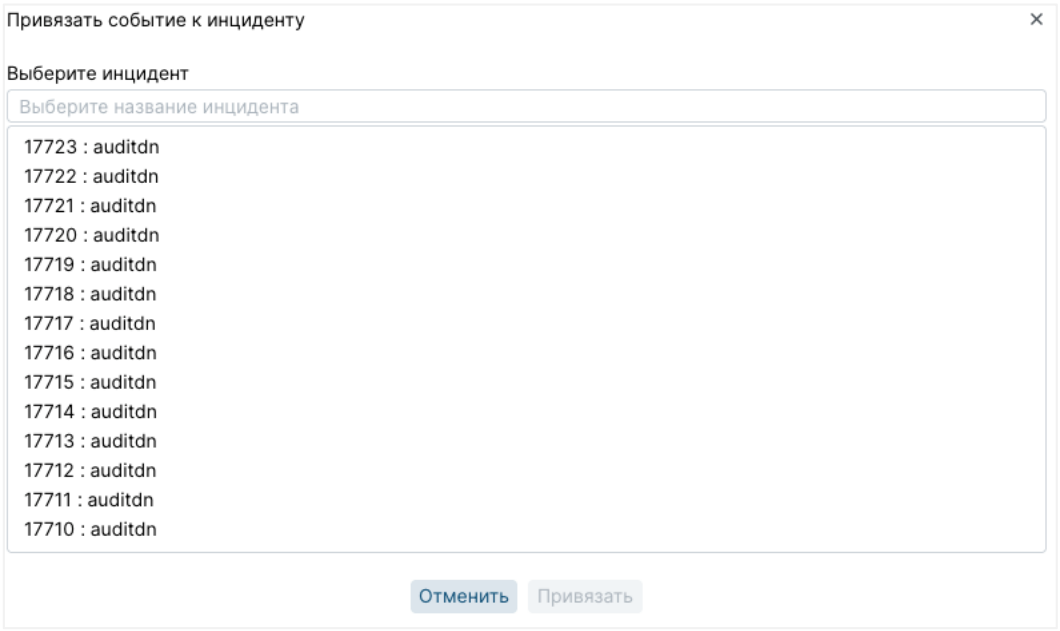


Рисунок 17 – Функция привязки события к инциденту

3.4.3 Выгрузка событий

Для того, чтобы выгрузить события, необходимо нажать  и выбрать опцию: «Скачать выбранные события» или «Скачать все события»:

- Если выбрана опция «Скачать выбранные события», то выгрузиться только выделенные в таблице события в формате csv;
- Если выбрали опцию «Скачать все события», то выгрузятся все события с учетом фильтрации и/или выбранного временного периода в формате csv. Однако, если не был выбран период или не произведена фильтрация, то по умолчанию, установлен лимит выгрузки за весь период с ограничение в 100 тысяч строк.

3.4.4 Группировка событий

На странице «События» доступна функция группировки событий по одному или нескольким полям.

Настроить группировку можно двумя способами:

- через правую боковую панель;
- с помощью модального окна «Группировка».

Оба способа взаимосвязаны: настройки группировки синхронизируются между интерфейсами. Поля, выбранные в правой панели, автоматически отображаются в модальном окне, и наоборот.

Для группировки событий через правую боковую панель необходимо выбрать одно или несколько полей из отображаемого списка. Максимальное

количество полей для группировки – 10. При достижении лимита возможность выбора дополнительных полей блокируется.

После выбора поле автоматически добавляется в область «Группы» на левой панели (рис. 18).

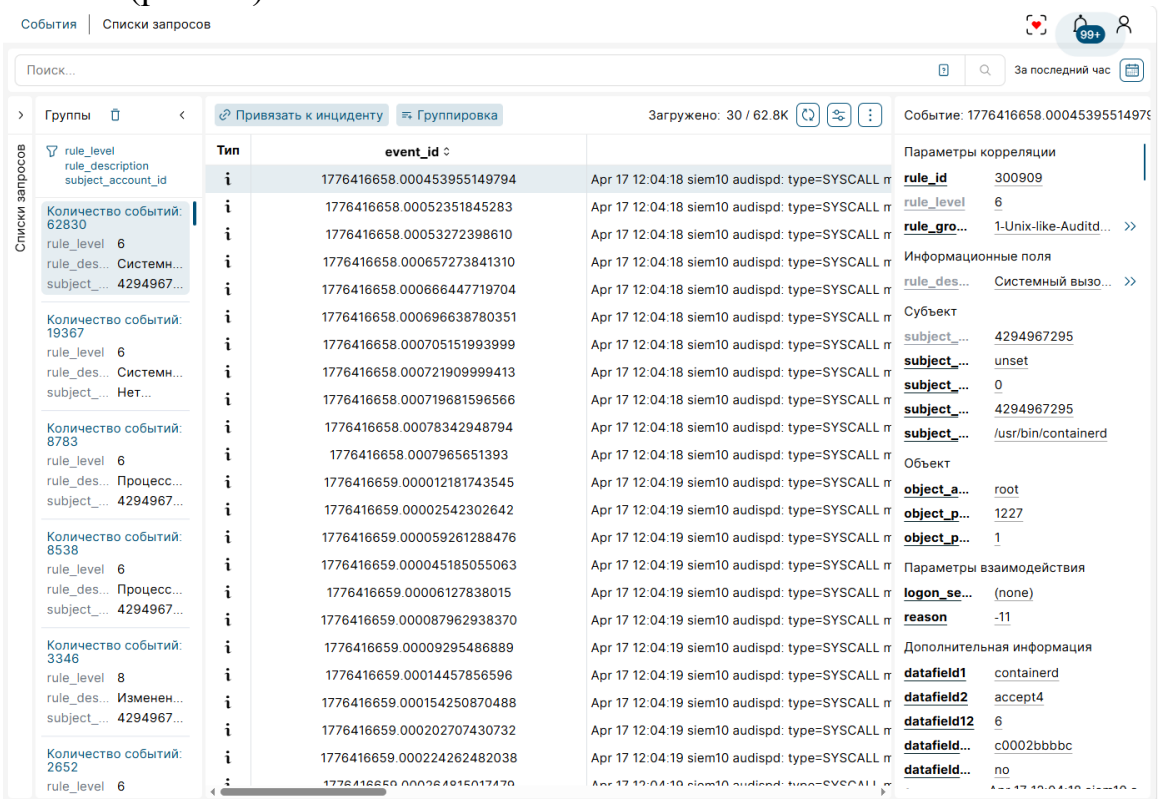


Рисунок 18 – Группировка событий

Выбранное поле остается подсвеченным в правой панели и становится недоступным для повторного выбора.

Следует обратить внимание на поля, по которым невозможно выполнить группировку: full_log, event_id, timestamp, previous_output.

Система позволяет сбросить как отдельное поле, так и всю настройку группировки целиком.

Для сброса отдельного поля необходимо в области «Группы» (левая панель) навести курсор на поле, которое нужно удалить. Далее нажать на появившуюся рядом с полем кнопку .

В случае если необходимо отменить всю группировку на странице, следует воспользоваться кнопкой .

Для настройки группировки событий с помощью модального окна необходимо выполнить следующие действия:

- **открыть модальное окно**, нажав кнопку Группировка на панели инструментов (рис. 19),

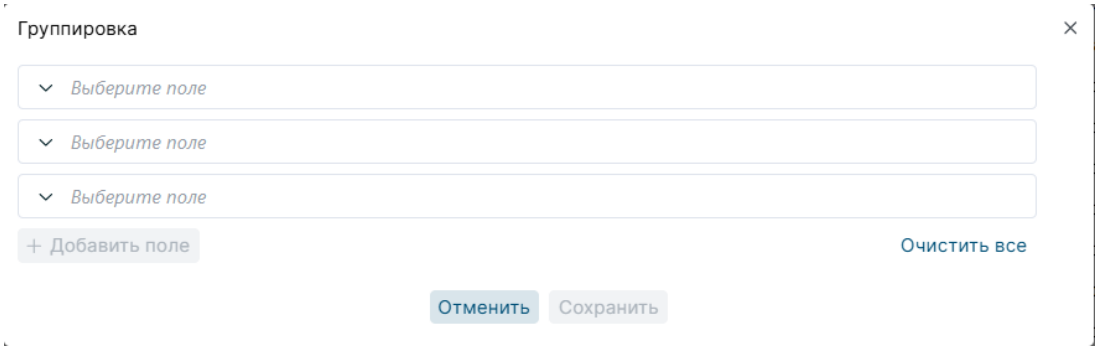


Рисунок 19 - Модальное окно "Группировка"

- **выбрать поля для группировки**, кликнув в поле и выбрав необходимое значение из выпадающего списка (по умолчанию отображаются 3 поля для выбора). Для поиска значения следует ввести его название в поисковую строку выпадающего списка (рис. 20).

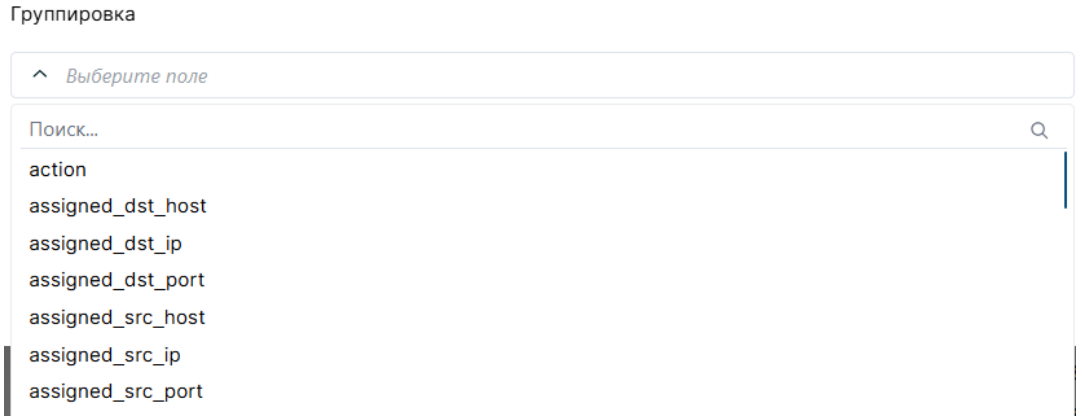


Рисунок 20 - Выбор значения из выпадающего списка

- **добавить дополнительные поля** (при необходимости), нажав кнопку + Добавить поле после заполнения трех полей,

- **удалить или очистить поле**, нажав кнопку (доступна для всех заполненных полей) (рис. 21).

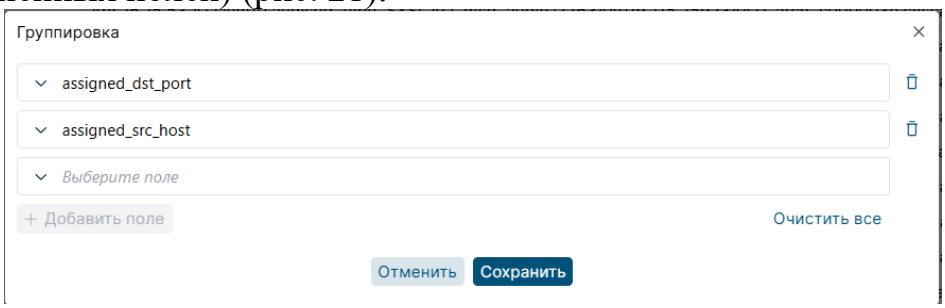


Рисунок 21 - Очистка или удаление поля

Кнопка имеет две функции: для первых трех полей – это очистка поля, начиная с четвертого поля – это удаление поля из модального окна.

- **сохранить настройки**, нажав кнопку Сохранить, которая активна при заполнении хотя бы одного поля. Как результат, модальное окно закроется,

выбранная группировка отобразится в области «Группы» на левой панели, а поля, добавленные в группировку, автоматически подсветятся в правой боковой панели.

- **отменить изменения**, нажав на кнопку Отменить или кликнув вне модального окна. В результате чего модальное окно закроется без сохранения изменений.

- **сбросить всю группировку**, нажав кнопку Очистить все . Как результат, все поля будут очищены, группировка удалена.

При переходе между страницами группировка сохраняется.

3.4.5 Работа с пользовательскими запросами

Для сохранения пользовательских запросов для последующего быстрого доступа к ним необходимо написать запрос в поисковую строку и нажать элемент (рис.22), который появится справа в поисковой строке.

Рисунок 22 – Ввод запроса в поисковую строку

Далее появится модальное окно, где некоторые поля будут заполнены («Наименование», «Запрос»), при необходимости их можно изменить. В поле «Описание», при необходимости, можно ввести данные, а в поле «Список запросов» выбрать к какому списку запросов отнести создаваемых запрос. Поля «Наименование», «Запрос» и «Список запросов» являются обязательными (рис.23).

Следует обратить внимание, что если необходимо быстро очистить данные в поисковой строке, то следует нажать на элемент × (рис.22).

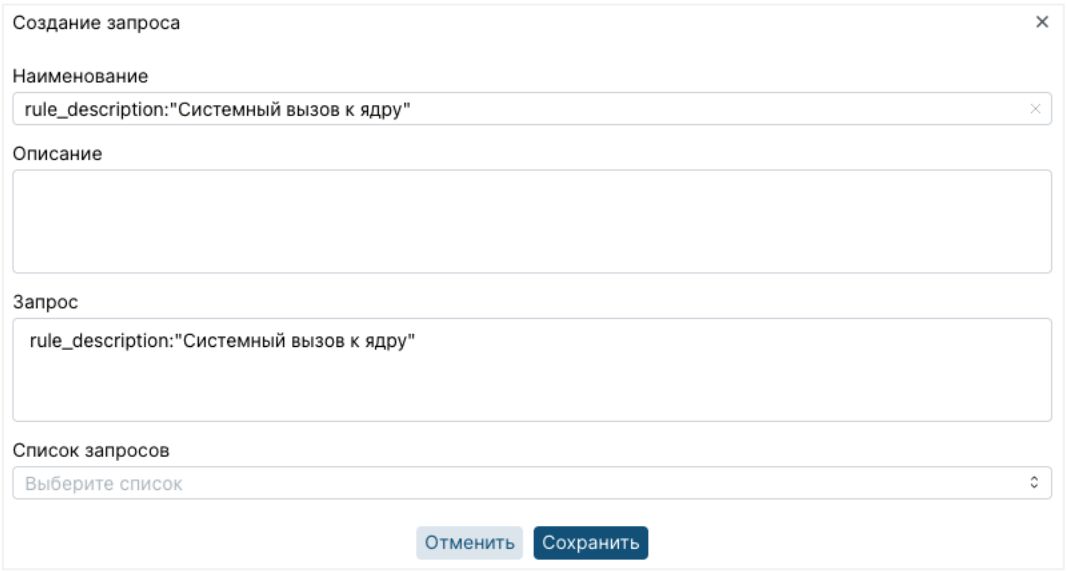


Рисунок 23– Сохранение запроса

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 открыть боковое меню «Списки запросов». После его раскрытия откроется информация с доступными списками запросов (рис.24). 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.

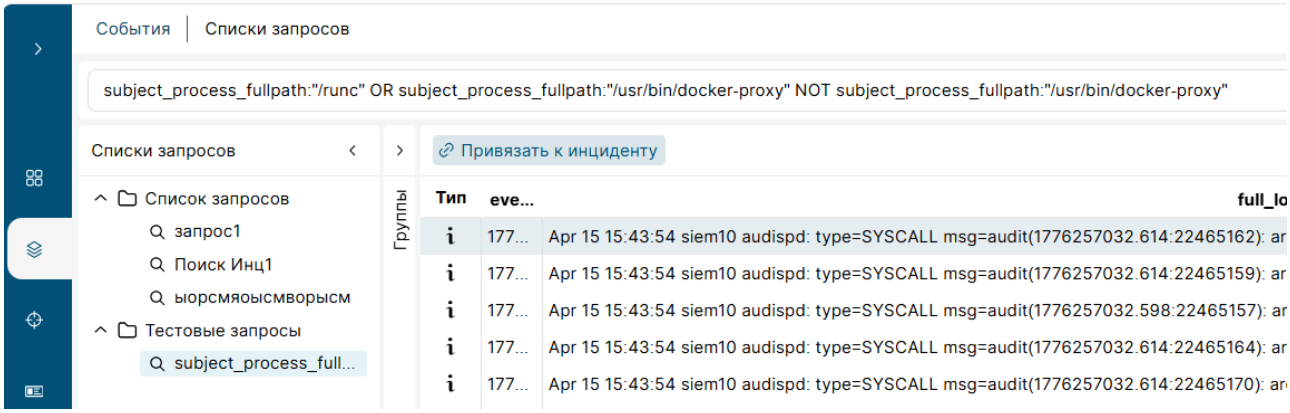


Рисунок 24 – Сохраненные списки запросов

Если список запросов пустой, то есть относящихся к нему запросов нет, то он будет выделен тусклым серым цветом и элемент › будет неактивным.

3.4.6 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.25), где необходимо заполнить поля. Поле «Наименование» является обязательным.

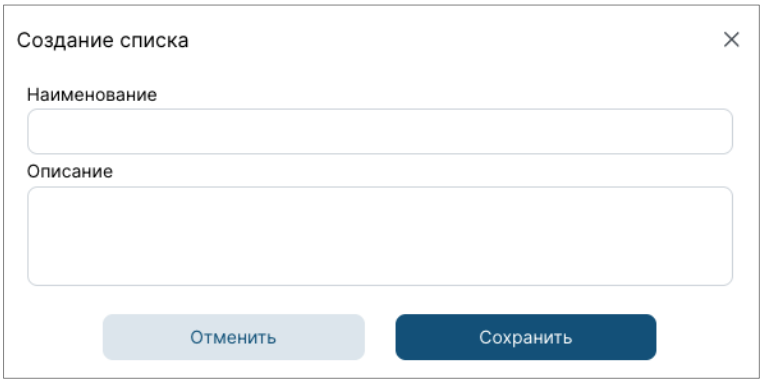


Рисунок 25 – Создание списка запросов

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 (рис. 26).

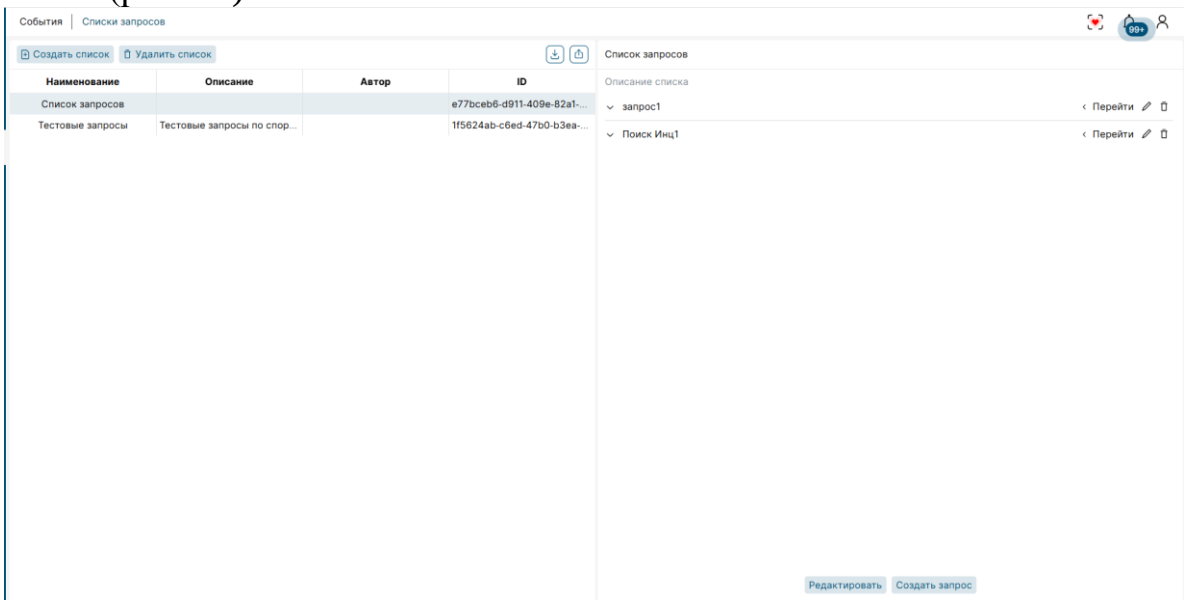


Рисунок 26 – Список пользовательских запросов

В целях управления наполнением списка запросов можно:

- просмотреть подробнее запрос, нажав на кнопку ⌄;
- добавить запрос в список, нажав кнопку Создать запрос. Откроется модальное окно (рис.23) с возможностью заполнения полей. Следует обратить внимание, поле «Список запросов» будет заполнено выбранным списком, однако данное поле можно редактировать;
- отредактировать запрос, нажав на кнопку ✎. Откроется модальное окно (рис.23) 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.27), 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 27 – Переход на страницу для быстрой фильтрации данных

Для того, чтобы отредактировать список запросов следует нажать на кнопку Редактировать. После чего появляется модальное окно (рис.28), в котором поля «Наименование» и «Описание» становятся доступны для изменения.

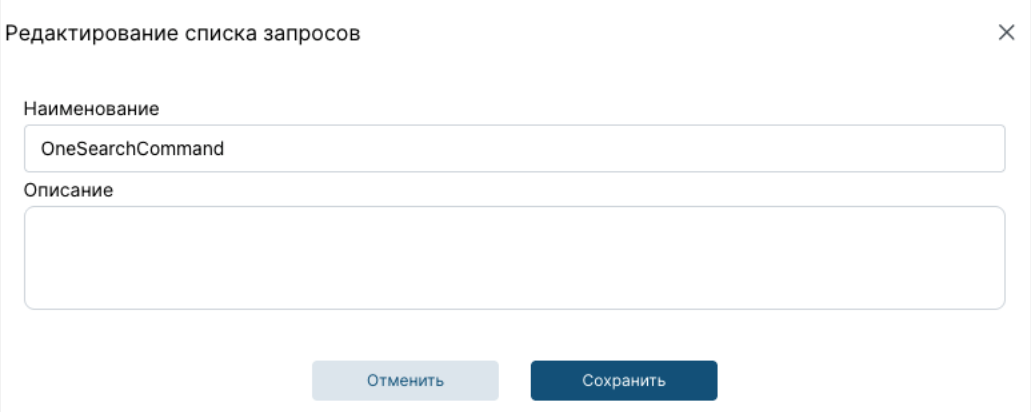


Рисунок 28 – Редактирование списка запросов

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

Для того, чтобы загрузить 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, после чего подтвердить действие в всплывающем уведомлении. Результат операции отобразится в уведомлениях.

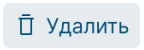
3.5 Интерфейс раздела «Инциденты»

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 страницы представлена поисковой строкой для ввода запросов (см. Руководство по созданию запросов) и совокупностью кнопок:

+ Создать – для регистрации нового инцидента вручную;

– для закрытия инцидента;



– для удаления инцидента;

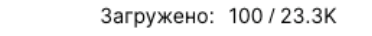
– для просмотра истории изменения инцидента;


– для фильтрации элементов в таблице по временному периоду;


– для обновления данных вручную;


– настройка периодичности обновления таблицы;


– для работы с гибкими таблицами (п. 2.5);



– 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 части: слева расположен список с преднастроенными фильтрами и группами инцидентов, в центре таблица с перечнем инцидентов, а справа – боковая панель с подробной информацией о выбранном инциденте. По умолчанию левые боковые панели отображаются в свернутом виде, правая панель – в развернутом. Для раскрытия левых панелей или закрытия правой необходимо нажать на кнопку раскрытия  или кнопку закрытия  соответственно.

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 по времени изменения. 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.15). 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).

Также можно сортировать инциденты в таблице при нажатии на наименование поля. При первом нажатии будет произведена сортировка по возрастанию, а при повторном нажатии – по убыванию.

Процесс фильтрации может быть осуществлен следующим образом:

- с помощью поисковой строки с использованием языка запросов;
- по ранее сохраненным запросам с использованием списков запросов;
- по преднастроенным запросам по статусам и критичности;
- по группам активов;
- по периоду с использованием календаря.

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

Для удобства ввода запросов в строке поиска предусмотрена функция подсказок. Система предлагает три типа подсказок:

- подсказки по полям (ключам);
- подсказки по логическим операторам;
- подсказки по значениям;

Подсказки по ключам содержат названия доступных полей для поиска (например, `severity_name, key_value, status_name`).

Подсказки по логическим операторам содержат операторы AND, OR, NOT для построения сложных поисковых запросов.

Подсказки по значениям отображаются только для полей с предопределенным набором значений:

- полю `severity_name` соответствуют значения: `Low, Medium, High`;
- полю `status_name` соответствуют значения: `New, InProgress, Closed, FalsePositive`.

Подсказки отображаются в виде выпадающего списка с возможностью прокрутки. Выбор осуществляется стрелками ↓↑ и клавишей Enter или кликом мыши по необходимому элементу.

В поисковой строке доступна кнопка [?] (по умолчанию активна), которая позволяет:

- временно отключить отображение подсказок;
- включить подсказки обратно.

Состояние кнопки (включено/ выключено) сохраняется при переходе между страницами.

Для того, чтобы воспользоваться фильтрацией по преднастроенным запросам, ранее сохраненным запросам или по группам активов следует открыть левую боковую панель. Для этого необходимо нажать в области Фильтры на элемент ›, и выбрать опцию из предложенных в списке (рис.29).

В случае, если необходимо отменить фильтрацию по преднастроенным запросам, следует воспользоваться кнопкой ✕.

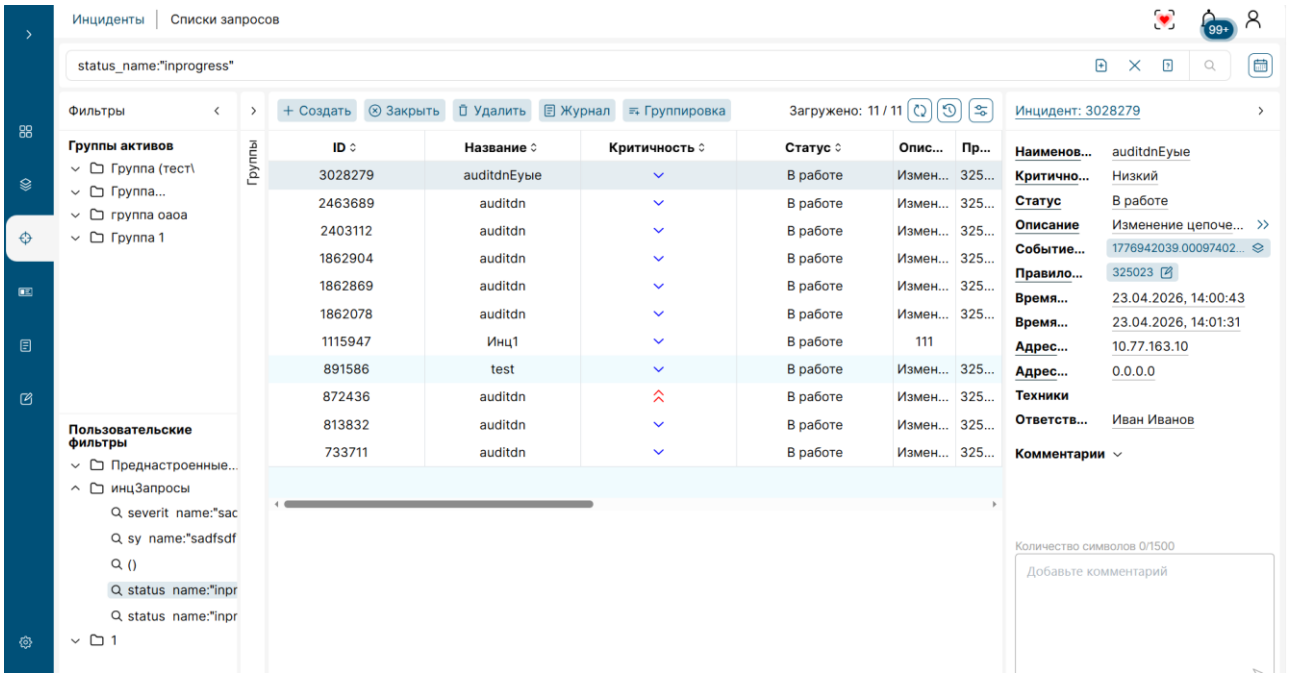


Рисунок 29 – Фильтры на странице «Инциденты»

3.6.2 Создание инцидента вручную

Для создания инцидента вручную следует нажать на кнопку на панели инструментов + Создать. Далее появится модальное окно с полями (рис.30) для заполнения.

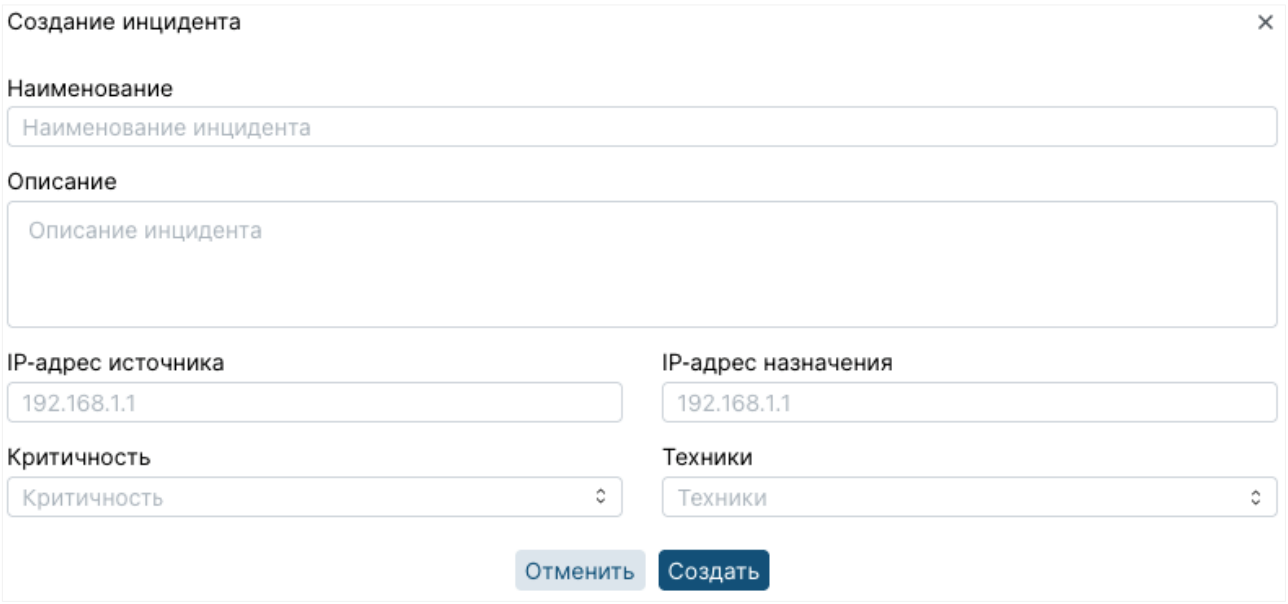


Рисунок 30 – Создание инцидента вручную

Следует обратить внимание, что в поле «Описание» есть ограничение в 250 символов, а в полях, содержащих IP-адреса, следует указывать данные в формате IPv4. В раскрывающемся списке «Критичность» необходимо выбрать уровень: высокий, средний или 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.31). Правая панель по умолчанию отображается в развернутом виде. При необходимости скрыть данную область следует нажать на кнопку закрытия › .

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.

Информация о инциденте в правой части рабочей области разделена по полям (например, `Наименование`), при нажатии на значение которых появляется выбор оператора (`OR`, `AND` или `NOT`), который, соответственно, будет добавлен в поисковую строку для быстрой навигации по инцидентам. А поля «Событие» и «Правило корреляции» используются для перехода к дополнительной информации.

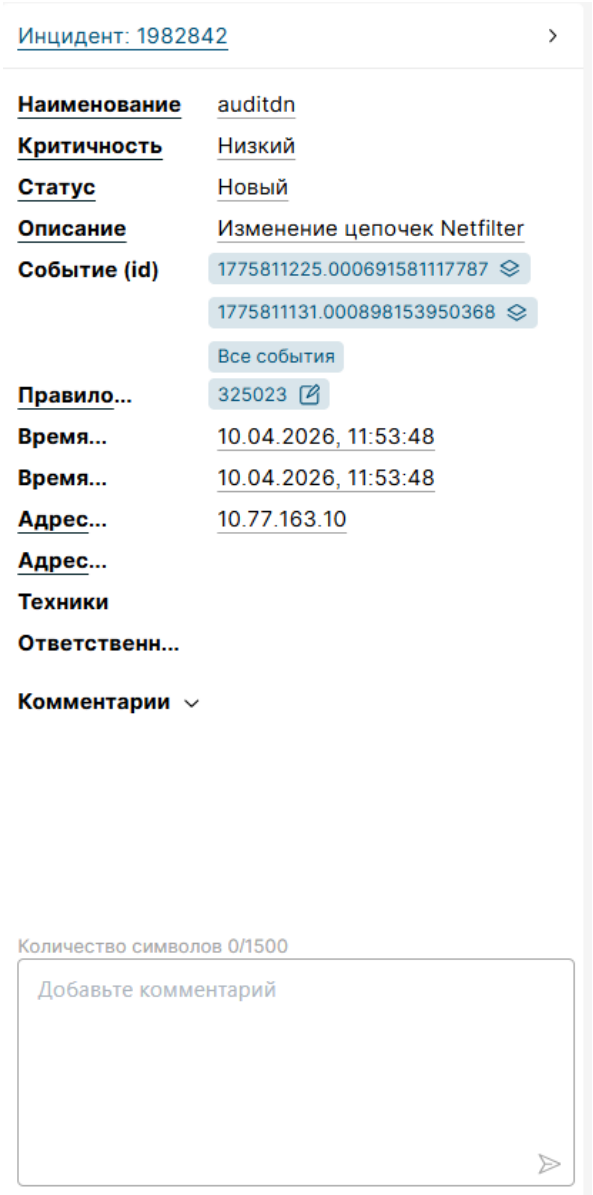
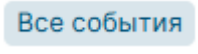


Рисунок 31 – Просмотр инцидента

Для просмотра информации о событии следует нажать на кнопку идентификатора события вида 

, после чего появится модальное окно (рис.32) с подробной информацией о событии, где все поля разделены на категории.

На правой боковой панели с подробной информацией об инциденте расположена кнопка 

, которая отображается только при наличии двух и более связанных событий у инцидента. Для перехода на страницу с отфильтрованным перечнем всех связанных событий следует нажать на данную кнопку.

Можно также скопировать `full_log` (событие), для чего надо навести на значение поля и нажать на элемент  . В случае успешности, система уведомит пользователя и элемент  изменится на  .

Для того, чтобы закрыть окно с информацией о событии следует нажать на ← или вне области модального окна.

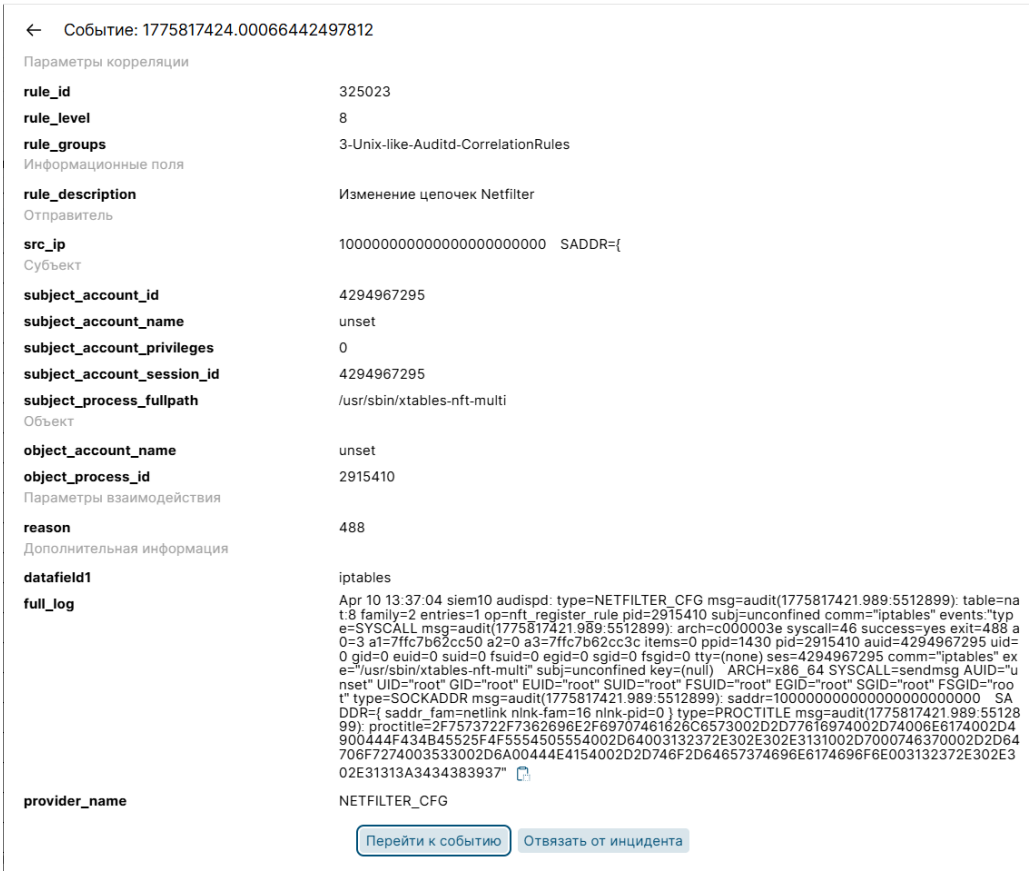


Рисунок 32 – Просмотр события через страницу «Инциденты»

При нажатии на кнопку Перейти к событию или на клавишу Enter 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.

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. Далее появится боковое модальное окно, в котором можно раскрыть подробную информацию о выбранном состоянии инцидента (рис.33), при этом элемент ⌄ изменится на ⌃.

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

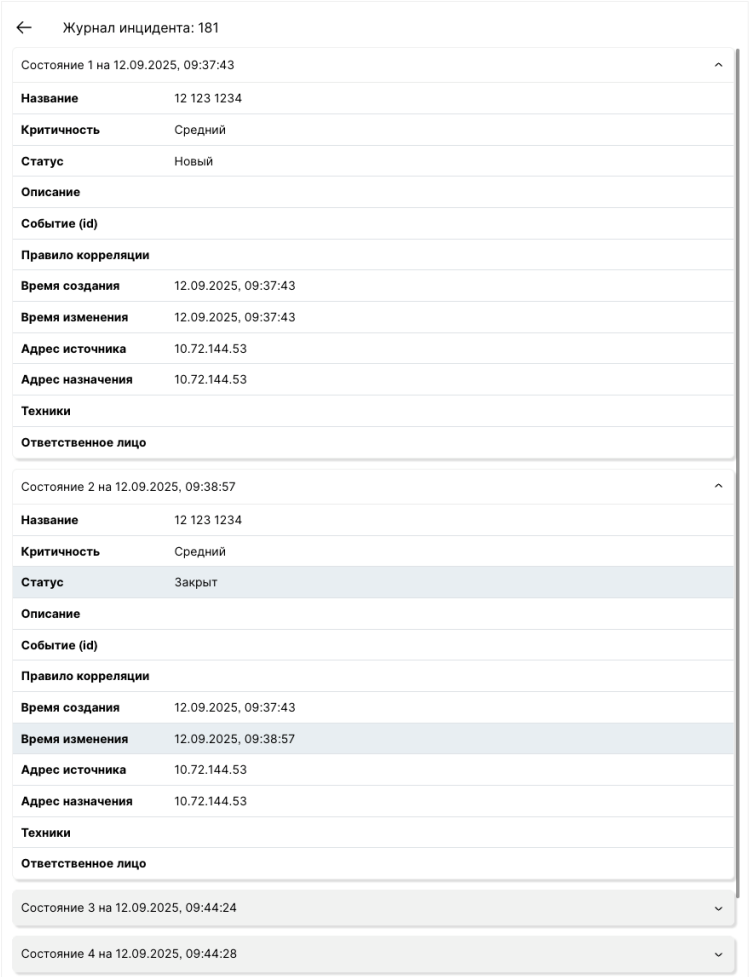


Рисунок 33 – Журнал инцидента

Следует обратить внимание, что поля, значение которых было изменено, будут выделены цветом, как показано на рис.33.

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. 31) следует нажать на название инцидента Инцидент: 12876. Система откроет новую страницу, где появится возможность внесения изменений (рис. 34).

Можно также перейти на сущность «Карточка инцидента» двойным нажатием на строку в таблице с перечнем инцидентов.

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

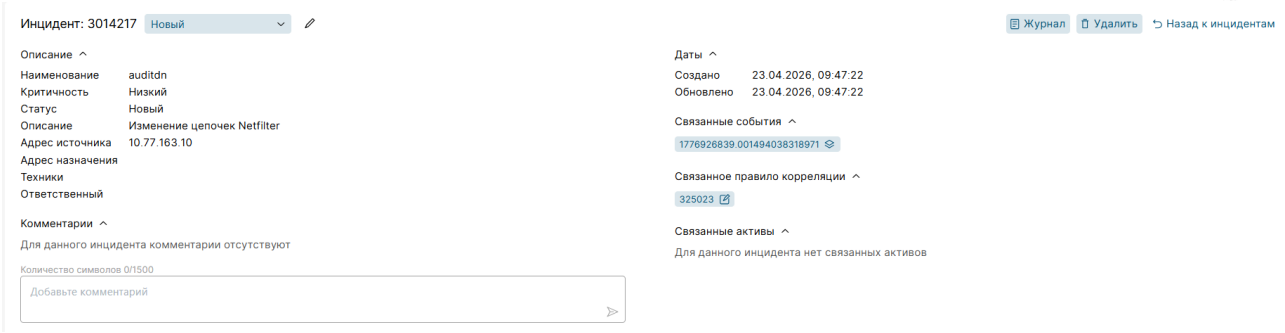
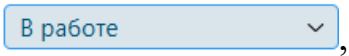


Рисунок 34 – Карточка инцидента

Для изменения статуса инцидента нужно открыть раскрывающий список 

, который находится рядом с названием инцидента, и выбрать нужный вариант. Показатели статуса: новый, в работе, закрыт, закрыт как ложноположительный.

Следует обратить внимание, что, когда пользователь меняет статус на «В работе», он автоматически назначается ответственным за данный инцидент.

Для редактирования полей необходимо нажать на элемент ✎ и все значения полей в блоке «Описание» станут доступны для изменения (рис. 35).

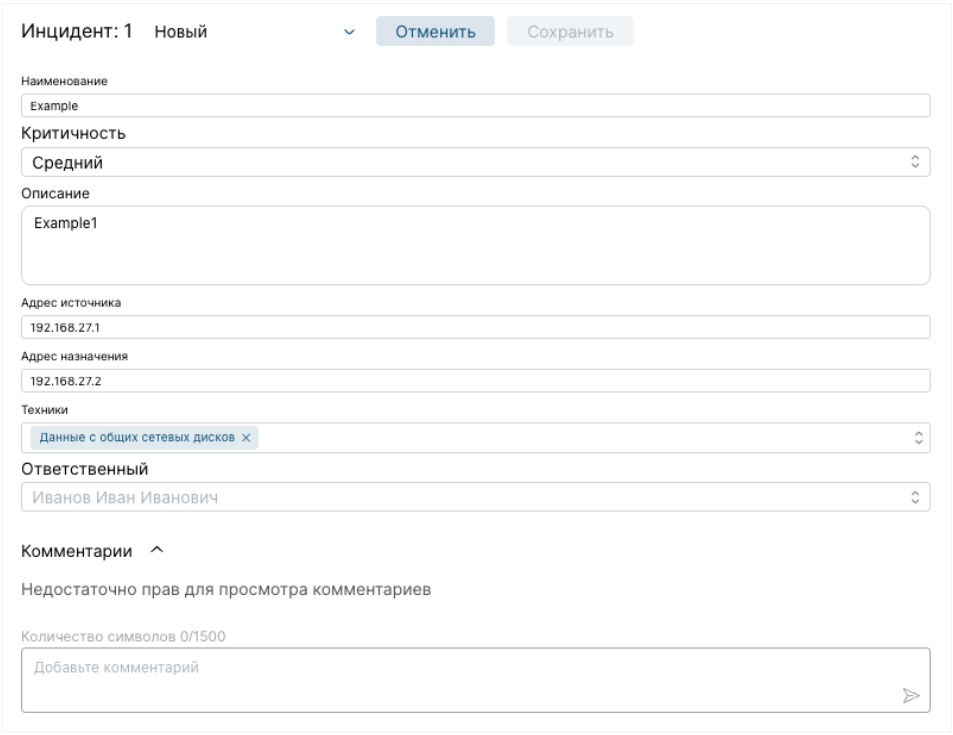


Рисунок 35 – Редактирование инцидента

Следует обратить внимание, что в поле «Описание» есть ограничение в 250 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».

Через страницу «Карточка инцидента» доступны возможности:

- создания комментариев, в также просмотр их истории (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 (алгоритм аналогичен пункту 3.6.5);
- просмотр истории инцидента (алгоритм аналогичен пункту 3.6.3).

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

.

3.6.5 Закрытие и удаление инцидента, множественное закрытие инцидентов.

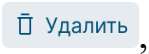
Для того, чтобы присвоить инциденту статус «Закрыт», достаточно выбрать элемент в таблице на странице «Инциденты» и нажать на кнопку 

. В открывшемся окне необходимо выбрать опцию «Закрыть выбранные». Затем в модальном окне следует указать статус закрытия инцидента «Закрыт» или «Закрыт как ложноположительный». После выбора статуса станет доступна кнопка «Закрыть». При нажатии на нее инцидент будет закрыт с указанным статусом.

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

Предусмотрена возможность множественного закрытия инцидентов. Она доступна для двух и более инцидентов, выбранных вручную, или для всего списка, отфильтрованного с помощью фильтров или группировок. Для выполнения операции необходимо нажать на кнопку 

и далее процедура аналогична закрытию одного инцидента.

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 ×.

3.6.6 Группировка инцидентов

На странице «Инциденты» доступна функция группировки инцидентов по одному или нескольким полям.

Настроить группировку можно двумя способами:

- через правую боковую панель;
- с помощью модального окна «Группировка».

Оба способа взаимосвязаны: настройки группировки синхронизируются между интерфейсами – поля, выбранные в правой панели, автоматически отображаются в модальном окне, и наоборот.

Для группировки событий через правую боковую панель необходимо выбрать одно или несколько полей из отображаемого списка. Максимальное количество полей для группировки – 10. При достижении лимита возможность выбора дополнительных полей блокируется.

После выбора поле автоматически добавляется в область «Группы» на левой панели (рис. 36).

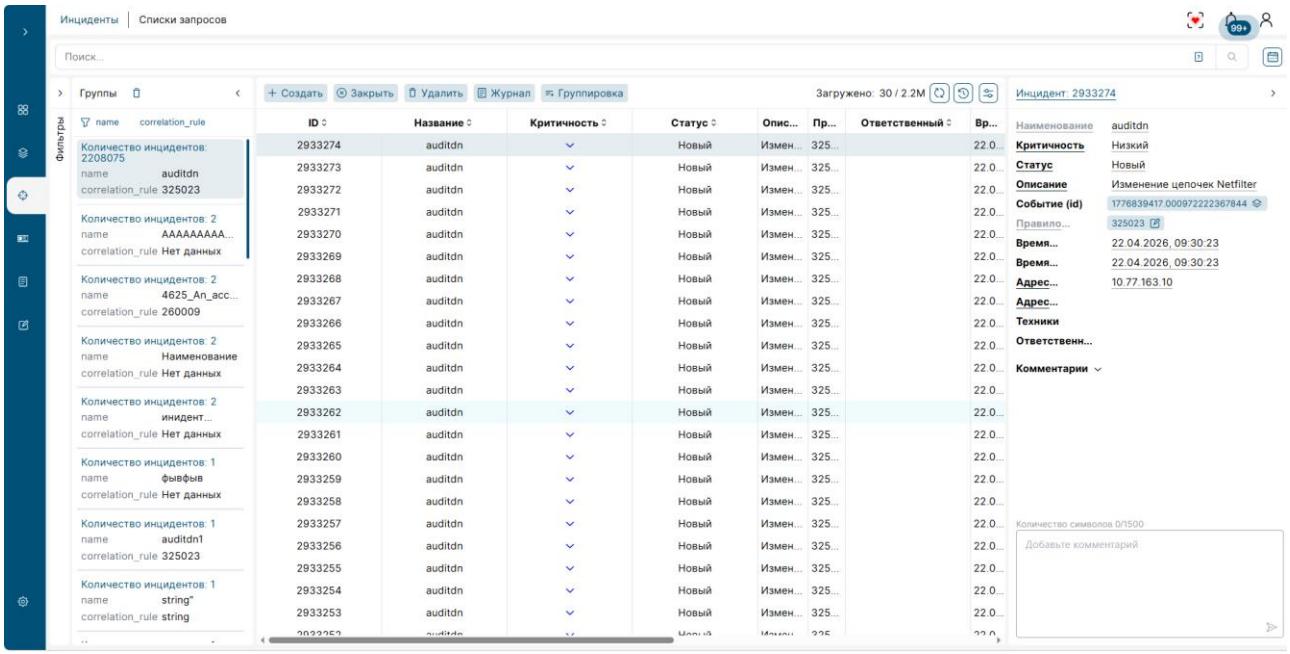


Рисунок 36 - Группировка инцидентов

Выбранное поле остается подсвеченным в правой панели и становится недоступным для повторного выбора.

Следует обратить внимание на поля, по которым невозможно выполнить группировку: `Событие(id), Время создания, Время изменения, Техники, Ответственный.`

Система позволяет сбросить как отдельное поле, так и всю настройку группировки целиком.

Для сброса отдельного поля в области «Группы» (левая панель) следует навести курсор на поле, которое нужно удалить. Далее необходимо нажать на появившуюся рядом с полем кнопку .

В случае если необходимо отменить всю группировку на странице, следует воспользоваться кнопкой .

Для настройки группировки инцидентов с помощью модального окна необходимо выполнить следующие действия:

- **открыть модальное окно**, нажав кнопку Группировка на панели инструментов (рис.37),

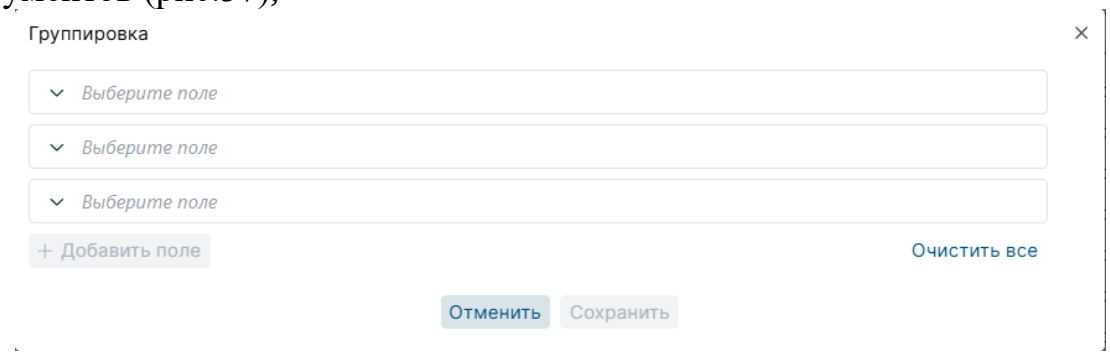


Рисунок 37 - Модальное окно "Группировка"

- **выбрать поля для группировки**, кликнув в поле и выбрав необходимое значение из выпадающего списка (по умолчанию отображаются 3 поля для выбора). Для поиска значения следует ввести его название в поисковую строку выпадающего списка (рис. 38).

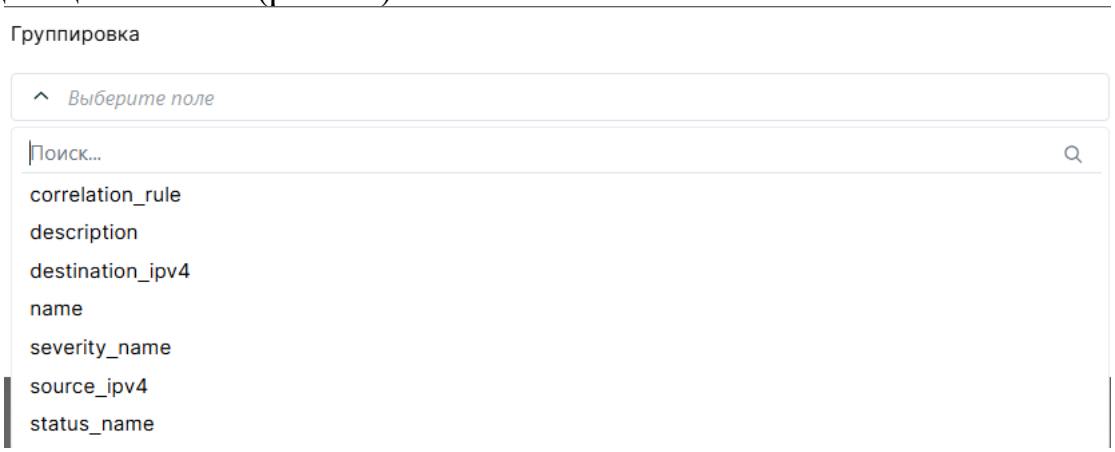


Рисунок 38 - Выбор значения из выпадающего списка

- **добавить дополнительные поля** (при необходимости), нажав кнопку + Добавить поле после заполнения трех полей,

- **удалить или очистить поле**, нажав кнопку (доступна для всех заполненных полей) (рис. 39).

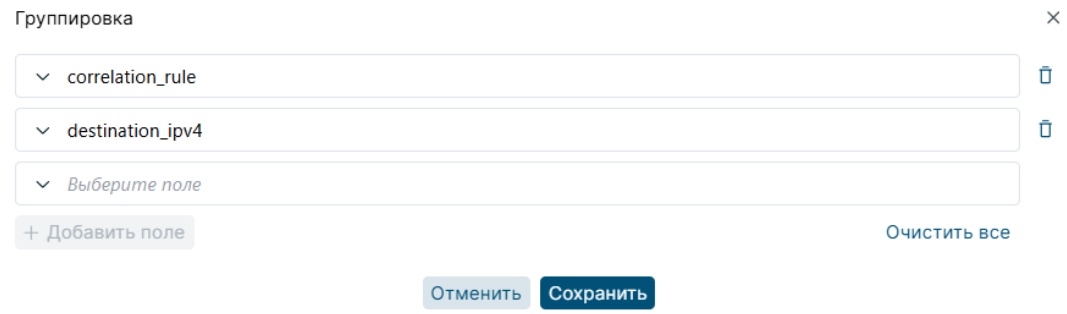


Рисунок 39 - Очистка или удаление поля

Кнопка имеет две функции: для первых трех полей – это очистка поля, начиная с четвертого поля – это удаление поля из модального окна.

- **сохранить настройки**, нажав кнопку Сохранить, которая активна при заполнении хотя бы одного поля. Как результат, модальное окно закроется, выбранная группировка отобразится в области «Группы» на левой панели, а поля, добавленные в группировку, автоматически подсветятся в правой боковой панели.

- **отменить изменения**, нажав на кнопку Отменить или кликнув вне модального окна. В результате чего модальное окно закроется без сохранения изменений.

- **сбросить всю группировку**, нажав кнопку Очистить все . Как результат, все поля будут очищены, группировка удалена.

При переходе между страницами группировка сохраняется.

3.6.7 Работа с пользовательскими запросами

Для сохранения пользовательских запросов для последующего быстрого доступа к ним необходимо написать запрос в поисковую строку и нажать элемент (рис.40), который появится справа в поисковой строке.

Далее появится модальное окно, где некоторые поля будут заполнены («Наименование», «Запрос»), при необходимости их можно изменить.

Рисунок 40 – Ввод запроса в поисковую строку

В поле «Описание» при необходимости можно ввести данные, а в поле «Список запросов» выбрать к какому списку запросов отнести создаваемый запрос. Поля «Наименование», «Запрос» и «Список запросов» являются обязательными (рис.41).

Следует обратить внимание, что если необходимо быстро очистить данные в поисковой строке, то следует нажать на элемент × (рис.40).

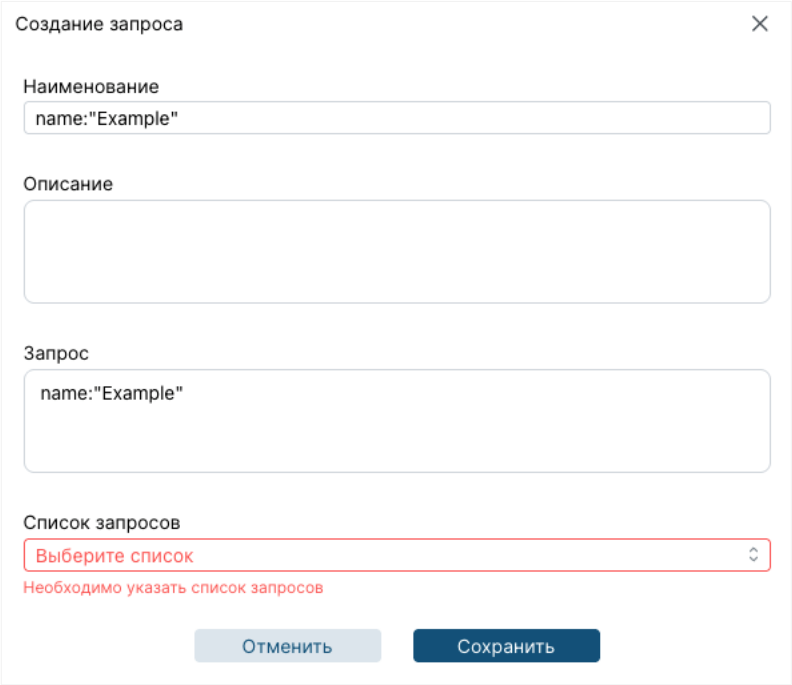


Рисунок 41 – Сохранение запроса

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 открыть боковое меню «Списки запросов». После его раскрытия откроется информация с доступными списками запросов (рис.42). 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.

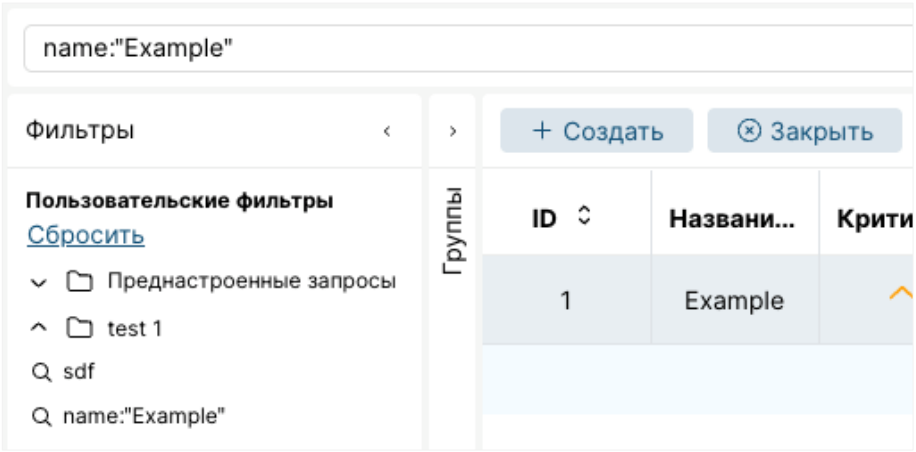


Рисунок 42 – Сохраненные списки запросов

Если список запросов пустой, то есть относящихся к нему запросов нет, то он будет выделен тусклым серым цветом и элемент › будет неактивным.

3.6.8 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.43), где необходимо заполнить поля. Поле «Наименование» является обязательным.

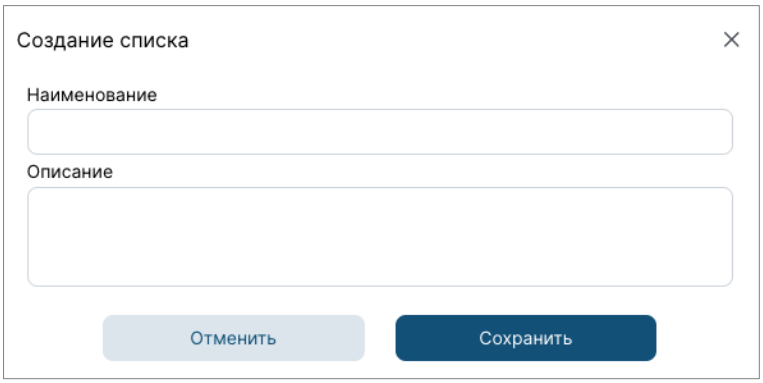


Рисунок 43 – Создание списка запросов

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 (рис. 44).

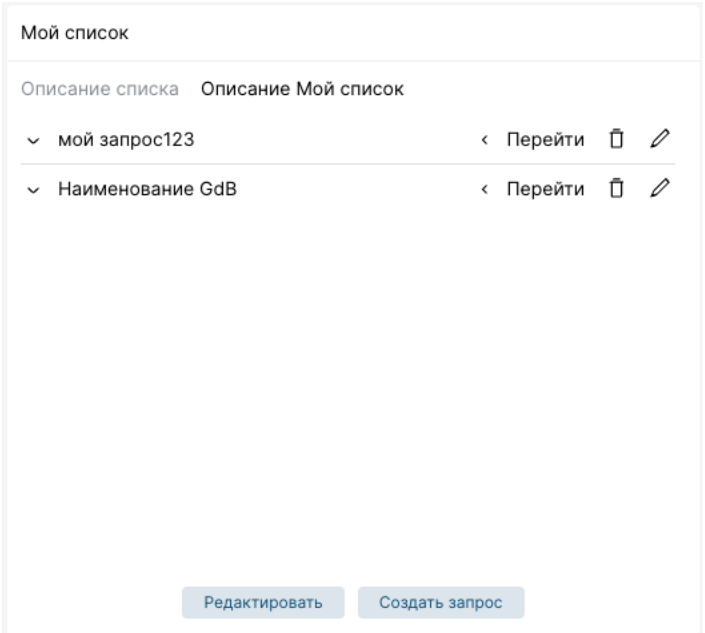


Рисунок 44 – Список пользовательских запросов

В целях управления наполнением списка запросов можно:

- просмотреть подробнее запрос, нажав на кнопку ;
- добавить запрос в список, нажав кнопку Создать запрос. Откроется модальное окно (рис.41) с возможностью заполнения полей. Следует обратить внимание, поле «Список запросов» будет заполнено выбранным списком, однако данное поле можно редактировать;
- отредактировать запрос, нажав на кнопку . Откроется модальное окно (рис.36) 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.45), произойдет переход на страницу «Инциденты», 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 .

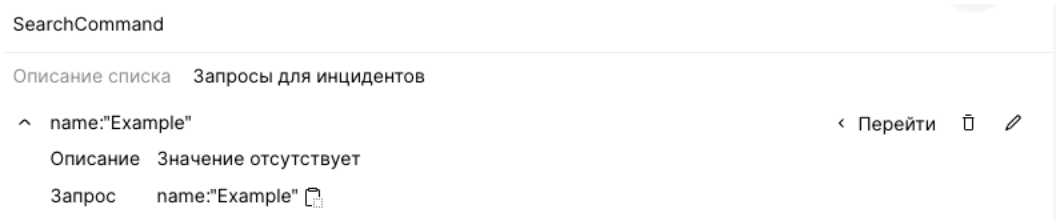


Рисунок 45 – Переход на страницу для быстрой фильтрации данных

Созданный запрос также отобразиться на странице «Инциденты» в левом боковом меня в блоке «Фильтры».

Для того, чтобы отредактировать список запросов следует нажать на кнопку Редактировать. После чего появляется модальное окно (рис.46), в котором поля «Наименование» и «Описание» становятся доступны для изменения.

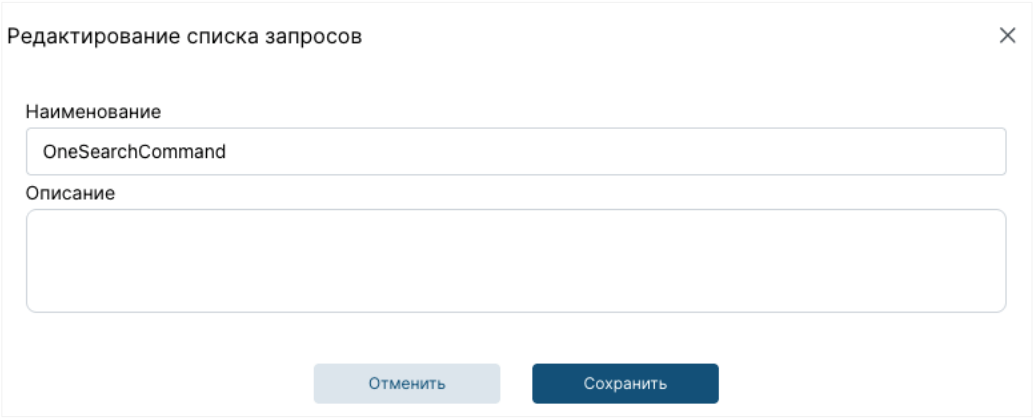
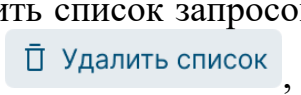


Рисунок 46 – Редактирование списка запросов

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

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

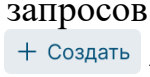
Для того, чтобы удалить список запросов необходимо выбрать элемент в перечне и нажать на кнопку 

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

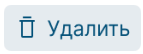
3.7 Интерфейс раздела «Активы»

На странице «Активы» представлен функционал для работы с активами и их группами. На странице представлены функции просмотра, создания, фильтрации, редактирования, а также удаления активов и групп.

Панель инструментов страницы представлена поисковой строкой для ввода запросов и совокупностью кнопок:



– для регистрации нового актива;

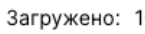


– для удаления актива;

 – для обновления данных вручную;

 – настройка периодичности обновления таблицы;

 – для работы с гибкими таблицами (п. 2.5);



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

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

Рабочая область страницы разделена на части: слева расположен список с группами активов, в центре таблица с перечнем активов, а справа – боковая панель с подробной информацией о выбранном активе. По умолчанию левая боковая панель отображается в свернутом виде, правая панель – в развернутом. Для раскрытия левой панели или закрытия правой необходимо нажать на кнопку раскрытия  или кнопку закрытия  соответственно.

3.8 Работа с активами

3.8.1 Фильтрация данных на странице «Активы»

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

Для удобства ввода запросов в строке поиска предусмотрена функция подсказок. Система предлагает три типа подсказок:

- подсказки по полям (ключам);

- подсказки по логическим операторам;
- подсказки по значениям.

Подсказки по ключам содержат названия доступных полей для поиска (например, `ip`, `importance_name`, `is_active`).

Подсказки по логическим операторам содержат операторы AND, OR, NOT для построения сложных поисковых запросов.

Подсказки по значениям отображаются только для полей с предопределенным набором значений:

- полю `importance_name` соответствуют значения: `Low`, `Medium`, `High`;
- полю `is_monitored` соответствуют значения: `True`, `False`;
- полю `is_active` соответствуют значения: `True`, `False`.

Подсказки отображаются в виде выпадающего списка с возможностью прокрутки. Выбор осуществляется стрелками ↓↑ и клавишей Enter или кликом мыши по необходимому элементу.

В поисковой строке доступна кнопка [?] (по умолчанию активна), которая позволяет:

- временно отключить отображение подсказок;
- включить подсказки обратно.

Состояние кнопки (включено/ выключено) сохраняется при переходе между страницами.

3.8.2 Создание актива

Для создания актива следует нажать на кнопку на панели инструментов [+ Создать]. Далее появится модальное окно с полями (рис.47) для заполнения.

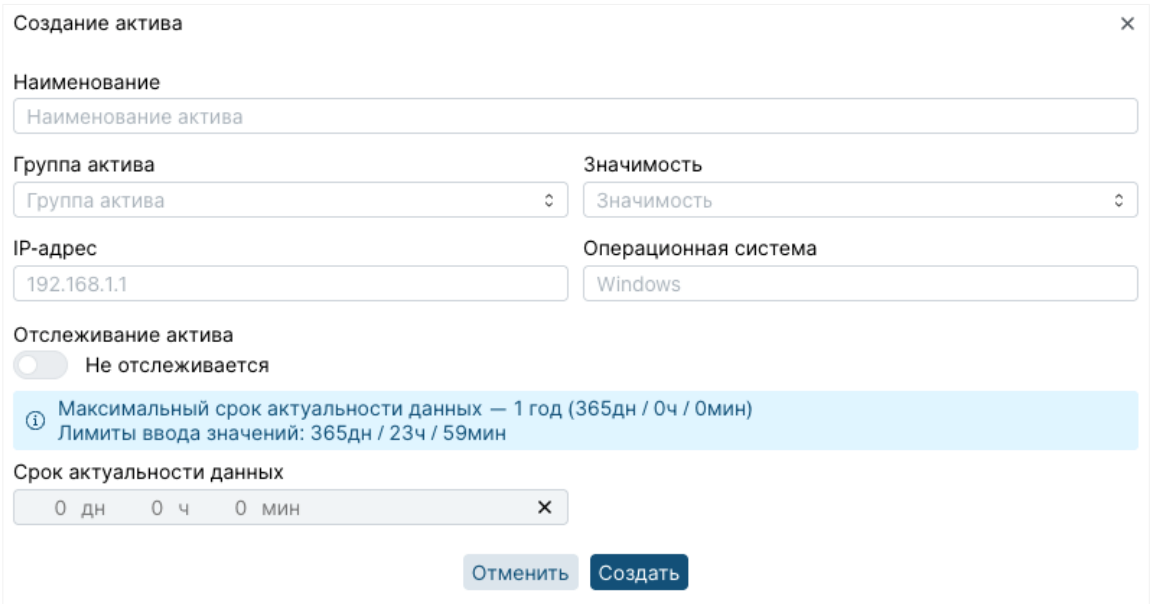


Рисунок 47 – Создание актива

Следует обратить внимание, что в поле «Наименование» есть ограничение в 255 символов, в поле «Операционная система» ограничение в 50 символов, а в поле «IP-адрес» следует указывать данные в формате IPv4. В раскрывающемся списке «Значимость» необходимо выбрать уровень: высокая, средняя или низкая, а в раскрывающемся списке «Группа актива» – группу активов.

Если выбрана опция «Не отслеживается», то актив при мониторинге пришедших событий с него будет игнорироваться, однако если выбрана опция «Отслеживается», то актив подлежит мониторингу активов.

Мониторинг активов – отслеживание сбора событий с актива и в случае отсутствия событий с активов на основании установленного значения времени будет отправляться уведомление в системе и на почту (если настроено).

В поле «Срок актуальности данных» указывается данные о периоде. Однако, если данные в поле не указаны, то в зависимости от значимости система назначит период:

- Высокая значимость – отсутствие событий с актива 3 часа;
- Средняя значимость – отсутствие событий с актива 3 дня;
- Низкая значимость – отсутствие событий с актива 1 неделю.

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

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

3.8.3 Отображение информации о конкретном активе, сортировка

Сортировать активы в таблице можно при нажатии на наименование поля. При первом нажатии будет произведена сортировка по возрастанию, а при повторном нажатии меняется на противоположную.

Для отображения полной информации в правой части рабочей области нужно выбрать актив в таблице (рис.48). Правая панель по умолчанию отображается в развернутом виде. При необходимости скрыть данную область следует нажать на кнопку закрытия ›.

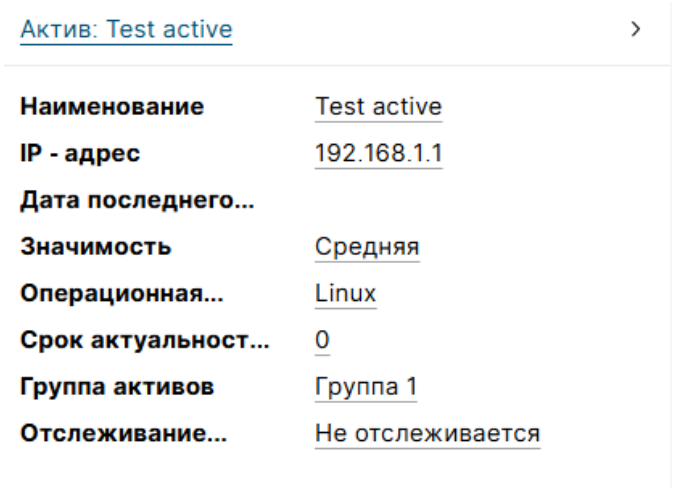


Рисунок 48 – Просмотр актива

Информация об активе в правой части рабочей области разделена по полям (например, `IP-адрес`), при нажатии на значение которых появляется выбор оператора (`OR`, `AND` или `NOT`), который, соответственно, будет добавлен в поисковую строку для быстрой навигации по активам.

3.8.4 Редактировании информации о конкретном активе

Для того, чтобы отредактировать актив необходимо перейти на сущность «Карточка актива». Для этого в правой части рабочей области страницы «Активы» (рис. 48) следует нажать на название актива Актив: DC1. Система откроет новую страницу, где появится возможность внесения изменений (рис. 49).

Можно также перейти на сущность «Карточка актива» двойным нажатием на строку в таблице с перечнем активов.

Следует обратить внимание, что скрывать и раскрывать блоки на странице «Карточка актива» необходимо с помощью элементов ^ и v соответственно.

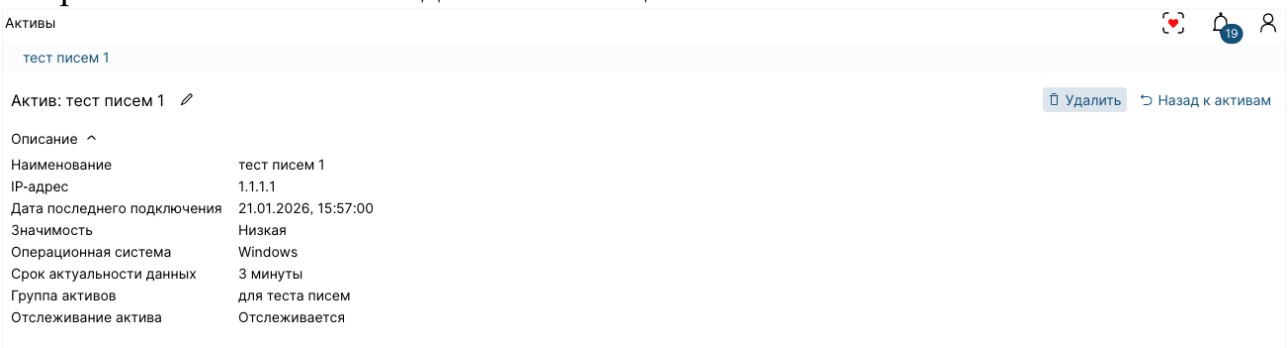


Рисунок 49 – Карточка актива

Для редактирования полей необходимо нажать на элемент ✎ и все значения полей в блоке «Описание» станут доступны для изменения (рис. 50).

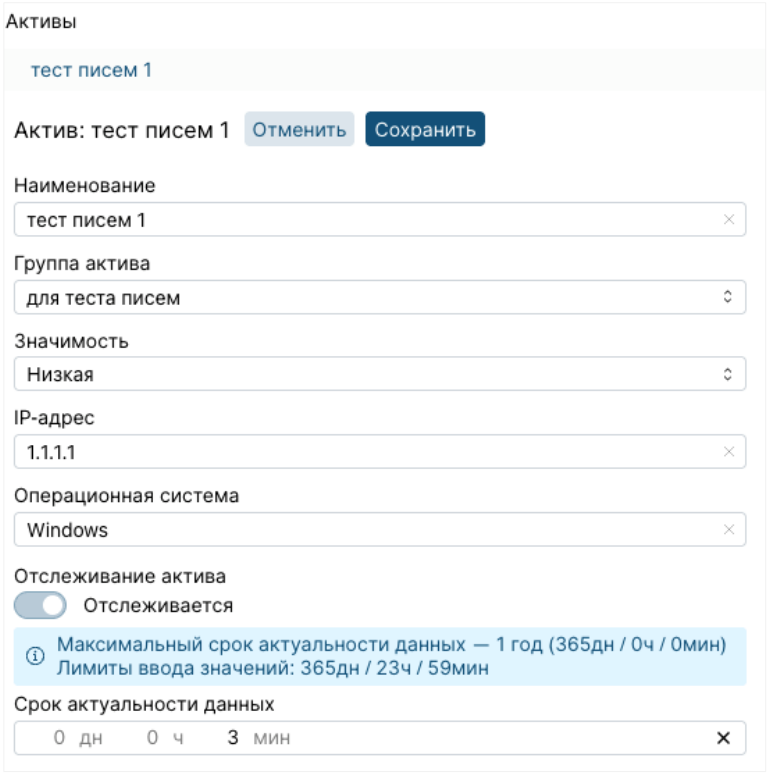


Рисунок 50 – Редактирование актива

Следует обратить внимание, что в поле «Наименование» есть ограничение в 255 символов, в поле «Операционная система» ограничение в 50 символов, а в поле «IP-адрес» следует указывать данные в формате IPv4. В раскрывающемся списке «Значимость» необходимо выбрать уровень: высокая, средняя или низкая, а в раскрывающемся списке «Группа актива» – группу активов.

Если выбрана опция «Не отслеживается», то актив при мониторинге пришедших событий с него будет игнорироваться, однако если выбрана опция «Отслеживается», то актив подлежит мониторингу активов.

Мониторинг активов – отслеживание сбора событий с актива и в случае отсутствия событий с активов на основании установленного значения времени будет отправляться уведомление в системе и на почту (если настроено).

В поле «Срок актуальности данных» указывается данные о периоде. Однако, если данные в поле не указаны, то в зависимости от значимости система назначит период:

- Высокая значимость – отсутствие событий с актива 3 часа;
- Средняя значимость – отсутствие событий с актива 3 дня;
- Низкая значимость – отсутствие событий с актива 1 неделю.

Для сохранения внесенных изменений нужно нажать на кнопку «Сохранить», а для отмены – «Отменить».

3.8.5 Удаление актива

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

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

Через страницу «Карточка актива» доступна также возможность удаления актива. Для того, чтобы удалить актив необходимо выбрать элемент в таблице и нажать на кнопку Удалить, подтвердить действие в всплывающем уведомлении. Результат операции отобразится в уведомлениях.

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

Также можно удалить актив через левое боковое меню (рис. 51), нажав на кнопку . В случае успешности появится соответствующее уведомление.

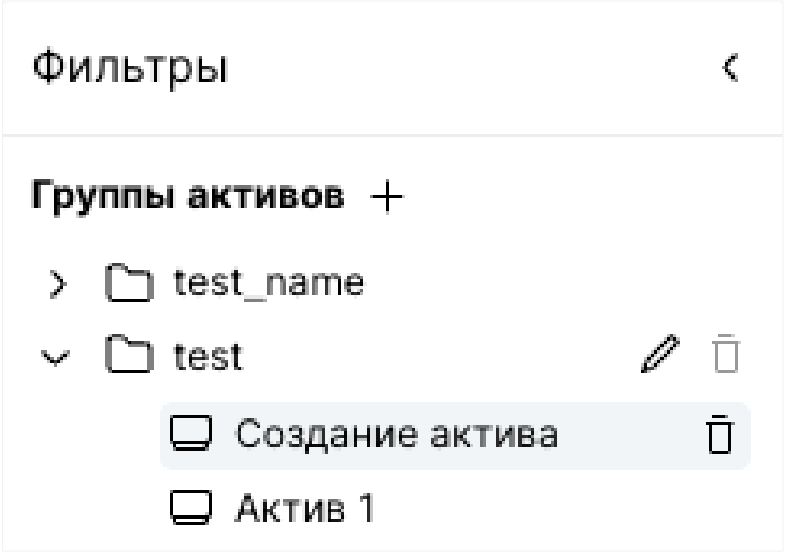


Рисунок 51 – Удаление актива

3.8.6 Работа с группами активов

Для того, чтобы создать папку необходимо в левой боковой панели нажать на элемент + (рис.51), после чего появится модальное окно (рис.52), в котором следует ввести название группы. Следует обратить внимание на ограничение в 255 символов в поле «Наименование».

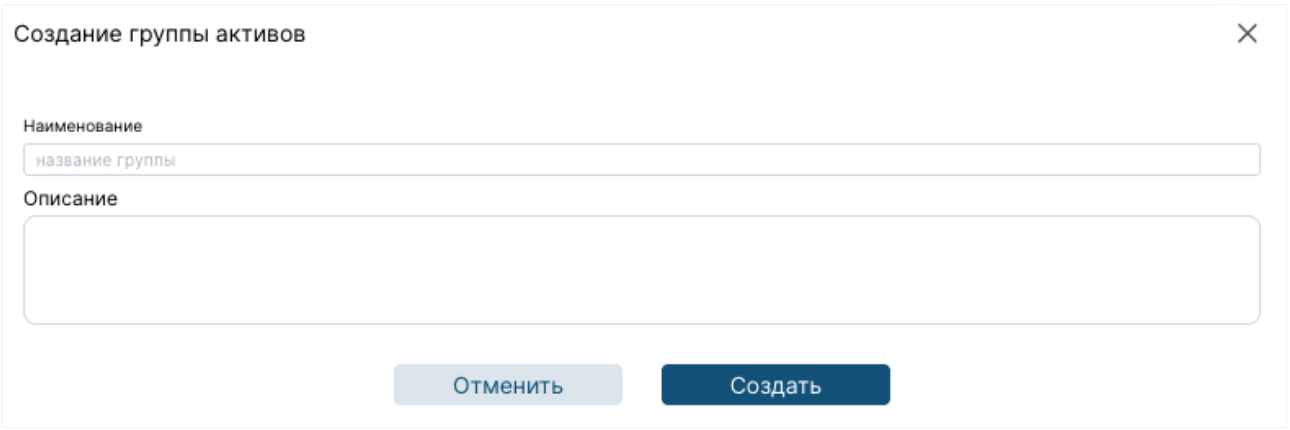


Рисунок 52 – Создание группа активов

Для того, чтобы отредактировать группу необходимо выбрать группу в левой боковой панели на странице «Активы» (рис.51) и нажать на , после чего появится модальное окно с возможностью изменения наименования группы (рис.53).

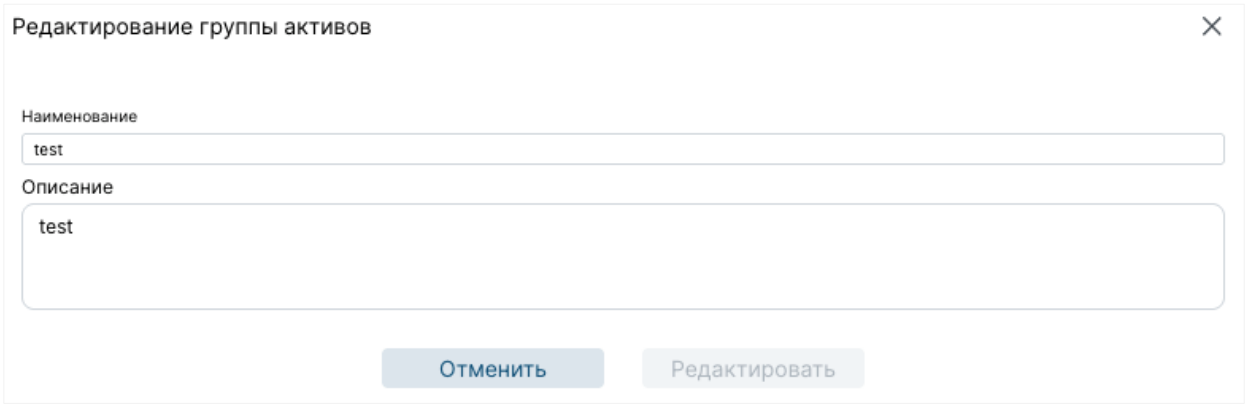


Рисунок 53 – Редактирование группа активов

Для того чтобы удалить группу необходимо выбрать папку в левой боковой панели на странице «Активы» (рис.51) и нажать . Результат операции отобразится в уведомлениях.

Следует обратить внимание, что группа, выбранная для удаления, должна быть пустой.

3.9 Интерфейс раздела «Отчеты»

Группа страниц предназначена для работы с отчетами и представлена страницами: «Системные отчеты», «Пользовательские отчеты».

На странице «Системные отчеты» представлен функционал для генерации отчетов по инцидентам и активам. Данные в отчет выгружаются за определенный период времени.

На странице «Пользовательские отчеты» представлен функционал для разработки отчетов с помощью конструктора отчета. Панель инструментов представлена совокупностью кнопок:

– для удаления отчета;

– для выгрузки отчета;

– функция предпросмотра созданного отчета;

– для вставки элементов в отчет;

– для работы с колонтитулами;

– для выбора ориентации страницы.

Рабочая область страницы разделена на части: слева расположено поле для предпросмотра отчета, в центре конструктор отчета, а справа – боковая панель с параметрами для настройки виджета. Боковая правая панель по умолчанию отображаются в свернутом виде и разворачивается нажатием на соответствующий элемент.

3.10 Работа с отчетами

3.10.1 Работа с системными отчетами. Выгрузка вручную

Для формирования и сохранения отчета необходимо выбрать блок: «Отчет по инцидентам» или «Отчет по активам» (рис.54).

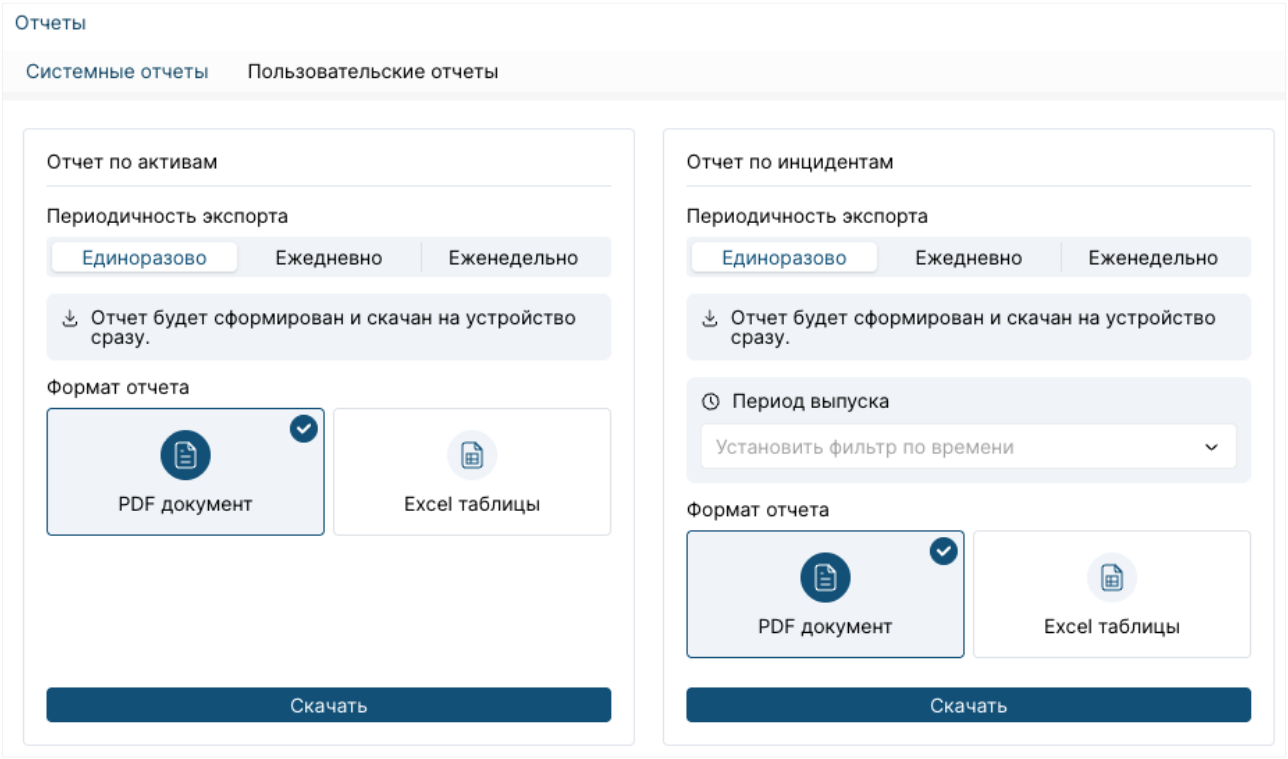


Рисунок 54 – Системные отчеты. Выгрузка вручную

Для того чтобы выгрузить отчет по инцидентам вручную, необходимо выбрать периодичность экспорта «Единоразово», выбрать период выпуска и формат отчета (xlsx или pdf). Далее следует нажать кнопку «Скачать». По нажатию на кнопку «Скачать» начинается процесс выгрузки отчета.

Отчет будет сформирован с указанием:

- периода, за который предоставляются данные;
- информации в сводной таблице об инцидентах, разбитых по статусам и критичности;
- виджеты с отображением круговых диаграмм инцидентов по статусам и критичности;
- подробная информация о каждом инциденте.

Следует обратить внимание, что в отчете в формате pdf круговые диаграммы не выгружаются.

Для того чтобы выгрузить отчет по активам вручную, необходимо выбрать периодичность экспорта «Единоразово» и формат отчета (xlsx или pdf). Далее следует нажать кнопку «Скачать». По нажатию на кнопку «Скачать» начинается процесс выгрузки отчета.

Отчет будет сформирован с указанием:

- информации в сводной таблице об активах;
- информации о количестве активов, разбитых по значимости и операционных системам;
- виджеты с отображением круговых диаграмм активов по значимости, статусам и операционным системам.

Следует обратить внимание, что в отчете в формате pdf круговые диаграммы не выгружаются.

3.10.2 Работа с системными отчетами. Настройка выгрузки по расписанию

Для настройки выгрузки отчета по расписанию необходимо выбрать блок: «Отчет по инцидентам» или «Отчет по активам» (рис.55).

Следует обратить внимание, что настройка выгрузки отчета осуществляется для всей системы, а не для конкретного пользователя.

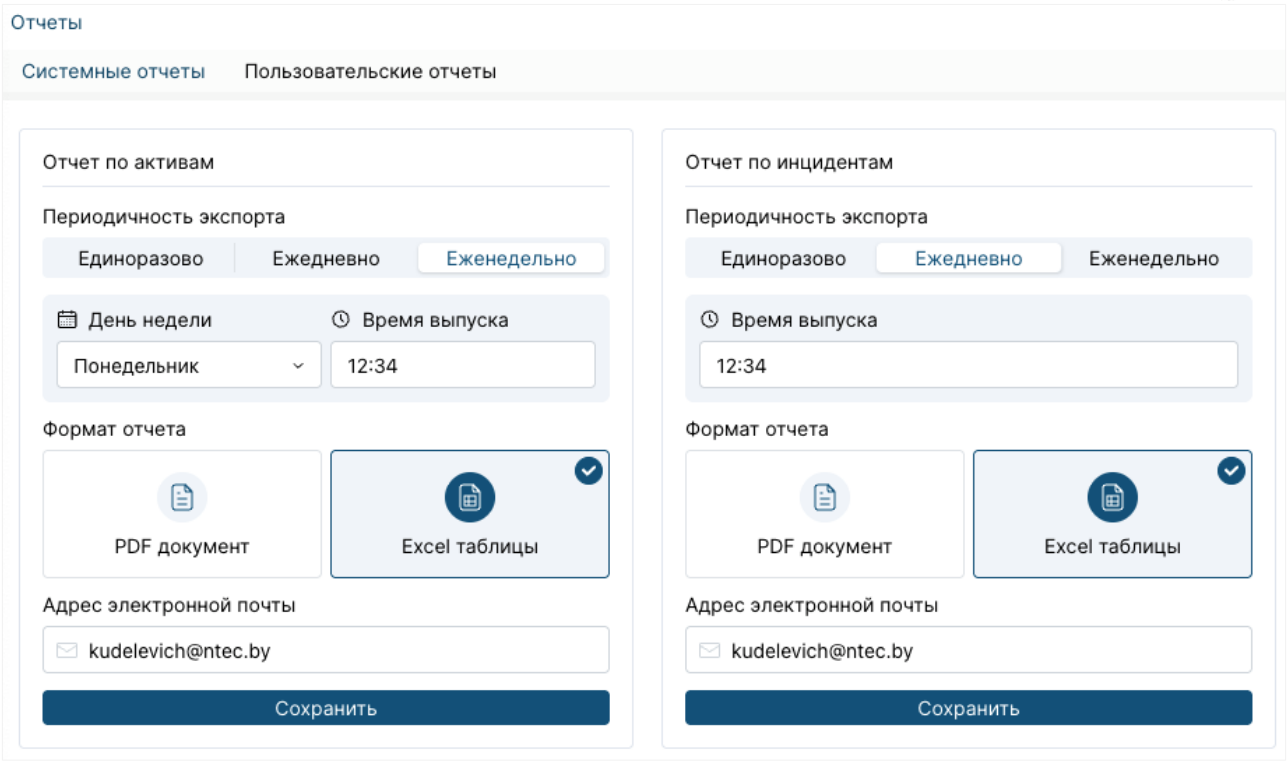


Рисунок 55 – Системные отчеты. Настройка выгрузки по расписанию

Можно настроить выгрузку отчета по периодичности экспорта «Ежедневно» и/или «Еженедельно» и по формату в «Exlsx таблицы» или «Pdf-документ».

Следует обратить внимание, что при выгрузке отчета размер файла не должен превышать 50 МБ.

Для отчета по активам: если выбрана опция «Ежедневно» или «Еженедельно», то отчет будет отправляться в указанное время пользователем и содержать данные за весь период на время формирования файла.

Для отчета по инцидентам: если выбрана опция «Еженедельно», то отчет будет отправляться в указанный пользователем день и время. Отчет содержит данные за 7 дней (с 00:00 первого дня до 23:59:59 последнего дня) предыдущей недели. Если выбрана опция «Ежедневно», то отчет по инцидентам будет содержать данные с 00:00 до 23:59 предыдущего дня, считая от выбранного пользователем дня. Отчет отправляется ежедневно в выбранное пользователем время.

Для того чтобы настроить выгрузку отчета по инцидентам, необходимо выбрать периодичность экспорта, время выпуска, день недели, формат отчета (xlsx или pdf) и ввести почту(-ы). Если вводится несколько адресов электронной почты, следует их отделять запятой и без пробелов. Далее следует нажать кнопку «Сохранить».

Отчет будет сформирован с указанием:

- периода, за который предоставляются данные;
- информации в сводной таблице об инцидентах, разбитых по статусам и критичности;

- виджеты с отображением круговых диаграмм инцидентов по статусам и критичности;
- подробная информация о каждом инциденте.

Следует обратить внимание, что в отчете в формате pdf круговые диаграммы не выгружаются.

Для того чтобы настроить выгрузку отчета по активам, необходимо выбрать периодичность экспорта, время выпуска, день недели, формат отчета (xlsx или pdf) и ввести почту(-ы). Если вводится несколько адресов электронной почты, следует их отделять запятой и без пробелов. Далее следует нажать кнопку «Сохранить».

Отчет будет сформирован с указанием:

- информации в сводной таблице об активах;
- информация о количестве активов, разбитых по значимости и операционных системам;
- виджеты с отображением круговых диаграмм активов по значимости и операционным системам.

Следует обратить внимание, что в отчете в формате pdf круговые диаграммы не выгружаются.

3.10.3 Работа с пользовательскими отчетами

Для того чтобы сконструировать пользовательский отчет, можно воспользоваться опциями: выбор предустановленных виджетов с их настройкой, вставка других элементов в отчет, настройка внешнего вида отчета (ориентация и колонтитулы), указание последовательности объектов отчета (рис.56).

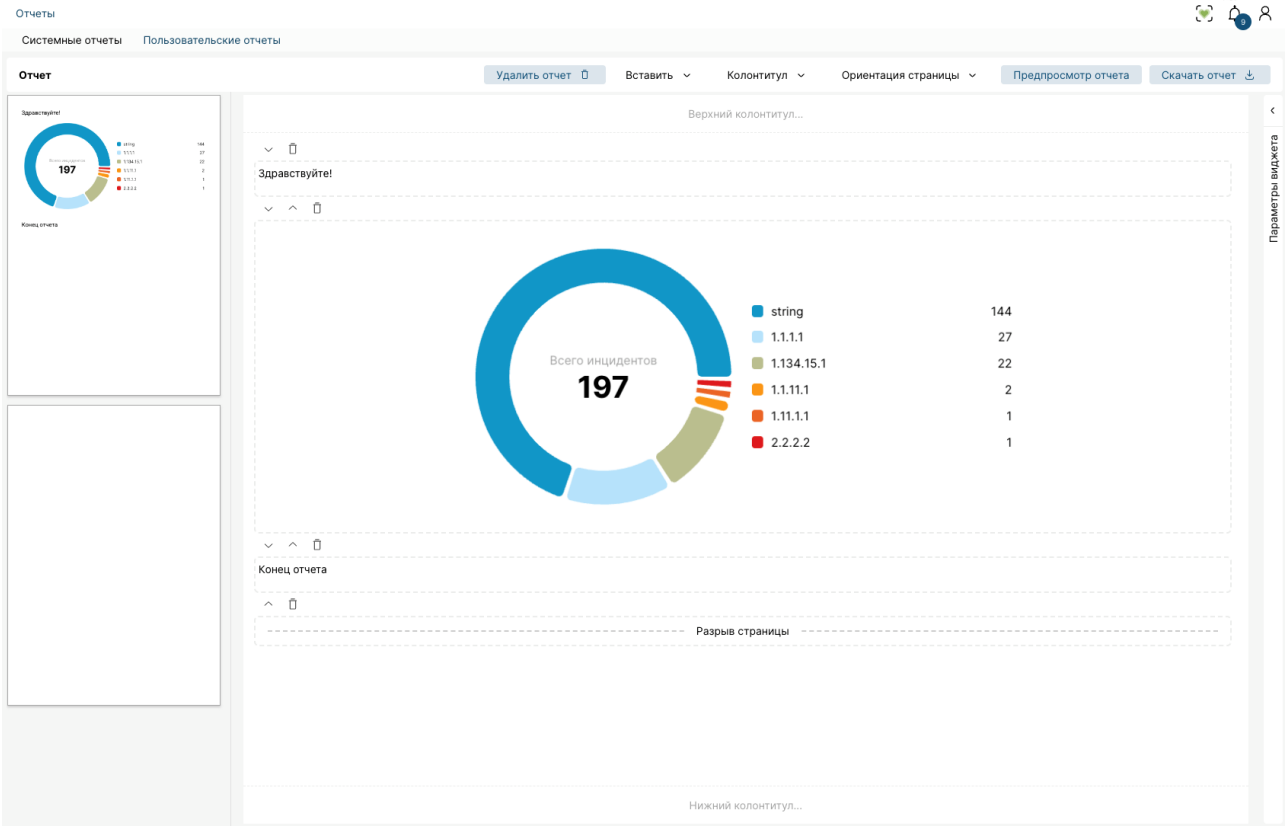


Рисунок 56 – Страница «Пользовательские отчеты»

Для составления отчета можно вставить элементы: текст, виджет, изображение и разрыв страницы. Для этого следует нажать кнопку Вставить и в выпадающем списке выбрать элемент для вставки. При помощи и можно менять местоположение элемента, а при удалении элемента следует воспользоваться (рис.57).

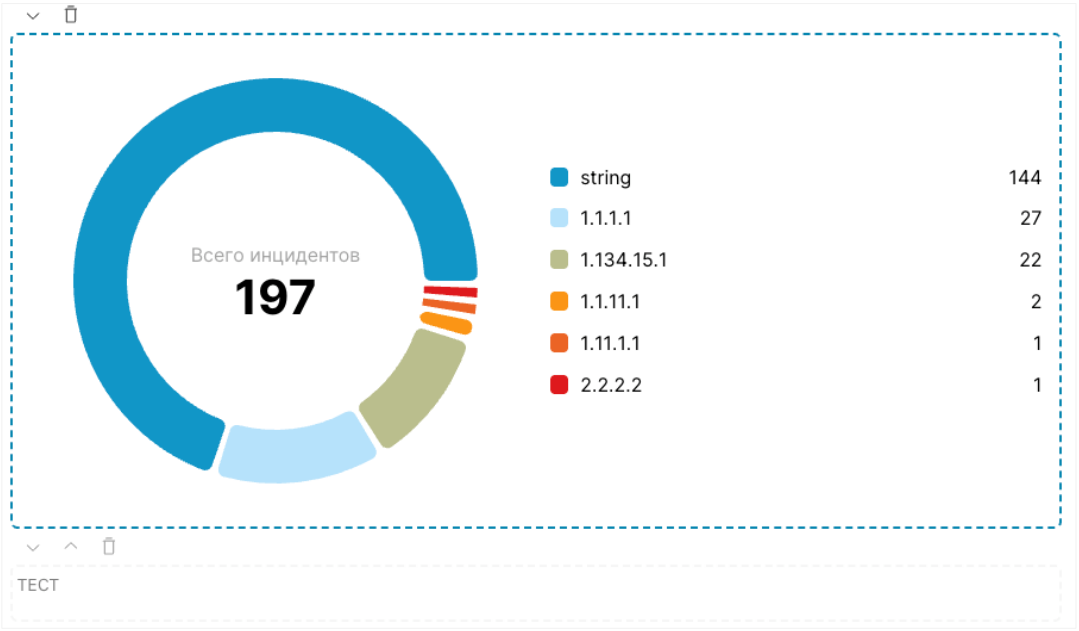


Рисунок 57 – Конструктор отчетов

Для настройки виджета следует выбрать его и раскрыть правую боковую панель (рис.58). После того, как все настройки сделаны, следует нажать кнопку «Применить изменения», иначе изменения не сохранятся.

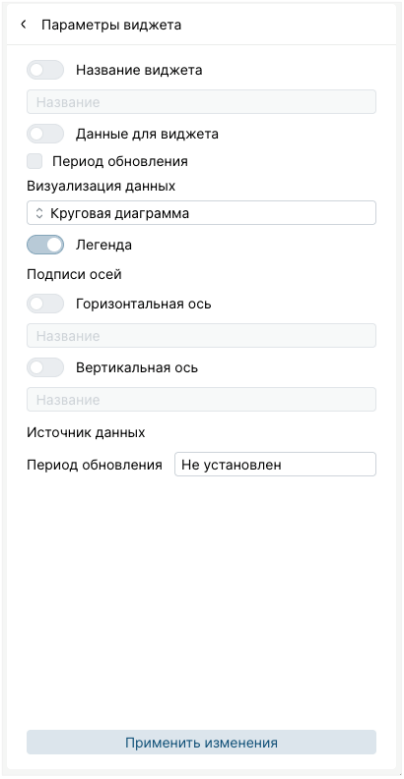


Рисунок 58 – Настройка параметров виджета

Для настройки общего вида отчета можно изменить колонтитулы и ориентацию страницы. Для настройки колонтитулов следует нажать Колонтитулы и выставить параметры (рис.59). А для выбора ориентации страниц следует нажать Ориентация страницы и из выпадающего списка выбрать: горизонтальная или вертикальная.

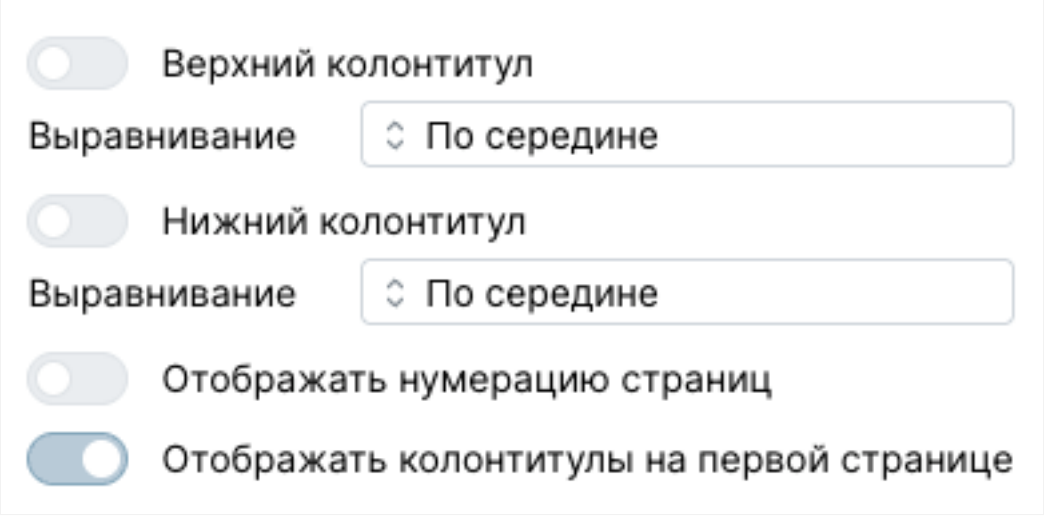


Рисунок 59 – Настройка колонтитулов

После конструирования отчета его можно предварительно просмотреть. Для этого следует нажать кнопку Предпросмотр отчета, и в левой боковой панели отобразится отчет в формате, соответствующем его виду в PDF.

Для того чтобы выгрузить отчет, следует нажать кнопку Скачать отчет, и сконструированный отчет сохранится в формате pdf.

Для того чтобы удалить отчет необходимо нажать кнопку Удалить отчет, которая становиться активной при внесении каких-либо данных в отчет. Результат операции отобразится в уведомлениях.

3.11 Интерфейс раздела «База правил»

Группа страниц «База правил» 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).

Группа страниц «База правил» представлена следующими страницами:

- страница «Драфт зона»;
- страница «Активные правила»;
- страница «Проверка правил».

Каждая страница имеет свой набор элементов: панель инструментов, рабочая зона и поисковая строка (см. «Руководство по созданию запросов»).

3.11.1 Страница «Драфт зона»

Страница предназначена для работы с правилами нормализации, корреляции, агрегации, а также табличными списками, предоставляя возможности просмотра, создания, удаления, запуска и остановки работы правил, а также их импорта и экспорта.

Панель инструментов представлена группой кнопок:

Экспорт – для экспорта правил и табличных списков;

Импорт – для импорта правил и табличных списков;

Создать правило – для создания нового правила и табличного списка;

Удалить из драфт зоны – для удаления из драфт зоны правила и табличного списка, не используемых в процессе обработки событий и выявления инцидентов;

Загрузить в систему – для загрузки правил и табличных списков в систему для применения их в процессе обработки событий и выявления инцидентов;

Перезагрузить менеджер – для перезапуска ядра системы для применения внесенных изменений.

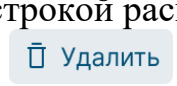
Рабочая область страницы разделена на части: слева расположен список со сгруппированными правилами, а справа – боковая панель с подробной информацией о выбранном элементе. Центральная часть приставлена таблицей с перечнем правил.

3.11.2 Страница «Активные правила»

Страница предназначена для просмотра и удаления активных правил и табличных списков. Страница «Активные правила» имеет категории:

- Нормализация;
- Корреляция;
- Агрегация;
- Табличные списки;
- Обогащение.

После наименования категории располагается поисковая строка. Для составления запроса следует обратиться в «Руководство по созданию запросов». Под строкой расположена панель инструментов (кроме «Обогащения»):



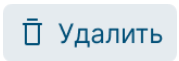
– для удаления правила или табличного списка;

В категориях (кроме «Обогащения») под строкой для настройки фильтрации располагается рабочая область, которая делится на две части: перечень правил или табличных списков и боковую панель для просмотра выбранного элемента базы правил (справа).

Категория «Обогащение» представляет собой рабочую область с таблицей и панелью инструментов над рабочей областью со следующими кнопками:

– для создания нового правила;

– для редактирования правила;



– для удаления правила.

Для написания правил и табличных списков следует обращаться в «Руководство по написанию правил».

3.11.3 Страница «Проверка правил»

Страница предназначена для осуществления проверки корректности работы правил.

На странице «Проверка правил» представлена рабочая область, которая разделена на две части: поле для ввода события, поле для получения результата обработки введенного события.

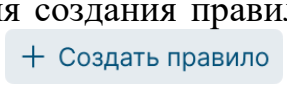
На странице панель инструментов представлена следующими кнопками:

– 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 правила необходимо перейти на страницу «Драфт зона» и нажать 

на панели инструментов, после чего откроется модальное окно (рис.60) с возможностью выбора папки, в которой будет создано правило.

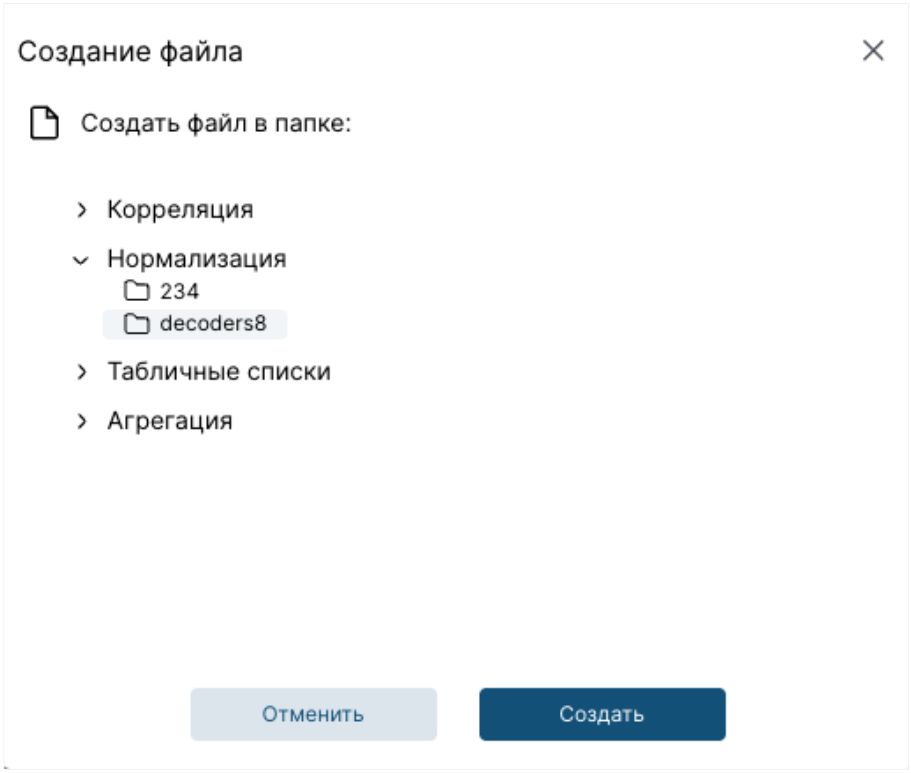


Рисунок 60 – Создание правила

После того как, выбрана папка, следует нажать 

. Как результат, появится модальное окно для создания правила (рис.61). В рабочую область следует ввести текст с правилом, а в поле «Наименование файла» – текст с наименованием. Следует обратить внимание на ограничение в 250 символов.

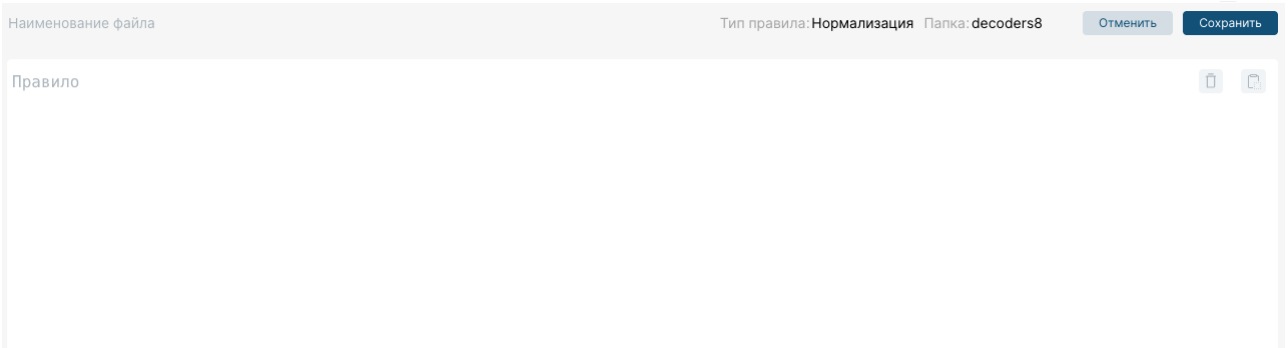


Рисунок 61 – Ввод правила с последующим сохранением

Когда рабочая зона будет заполнена хоть одним символом, появится возможность копировать текст с помощью кнопки . Кроме того, можно очистить введенный текст нажатием на . В целях корректной работы с базой правил следует обратиться к «Руководству по написанию правил».

Для того, чтобы сохранить правило следует нажать на кнопку Сохранить, после чего произойдет возврат на страницу «Драфт зона», новое правило добавится в систему и, соответственно, в таблицу, а также появится соответствующее 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, однако все введенные данные будут утеряны.

3.12.2 Редактирование правила

Для того, чтобы отредактировать правило, его нужно выбрать в таблице и нажать кнопку Редактировать. После нажатия открывается боковое модальное окно (рис.62), в котором текст правила и его название доступны для изменения.

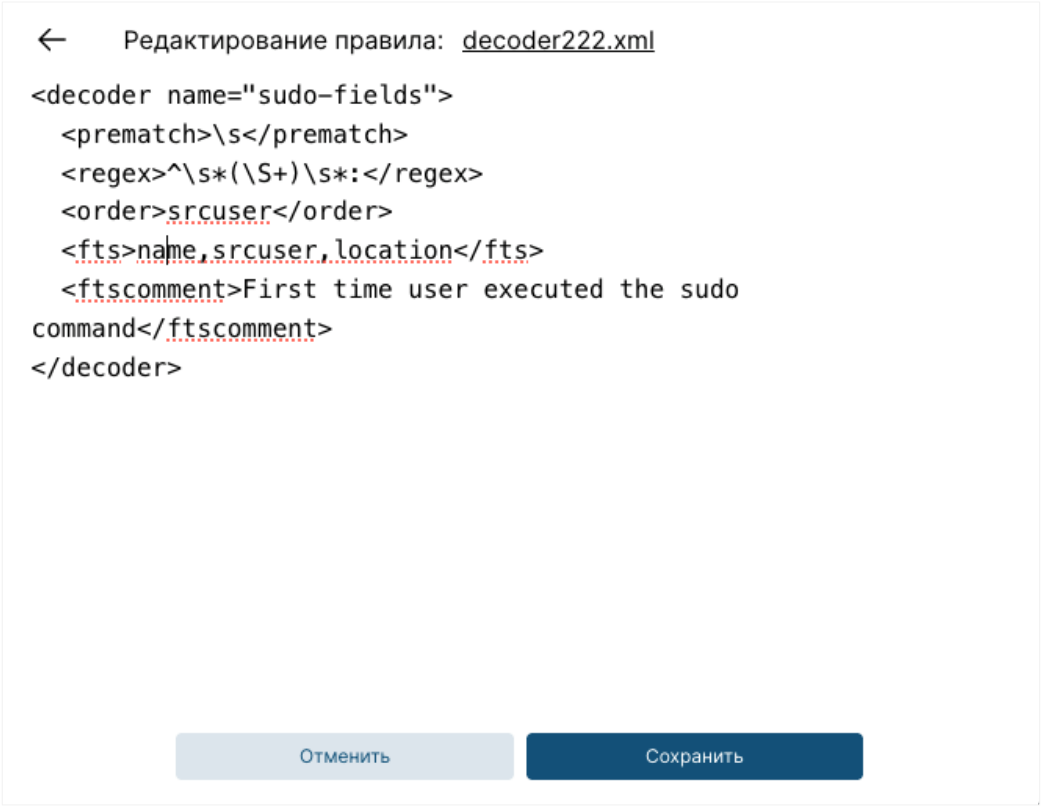


Рисунок 62 – Режим редактирования правила

Следует обратить внимание, что если правило активное, то есть уже загружено в систему, то нельзя изменить его наименование.

Вернуться на страницу с общим списком правил без сохранения изменений можно при нажатии на ←, на зону вне модального окна или на кнопку Отменить.

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

3.12.3 Создание табличного списка

Для создания правила необходимо перейти на страницу «Драфт зона» и нажать + Создать правило на панели инструментов, после чего откроется модальное окно (рис.63) с возможностью выбора категории. Необходимо выбрать категорию «Табличные списки» и папку в категории, в которой будет создан табличный список.

После того как, выбрана папка, следует нажать Создать и появится модальное окно для создания табличного списка с редактируемыми полями для названия файла и ввода значений (рис.63). Наименование табличного списка должно быть на латинице.

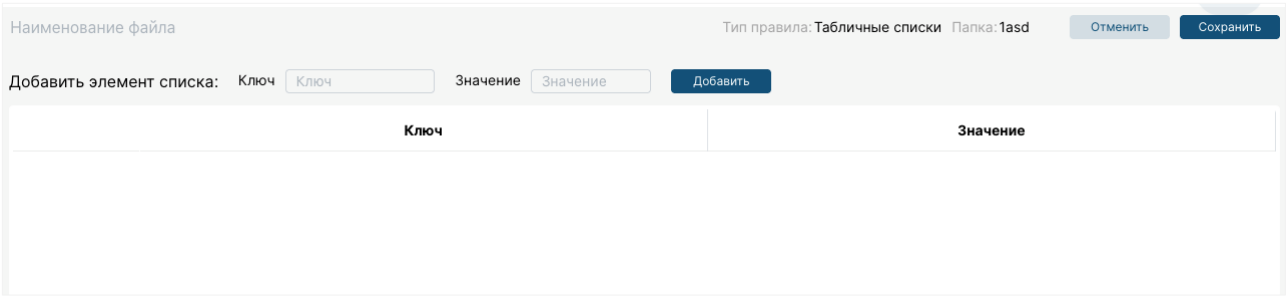


Рисунок 63 – Создание табличного списка

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

Для того, чтобы удалить элементы из списка необходимо нажать на кнопку в поле, которое необходимо удалить (рис.64).

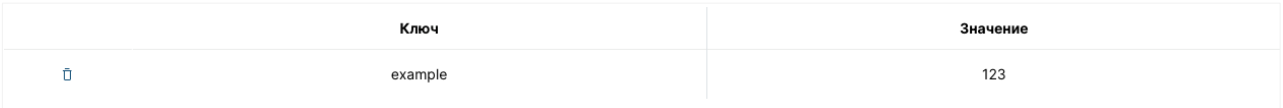


Рисунок 64 – Элемент в табличном списке

Для сохранения изменений необходимо нажать Сохранить. Далее происходит возврат на страницу «Драфт зона», новый список добавляется в систему и, соответственно, в таблицу, а также появляется соответствующее уведомление «Список создан успешно» (в случае неуспешности – уведомление «Не удалось создать список»).

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

3.12.4 Редактирование табличного списка

Для редактирования табличного списока, его следует выбрать в таблице и нажать на кнопку Редактировать в боковой панели. После нажатия открывается боковое модальное окно (рис.65), в котором можно добавить или удалить элемент списка, отредактировать пару «Ключ» и «Значение», изменить наименование файла.

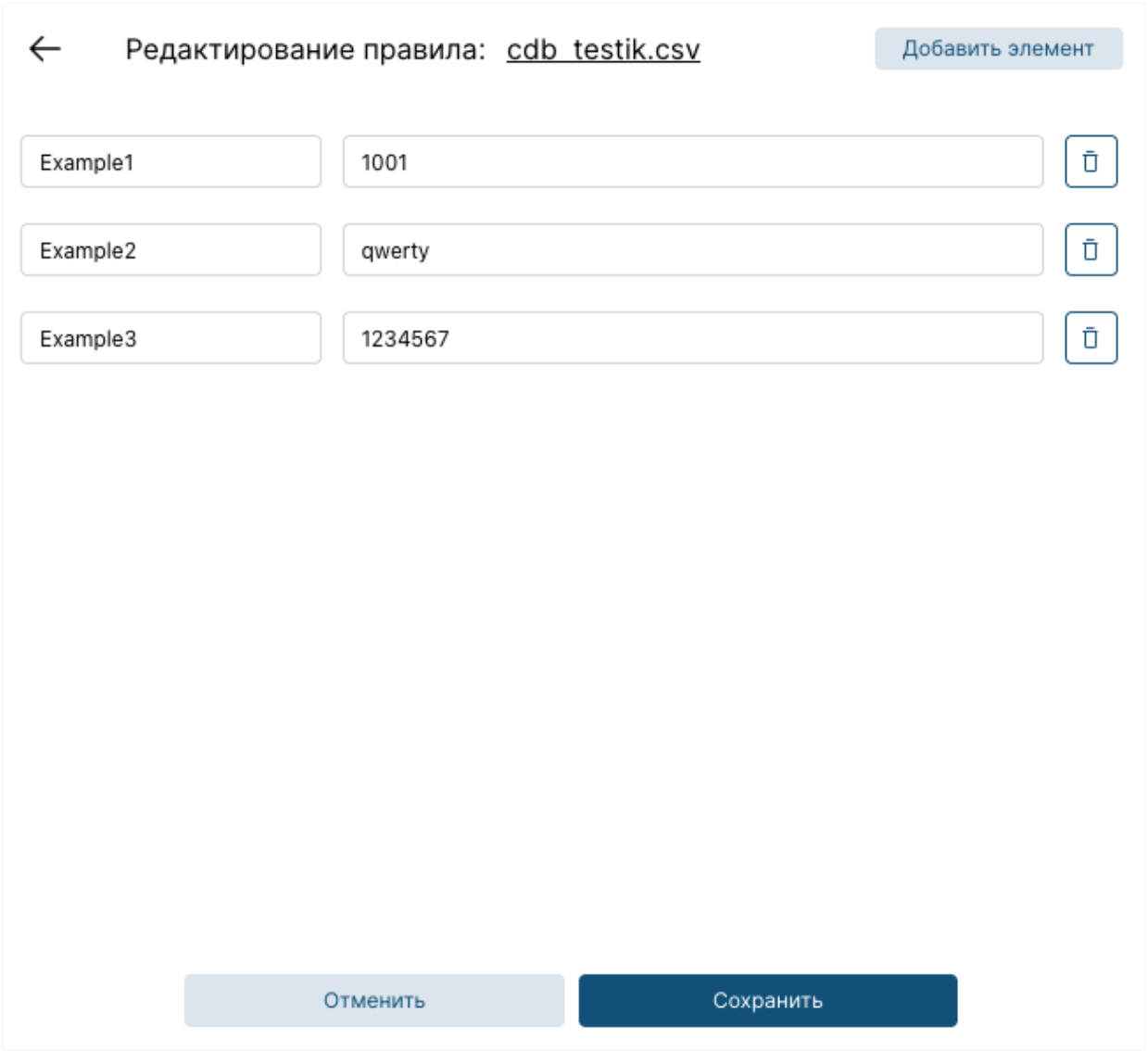


Рисунок 65 – Режим редактирования табличного списка

Для того, чтобы добавить новый элемент, следует воспользоваться кнопкой Добавить элемент, а для удаления – .

Вернуться на страницу с общим списком правил без сохранения изменений можно при нажатии на ←, на зону вне модального окна или на кнопку Отменить.

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

3.12.5 Удаление и загрузка файла в систему, экспорт и импорт файла на странице «Драфт зона»

Для того, чтобы удалить правило необходимо сначала удалить правило из активных на странице «Активные правила» , а затем уже выбрать его в таблице на странице «Драфт зона» и нажать кнопку Удалить из драфт зоны или можно воспользоваться элементом в левой боковой панели напротив представленного к удалению файлу (рис.66). Результат операции отобразится в уведомлениях.

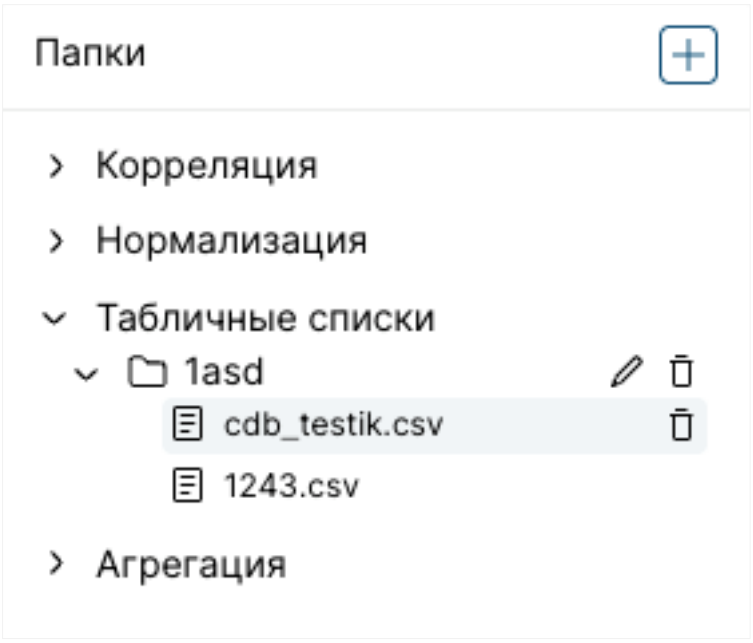
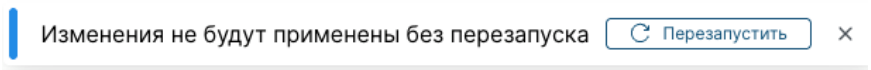


Рисунок 66 – Удаление файла

Для того, чтобы загрузить файл в систему, следует выбрать его или набор правил в списке и нажать кнопку Загрузить в систему. Результат операции отобразится в уведомлениях. Для применения внесенных изменений



следует нажать кнопку «Перезапустить».

Для того, чтобы экспортировать файл (набор файлов) необходимо выбрать его в списке правил и нажать кнопку Экспорт. Далее будет представлено модальное окно с выбором опции скачивания: скачать все файлы или только

выбранные. Если выбран один файл, то он будет скачан в формате .xml, а если выбран набор правил, то они будут объединены в архив. При опции «Скачать все файлы», они будут скачаны в виде архива с сохранением иерархической структуры.

Для того, чтобы импортировать правила, следует нажать кнопку 

, в появившемся модальном окне выбрать опцию импорта: одного или несколько файлов, архива с файлами или архива с папками и файлами.

Если будет выбрана опция загрузки одного или нескольких правил, то файлы будут добавлены в выбранную папку, если выбран архив с файлами – файлы из архива будут добавлены в выбранную папку, а если выбран архив с папками и файлами – папки с файлами будут загружены в корневой каталог.

При выборе опции «Архив с папками и файлами» необходимо, чтобы архив имел 4 папки со следующими наименованиями: «aggregation», «cdb», «decoder», «rule».

Загрузка правил происходит в формате xml, а табличных списков в формате – csv. Результат загрузки отобразится в уведомлениях.

Следует обратить внимание, что с системой поставляются правила от центра кибербезопасности НЦОТ, которые можно найти в папке `KnowledgeBase/` в распакованном архиве при процессе установки системы (см. «Руководство по установке»).

3.12.6 Работа с группами правил

Для того, чтобы создать папку необходимо в левой боковой панели нажать на элемент  (рис.66), после чего появится модальное окно (рис.67), в котором следует ввести название группы и выбрать категорию, где группа будет создана. Следует обратить внимание на ограничение в 250 символов.

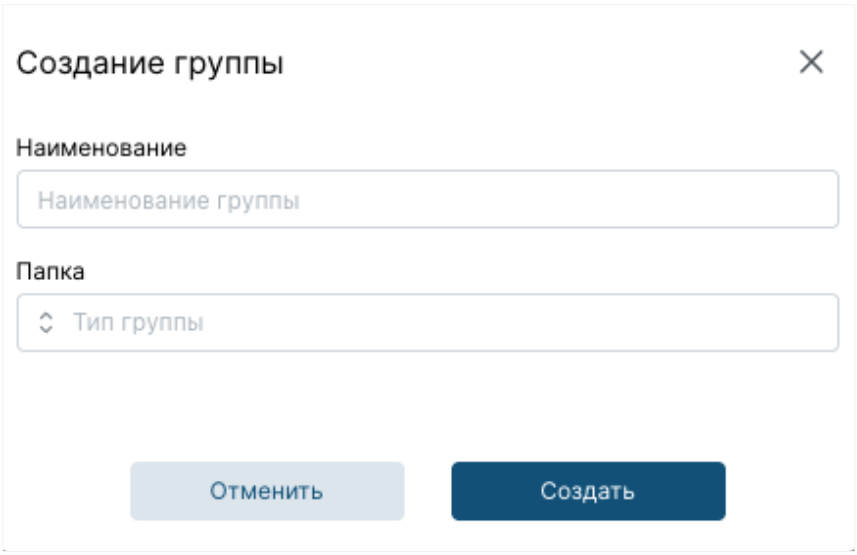


Рисунок 67 – Создание папки

Для того, чтобы отредактировать папку необходимо выбрать папку в левой боковой панели на странице «Драфт зона» (рис.59) и нажать на , после чего появится модальное окно с возможностью изменения наименования папки (рис.61).

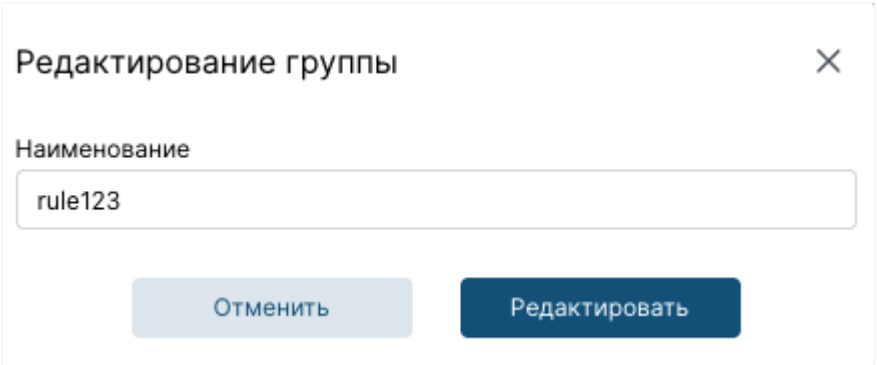


Рисунок 68 – Редактирование папки

Для того, чтобы удалить папку необходимо выбрать папку в левой боковой панели на странице «Драфт зона» (рис.66) и нажать . Результат операции отобразится в уведомлениях.

Следует обратить внимание, что папка, выбранная для удаления, должна быть пустой.

3.12.7 Создание правила обогащения

Для того, чтобы добавить правило обогащения необходимо перейти на страницу «Активные правила» категория «Обогащение» и нажать + Создать, после чего откроется модальное окно (рис.69) с полями для заполнения. Поля «Поле события» и «Новое поле события» являются обязательными для заполнения.

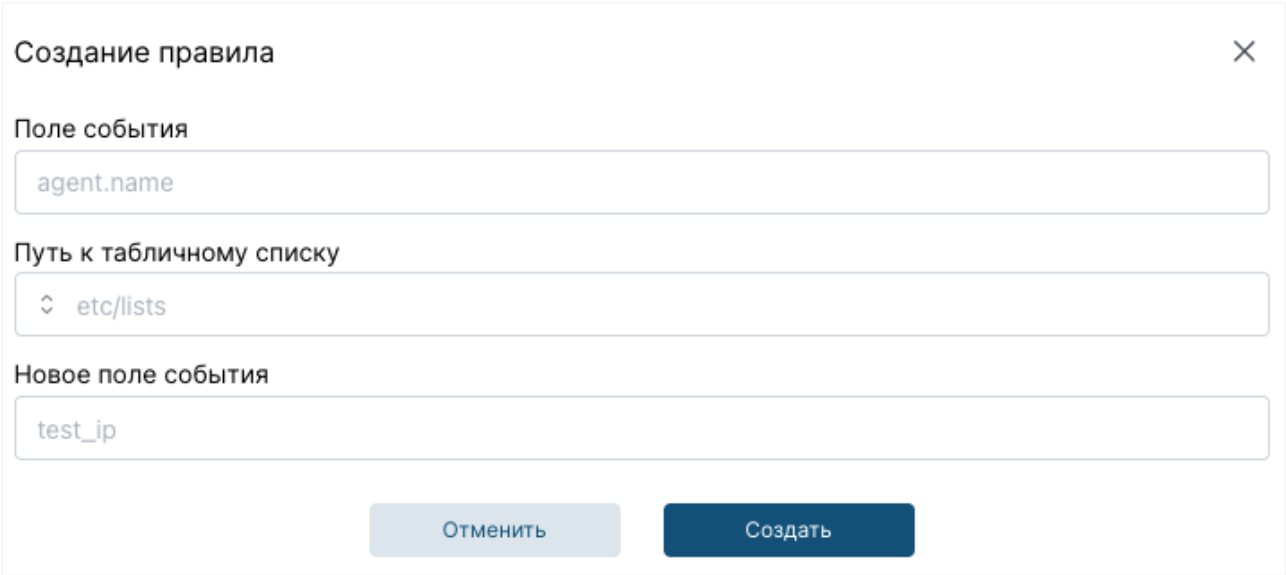


Рисунок 69 – Добавление нового правила обогащения

Для сохранения правила необходимо нажать на кнопку «Сохранить». Далее происходит возврат на ранее активную страницу из группы страниц «База правил», новый список добавляется 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.

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 Редактировать открывается боковое модальное окно (рис.70), в котором можно отредактировать «Путь к табличному списку» и «Новое поле события». Однако, «Поле события» является неизменным текстовым блоком.

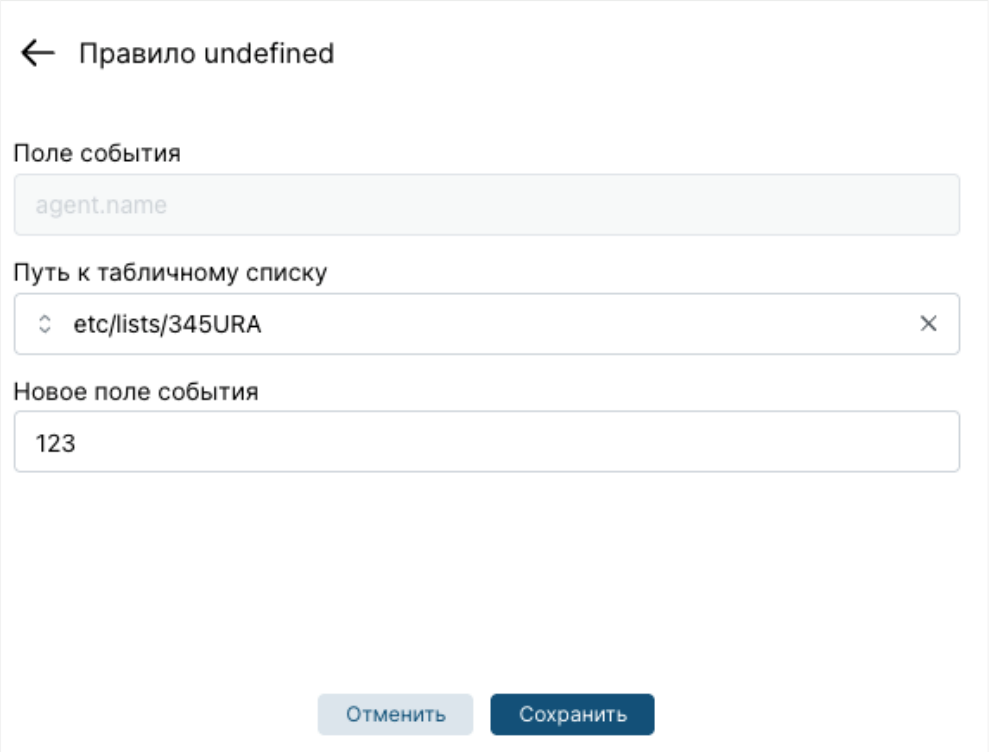


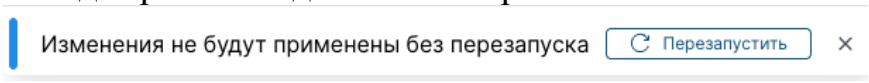
Рисунок 70 – Редактирование правила обогащения

3.10.9 Удаление правила обогащения

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

Следует обратить внимание, что после добавления, удаления или редактирования правила появится уведомление о необходимости перезагрузить

менеджер для применения внесенных изменений



. Следует нажать кнопку «Перезапустить».

3.12.10 Проверка правил

Для того, чтобы проверить набор правил, существующий в системе, можно воспользоваться страницей «Проверка правил» (рис.71).

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

. 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  .

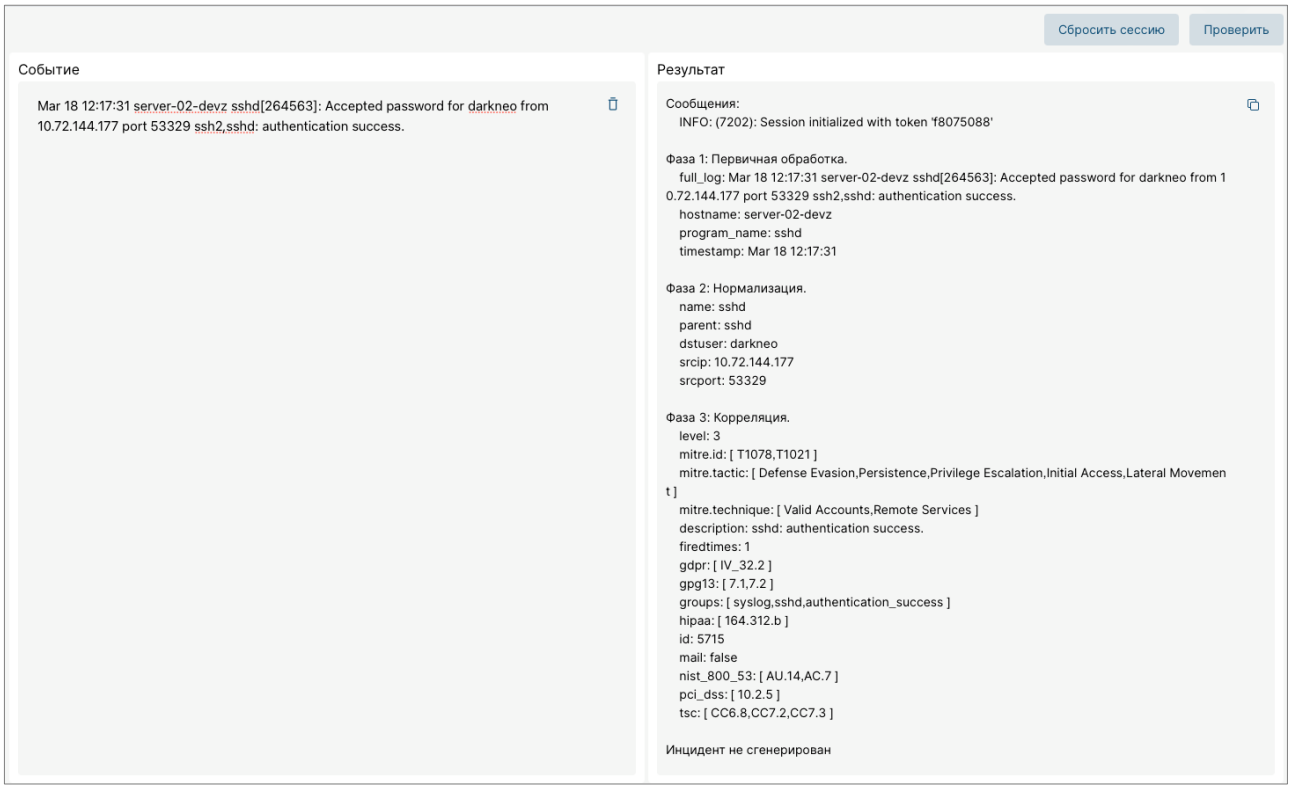


Рисунок 71 – Страница «Проверка правил»

Следует обратить 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.

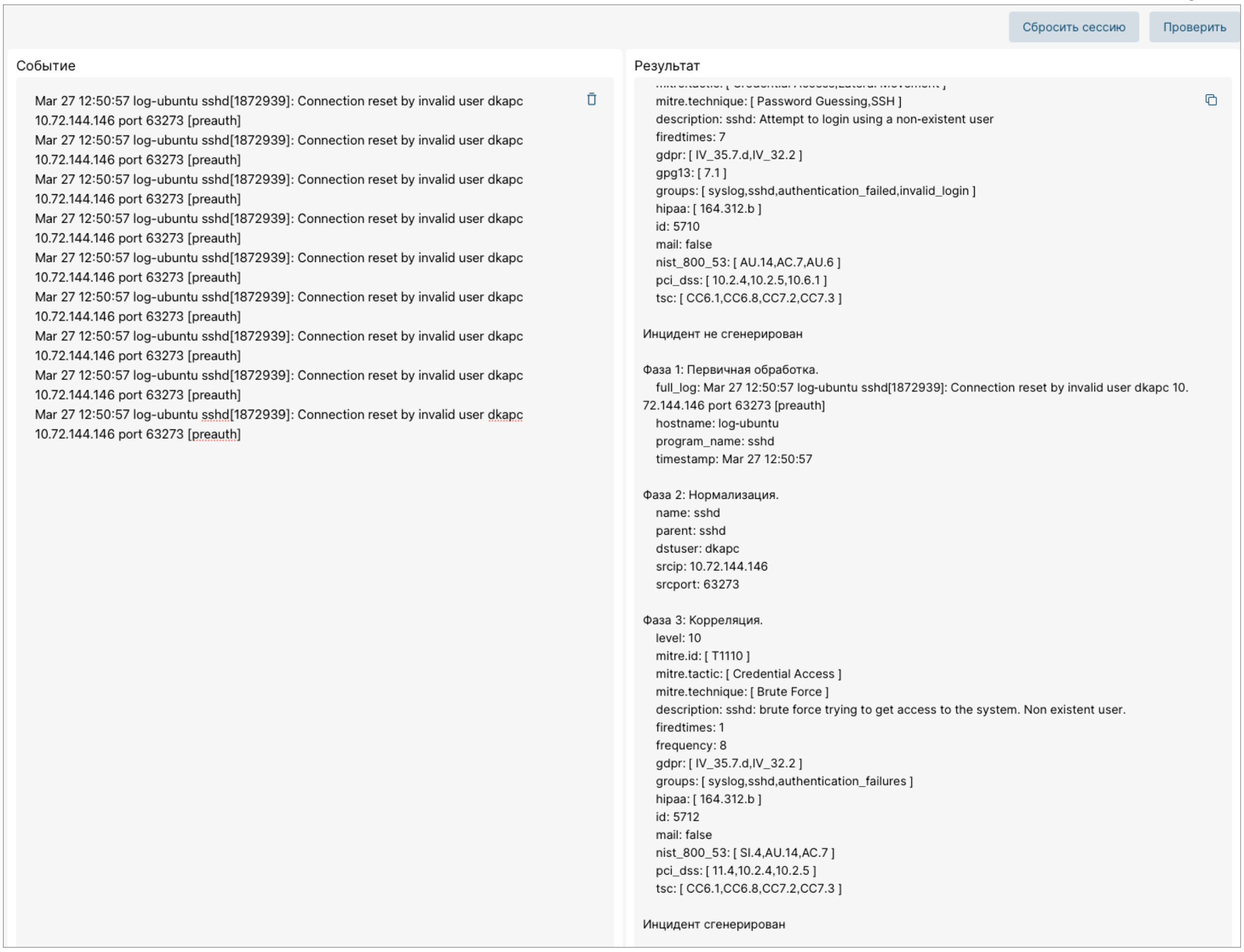
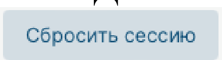


Рисунок 72 – Проверка правил с корреляцией событий

Как видно из рисунка 72, 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, журналом действий пользователей, лицензированием, интеграциями, а также настройки интеграции с SOAR-системой, почтовой рассылки и настройка уведомлений.

3.13.1 Страница «Управление пользователями»

Страница предназначена для работы с пользователями и их ролями. Страница «Управление пользователями» имеет категории:

- Пользователи;
- Роли;
- Журнал действий;
- Интеграции;
- Настройки LDAP.

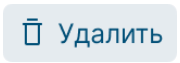
Рабочая область категории «Пользователи» разделена на две части: левая часть представляет собой список с пользователями, правая – таблицу с подробной информацией о выбранном пользователе. Правая панель по умолчанию отображается в развернутом виде. При необходимости скрыть данную область следует нажать на кнопку закрытия › .

Для каждого пользователя в списке указан набор параметров:

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

Панель инструментов содержит кнопки:

– для регистрации нового пользователя вручную;



– для удаления пользователя вручную.

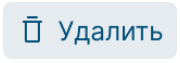
Рабочая область категории «Роли» так же разделена на две части: левая часть представляет собой список с ролями, правая – таблицу с подробной информацией о выбранной роли. Правая панель по умолчанию отображается в развернутом виде. При необходимости скрыть данную область следует нажать на кнопку закрытия › .

Для каждой роли в списке указан набор параметров:

- Наименование;
- Описание.

Панель инструментов содержит кнопки:

– для регистрации новой роли пользователем;



– для удаления роли.

Рабочая область категории «Журнал действий пользователей» предназначена для мониторинга и анализа активности пользователей в системе.

Журнал действий пользователей представлен в виде таблицы, которая содержит следующие колонки:

- Время – точная дата и время совершения действия;
- IP- адрес – сетевой адрес, с которого было инициировано действие;
- Логин – учетная запись пользователя, совершившего действие;

- Метод – HTTP метод запроса;
- Путь – конкретный ресурс, к которому обращался пользователь;
- Статус выполнения действия – результат обработки запроса системой.

По умолчанию отображаемые данные в таблице отсортированы от новых к более старым записям и за последний час.

Панель инструментов содержит поисковую строку для фильтрации логов по всем доступным полям таблицы с помощью языка запросов (см. Руководство по создание запросов).

Для удобства ввода запросов в строке поиска предусмотрена функция подсказок. Система предлагает два типа подсказок:

- подсказки по полям (ключам);
- подсказки по логическим операторам.

Подсказки по ключам содержат названия доступных полей для поиска (например, `user_ip, path, status`).

Подсказки по логическим операторам содержат операторы AND, OR, NO для построения сложных поисковых запросов.

Подсказки отображаются в виде выпадающего списка с возможностью прокрутки. Выбор осуществляется стрелками ↓↑ и клавишей Enter или кликом мыши по необходимому элементу.

В поисковой строке доступна кнопка [?] (по умолчанию активна), которая позволяет:

- временно отключить отображение подсказок;
- включить подсказки обратно.

Состояние кнопки (включено/ выключено) сохраняется при переходе между страницами.

При необходимости, можно отфильтровать информацию по определенному временному периоду. Для этого необходимо нажать на кнопку «Календарь»  и выбрать временной интервал.

При нажатии на кнопку × происходит очистка поисковой строки.

Рабочая область категории «Интеграции» представляет собой список со всеми интеграциями.

Панель инструментов содержит кнопки:

Создать интеграцию – для создания новой интеграции.

Рабочая область категории «Настройки LDAP» так же разделена на части: левая часть представляет собой форму для ввода параметров для подключения к серверу MAD, правая – кнопкой Тестировать подключение, которая используется для тестирования подключения к серверу MAD. Центральная часть представлена формой для сопоставления групп и ролей.

3.13.2 Страница «Лицензирование»

На странице «Лицензирование» представлен функционал, позволяющий просматривать информацию о лицензии (рис.73) и проверять состояние лицензии с помощью кнопки Проверить статус. Инструкция по добавлению лицензии описана в Руководстве по установке.

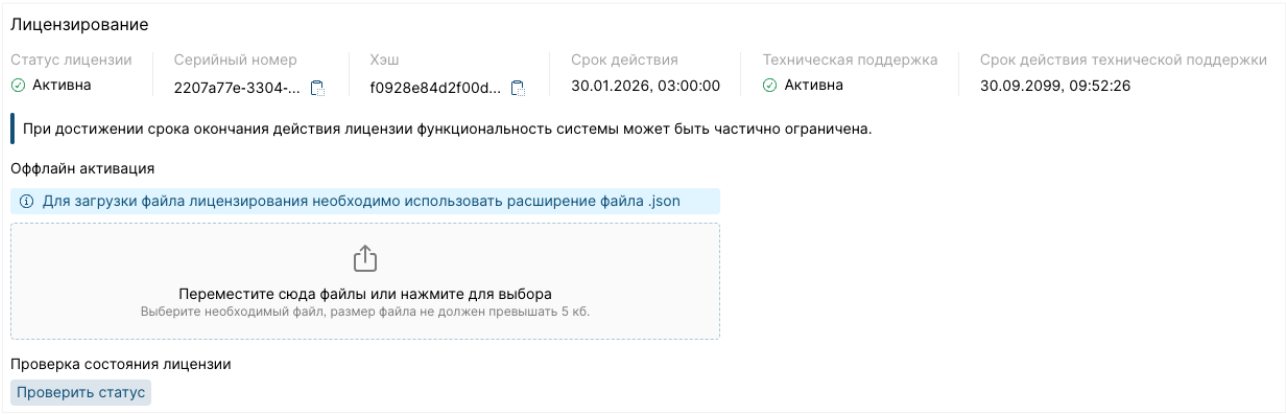


Рисунок 73 – Страница «Лицензирование»

3.13.3 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 настройка уведомлений (рис. 74).

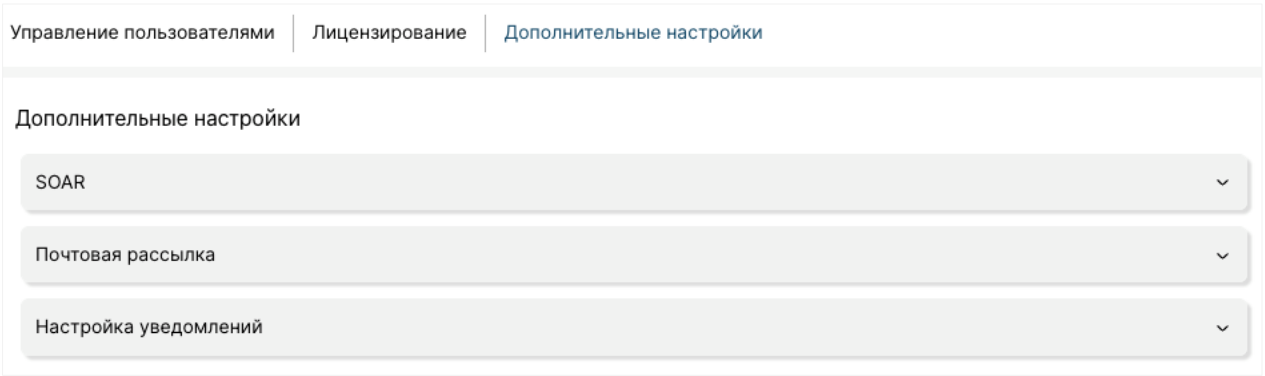


Рисунок 74 – Блоки для дополнительных настроек

3.14 Работа с настройками системы

3.14.1 Создание пользователя

Для создания нового пользователя нажать на кнопку + Создать в категории «Пользователи». После этого появится модальное окно с полями для ввода информации (рис.75).

Поля «Имя пользователя», «Пароль», «Фамилия», «Имя», «Отчество», «Электронная почта» и «Роль» являются обязательными для заполнения.

Минимальное количество символов в поле «Пароль» – 10, включая латинские заглавные и строчные буквы, специальные символы !@#$%^&*()_+ и цифры. 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 и прописные буквы, а таже символы «_», «-», «.».

Пользователю можно присвоить статус активности Статус Неактивен. Если задан статус Активен, пользователь может авторизоваться в системе и иметь доступ к интерфейсу в соответствии с выданными ему привилегиями. В случае если задан статус Неактивен, у пользователя отсутствует доступ к системе.

По умолчанию при создании пользователя переходник будет в состоянии «Неактивен».

Следует обратить внимание, что нельзя деактивировать системного пользователя с ролью «Суперадминистратор».

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

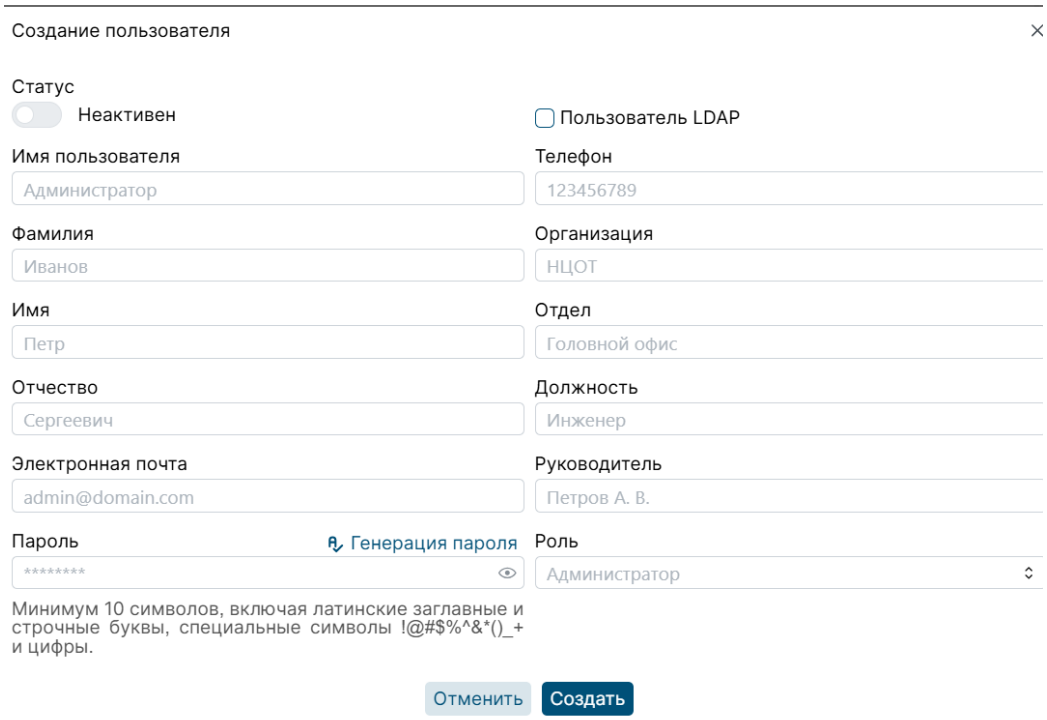


Рисунок 75 – Создание нового пользователя

Для создания пользователя LDAP необходимо поставить галочку Пользователь LDAP и появится форма (рис.76).

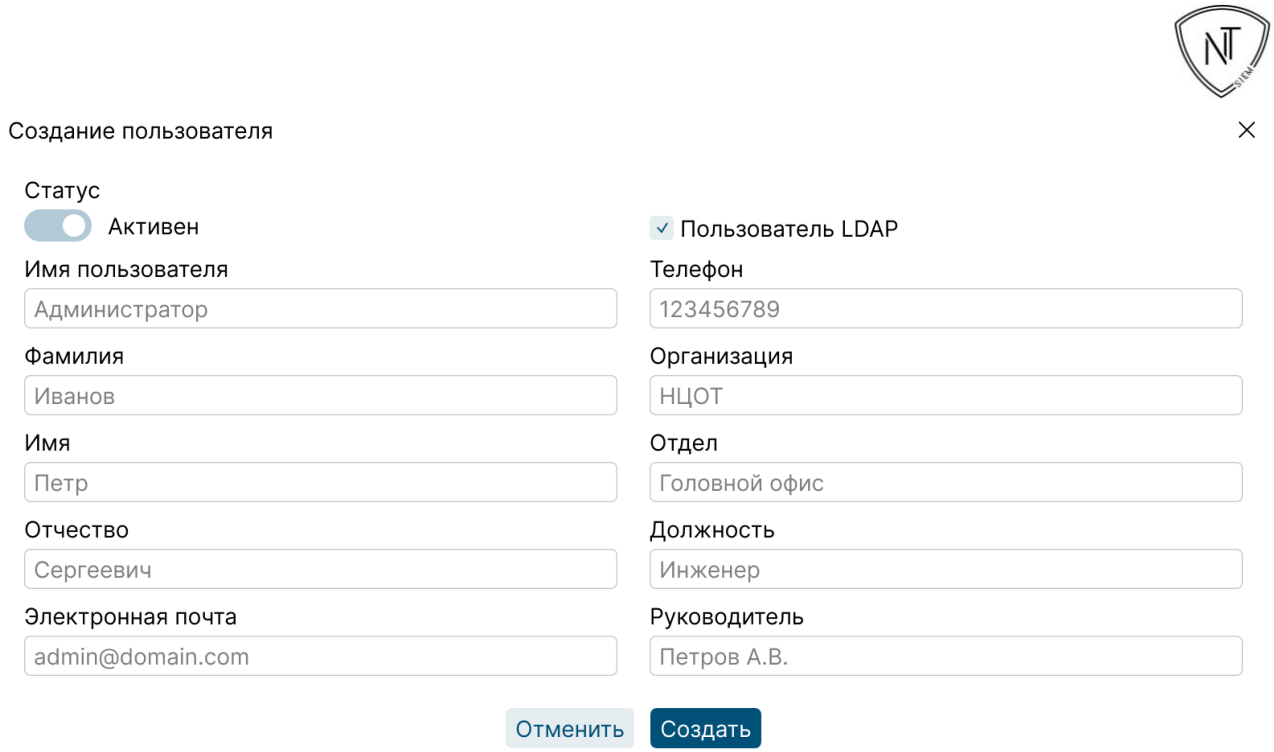


Рисунок 76 – Создание нового пользователя LDAP

3.14.2 Редактирование пользователя

Для редактирования информации о пользователе необходимо нажать на кнопку «Редактировать» в таблице с подробной информацией о пользователе. При нажатии на нее открывается боковое модальное окно, в котором поля с текстовой информацией станут доступными для изменения (рис. 77).

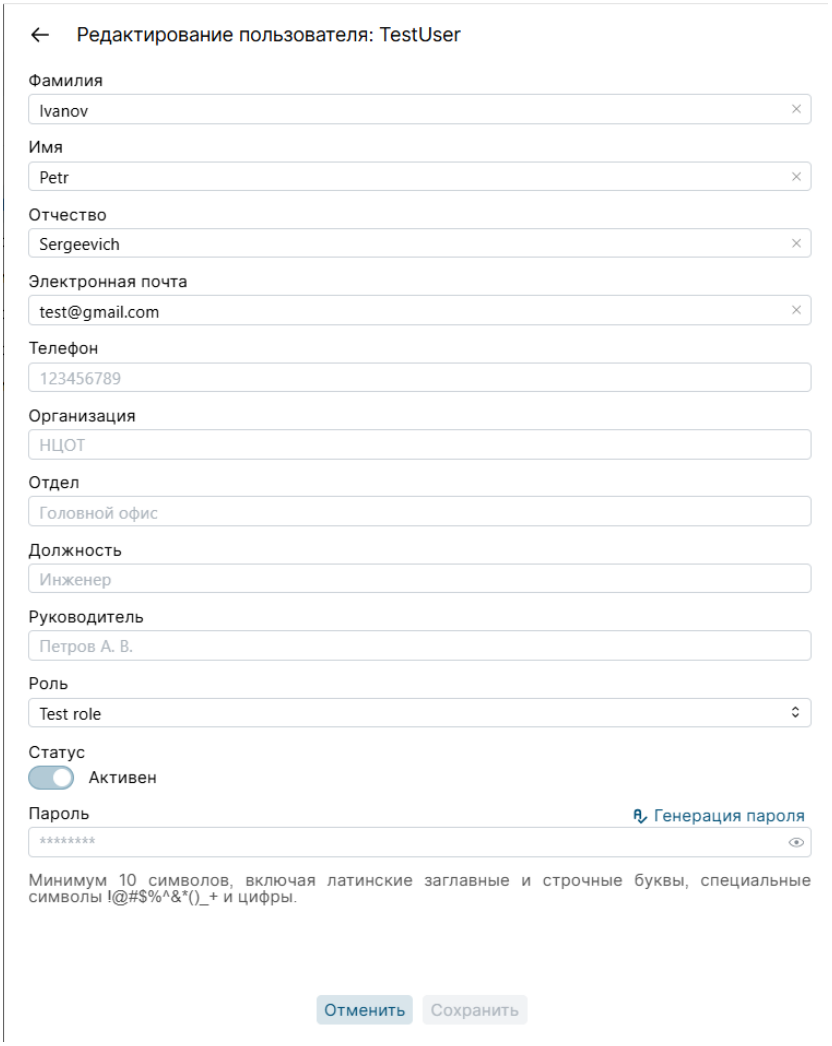


Рисунок 77 – Редактирование пользователя

Для сохранения изменений нужно нажать на кнопку «Сохранить». Если пользователь не подтверждает свое действие или нажимает 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.

Для редактирования информации о пользователе LDAP необходимо нажать на кнопку «Редактировать» в таблице с подробной информацией о пользователе. При нажатии на нее открывается боковое модальное окно, в котором поля с текстовой информацией станут доступными для изменения (рис.78).

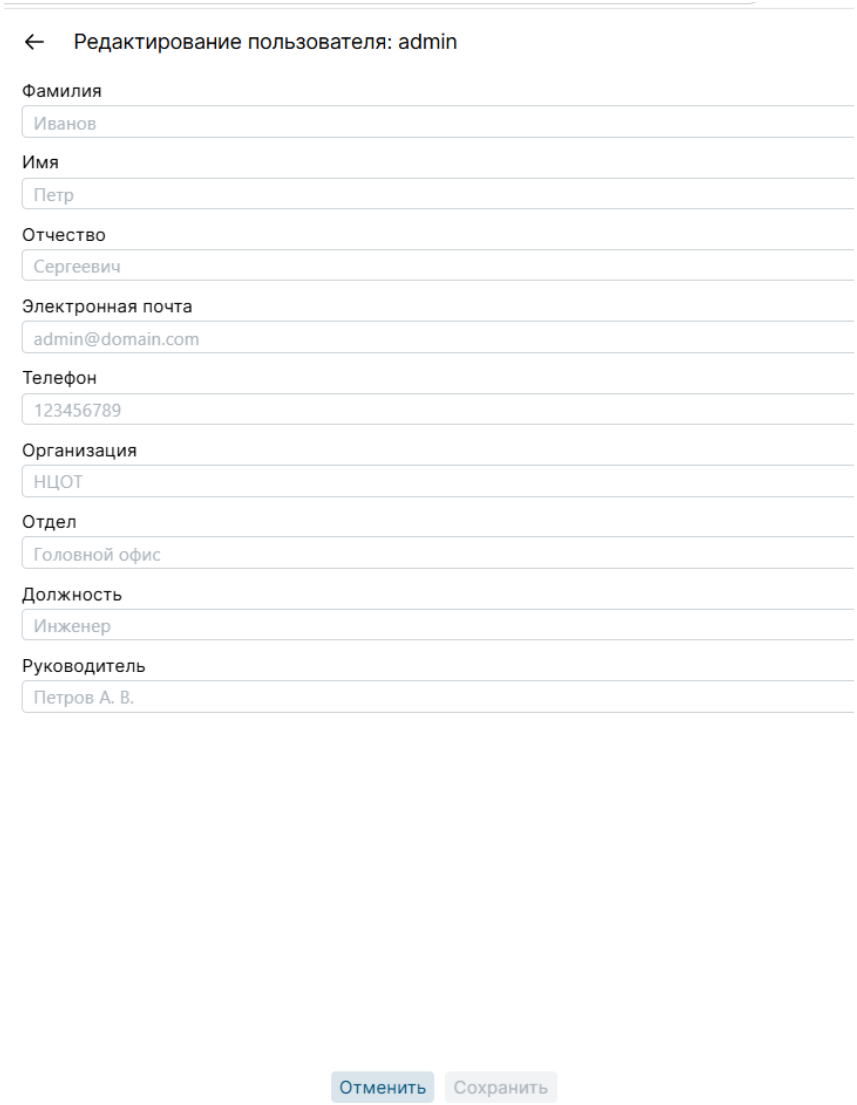
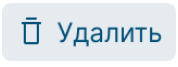


Рисунок 78 – Редактирование пользователя LDAP

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.

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 А).

В системе реализована ролевая модель управления доступом с набором стандартных ролей «Администратор» и «Оператор» (Приложение А). Каждая

роль содержит набор привилегий, которые определяют доступные для Пользователя разделы интерфейса и операции в системе.

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

Стандартная роль «Оператор» имеет набор привилегий: работа с дашбордами, работа с инцидентами, событиями, 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 + Создать на странице «Роли». Далее появится модальное окно (рис.79), в котором необходимо ввести данные в поля «Наименование» и «Описание», а также в раскрывающемся списке «Привилегии» выбрать набор прав для создаваемой роли (Приложение А). Поле «Наименование» и «Выбор привилегий» не могут быть пустыми.

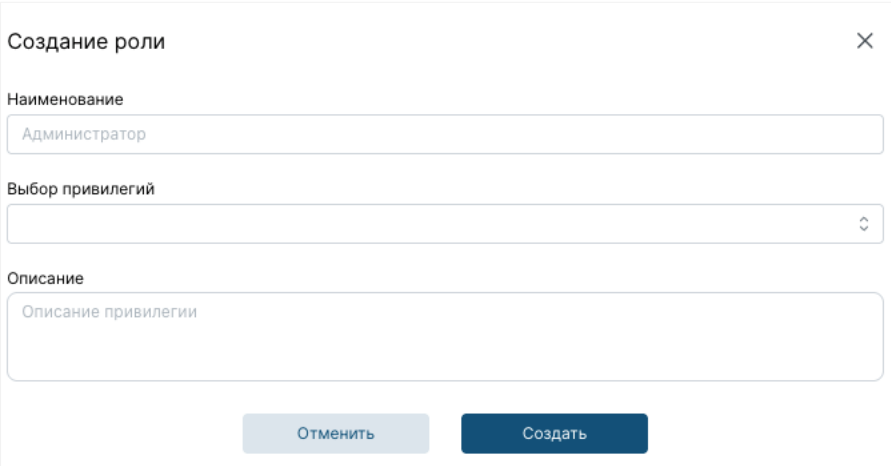


Рисунок 79 – Создание роли

Для сохранения новой роли нужно нажать на кнопку «Создать». 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 в боковом окне с подробной информацией нажать на кнопку «Редактировать», появится модальное окно и поля станут доступными для изменения (рис. 80).

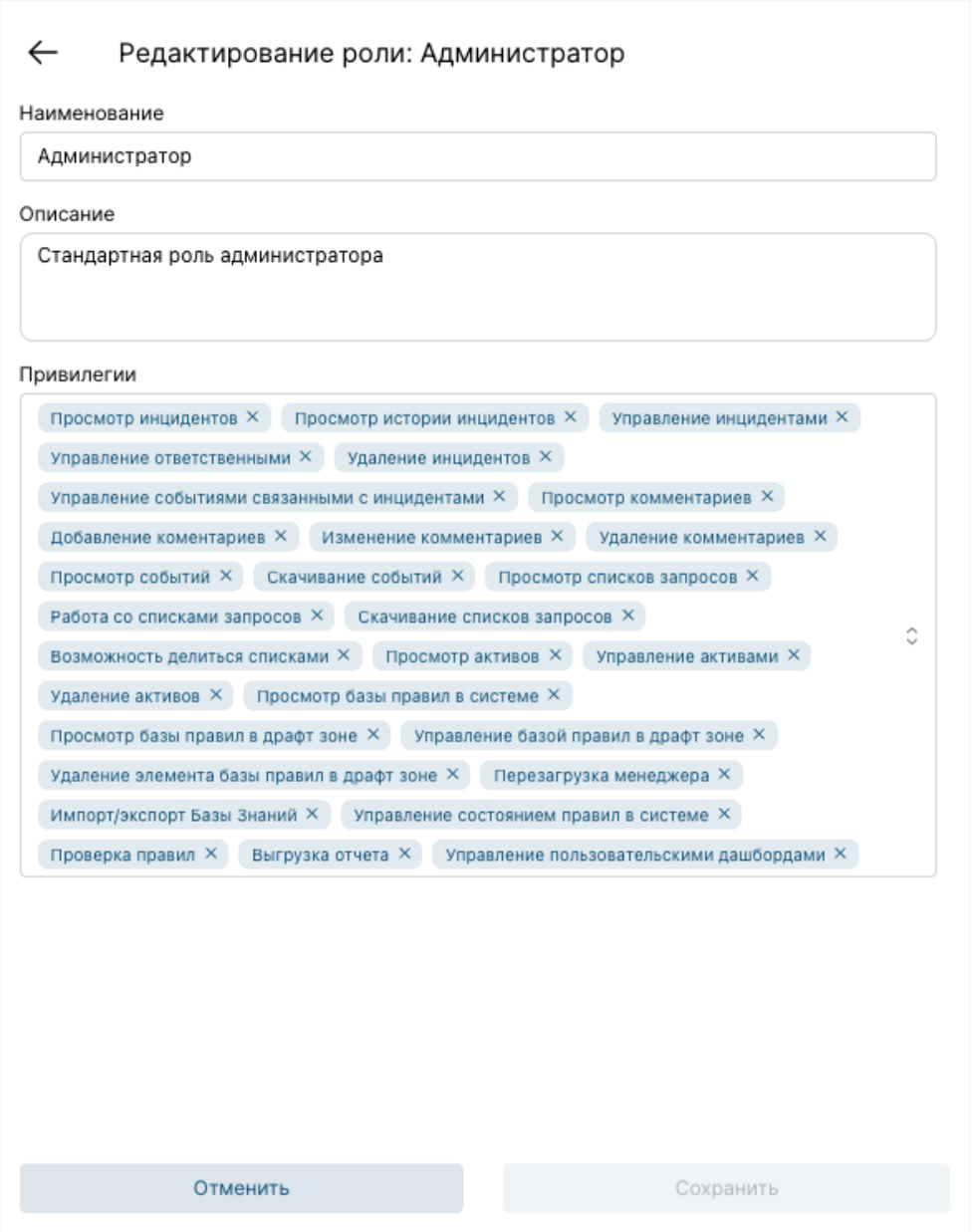
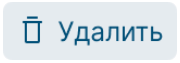


Рисунок 80 – Редактирование роли

Для сохранения изменений нужно нажать на кнопку «Сохранить». Если пользователь не подтверждает свое действие, нажав 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 интеграциями

Для того, чтобы создать интеграцию следует нажать Создать интеграцию, в появившемся модальном окне заполнить поля «Наименование» и «Дата окончания действия» (рис.81):

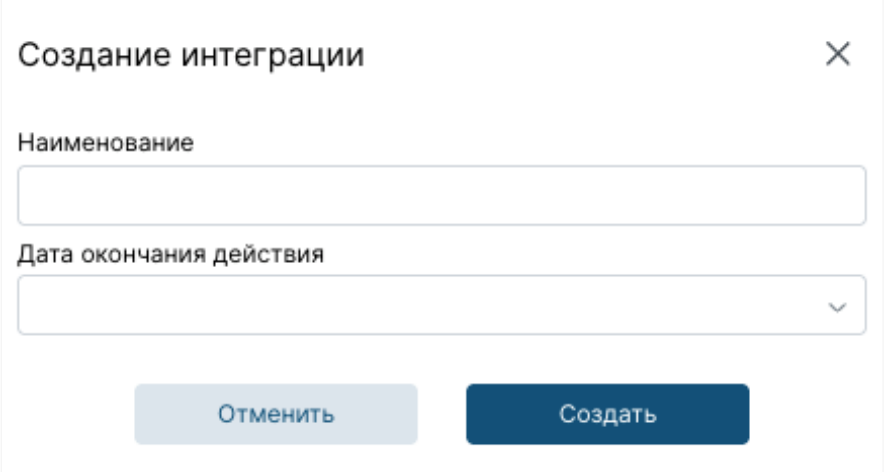


Рисунок 81 – Создание интеграции

При нажатии на поле «Дата окончания действия» появится календарь с возможностью выбора даты (рис.82). После того, как выбранный срок истек токен станет неактуальный, и, соответственно, интеграция с системой станет невозможной:

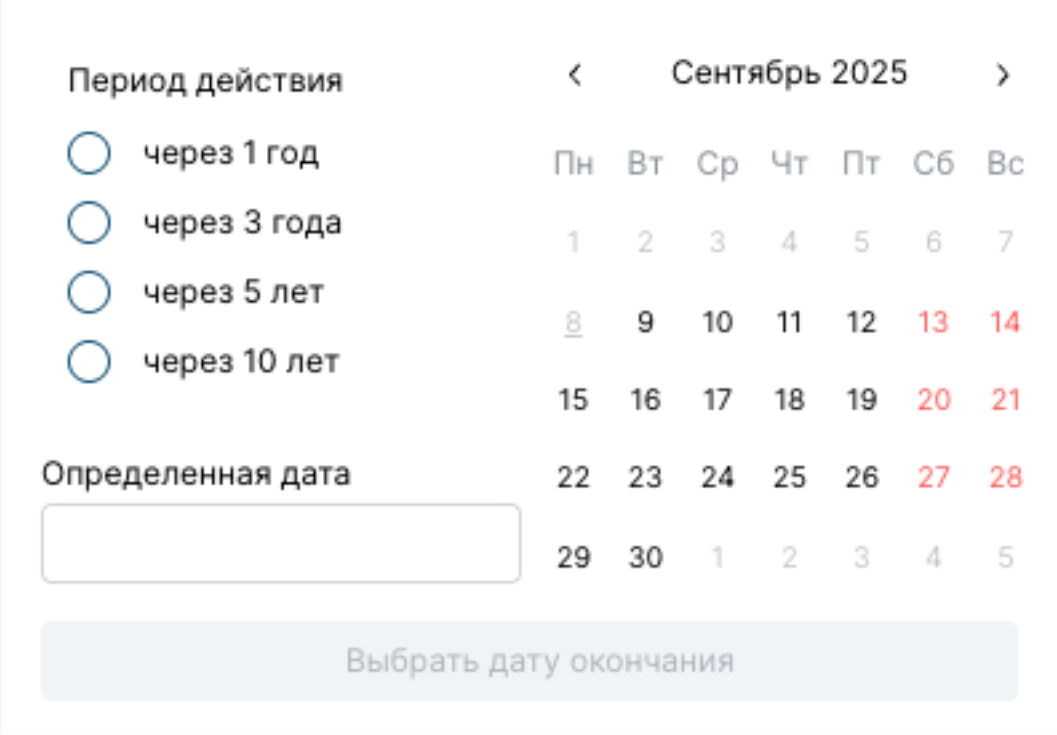


Рисунок 82 – Календарь для выбора периода

Для редактирования информации об интеграции необходимо нажать , появится модальное окно и поля станут доступными для изменения (рис.83).

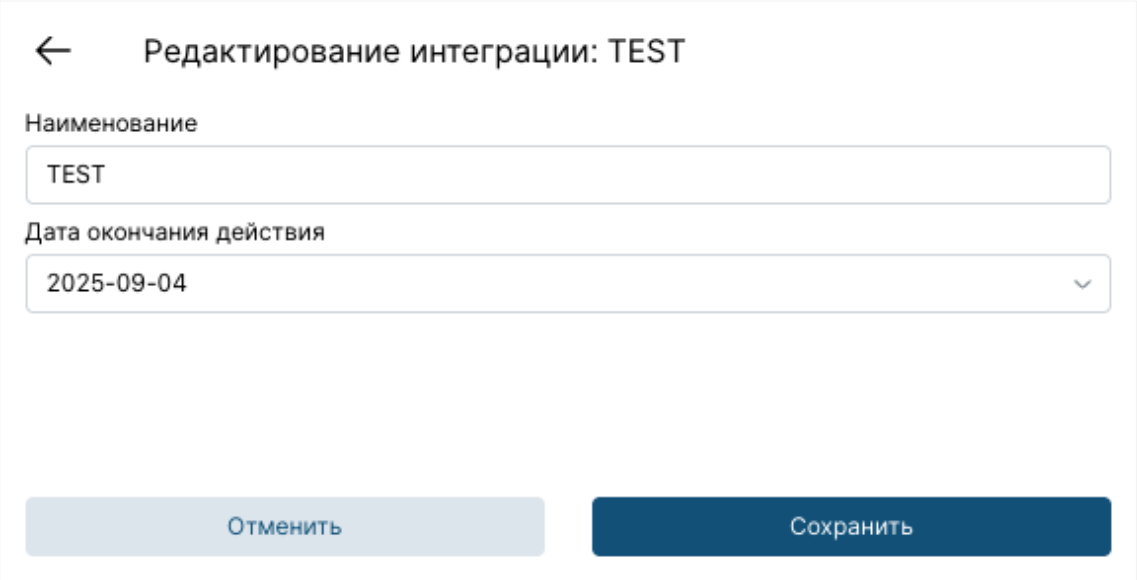


Рисунок 83 – Редактирование интеграции

Для сохранения новой интеграции нужно нажать на кнопку «Сохранить». Если пользователь не подтверждает свое действие, нажав кнопку «Отменить» или ←, то несохраненные данные будут утеряны.

Для удаления интеграции следует воспользоваться элементом , а для копирования токена следует воспользоваться элементом .

3.14.8 Работа с настройками LDAP

В NTechnology SIEM система обеспечивает возможность аутентификации двумя способами: локально или по протоколу LDAP.

Для того чтобы производить аутентификацию по протоколу LDAP, необходимо настроить соединение между NTechnology SIEM и сервером, где расположена система аутентификации. Для этого необходимо заполнить параметры для подключения на странице «Настройки LDAP» (рис. 84).

Поля «Наименование», «Адрес AD», «Порт», «Домен», «Логин пользователя» и «Пароль» являются обязательными для заполнения.

В полях «Логин пользователя» и «Пароль» вводятся данные учетной записи, с помощью которой будет производиться доступ на MAD сервер.

Для того, чтобы очистить значения поля, следует воспользоваться элементом .

По умолчанию по протоколу LDAP передаются сообщения в виде открытого текста, следовательно, необходимо настроить защищённое соединение LDAP по SSL.

При необходимости подключения по протоколу LDAPS, следует изменить состояние переключателя Зашифрованное соединение и загрузить доверенный

сертификат корневого центра сертификации, который используется LDAP-сервером для обеспечения безопасности и шифрования трафика в формате `.cer`.

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

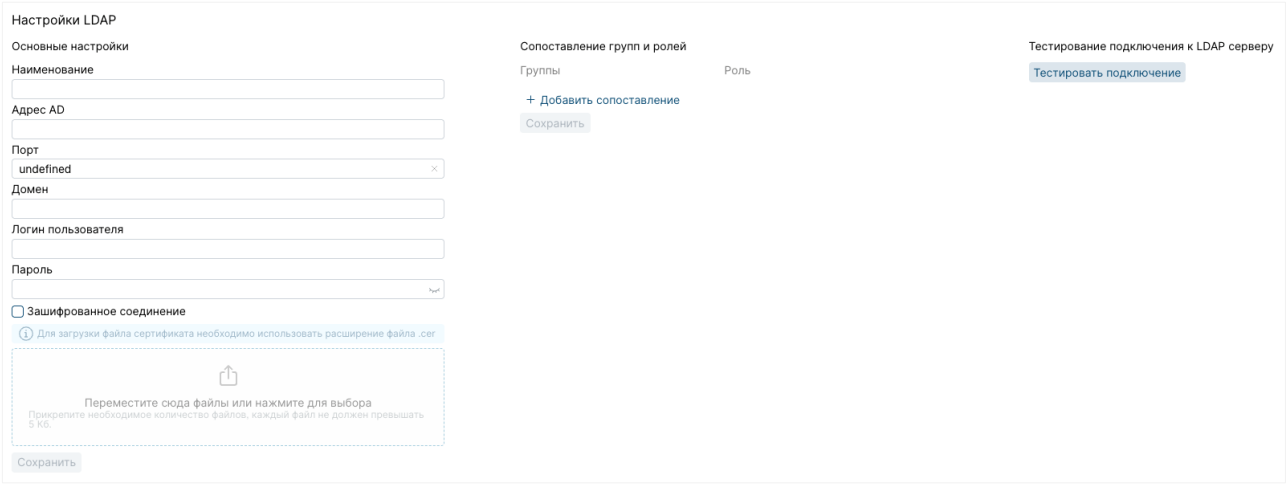


Рисунок 84 – Страница для настройки LDAP

Для того, чтобы у пользователей была возможность взаимодействовать с системой, необходимо настроить сопоставление групп пользователей MAD и ролей в системе.

Для этого в блоке «Сопоставление групп и ролей» необходимо нажать + Добавить сопоставление. В появившемся поле «Группы» вводить наименование группы, в которой состоит пользователь. А в выпадающем списке «Роль» выбрать роль из системы NTechnology SIEM, которая будет сопоставляться с группой на сервере MAD (рис.85).

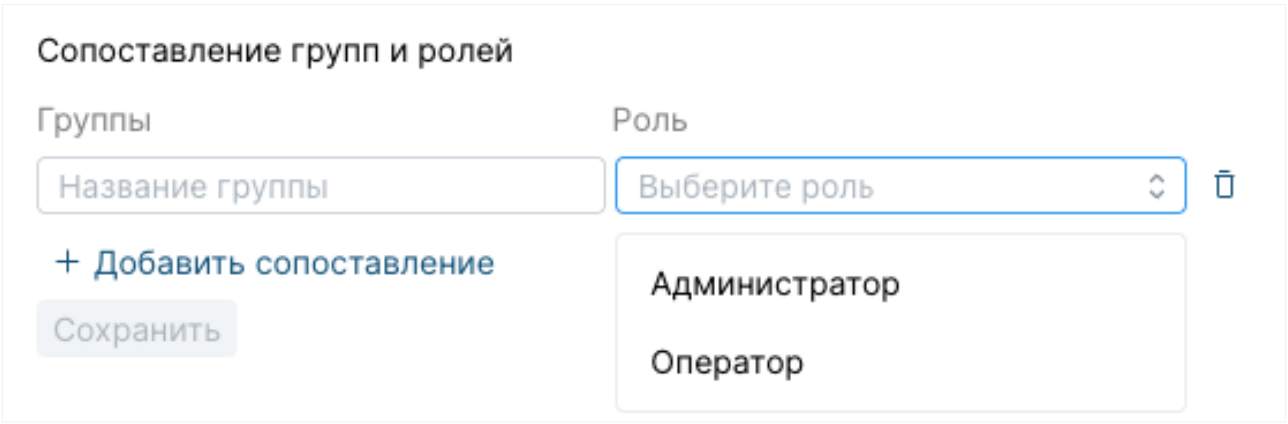


Рисунок 85 – Сопоставление групп и ролей

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

Для удаления пары группа-роль следует воспользоваться элементом 🗑.

Для тестирования подключения к серверу MAD следует воспользоваться кнопкой Тестировать подключение.

3.14.9 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.

3.14.10 Интеграция с SOAR-системой

Для интеграции с SOAR-системой в соответствующем блоке (рис.86) 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» следует ввести название предприятия, в котором установлена система. В поле «Группа» следует присвоить группу, для получаемых значений, например, инциденты ООО «Компания1».

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

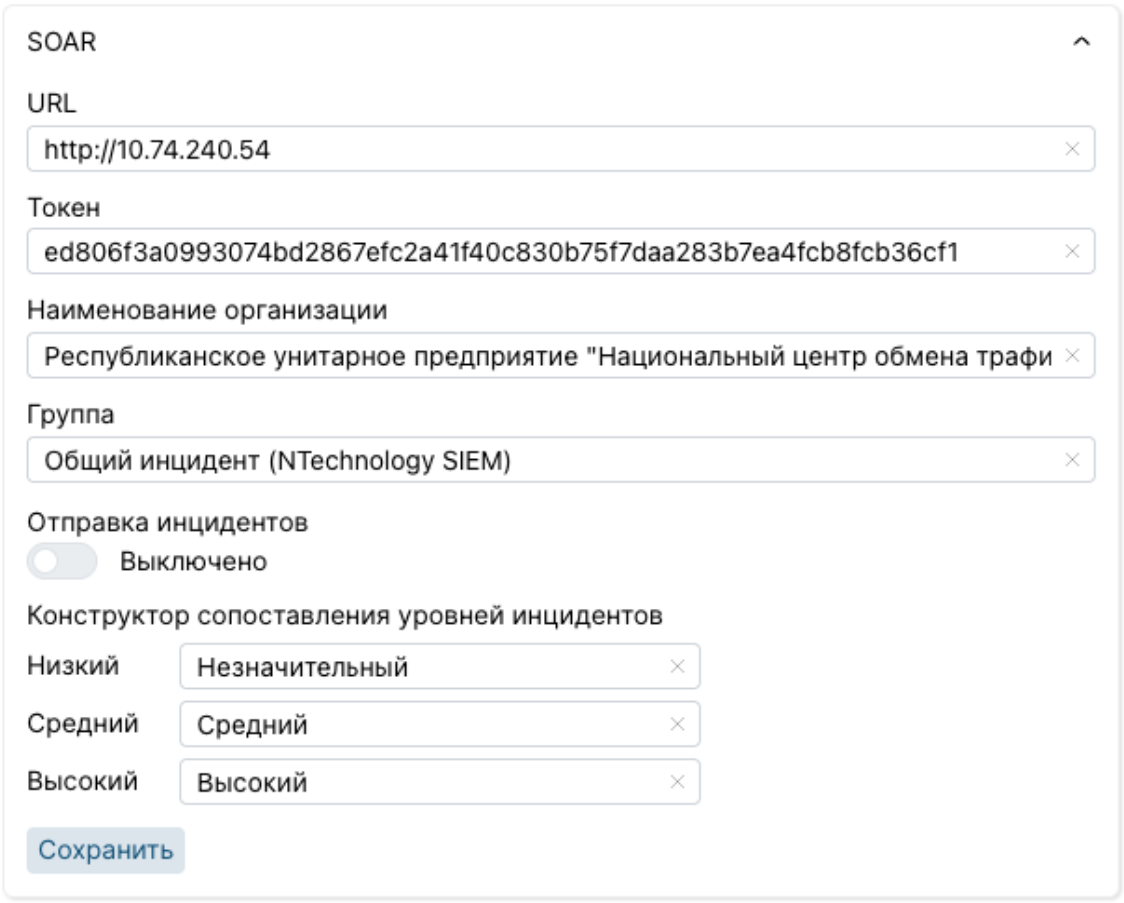


Рисунок 86 – Блок «SOAR»

Для того, чтобы настроить, какие данные передавать, следует использовать переключатели «Отправка инцидентов», для этого необходимо поменять состояние на переключателе на «Включено»:

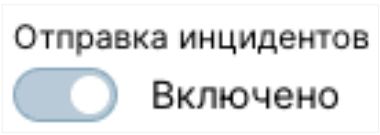


Рисунок 87 – Активный переключатель «Отправка инцидентов»

В системе NT SIEM есть 3 уровня инцидента: низкий, средний и высокий, в то время как 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.

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

3.14.11 Реализация почтовой рассылки

Для реализации почтовой рассылки в соответствующем блоке на странице представлены поля, которые доступны для редактирования (рис. 88).

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»).

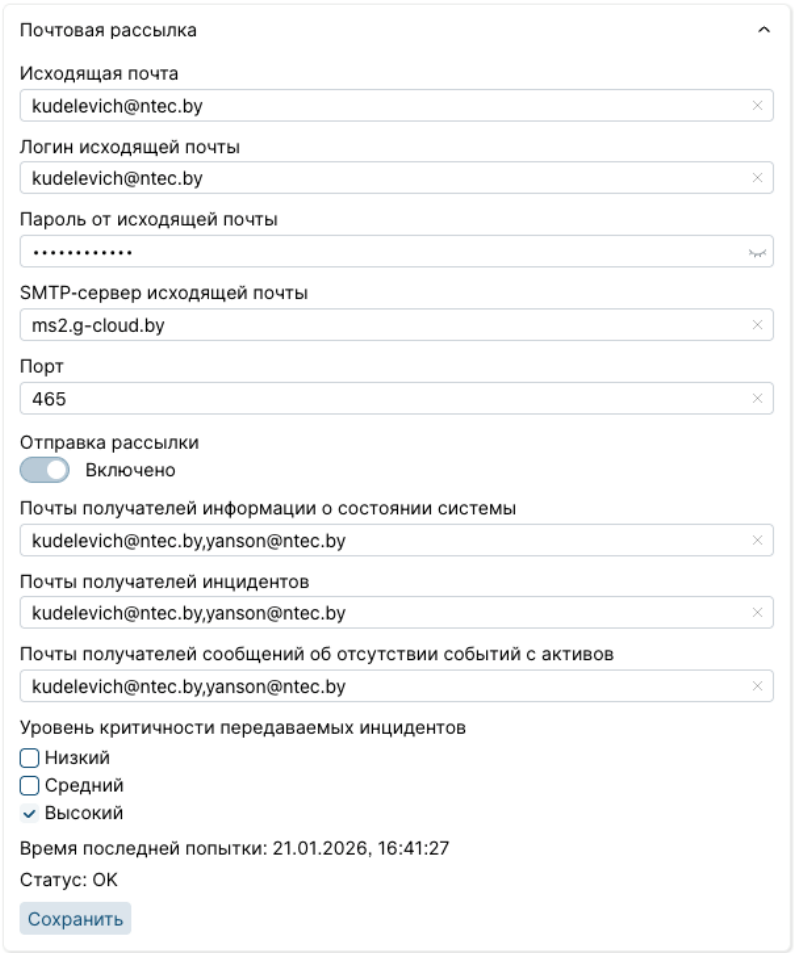


Рисунок 88 – Блок «Почтовая рассылка»

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 и при превышении лимитов свободного пространства на жестком диске,

в поле «Почты получателей инцидентов» – об инцидентах, а в поле «Почты получателей сообщений об отсутствии событий с активов» – уведомление о статусе активов.

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 с почтами получателей перечисление электронных почт получателей происходит через запятую.

Для того, чтобы деактивировать почтовую рассылку необходимо изменить состояние переключателя на «Выключено» (рис.89):

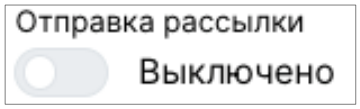


Рисунок 89 – Переключатель «Отправка рассылки»

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 90, являются обязательными для заполнения.

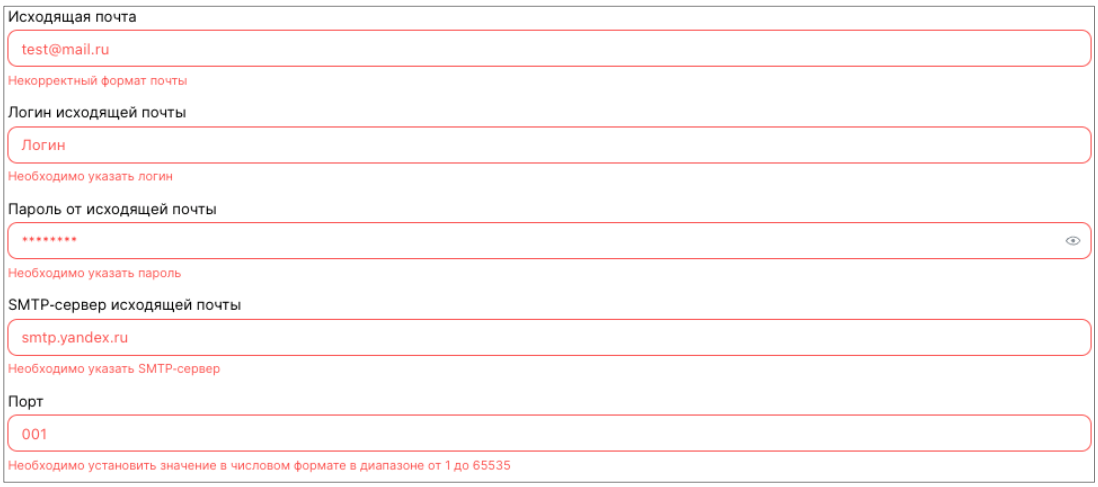


Рисунок 90 – Часть блока «Почтовая рассылка»

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

3.14.12 Настройка уведомлений

Для реализации настроек уведомлений в соответствующем блоке на странице представлены поля, доступные для редактирования (рис. 91). В каждое

поле можно внести пороговые значения свободного пространства на жестком диске, при достижении которых будут отправлены системные уведомления.

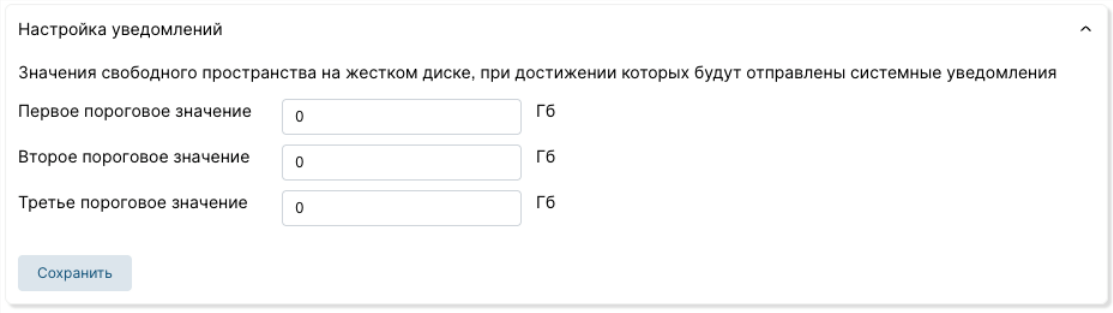


Рисунок 91 – Настройка уведомлений

Приложение А

Таблица 1 – Таблица привилегий ролей в системе NT SIEM

№ п/п	Привилегия	Суперадминистратор	Администратор	Оператор
Пользователи				
1.1	Просмотр пользователей	✓		
1.2	Изменение паролей других пользователей	✓		
1.3	Создание пользователей	✓		
1.4	Редактирование пользователей	✓		
1.5	Удаление пользователей	✓		
1.6	Управление ролями пользователей	✓		
1.7	Просмотр действий пользователей	✓		
1.8	Управление LDAP	✓		
Роли				
2.1	Просмотр ролей	✓		
2.2	Создание ролей	✓		
2.3	Редактирование ролей	✓		
2.4	Удаление ролей	✓		
Инциденты				
3.1	Просмотр инцидентов	✓	✓	✓
3.2	Просмотр истории инцидента	✓	✓	✓
3.3	Управление инцидентами	✓	✓	✓
3.4	Управление ответственными	✓	✓	

№ п/п	Привилегия	Суперадминистратор	Администратор	Оператор
3.5	Удаление инцидентов	✓	✓	✓
3.6	Управление событиями, связанными с инцидентами	✓	✓	✓
3.7	Просмотр комментариев	✓	✓	✓
3.8	Добавление комментариев	✓	✓	✓
3.9	Изменение комментариев	✓	✓	
3.10	Удаление комментариев	✓	✓	
	События			
4.1	Просмотр событий	✓	✓	✓
4.2	Скачивание событий	✓	✓	
4.3	Просмотр списков запросов	✓	✓	✓
4.4	Работа со списками запросов	✓	✓	✓
4.5	Скачивание списков запросов	✓	✓	
4.6	Возможность делиться списками	✓	✓	
	Активы			
5.1	Просмотр активов	✓	✓	✓
5.2	Управление активами	✓	✓	
5.3	Удаление активов	✓	✓	
	База правил			
6.1	Просмотр базы правил в системе	✓	✓	
6.2	Просмотр базы правил в драфт зоне	✓	✓	

№ п/п	Привилегия	Суперадминистратор	Администратор	Оператор
6.3	Управление базой правил в драфт зоне	✓	✓	
6.4	Удаление элемента базы правил в драфт зоне	✓	✓	
6.5	Перезагрузка менеджера	✓	✓	
6.6	Импорт/экспорт Базы Знаний	✓	✓	
6.7	Управление состоянием правил в системе	✓	✓	
6.8	Проверка правил	✓	✓	
Отчеты				
7.1	Выгрузка отчета	✓	✓	✓
7.2	Настроить выгрузку отчетов по расписанию	✓	✓	
Панель мониторинга				
8.1	Управление пользовательскими дашбордами	✓	✓	✓
Лицензирование				
9.1	Управление лицензией	✓		
Настройки системы				
10.1	Управление настройками SOAR	✓		
10.2	Управление настройками почты	✓		
10.3	Управление настройками лимитов дискового пространства	✓		
Интеграции				
11.1	Просмотр интеграций	✓		

№ п/п	Привилегия	Суперадминистратор	Администратор	Оператор
11.2	Создание интеграций	✓		
11.3	Редактирование интеграций	✓		
11.4	Удаление интеграций	✓		