|  |
| --- |
|  |
| U-SIEM |
| Руководство пользователя |

**АННОТАЦИЯ**

Настоящий документ представляет собой руководство оператора системы анализа и визуализации рисков в управленческих системах (далее U-SIEM).

Руководство описывает порядок действий при работе с системой по созданию, просмотру и редактированию основных средств анализа, визуализации и отчётности, предоставляемых системой.

Перед работой пользователя с U-SIEM рекомендуется внимательно ознакомиться с настоящим руководством**.**

**СОДЕРЖАНИЕ**

[СОКРАЩЕНИЯ И ТЕРМИНЫ 6](#_Toc167203467)

[АВТОРИЗАЦИЯ В СИСТЕМЕ 7](#_Toc167203468)

[ОСНОВНЫЕ ЭЛЕМЕНТЫ КОНСОЛИ 9](#_Toc167203469)

[1. Ресурсы консоли 9](#_Toc167203470)

[2. Кастомизация окон рабочих пространств 10](#_Toc167203471)

[ФУНКЦИИ КОНТЕКСТНОГО МЕНЮ 12](#_Toc167203472)

[ИЗБРАННОЕ 13](#_Toc167203473)

[АКТИВНЫЕ КАНАЛЫ 14](#_Toc167203474)

[1. Основные элементы активного канала 14](#_Toc167203475)

[Радар 14](#_Toc167203476)

[Таблица АК 15](#_Toc167203477)

[2. Создание активного канала 16](#_Toc167203478)

[3. Изменение временного интервала и количества записей 17](#_Toc167203479)

[4. Добавление полей данных 18](#_Toc167203480)

[5. Написание условий 20](#_Toc167203481)

[6. Открытие/запуск активного канала 22](#_Toc167203482)

[7. Редактирование активного канала 24](#_Toc167203483)

[Фильтрация событий 27](#_Toc167203484)

[Группировка событий 29](#_Toc167203485)

[Выгрузка и печать 33](#_Toc167203486)

[8. Локальные настройки активного канала 33](#_Toc167203487)

[9. Глобальные настройки активного канала 33](#_Toc167203488)

[АКТИВНЫЕ СПИСКИ 35](#_Toc167203489)

[1. Создание активного списка 35](#_Toc167203490)

[2. Наполнение активного списка 38](#_Toc167203491)

[3. Управление активным списком 41](#_Toc167203492)

[4. Удаление активного списка 43](#_Toc167203493)

[УВЕДОМЛЕНИЯ 44](#_Toc167203494)

[ШАБЛОНЫ УВЕДОМЛЕНИЙ 45](#_Toc167203495)

[ПРАВИЛА 46](#_Toc167203496)

[1. Создание правил 46](#_Toc167203497)

[Стандартные правила 48](#_Toc167203498)

[Агрегационные правила 58](#_Toc167203499)

[2. Управление правилами 61](#_Toc167203500)

[3. Редактирование правила 62](#_Toc167203501)

[4. Удаление правила 62](#_Toc167203502)

[ФУНКЦИИ ПЕРЕМЕННЫХ 64](#_Toc167203503)

[1. Арифметические функции 64](#_Toc167203504)

[2. Дата и время 73](#_Toc167203505)

[3. Пользовательские функции 78](#_Toc167203506)

[4. Строковые функции 82](#_Toc167203507)

[5. Функции для работы с активными списками 90](#_Toc167203508)

[6. Преобразование типа 91](#_Toc167203509)

[ПРАВИЛА ОБОГАЩЕНИЯ 94](#_Toc167203510)

[РЕТРОСПЕКТИВНЫЕ ПРАВИЛА 96](#_Toc167203511)

[ФИЛЬТРЫ 100](#_Toc167203512)

[1. Создание фильтра 100](#_Toc167203513)

[2. Изменение фильтра 100](#_Toc167203514)

[3. Удаление фильтра 101](#_Toc167203515)

[4. Создание условий 102](#_Toc167203516)

[5. Сохранение условий 103](#_Toc167203517)

[6. Удаление условий 104](#_Toc167203518)

[7. Создание группы условий 104](#_Toc167203519)

[8. Копирование и вставка условий 104](#_Toc167203520)

[SQL ЗАПРОСЫ 106](#_Toc167203521)

[1. Создание SQL запроса 106](#_Toc167203522)

[2. Изменение SQL запроса 108](#_Toc167203523)

[3. Удаление SQL запроса 109](#_Toc167203524)

[ВИЗУАЛИЗАЦИЯ ДАННЫХ 110](#_Toc167203525)

[1. Создание визуализации 110](#_Toc167203526)

[2. Изменение визуализации 111](#_Toc167203527)

[3. Удаление визуализации 111](#_Toc167203528)

[ДАШБОРДЫ 113](#_Toc167203529)

[1. Создание дашборда 113](#_Toc167203530)

[2. Изменение дашборда 114](#_Toc167203531)

[3. Удаление дашборда 115](#_Toc167203532)

[НАБОРЫ ПОЛЕЙ 116](#_Toc167203533)

[1. Создание набора полей 116](#_Toc167203534)

[2. Изменение набора полей 117](#_Toc167203535)

[3. Удаление набора полей 117](#_Toc167203536)

[КОНТЕКСТНЫЙ ПОИСК 119](#_Toc167203537)

# **СОКРАЩЕНИЯ И ТЕРМИНЫ**

|  |  |
| --- | --- |
| Сокращение/Термины | Расшифровка/Описание |
| АК | Активный канал |
| АС | Активный список |
| БД | База данных |
| ИБ | Информационная безопасность |
| ЛКМ | Левая кнопка мыши |
| ПКМ | Правая кнопка мыши |
| ПМ | Пункт меню |
| Правила | Правила корреляции событий в режиме реального времени |

# **АВТОРИЗАЦИЯ В СИСТЕМЕ**

При первоначальном входе в консоль потребуется сконфигурировать её для дальнейшей работы. Для этого необходимо перейти в окно «Настройки» с помощью кнопки в правом нижнем углу окна авторизации . В открывшемся диалоговом окне необходимо добавить IP адрес менеджера U-SIEM в разделе «Адрес». При необходимости следует настроить Порт, Тип подключения и TLS. (см. Рисунок 1).

Также в данном окне можно сменить язык интерфейса, система поддерживает русский и английский язык.



Рисунок 1. Настройки подключения

Рекомендуется обратиться к администратору U-SIEM для получения данных по конфигурации системы. Для сохранения конфигурации и продолжения аутентификации необходимо нажать кнопку «Вернуться».

В открывшемся диалоговом окне ввести Логин и пароль и нажать на кнопку «Вход» (см. Рисунок 2). При использовании доменной аутентификации, также необходимости выбрать домен.

****

Рисунок 2. Аутентификация в системе

# **ОСНОВНЫЕ ЭЛЕМЕНТЫ КОНСОЛИ**

## **Ресурсы консоли**

Элементы, расположенные в левой части консоли U-SIEM, представляют собой «Меню ресурсов», посредством которого осуществляется выбор и работа с ресурсами.

Основными ресурсами являются:

|  |  |  |
| --- | --- | --- |
| Иконка | Название | Описание |
|  | Избранное | Предназначено для работы с наиболее часто используемыми ресурсами в целях упрощения навигации |
|  | Активные каналы | Предназначены для работы с событиями и инцидентами ИБ. С помощью АК можно производить поиск событий безопасности и расследовать инциденты ИБ |
|  | Дашборды | Предназначены для удобного мониторинга событий и инцидентов ИБ на основе одного или нескольких графиков. Настраиваются для каждого пользователя на основе заранее созданных визуализаций |
|  | Визуализация | Предназначены для визуализации данных |
|  | Уведомления | Предназначены для создания Получателей уведомлений от системы об инцидентах ИБ |
|  | Администрирование | Предназначено для управления пользователями, параметрами консоли, настройками графических элементов (тем), стартовым дашбордом |
|  | Правила | Предназначены для корреляции событий и выявления инцидентов ИБ |
|  | Правила обогащения | Предназначены для обогащения данными событий безопасности до их записи в БД |
|  | Ретроспективные правила | Предназначены для проведения ретроспективного анализа по историческим данным |
|  | Шаблоны | Предназначены для создания типовых шаблонов уведомлений об обнаружении инцидентов ИБ |
|  | Фильтры | Предназначены для разграничения доступа пользователей к ресурсам. Так же могут использоваться в правилах корреляции событий ИБ |
|  | Наборы полей | Предназначены для создания различных наборов полей. |
|  | Активные списки | АС – это справочники, содержащие статическую и динамическую информацию. Предназначены для создания белых и черных списков, на основе которых могут создаваться цепочки срабатывания правил корреляции событий ИБ |
|  | Контекстный поиск | Предназначен для навигации между ресурсами в консоли управления. Позволяет выполнять поиск ресурсов по имени, их id в Системе, ссылкам в иных ресурсах, упоминаниям в условиях фильтрации. |
|  | SQL-запросы | Предназначены для создания SQL запросов, используемых для построения объектов визуализации данных |
|  | Отчеты | Предназначены для подготовки отчетов |
|  | Глобальные переменные | Предназначены для создания универсальных переменных доступных для интеграции в ресурсы консоли |

*При неактивности одного или нескольких из перечисленных ресурсов следует обратиться к администратору U-SIEM.*

## **Кастомизация окон рабочих пространств**

Консоль U-SIEM поддерживает настройку окон под нужды любого специалиста. Окна в рабочем пространстве можно перемещать в любое место и прикреплять к другим. Для изменения расположения окон необходимо зажать строку заголовка и переместить его на желаемое место, используя специальный элемент управления. Синий прямоугольник элемента управления указывает в каком месте расположится и к какому окну прикрепится переносимое окно (см. Рисунок 3). После сохранения ресурса положение окон также сохраниться, для возвращения окно к стандартному виду необходимо нажать на кнопку .

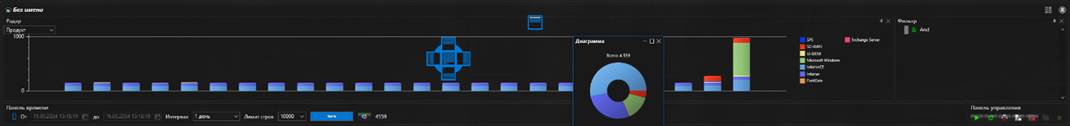


Рисунок 3. Элемент управления для перемещения окон в рабочем пространстве

Кастомизировать рабочие пространства можно у любого ресурса системы. На рисунке ниже представлен пример кастомизации окон в рабочем пространстве активного канала.

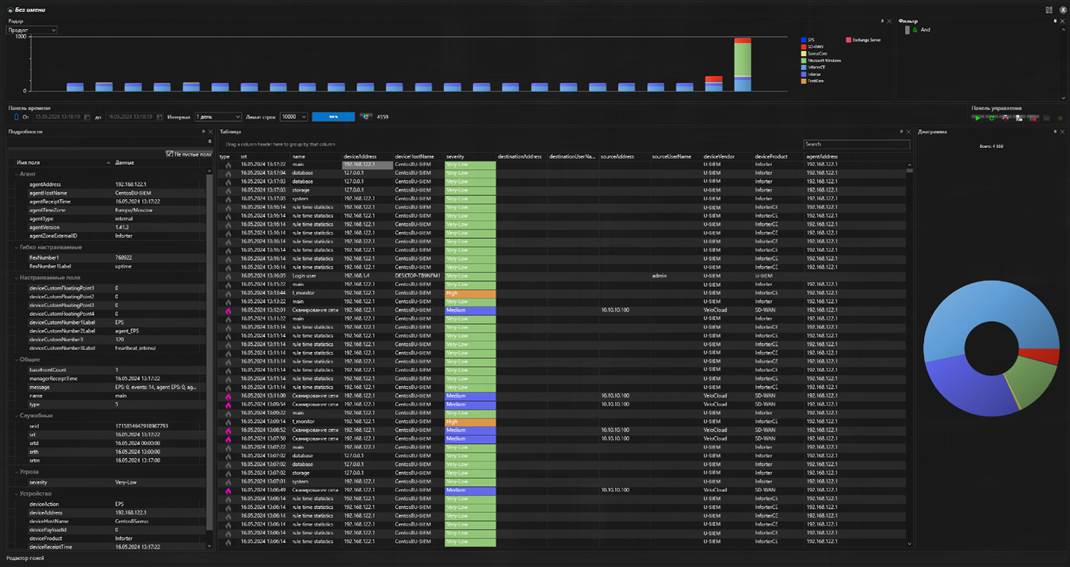


Рисунок 4. Пример изменённого положения окон в АК

# **ФУНКЦИИ КОНТЕКСТНОГО МЕНЮ**

Взаимодействие с ресурсами консоли происходит через контекстное меню появляющееся при нажатии ПКМ.

Основные функции контекстного меню:

|  |  |  |  |
| --- | --- | --- | --- |
| Иконка | Название | Описание | Примечание |
|  | Переименовать | Предназначено для изменения названия ресурса |  |
|  | Сохранить как | Предназначено для сохранения копии ресурса | Доступно также и для выключенных ресурсов |
|  | Создать папку | Предназначено для создания папок |  |
|  | Создать | Предназначено для редактирования ресурсов |  |
|  | Редактировать | Предназначено для редактирования ресурсов | Предназначено для визуализаций и дашбордов |
|  | Открыть | Предназначено для открытия ресурсов |  |
|  | Экспорт | Предназначено для экспорта ресурсов |  |
|  | Импорт | Предназначено для одиночного импорта ресурса |  |
|  | Групповой импорт | Предназначено для группового импорта ресурсов |  |
|  | Удалить | Предназначено для удаления ресурса. | Для полного удаления необходимо выполнить удаление два раза, в первый раз ресурс будет отключен. |
|  | Включить | Предназначено для включения ресурса | Предназначено для правил |
|  | Отключить | Предназначено для отключения ресурса | Предназначено для правил |
|  | Восстановить | Предназначено для восстановления удаленного ресурса |  |
|  | Права доступа | Предназначено для просмотра прав доступа и их редактирования |  |
|  | Зависимость ресурсов | Предназначено для просмотра дерева ресурсов |  |
|  | Добавить в избранное | Предназначено для добавления в Избранное |  |

# **ИЗБРАННОЕ**

Раздел «Избранное» предназначен для работы с наиболее часто используемыми ресурсами в целях упрощения навигации.

Для добавления ресурса в «Избранное» необходимо нажать ПКМ на ресурс и появившемся меню выбрать «Добавить в Избранное» или нажать ЛКМ на кнопку . После чего выбранные ресурсы появятся в списке во вкладке «Избранное».

Для удаления необходимо нажать ЛКМ , после чего ресурс будет удален из «Избранного.

# **АКТИВНЫЕ КАНАЛЫ**

## **Основные элементы активного канала**

АК предназначены для отображения и работы с событиями ИБ, хранящимися в БД, их поиска и анализа, ниже представлен пример АК.



Рисунок 5. Пример Активного канала

Рассмотрим подробнее основные элементы АК.

### Радар

Предназначен для графического отображения событий ИБ в различных разрезах. Можно задать следующие параметры группировки событий в радаре События (по количеству событий), Опасность (по критичности см. Рисунок 6), Производитель (по вендорам см. Рисунок 7), Продукт (по продуктам), Тип (по типам событий). Для смены типа группировки радара следует в верхнем левом углу выбрать необходимый в выпадающем списке.

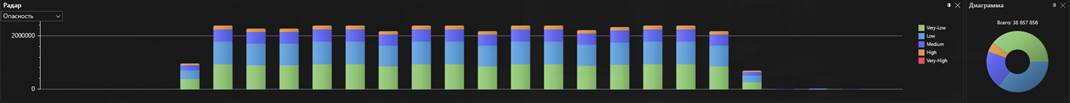


Рисунок 6. Пример Радара по уровню опасности

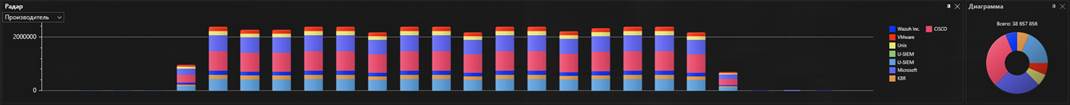


Рисунок 7. Пример Радара по производителям

### Таблица АК

Основной элемент отображения событий — это таблица, в которую выводятся все необходимые поля событий ИБ (см. Рисунок 8).

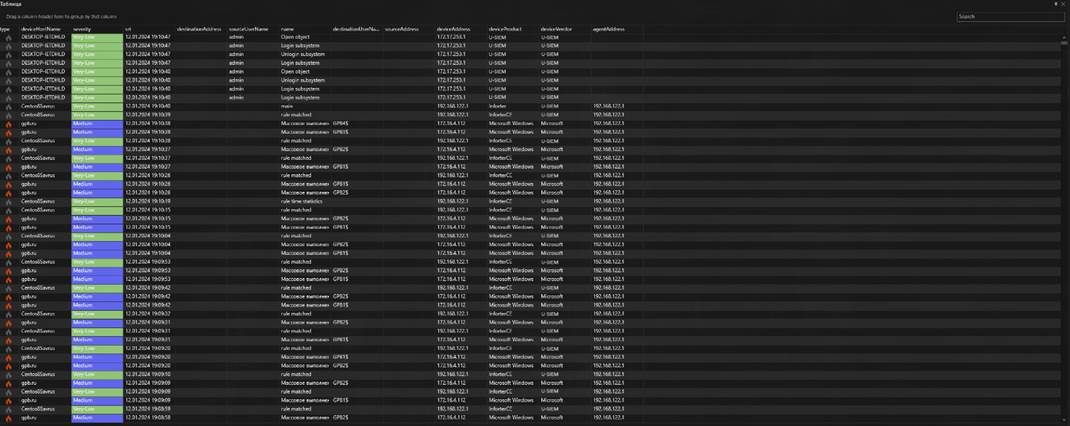


Рисунок 8. Активный канал в табличном представлении

Также возможно отображения событий ИБ в виде различного рода сгруппированных диаграмм и таблиц (см. Рисунок 9) для этого необходимо нажать на кнопку , для отмены кнопку – .

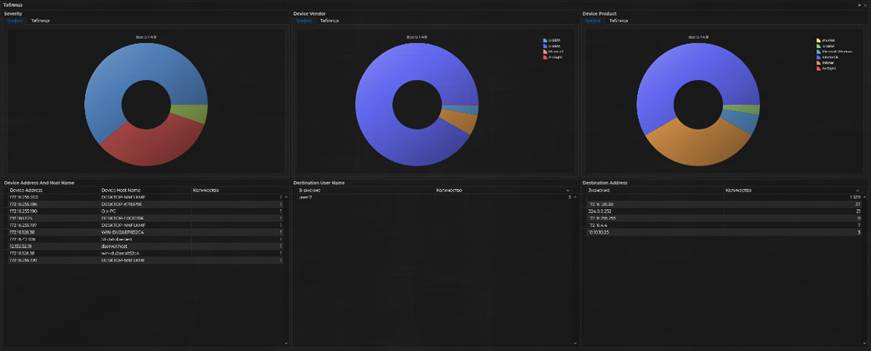


Рисунок 9. Активный канал в виде диаграмм

## **Создание активного канала**

Для создания АК необходимо в меню ресурсов перейти на вкладку «Активные каналы» выбрать необходимую папку, в которой будет новый АК или создать новую папку и выбрать ПМ «Создать» (см. Рисунок 10).

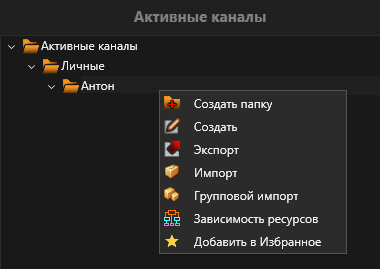


Рисунок 10. Меню Активного канала

Откроется интерфейс управления АК. По умолчанию появится АК со стандартными параметрами, в котором в зависимости от вашей задачи необходимо:

* настроить временной интервал отображения данных и количество записей (см. раздел «Изменение временного интервала и количества записей»);
* добавить/убрать поля данных (см. раздел «Добавление полей данных»);
* добавить условия выборки данных (фильтр) (см. раздел «Написание условий»).

Подробное описание элементов АК представлено в таблице ниже.

Таблица 1. Описание полей окна создания АК

|  |  |  |
| --- | --- | --- |
| Название | Описание | Примечание |
| Название | Имя создаваемого АК | Название канала в дальнейшем можно изменить |
| Начальная дата | Дата, с которой начинается подбор событий | Временной диапазон можно редактировать при работе с АК |
| Конечная дата | Дата, на которой заканчивается подбор событий | Временной диапазон можно редактировать при работе с АК |
| Поля данных | Перечень выводимых на экран полей данных возвращаемых событий | Перечень полей можно редактировать при работе с АК |
| Условие | Перечень условий, для вывода событий | Перечень условий можно редактировать при работе с АК |

В произвольном временном интервале для запуска загрузки данных необходимо нажать кнопку , в непроизвольном загрузка данных будет осуществляться периодически по таймеру (согласно системным настройкам). Для остановки загрузки данных необходимо нажать кнопку . Для обновления АК необходимо нажать кнопку .

Чтобы изменить поля отображаемые в таблице АК следует нажать кнопку «Редактор полей» подробнее описано в разделе «Добавление полей данных».

Для завершения создания АК необходимо щёлкнуть по кнопке , задать имя и нажать на кнопку «OK». После чего АК отобразится в дереве каналов на вкладке «Активные каналы».

При необходимости данные из АК можно вывести на печать для этого следует нажать кнопку .

При необходимости АК можно добавить в «Избранное» для этого следует нажать кнопку .

## **Изменение временного интервала и количества записей**

В АК можно менять временной диапазон и количество записей, для этого используется Панель времени (см. Рисунок 11).



Рисунок 11. Панель времени

Временной диапазон можно выбрать из следующих видов:

* произвольный – автоматически не обновляемый канал, с возможностью произвольного ввода начальной и конечной границы диапазона выборки;
* 30 минут – выборка событий за последние 30 минут (автоматически обновляемый);
* 1 час – выборка событий за последний час (автоматически обновляемый);
* 4 часа– выборка событий за последние 4 часа (автоматически обновляемый);
* 12 часов – выборка событий за последние 12 часов (автоматически обновляемый);
* 1 день – выборка событий за последний день (автоматически обновляемый);
* 2 дня – выборка событий за последние 2 дня (автоматически обновляемый);
* 1 неделя – выборка событий за последнюю неделю (автоматически обновляемый).

В произвольном режиме можно выбрать количество загружаемых данных в АК, для этого в выпадающем списке следует выбрать одно из следующих значений и перезапустить АК:

* 1 000;
* 10 000;
* 25 000;
* 50 000;
* 100 000.

## **Добавление полей данных**

Добавление полей данных в АК осуществляется с помощью редактора полей. Для этого необходимо нажать на кнопку  или в левой нижней части экрана на «Редактор полей» и откроется диалоговое окно редактора полей (см. Рисунок 12). В левой части расположен список всех имеющихся в системе полей данных, а в правой части – отображаемые в данный момент в АК. Для добавления нового поля данных его необходимо перетащить из списка полей в область отображаемых полей. Порядок отображения полей данных в АК зависит от их порядкового номера в редакторе условий, его также можно изменить, перетащив поле данных на необходимую позицию.

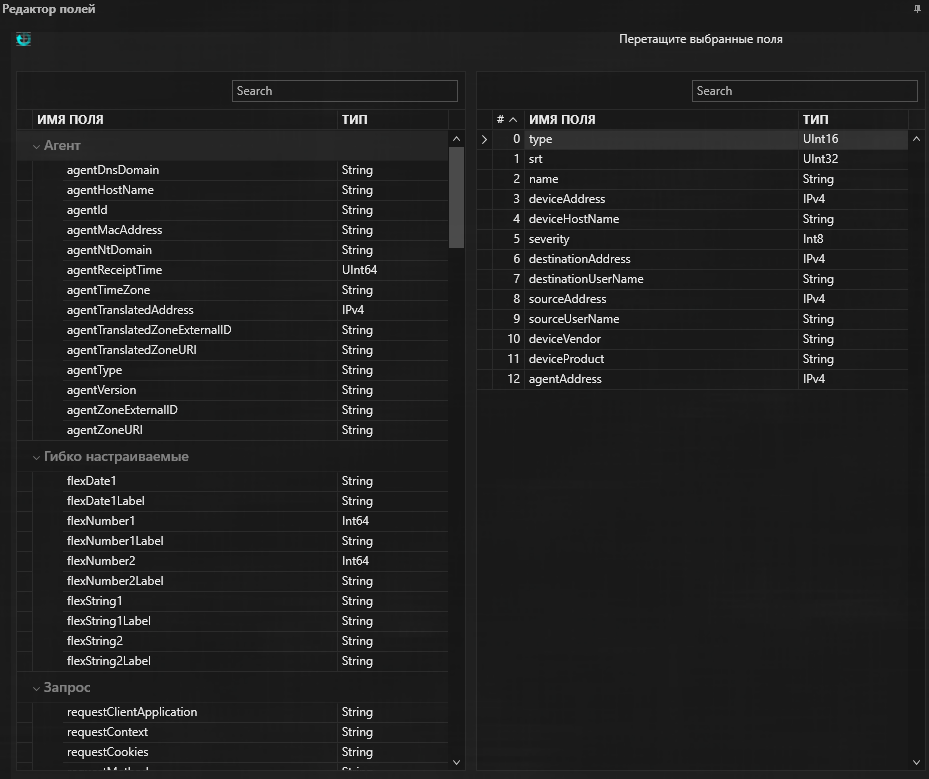


Рисунок 12. Редактор полей

В верхней части редактора запросов расположен элемент поиска полей данных по названию (см. Рисунок 13). Поисковые запросы полей не чувствительны к регистру.

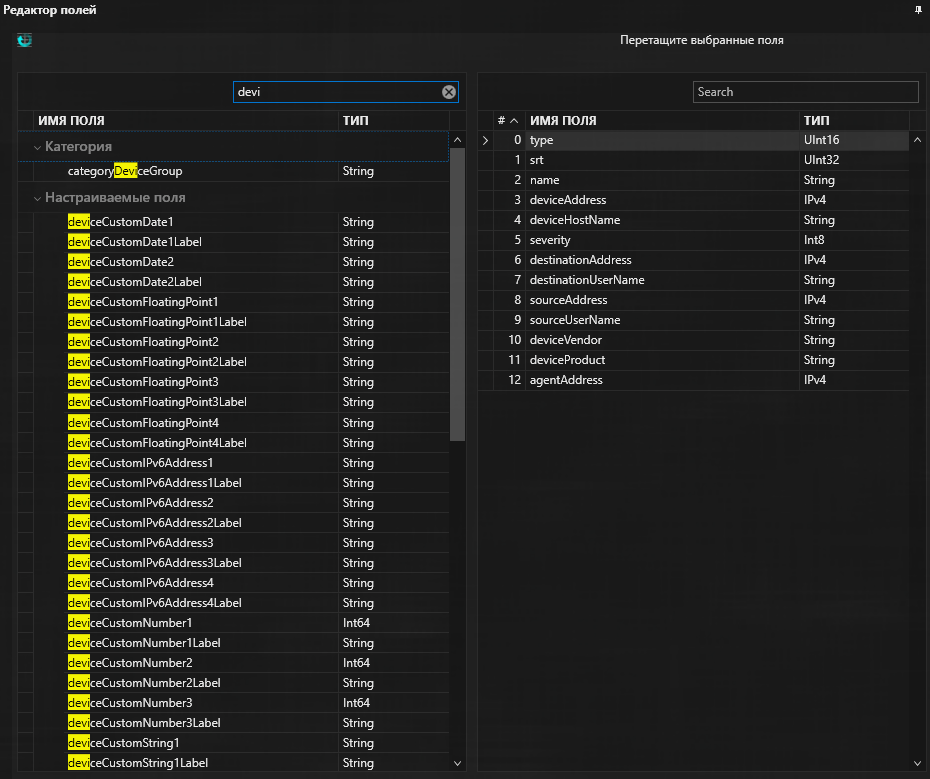


Рисунок 13. Пример поиска

Для сброса настроек редактора полей необходимо нажать на кнопку «По умолчанию» .

## **Написание условий**

При необходимости в запрос можно добавить различные условия (фильтры), для этого используется конструктор условий. Для добавления условия необходимо щёлкнуть ПКМ по условию And, и в контекстном меню пункт «Добавить условие» (см. Рисунок 14), и дважды щёлкнуть ЛКМ по полю условия.

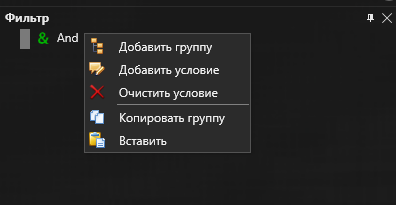


Рисунок 14. Контекстное меню редактора условий

После чего откроется диалоговое окно «Редактирования условий» (см. Рисунок 15) в котором необходимо выбрать поле данных, на которое будет накладываться условие, параметр условия и значение, которое необходимо вывести в АК. В зависимости от поля данных перечень параметров условий, которые можно использовать в условии, будет меняться. После чего нажать на кнопку «OK». Для удаления условия необходимо нажать по нему ПКМ и в контекстном меню выбрать пункт «удалить условие».

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 15. Редактирование условий

При необходимости можно добавить группу условий, для этого в конструкторе запросов необходимо щёлкнуть ПКМ и в контекстном меню выбрать пункт «Добавить группу», после чего сформировать условие. На рисунке ниже представлен пример сформированного условия.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 16. Пример условия

Также необходимо сохранить изменения в канале. Для этого нужно нажать на кнопку «Сохранить» или «Сохранить как.

## **Открытие/запуск активного канала**

Для просмотра АК необходимо перейти на вкладку «Активные каналы», где откроется перечень всех созданных в системе АК. Для открытия необходимого канала следует найти его в списке и дважды щёлкнуть по нему ЛКМ, или же щёлкнуть ПКМ и в выпадающем меню выбрать «Открыть». При необходимости можно переименовать АК, выбрав пункт «Переименовать». Также АК можно удалить для этого в выпадающем меню выбрать «Удалить», после этого АК будет помечен как удалённый. Для его полного удаления в выпадающем меню ещё раз выбираем ПМ «Удалить», после этого АК будет удалён.

Перечень вкладок (см. Рисунок 17) представлен с открытыми АК для быстрого переключения между ними.

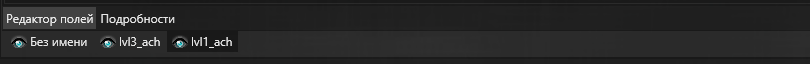


Рисунок 17. Перечень вкладок

Инфографика событий/радар (см. Рисунок 18). При наведении курсора на любую из диаграмм можно просмотреть детали событий, такие как промежуток времени, кол-во событий и их критичность. Также если дважды щёлкнуть ЛКМ по интересующей части диаграммы на радаре, то построится АК за данный промежуток.

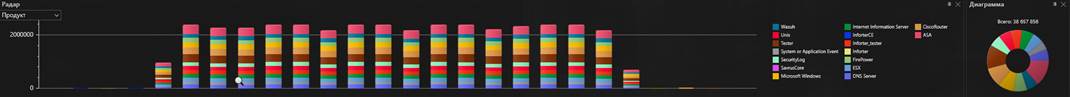


Рисунок 18. Радар

При необходимости быстрого поиска конкретного значения можно использовать окно поиска (см. Рисунок 19). Поиск не чувствителен к регистру.

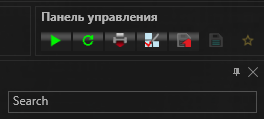


Рисунок 19. Поиск в таблице АК

Также в окно АК канала можно вывести детальное описание события для этого необходимо в левой нижней части окна выбрать вкладку «Подробности», после чего они отобразятся в правой части окна.

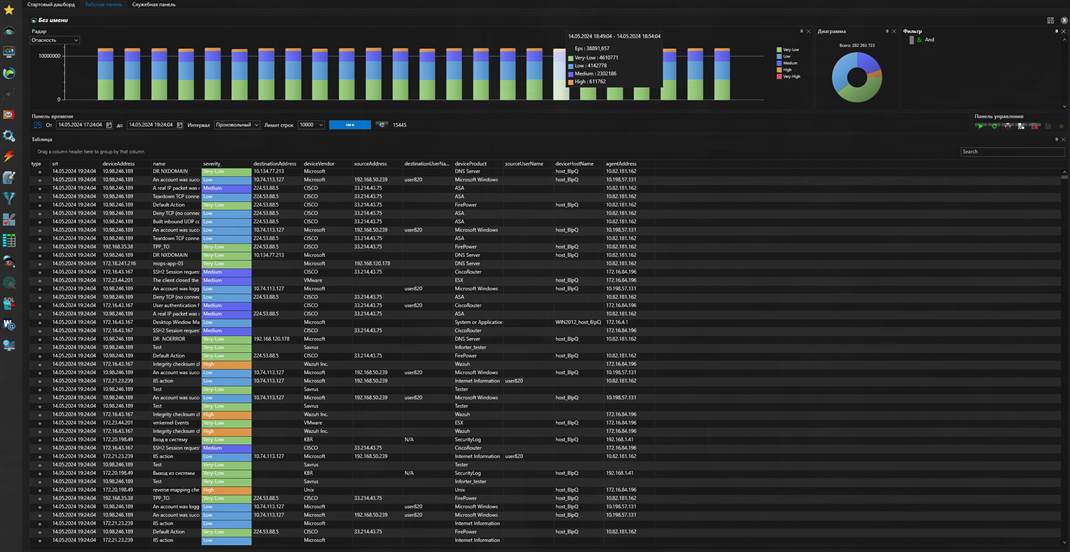


Рисунок 20. Пример активного канала с разделом "Подробности"

Для детального просмотра события необходимо дважды щёлкнуть по событию, представленному в таблице. Поля события объединены по логическим группам о отсортированы по алфавиту (см. Рисунок 21).

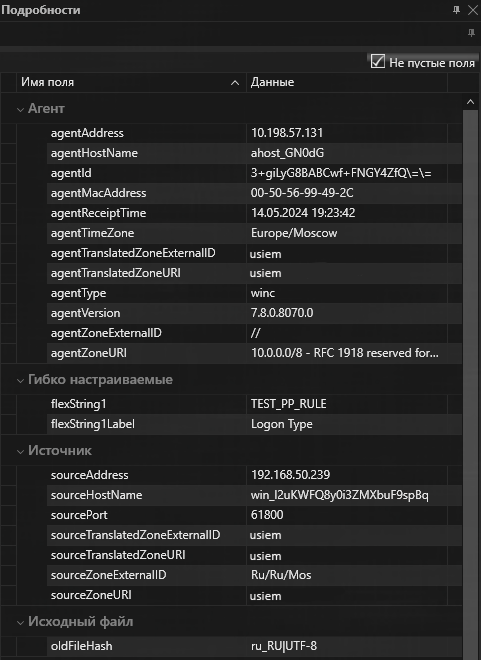


Рисунок 21. Описание события

## **Редактирование активного канала**

Для редактирования АК необходимо открыть нужный канал, подробное описание открытия представлено в разделе «6.Открытие/запуск активного канала» данного руководства. Для изменения или добавления условия используйте конструктор условий (см. «Написание условий»). Если необходимо изменить список полей данных, то используйте кнопку  (см. «Добавление полей данных»).

Порядок столбцов в таблице можно менять в окне АК, для этого необходимо зажать нужный столбец и передвинуть его на то место, где хотите его расположить.

Также в шапке полей АК можно установить фильтр. ЛКМ щёлкнуть по иконке фильтра в названии столбца и установить галочки напротив искомых значений (см. Рисунок 22). Данный фильтр отображается значения в данной колонки уже созданного канала.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 22. Диалоговое окно фильтра

В случае необходимости сохранения изменений следует нажать на кнопку .

Добавлять фильтры, можно с использованием контекстного меню (см. Рисунок 23) в канале, щёлкнув ПКМ по интересующему столбцу события. Выбранное условие автоматически отобразится в конструкторе условий.

Перечень параметров:

* and «имя столбца» = «имя события»;
* and «имя столбца» <> «имя события»;
* or «имя столбца» = «имя события»;
* or «имя столбца» <> «имя события».

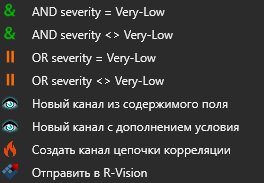


Рисунок 23. Условия/фильтры

Для фильтрации и сортировки событий в АК, необходимо ПКМ щёлкнуть по названию полей и в контекстном меню выбрать необходимую функцию (см. Рисунок 24).

Перечень функций для сортировки/фильтрации событий:

* Sort Ascending – сортировка по алфавиту от A до Z;
* Sort Descending – сортировка по алфавиту от Z до A;
* Clear Sorting – отменяет все применённые условия сортировки;
* Group By This Column – группировка событий по выбранному столбцу;
* Hide Group Panel – скрывает панель сгруппированных столбцов;
* Show Group Panel – диалоговое окно, в котором можно выбрать столбцы для отображения;
* Best Fit – подбор размера колонки по содержимому;
* Best Fit (all columns) (все колонки) - подбор размера всех колонок по содержимому;
* Filter Editor...– конструктор для создания фильтров.

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

Рисунок 24. Фильтрация и сортировка

### Фильтрация событий

Для применения фильтра необходимо щёлкнуть ПКМ по названию необходимого столбца и в контекстном меню выбрать пункт «Filter Editor». Откроется диалоговое окно создания фильтров (см. Рисунок 25). Принцип создания фильтра похож на создание условия, необходимо выбрать логический оператор, а после чего в выпадающем списке выбрать пункт «Добавить условие».

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 25. Диалоговое окно создание фильтра

В появившейся конструкции  необходимо заполнить поля «\_seid» – имя поля, «Equals» – параметр условия, «<enter a value>» – искомое значение поля. Имя поля и параметр условия выбирается из выпадающего меню, а значение можно прописать вручную или, в некоторых случаях, выбрать из списка (см. Рисунок 26).

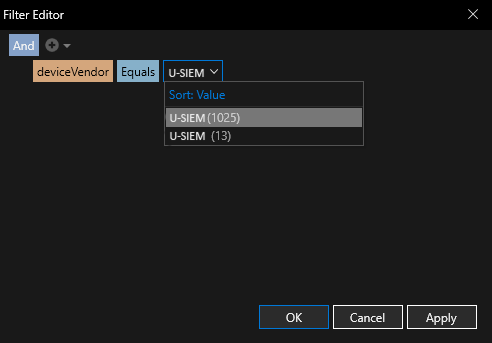


Рисунок 26. Выбор значения из предложенных вариантов

Пример: колонка deviceVendor содержит значение. И на выбор то, что уже есть в колонке открывается при наведении на стрелочку рядом с полем. Либо, значение можно внести вручную. Для добавления ещё одного условия необходимо нажать на кнопку , а для удаления – кнопку .

Если необходимо добавить условие с другим оператором, следует открыть выпадающее меню и выбрать ПМ «Add Group» (см. Рисунок 27) и в новой группе сменить оператора.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 27. Выпадающий список

После добавления всех условий необходимо нажать на кнопку «Apply».

Для отмены фильтрации нажать на кнопку «Cansel», а для закрытия окна создания фильтров нажать кнопку «OK».

### Группировка событий

Группировать события в системе можно 2-мя способами:

* методом drag&drop;
* с помощью контекстного меню столбца.

Для группировки полей с помощью контекстного меню столбца, в АК следует нажать ПКМ по нужной колонке и в контекстном меню выбрать пункт «Group By This Column» (см. Рисунок 28). Если необходимо группировать события внутри уже сгруппированных событий, следует повторить процедуру и события перейдут на следующий уровень группировки.

Изображение выглядит как текст, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 28. Контекстное меню группировки

Для отмены группировки, в поле группировки щёлкнуть ПКМ в пустой части поля, рядом с названием группировки и в контекстном меню выбрать пункт «Clear Grouping».

Для группировки полей методом drag&drop, в АК следует перетянуть название столбца, по которому будет производиться группировка, в панель группировки. Если необходимо группировать события внутри уже сгруппированных событий, то следует перетащить необходимый столбец в панель группировки.

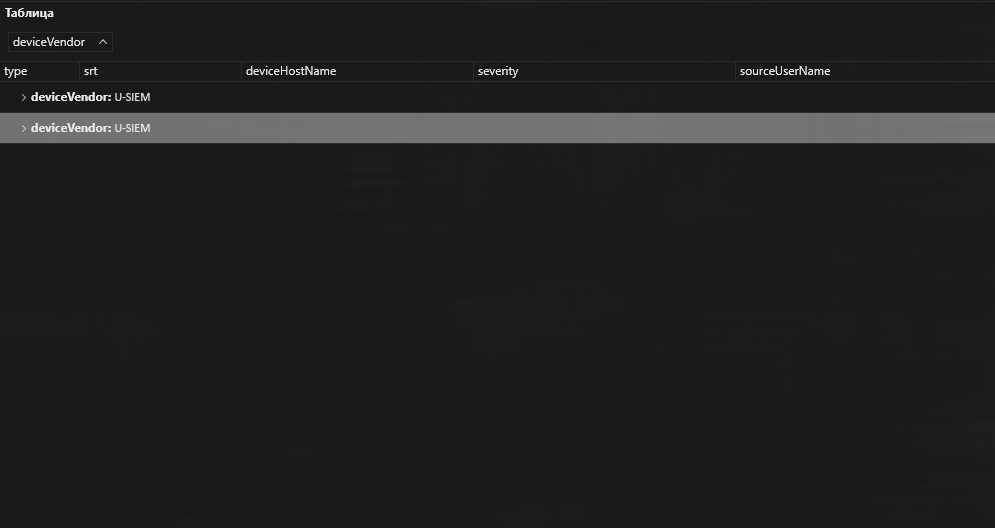


Рисунок 29. Группировка событий

Чтобы снять группировку со столбца, следует нажать ПКМ по нему в панели группировки и в контекстном меню выбрать пункт «Ungroup». Для снятия группировки со всех столбцов необходимо нажать ПКМ по панели группировки и в контекстном меню выбрать пункт «Clear Grouping», или просто перетянуть необходимый столбец обратно в область таблицы АК. Пункты меню «Full Collapse» и «Full Expandе» предназначены для развёртывания и скрытия всех событий, во всех блоках группировки соответственно. При нажатии на имя столбца в панели группировки происходит сортировка группировки по алфавиту от A до Z, а при повторном нажатие сортировка от Z до A.

«Show Column Chooser» позволяет включать и выключать отображение столбцов в АК.

«Best fit» автоматически подбирает размер столбца.

При необходимости вывести подсчёт количества сгруппированных событий, следует нажать ПКМ по любому столбцу в панели группировки и в контекстном меню выбрать пункт «Group Summary Editor...» (см. Рисунок 30).

Изображение выглядит как текст, снимок экрана, программное обеспечение, Шрифт

Автоматически созданное описание

Рисунок 30. Контекстное меню элемента панели группировки

После чего откроется окно «Group Summaries», в котором необходимо поставить галочку у поля «Show row count» и нажать кнопку «OK» (см. Рисунок 31).

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 31. Окно редактора группировки

Пример группировки с подсчётом количества событий представлен на рисунке ниже.



Рисунок 32. Вид группировки с подсчётом количества событий

Также с помощью редактора группировки на вкладке «Элементы» по каждому столбцу можно вывести следующие значения:

* Max;
* Min;
* Average;
* Sum.

На вкладке «Order» каждому значению группировки можно изменить формат числа и присвоить префикс и/или постфикс (см. Рисунок 33).

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Автоматически созданное описание

Рисунок 33. Редактор группировки

### Выгрузка и печать

Для печати или выгрузки во внешний файл данных АК следует нажать на кнопку  и выбрать необходимые параметры печати, также можно выгрузить отчёт по сгруппированным столбцам.

Сохранение внесённых изменений осуществляется нажатием на кнопку «Сохранить» или «Сохранить как». *Если изменения не были сохранены, то после запуска АК они удалятся.*

## **Локальные настройки активного канала**

Для редактирования локальных настроек активного канала необходимо перейти на вкладку «Администрирование» и выбрать кнопку «Параметры программы».

Для внесения изменений необходимо нажать на кнопку . В данном окне есть возможность изменять настройки АК (см. Рисунок 34). После внесения изменений в настройки АК необходимо нажать на кнопку .

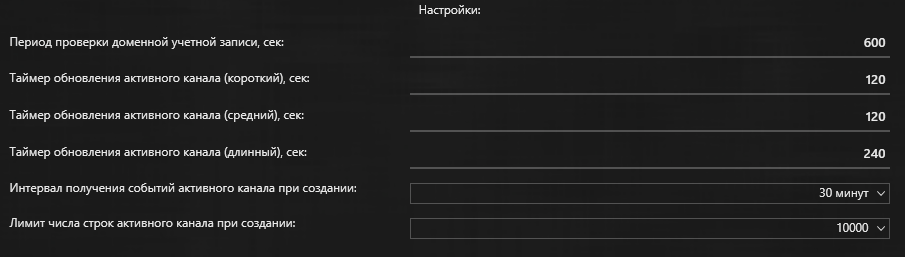


Рисунок 34. Локальные настройки

## **Глобальные настройки активного канала**

Для редактирования глобальных настроек активного канала необходимо перейти на вкладку «Администрирование» и выбрать кнопку «Параметры сервера».

Для внесения изменений необходимо нажать на кнопку . В данном окне есть возможность изменять настройки АК (см. Рисунок 35). После внесения изменений в настройки АК необходимо нажать на кнопку .

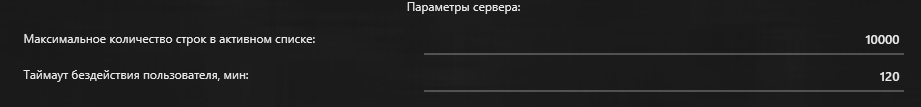


Рисунок 35. Глобальные настройки

# **АКТИВНЫЕ СПИСКИ**

## **Создание активного списка**

Для создания нового активного списка необходимо перейти на вкладку «Активные списки». Далее, нажав ПКМ на папку, выбрать кнопку «Создать» (см. Рисунок 36).

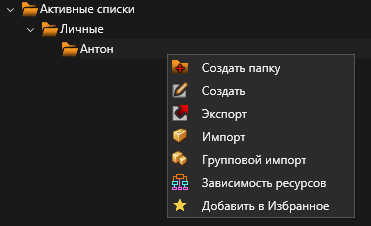


Рисунок 36. Дерево ресурсов АС

Далее, необходимо ввести параметры активного списка (см. Рисунок 37) в соответствии с таблицей 1 и создать его структуру.

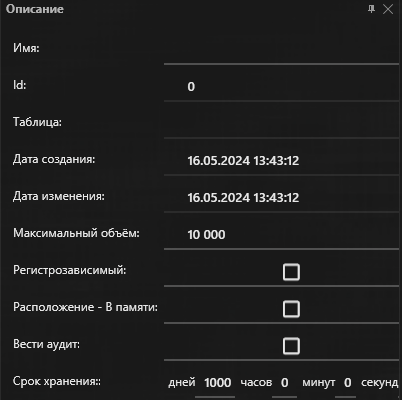


Рисунок 37. Параметры АС

Параметры активного списка указаны в таблице Описание полей окна создания АК

Таблица 2. Параметры активного списка

|  |  |  |  |
| --- | --- | --- | --- |
| № | Наименование | Описание | Примечание |
| 1. | Имя | Наименование Активного списка | Рекомендуется использовать уникальное наименование |
| 2. | Id | Идентификатор ресурса | Устанавливается автоматически |
| 3. | Таблица | Таблица хранения данных | Устанавливается автоматически |
| 4. | Дата создания | Дата создания | Устанавливается автоматически |
| 5. | Дата изменения | Дата изменения | Устанавливается автоматически |
| 6. | Максимальный объем | Максимальный объем строк, хранимых в активном списке | При превышении значения начинается перезапись |
| 7. | Регистрозависимый | Зависимость от регистра | Опционально |
| 8. | Расположение – В памяти | Размещение АК в оперативной памяти | Опционально |
| 9. | Вести аудит | Ведение аудита АК | Опционально |
| 10. | Срок хранения (сек) | Время хранения данных до ротации | По окончанию периода данные стираются |

Для создания структуры активного списка необходимо в разделе «Создание» нажать ПКМ по свободному месту и выбрать «Добавить строку» (см. Рисунок 38).

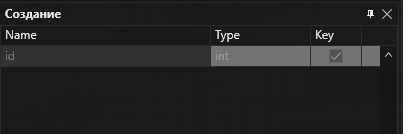


Рисунок 38. Окно добавления столбцов в активный список

В появившейся строке необходимо заполнить имя, которое будет присвоено столбцу активного списка, и тип данных, который будет в нем храниться, а также при необходимости установить галочку ключевого поля (см. Рисунок 39).

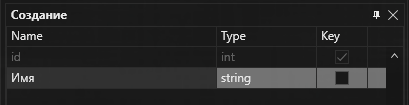


Рисунок 39. Настройка строки активного списка

Для удаления столбца из активного списка необходимо нажать ПКМ по созданному столбцу и нажать «Удалить» (см. Рисунок 40).

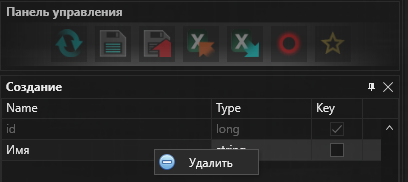


Рисунок 40. Удаление столбца

Для сохранения изменений необходимо нажать на кнопку «Сохранить активный список» .

В меню «Управление таблицей» располагаются кнопки взаимодействия с активными списком.

После добавления структуры активного списка следует добавить в него информацию, это можно сделать в ручном режиме или загрузить данные из Excel.

Строки можно заполнять вручную, для этого следует в необходимом активном списке нажать кнопку «Добавить строку» (см. Рисунок 41).

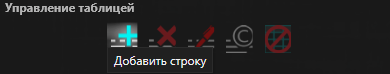


Рисунок 41. Редактирование активного списка

В открывшемся окне следует заполнить столбец «Value» необходимыми значениями. После заполнения активного списка данными необходимо нажать кнопку «OK» (см. Рисунок 42).

Изображение выглядит как снимок экрана, текст, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 42. Окно изменения строки

## **Наполнение активного списка**

При нажатии ПКМ на строку в таблице активного списка появляется контекстное меню взаимодействия со строками (см. Рисунок 43).

Изображение выглядит как снимок экрана, программное обеспечение, компьютер, текст

Автоматически созданное описание

Рисунок 43. Меню взаимодействия со строкой

Для удаления строки из активного списка необходимо нажать ПКМ на строку и выбрать пункт меню «Удалить» затем подтвердить удаление (см. Рисунок 44). Или выделить необходимые строки и в разделе «Управление таблицей» нажать «Удалить строку» и после чего подтвердить удаление (см. Рисунок 45).

Изображение выглядит как снимок экрана, текст, Мультимедийное программное обеспечение, программное обеспечение

Автоматически созданное описание

Рисунок 44. Удаление строки

Изображение выглядит как текст, снимок экрана, программное обеспечение, мультимедиа

Автоматически созданное описание

Рисунок 45. Удаление строки

В таблице активного списка имеется возможность производить сортировку и фильтрацию данных. Для добавления фильтра необходимо нажать ПКМ по столбцу и выбрать в контекстном меню «Filter Editor» (см. Рисунок 46).

Изображение выглядит как текст, снимок экрана, программное обеспечение, компьютер

Автоматически созданное описание

Рисунок 46. Добавление фильтра

В появившемся окне выставляем необходимые настройки и наживаем «ОК» (см. Рисунок 47). Подробнее про настройку фильтров описано в разделе «Фильтрация событий».

Изображение выглядит как снимок экрана, текст, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 47. Окно настройки фильтра

Для удаления фильтра необходимо нажать ПКМ по столбцу и выбрать в контекстном меню «Clear Filter» (см. Рисунок 48).

Изображение выглядит как текст, снимок экрана, программное обеспечение, компьютер

Автоматически созданное описание

Рисунок 48. Окно удаления фильтра

Таблица активного списка вмещает на одной странице порядка 1000 строк. Для перемещения между страницами в таблице используются соответствующие кнопки (см. Рисунок 49).

Изображение выглядит как снимок экрана, программное обеспечение, текст, компьютер

Автоматически созданное описание

Рисунок 49. Кнопки переключения страниц

Для сохранения активного списка необходимо нажать на кнопку «Сохранить активный список» .

## **Управление активным списком**

Для управления АЛ следует использовать кнопки, описанные в таблице ниже.

Таблица 3. Элементы управления АЛ

|  |  |  |
| --- | --- | --- |
| Иконка | Наименование | Назначение |
|  | Обновить активный список | Используется для обновления данных в АС |
|  | Сохранить активный список | Используется для сохранения изменений в АС |
|  | Сохранить как | Используется для сохранения в новый АС |
|  | Выгрузить в файл | Используется для выгрузки данных из АС в файл Excel |
|  | Загрузить из файла | Используется для загрузки данных из файла Excel в АС |
|  | Активировать | Используется для мгновенной активации АС. Без активации данной функции активный список начинает работать спустя некоторое время после сохранения |
|  | Добавить в Избранное | Используется для добавления в «Избранное» |

В разделе «Управление таблицей» располагаются кнопки взаимодействия со строками в активном списке. Подробно описано в таблице ниже.

Таблица 4. Кнопки взаимодействия со строками в АС

|  |  |  |
| --- | --- | --- |
| Иконка | Наименование | Назначение |
|  | Добавить строку | Используется для добавления новых строк в АС |
|  | Удалить строку | Используется для удаления выбранных строк в АС |
|  | Редактировать строку | Используется для редактирования значений строк в АС |
|  | Копировать сроку | Используется для копирования строк в АС |
|  | Отчистить таблицу | Используется для мгновенной отчистки таблицы от всех значений |

## **Удаление активного списка**

Для удаления активного списка необходимо перейти на вкладку «Активные списки». Далее, нажав правой кнопкой мыши (ПКМ) на активный список, выбрать кнопку «Удалить» (см. Рисунок 50). После подтверждения удаления активный список будет помечен на удаление. Для полного удаления необходимо нажать «Удалить» повторно и подтвердить удаление.

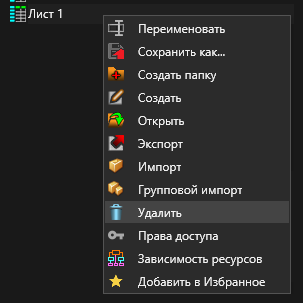


Рисунок 50. Удаление активного списка

# **УВЕДОМЛЕНИЯ**

Для настройки отправки Уведомлений необходимо в меню ресурсов перейти на вкладку «Уведомления» и выбрать необходимую папку, в которой будет располагаться новый Получатель, или создать новую, после чего выбрать ПМ «Создать» (см. Рисунок 51).

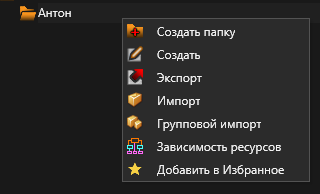


Рисунок 51. Дерево правил

В открывшемся окне создания Получателя (см. Рисунок 52) необходимо указать Имя получателя, способ получения (по почте или cefsyslog), адрес почты или данные для отправки cefsyslog (хост, порт и протокол). Для сохранения пользователя необходимо нажать на кнопку . После сохранения пользователь отобразится в дереве Получателей уведомлений.

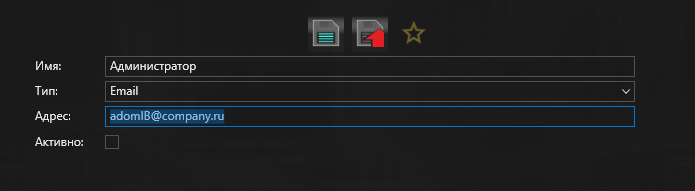


Рисунок 52. Окно создания получателя

# **ШАБЛОНЫ УВЕДОМЛЕНИЙ**

Для создания Шаблонов Уведомлений в меню ресурсов необходимо перейти на вкладку «Шаблоны» и выбрать необходимую папку, в которой будет располагаться новый Шаблон, или создать новую, после чего выбрать ПМ «Создать» (см. Рисунок 53).

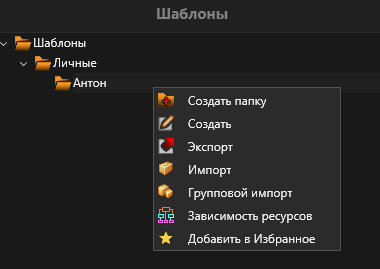


Рисунок 53. Дерево Шаблонов

После чего откроется окно создания Шаблона (см. Рисунок 54). В данном окне в поле «Имя» необходимо задать название Шаблона, в поле «Имя» добавить необходимое описание уведомление в поле «Текст». В описание уведомления в конструкции ‘$’ указываются наименование полей, данные из которых необходимо вывести в уведомлении. После чего сохранить Шаблон, нажатием на кнопку .

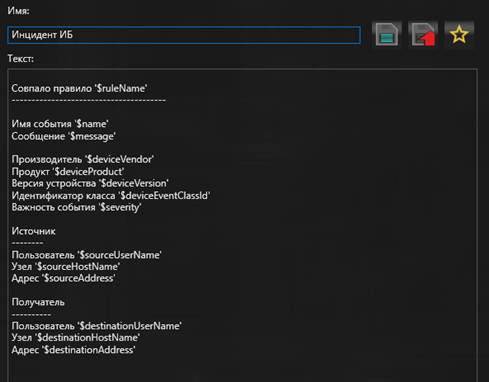


Рисунок 54. Пример Шаблона

# **ПРАВИЛА**

## **Создание правил**

Для создания правил в меню ресурсов необходимо перейти на вкладку «Правила» и выбрать необходимую папку, в которой будет располагаться новое правило, или создать новую, после чего выбрать пункт меню «Создать» (см. Рисунок 55).

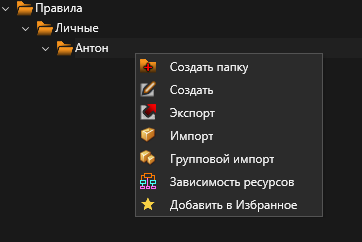


Рисунок 55. Дерево правил

После чего откроется окно конструктора написания правил корреляции (см. Рисунок 56).

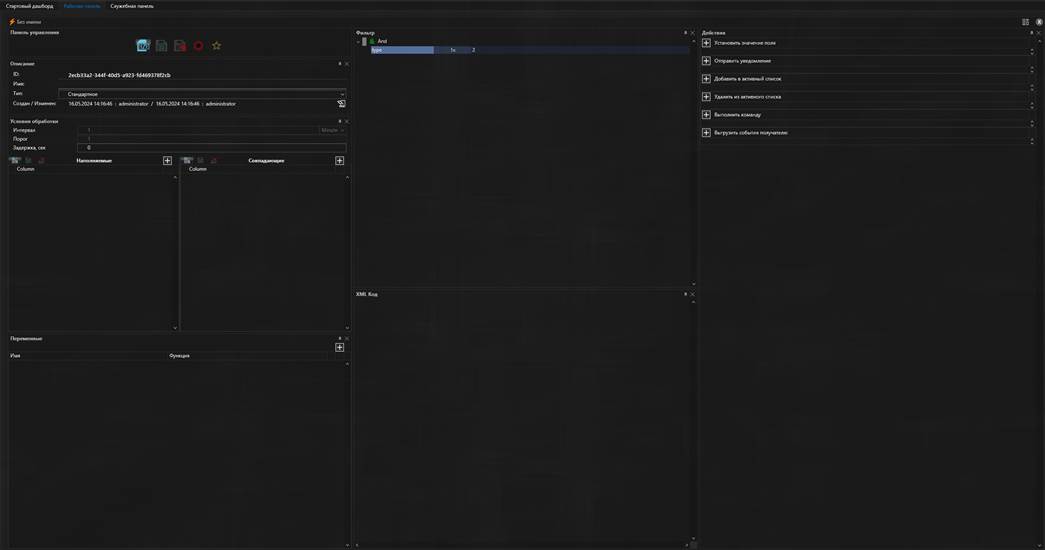


Рисунок 56. Конструктор создания правил

Для создания правил в первую очередь необходимо заполнить основную информацию (см. Рисунок 57), где:

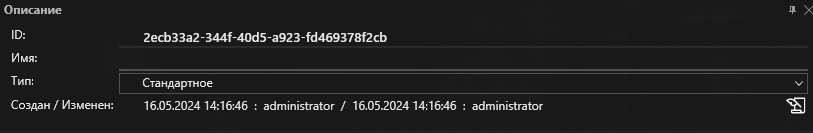


Рисунок 57. Основная информация по Правилу

* ID – уникальный идентификатор Правила присваивается автоматически;
* Имя – наименование правила;
* Тип – Тип правила;
* Дата создания/изменения – Дата и время создания/изменения правила, присваивается автоматически.

Для просмотра истории изменения необходимо нажать на кнопку .

Система поддерживает 2 типа правил корреляции событий в режиме реального времени: Стандартные и Агрегационные.

* Стандартные правила всегда срабатывают на одно событие.
* Агрегационные правила срабатывают от нескольких событий в зависимости от выбранных настроек при создании правила. Данный тип правил сильно увеличивает нагрузку на систему.

### Стандартные правила

#### Условия обработки

Для начала следует настроить условия обработки (см. Рисунок 58). В данном поле «Задержка» указывает период времени, в котором правило не будет реагировать на повторные события, также есть возможность настроить наполняемые и совпадающие поля.

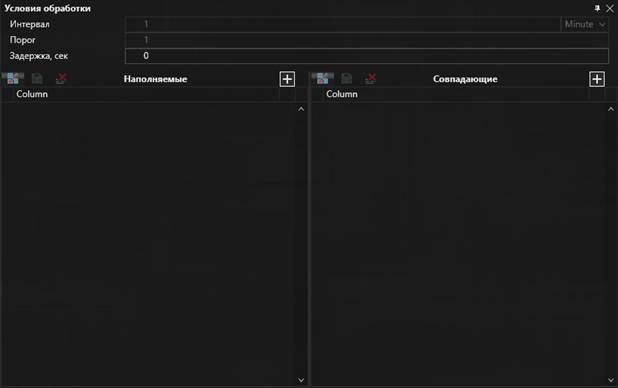


Рисунок 58. Условия обработки

#### Фильтры

После добавления основной информации по Правилу следует добавить условия в разделе «Фильтр» (см. Рисунок 59). По умолчанию Правило создаётся с условием type !=2, это сделано для того, чтобы оно не уходило в рекурсию.

Для добавления условия необходимо щёлкнуть ПКМ по условию And, и в контекстном меню пункт «Добавить условие» (см. Рисунок 59), и дважды щёлкнуть ЛКМ по полю условия.

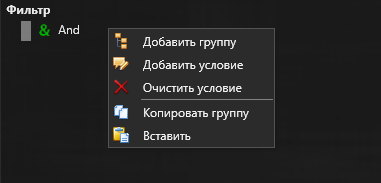


Рисунок 59. Контекстное меню редактора условий

После чего откроется диалоговое окно «Редактирования условий» (см. Рисунок 60), в котором необходимо выбрать поле данных, на которое будет накладываться условие, параметр условия и значение, с которым будет производиться сравнение. В зависимости от поля данных перечень параметров условий, которые можно использовать в условии, будет меняться. После чего нажать на кнопку «OK». Для удаления условия необходимо нажать по нему ПКМ и в контекстном меню выбрать пункт «удалить условие».

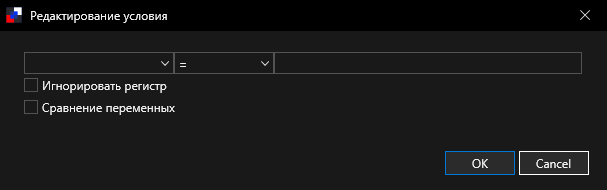


Рисунок 60. Редактирование условий

Перечень параметров условия:

* = – равно;
* != – не равно;
* contains – содержит;
* StartsWith – начинается с;
* EndsWith – оканчивается на;
* is – является (NULL/NOT NULL);
* In Filter – содержится в фильтре;
* > – больше;
* < – меньше;
* >= –больше или равно;
* <= – меньше или равно;
* Matches – поиск совпадения в формате регулярных выражений;
* Like – поиск совпадения в формате SQL;
* In Active List – находится в активном списке.

При необходимости можно добавить группу условий, для этого в конструкторе запросов необходимо щёлкнуть ПКМ и в контекстном меню выбрать пункт «Добавить группу», после чего сформировать условие. На Рисунок представлен пример сформированного условия (см. Рисунок 61).

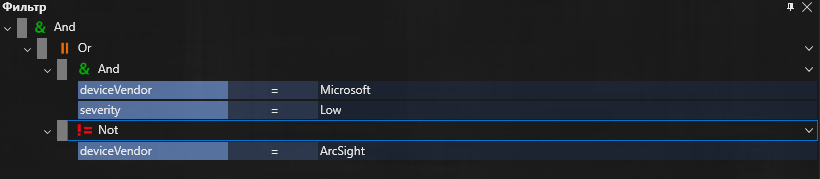


Рисунок 61. Пример условия

#### Отработка и порядок добавления условий

При выборке событий условия отрабатывают в том порядке, в котором они указаны в xml-коде в разделе «Condition».

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

Рисунок 62. Порядок условий в xml-коде

Чтобы не перегружать систему и правило отрабатывало корректно следует придерживаться следующего правила: «сложные условия должны выполняться последними». Рекомендуемых порядок добавления условий от простых к сложным указан на рисунке ниже.

Рисунок 63. Порядок добавления условий.

Рассмотри на примере оптимизацию Условий в правиле. На рисунке ниже представлен пример условия со следующим порядком отработки:

Изображение выглядит как текст, программное обеспечение, Мультимедийное программное обеспечение, мультимедиа

Автоматически созданное описание

Рисунок 64. Некорректный порядок условий

1. Сначала отработает условие «In Active List», которое на потоке событий будет искать совпадения в АС.
2. После чего отработает группа условий по совпадению полей событий «DeviceVendor», «DeviceProduct», «Externalid» заданному значению.
3. И последним отработает условие type != 2, которое отсеивает все корреляционные события.

Данное условие на большом потоке системы может привести к остановке работы системы, т.к. условия требующие большого количества вычислительных ресурсов выполняются первыми.

Оптимизируем Условие, чтобы оно корректно отрабатывало и не нагружало систему. На рисунке ниже представлено оптимизированное условие, которое имеет следующий порядок отработки:

Изображение выглядит как текст, Мультимедийное программное обеспечение, программное обеспечение, снимок экрана

Автоматически созданное описание

Рисунок 65. Корректный порядок условий

1. Первым отрабатывает условие type != 2, которое отсеивает все корреляционные события и уберёт часть событий.
2. После чего отработает группа условий по совпадению полей событий «DeviceVendor», «DeviceProduct», «Externalid» заданному значению, которая также отсеит значительную часть событий.
3. И последним отработает условие «In Active List», которое на оставшихся событиях будет искать совпадения в АС.

Данный порядок условий значительно легче обрабатывается системой и не приведет к остановке работы.

#### Действия

После создания фильтров правилу можно назначить определённые действия, т.е. что Правило должно сделать после срабатывания.

Правилу можно назначить следующие действия:

**Установить значение поля** (см. Рисунок 62) – система во вновь созданном корреляционном событии присвоит выбранным полям назначенные параметры. Кнопка предназначена для добавления нового поля, кнопка  предназначена для удаление добавленного поля.

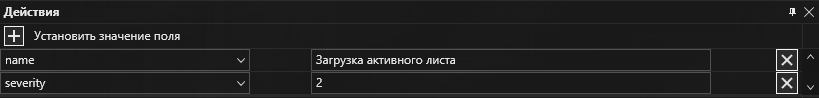


Рисунок 66. Окно установки значений полям

* **Отправить уведомление** (см. Рисунок 63) – система позволяет направлять уведомление ответственным лицам о срабатывании правил. Для этого необходимо в поле «Тема» указать тему уведомления и выбрать «Получателя» и «Шаблон». «Получателя» и «Шаблон» необходимо создать заранее.

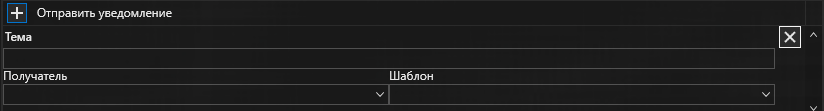


Рисунок 67. Окно настройки отправки уведомлений

* **Добавить в АС /Удалить из АС** – на основе Правил можно обновлять данные в ранее созданных АС. Для этого необходимо выбрать раздел «Добавление в активный список» или «Удаление из активного списка» и в поле «Активный список» выбрать АС, в который будут вноситься изменения. Далее отобразятся поля АС для которых необходимо выбрать значения, которые следует в них добавить после срабатывания Правила (см. Рисунок 64). Данной иконкой обозначаются ключевые поля в активных списках.

Изображение выглядит как снимок экрана, текст

Автоматически созданное описание

Рисунок 68. Окно обновления данных в АС

#### Наполняемые поля

Наполняемые поля – предназначены для обогащения корреляционных событий данными. Для обогащения необходимо в раздел «Наполняемые поля» выбрать поля, которые будут дополнительно выводиться в воссозданном корреляционном событии. (см. Рисунок 65).

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

Рисунок 69. Окно агрегированных полей

#### Переменные

Переменные – при необходимости в Правила можно добавлять различные переменные (см. Рисунок 66).

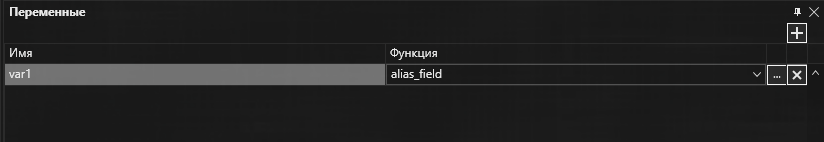


Рисунок 70. Окно добавления Переменных

Полный перечень поддерживаемых функций переменных представлен в таблице ниже.

Таблица 5. Функции переменных

|  |  |  |
| --- | --- | --- |
| № | Наименование функции | Описание |
| Арифметические функции | | |
|  | Absolute | Данная функция возвращает абсолютное значение (числовое значение без учёта знака) аргумента |
|  | Add | Данная функция возвращает результат сложения двух числовых аргументов |
|  | Ceil | Данная функция выполняет округление данного аргумента и возвращает наименьшее целое значение, которое не меньше заданного аргумента. (Округление до ближайшего целого в большую сторону) |
|  | Divide | Данная функция возвращает результат деления двух числовых аргументов. Первый аргумент может принимать любые значения, а второй не может быть равен 0 |
|  | Floor | Данная функция выполняет округление данного аргумента и возвращает наибольшее целое значение, не превышающее числовой аргумент. (Округление до ближайшего целого в меньшую сторону) |
|  | Multiply | Данная функция возвращает произведение двух числовых аргументов |
|  | Round | Данная функция возвращает ближайшее целое число к числовому аргументу (Обычное округление) |
|  | RoundN | Данная функция возвращает результат округления с точностью до указанного знака после запятой |
|  | Subtract | Данная функция возвращает результат вычитания второго числового аргумента из первого числового аргумента |
| Строковые функции | | |
|  | Concat | Данная функция возвращает результат объединения нескольких строковых аргументов. Кол-во аргументов не ограничено. |
|  | Substring | Данная функция возвращает часть строкового аргумента, начиная с позиции (индекс начала – отсчёт начинается с 1), указанной в первом числовом аргументе, и в количестве необходимых символов, указанном во втором числовом аргументе. |
|  | To\_lower | Данная функция возвращает строковый аргумент, преобразованный в нижний регистр |
|  | To\_upper | Данная функция возвращает строковый аргумент, преобразованный в верхний регистр |
|  | Alias\_field | Данная функция создаёт альтернативное имя для указанного поля |
|  | Replace | Данная функция заменяет в выбранном поле первое вхождения символов, указанных во втором аргументе, на символы, указанные в третьем аргументе. |
|  | Replace\_all | Данная функция заменяет в выбранном поле все вхождения символов, указанных во втором аргументе, на символы, указанные в третьем аргументе. |
|  | Split | Данная функция возвращает группу значений на основе заднего разделителя и количества групп. |
| Функции для работы с датой и временем | | |
|  | Get\_hour\_of\_day | Данная функция возвращает целое число от 0 до 23 для представления часа дня на основе выбранной метки времени |
|  | Get\_day\_of\_week | Данная функция возвращает целое число от 0 до 6 (0 — воскресенье) для представления дня недели, на основе выбранной метки времени |
|  | Get\_current\_time | Данная функция текущее время в формате «ДД ММ ГГГГ», «чч:мм:сс», «TIMEZONE» |
|  | Get\_format\_time | Данная функция возвращает текущее время в заданном вами формате. (например, '%H часов %M минут %m.%d.%Y года') |
|  | Time\_Offset | Данная функция возвращает время с заданным смещение в формате Unix-time. |
| Функции для работы с активными списками | | |
|  | Get\_activeslist\_value | Данная функция возвращает значение, связанное с определённым полем указанного активного списка |
| Пользовательские функции | | |
|  | Custom\_condition\_function | Данная функция используется для написания пользовательских функций на основе фильтров |
|  | Regex | Данная функция возвращает значение на основе заданного регулярного выражения |
| 1. M | MultiRegex | Данная функция возвращает группу значений на основе заданного регулярного выражения. |
|  | Constant | Данная функция возвращает константу заданного типа. |
| Преобразование типа | | |
|  | Ip\_to\_int | Данная функция возвращает значение поля формата IP в формате int. |
|  | String\_to\_Float | Данная функция принимает строку в качестве аргумента и возвращает целое число в формате чиста с плавающей точкой. |
|  | String\_to\_Long | Данная функция принимает строку в качестве аргумента и возвращает целое число в формате длинное целое. |
|  | DateTime\_to\_UnixTime | Данная функция принимает строку в качестве аргумента в заданном формате и преобразует её значение Unixtime в формате длинное целое. |

После завершения создания правила необходимо нажать кнопку «Сохранить» .

### Агрегационные правила

#### Условия обработки

Для создания правил Агрегации необходимо выбрать условия обработки (см. Рисунок 67).

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 71. Условия обработки

* Интервал – интервал отслеживания одинаковых событий, необходимых для срабатывания правила.
* Порог – количество событий для срабатывания правила.
* Задержка, сек – период времени, в котором правило не будет реагировать на повторные события.

#### Наполняемые поля

При необходимости можно добавить обогащающие поля и для агрегационного правила.

#### Агрегационные поля

Далее необходимо выбрать поля для агрегации в окнах «Совпадающие» и «Уникальные» (см. Рисунок 68). По этим полям высчитывается хэш.

«Совпадающие» – это поля события, которые имеют одинаковое значение, например поле «Name». «Уникальные» – это поля события, которые содержать отличающиеся, уникальные значения, например поле «ID». На основе данных полей и будет производиться агрегация событий при отработке правила.

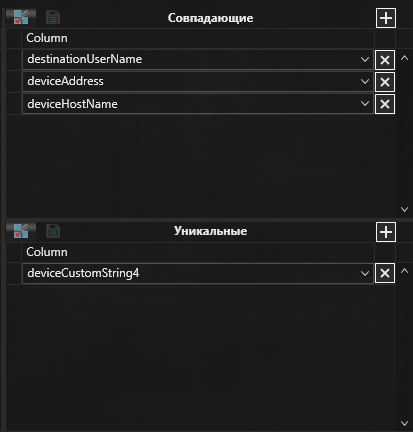


Рисунок 72. Поля агрегирования

#### Фильтры

Аналогичны условиям для стандартных правил.

#### Фильтры для активного канала

Окно «Фильтр для активного канала» заполняется автоматически на основе Фильтра и агрегационных полей.

#### Поля обогащения цепочки

«Поля обогащения цепочки» необходимы для АК и выбираются при создании правила (см. Рисунок 69). При нажатии ПКМ на правило в активном канале и выборе пункта меню «Создать канал цепочки корреляции», консоль создаст цепочку из полей, указанных в правиле.



Рисунок 73. Поля обогащения цепочки

#### In memory list

Также для Агрегационных правил доступен функционал «In memory list». Для того чтобы попасть в «In memory list» необходимо в конфигурационном файле «inforter\_ce/config.xml» установить значение «true «в строке «https enable» и указать необходимый порт. Далее подключиться к нужному IP адресу с добавлением указанного в конфигурационном файле порта, ввести пароль и логин, используемые для входа в консоль U-SIEM. Данный вспомогательный инструмент позволяется отслеживать работу правил и хранит в себе общие данные о системе.

Для просмотра данных о работе агрегационных правил необходимо выбрать вкладку Rules (см. Рисунок 70).



Рисунок 74. Функционал API

Далее необходимо найти нужное правило и нажать на кнопку hash size (см. Рисунок 71)



Рисунок 75. hash size

Далее откроется in memory list - активный лист, (см. Рисунок 72) в котором хранятся значения полей правила корреляции. Данный лист отчищается в указанный при создании агрегационного правила интервал. В случае если сервер будет отключен, то данные листа также будут отчищены. Просмотр in memory list доступен только в представленной API.

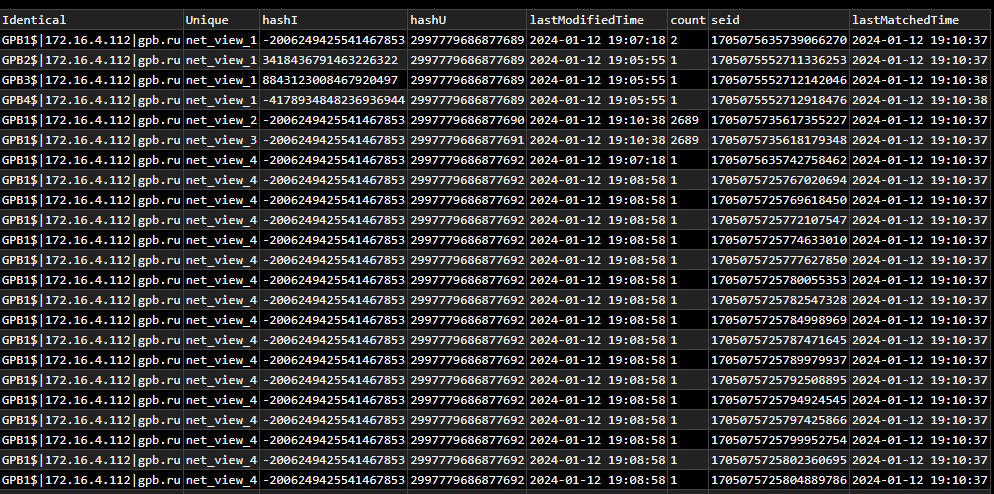


Рисунок 76. in memory list

## **Управление правилами**

В меню «Панель управления» располагаются кнопки взаимодействия с правилом. Подробнее о них описано в таблице ниже

Таблица 6. Кнопки взаимодействия с Правилами

|  |  |  |
| --- | --- | --- |
| Иконка | Наименование | Назначение |
|  | XML Код | Включает отображение XML Кода правила |
|  | Сохранить | Сохраняет правило |
|  | Сохранить как | Сохраняет копию правила |
|  | Включено/Выключено | Включает или выключает выполнение правила.  Красный цвет означает, что правило выключено, синий – включено |
|  | Добавить в Избранное | Позволяет добавлять в список избранного |

## **Редактирование правила**

Для редактирования правил в меню ресурсов необходимо перейти на вкладку «Правила» и двойным нажатием ЛКМ по правилу откроется меню редактирования правила (см. Рисунок 73).



Рисунок 77. Дерево правил

После завершения редактирования правила необходимо нажать кнопку «Сохранить» .

## **Удаление правила**

Для удаления Правил в меню ресурсов необходимо перейти на вкладку «Правила» и выбрать необходимое Правило, после чего выбрать «Удалить» (см. Рисунок 74). После подтверждения удаления правило деактивируется и пометиться как ресурс на удаление. Для полного удаления необходимо нажать «Удалить» повторно и подтвердить удаление.

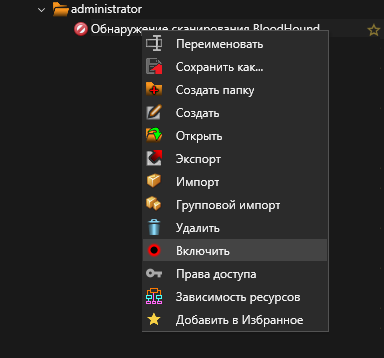


Рисунок 78. Управление правилами

# **ФУНКЦИИ ПЕРЕМЕННЫХ**

## **Арифметические функции**

#### Absolute

Данная функция возвращает абсолютное значение (числовое значение без учёта знака) аргумента. Может принимать на вход только одно значение аргумента.

Для создания переменной с функцией Absolute, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции (см. Рисунок 75). Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 79. Пример функции Absolute

#### Add

Данная функция возвращает результат сложения числовых аргументов.

Для создания переменной с функцией Add, необходимо нажать кнопку . В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 80. Пример функции Add

Далее, необходимо назначить аргументы функции (см. Рисунок 76). Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события и/или константу. Для добавления нескольких аргументов необходимо нажать на кнопку  и добавить либо «Поле» (Поле события), либо «Значение» (Константа). Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

#### Ceil

Данная функция выполняет округление данного аргумента и возвращает наименьшее целое значение, которое не меньше заданного аргумента. (Округление до ближайшего целого в большую сторону).

Для создания переменной с функцией Ceil, необходимо нажать кнопку в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции (см. Рисунок 77). Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

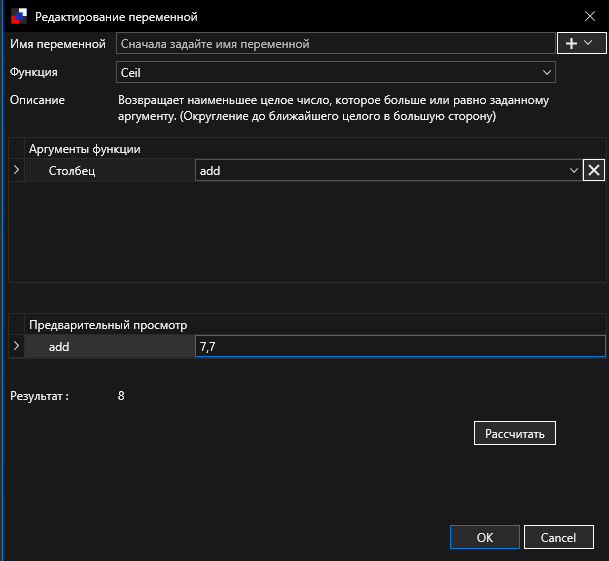


Рисунок 81. Пример функции Celi

#### Divide

Данная функция возвращает результат деления числовых аргументов.

Для создания переменной с функцией Divide, необходимо нажать кнопку . В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

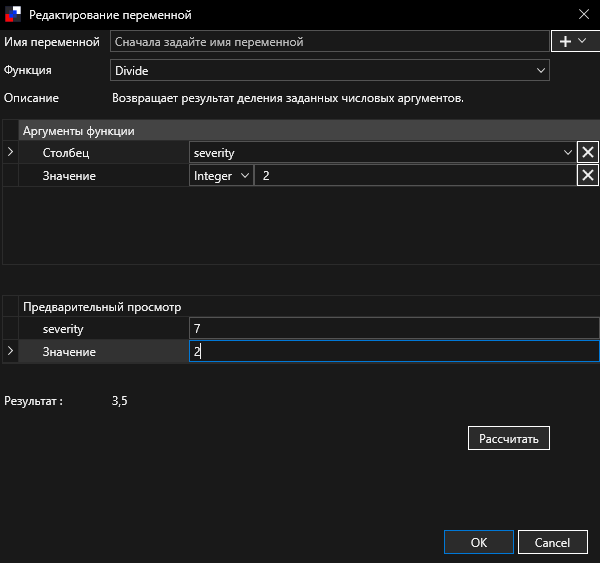


Рисунок 82. Пример функции Divide

Далее, необходимо назначить аргументы функции (см. Рисунок 78). Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события и/или константу. Для добавления нескольких аргументов необходимо нажать на кнопку  и добавить либо «Поле» (Поле события), либо «Значение» (Константа). Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

#### Floor

Данная функция выполняет округление данного аргумента и возвращает наибольшее целое значение, не превышающее числовой аргумент. (Округление до ближайшего целого в меньшую сторону).

Для создания переменной с функцией Floor, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции (см. Рисунок 79). Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 83. Пример функции Floor

#### Multiply

Данная функция возвращает произведение числовых аргументов.

Для создания переменной с функцией Multiply, необходимо нажать кнопку . В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 84. Пример функции Multiply

Далее, необходимо назначить аргументы функции (см. Рисунок 80). Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события и/или константу. Для добавления нескольких аргументов необходимо нажать на кнопку  и добавить либо «Поле» (Поле события), либо «Значение» (Константа). Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

#### Round

Данная функция возвращает ближайшее целое число к числовому аргументу (Обычное округление).

Для создания переменной с функцией Round, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции (см. Рисунок 81). Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 85. Пример функции Round

#### RoundN

Данная функция возвращает результат округления с точностью до указанного знака после запятой.

Для создания переменной с функцией RoundN, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции (см. Рисунок 82). Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события, в строке «Точность округления» ввести константу. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 86. Пример функции RoundN

#### Subtract

Данная функция возвращает результат вычитания числовых аргументов.

Для создания переменной с функцией Subtract, необходимо нажать кнопку . В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

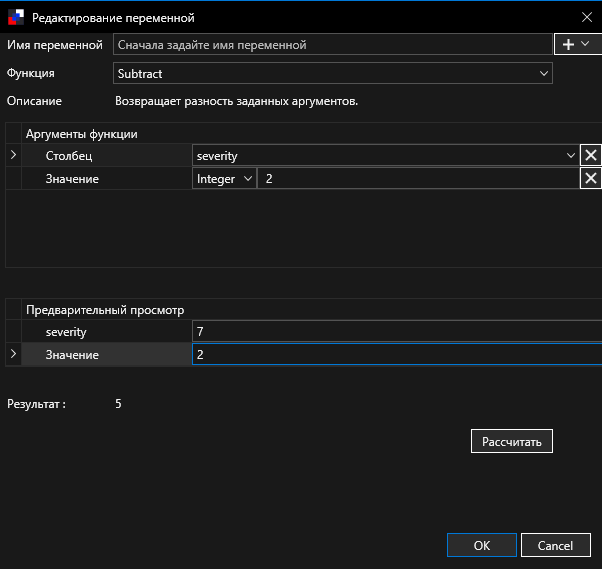


Рисунок 87. Пример функции Subtract

Далее, необходимо назначить аргументы функции (см. Рисунок 83). Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события и/или константу. Для добавления нескольких аргументов необходимо нажать на кнопку  и добавить либо «Поле» (Поле события), либо «Значение» (Константа). Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

## **Дата и время**

#### Get\_current\_time

Данная функция возвращает текущее время в заданном вами формате. (например, '%H часов %M минут %m.%d.%Y года').

Для создания переменной с функцией Get\_current\_time, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию (см. Рисунок 84). Для завершения создания переменной необходимо нажать кнопку ОК.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 88. Пример функции Get\_current\_time

#### Get\_day\_of\_week

Данная функция возвращает целое число от 0 до 6 (0 — воскресенье) для представления дня недели, на основе выбранной метки времени.

Для создания переменной с функцией Get\_day\_of\_week, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции (см. Рисунок 85). Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 89. Пример функции Get\_day\_of\_week

#### Get\_format\_time

Данная функция текущее время в формате «ДД ММ ГГГГ», «чч:мм:сс», «TIMEZONE».

Для создания переменной с функцией Get\_format\_time, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции (см. Рисунок 86). Для этого в строке «Формат» необходимо ввести формат времени. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 90. Пример функции Get\_format\_time

#### Get\_hour\_of\_day

Данная функция возвращает целое число от 0 до 23 для представления часа дня на основе выбранной метки времени.

Для создания переменной с функцией Get\_hour\_of\_day, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции (см. Рисунок 87). Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 91. Пример функции Get\_hour\_of\_day

#### Time\_Offset

Данная функция возвращает время с заданным смещение в формате Unix-time.

Для создания переменной с функцией Time-offset, необходимо нажать кнопку в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции (см. Рисунок 88). Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

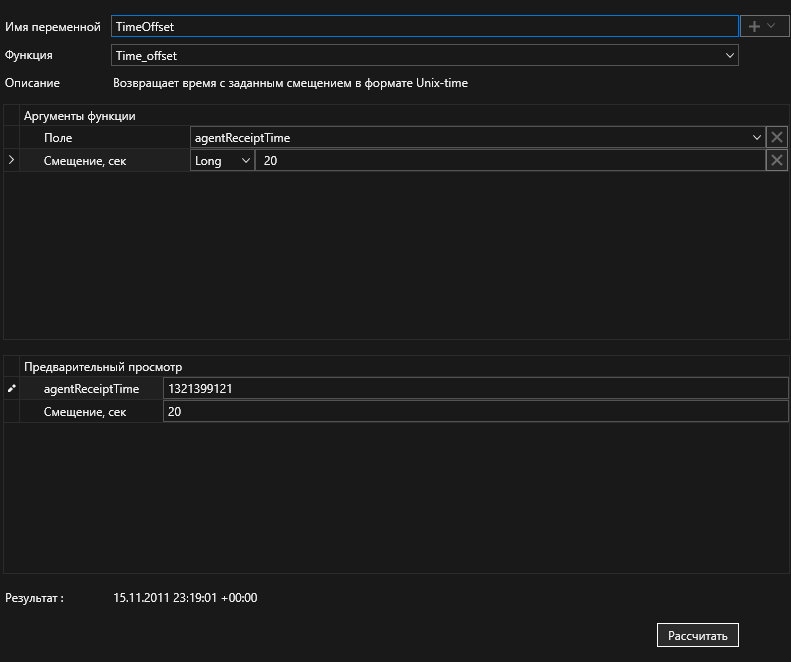


Рисунок 92. Пример функции Time\_offset

## **Пользовательские функции**

#### Constant

Данная функция возвращает константу заданного типа.

Для создания переменной с функцией Constant, необходимо нажать кнопку в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции (см. Рисунок 89). Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

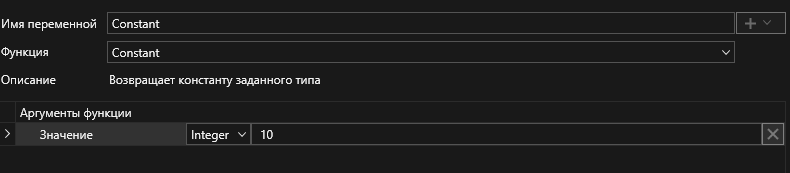


Рисунок 93. Пример функции Constant

#### Custom\_condition\_function

Данная функция используется для написания пользовательских функций на основе фильтров.

Для создания переменной с функцией Custom\_condition\_function, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо добавить условие в окне аргументы функции (см. Рисунок 90). Добавить Значение или Столбец для пунктов ИСТИНА и ЛОЖЬ, ввести значение или выбрать поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 94. Пример функции Custom\_condition\_function

#### MultiRegex

Данная функция возвращает группу значений на основе заданного регулярного выражения.

Для создания переменной с функцией MultiRegex, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции. Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события, в строке Регулярное выражение ввести Regex. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

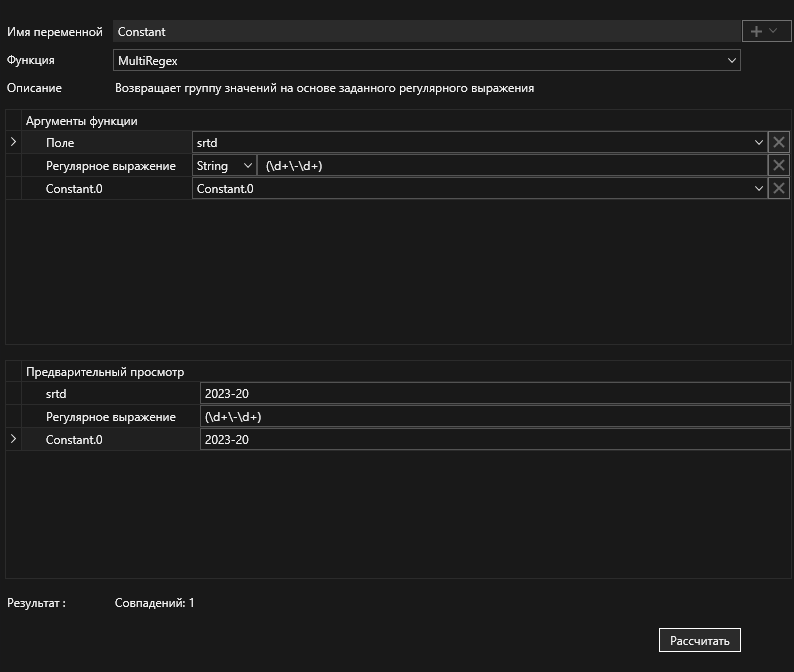


Рисунок 95. Пример функции MultiRegex

#### Regex

Данная функция возвращает значение на основе заданного регулярного выражения.

Для создания переменной с функцией Regex, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции. Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события, в строке Регулярное выражение ввести Regex. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 96. Пример функции Regex

## **Строковые функции**

#### Alias\_field

Данная функция создаёт альтернативное имя для указанного поля.

Для создания переменной с функцией Alias\_field, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции. Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Имя переменной и будет новым именем для указанного поля. Для завершения создания переменной необходимо нажать кнопку ОК.

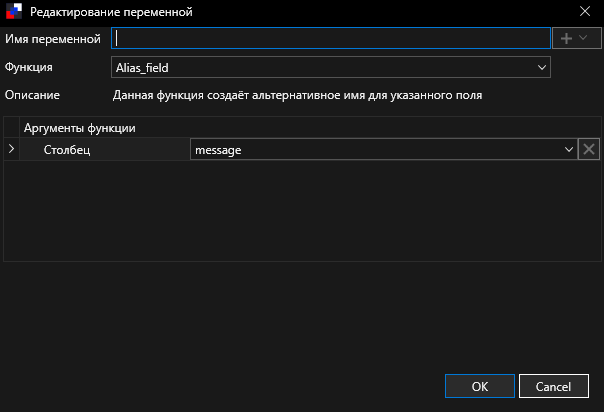


Рисунок 97. Пример функции Alias\_field

#### Concat

Данная функция возвращает результат объединения нескольких строковых аргументов. Кол-во аргументов не ограничено.

Для создания переменной с функцией Concat, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

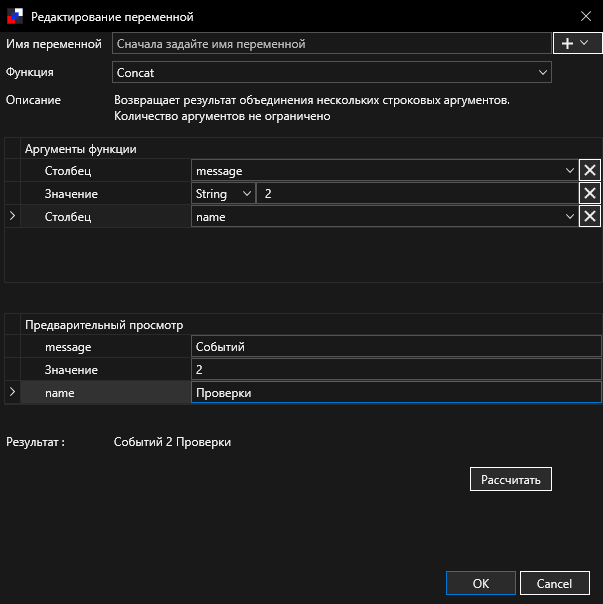


Рисунок 98. Пример функции Concat

Далее, необходимо назначить аргументы функции. Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события и/или константу. Для добавления нескольких аргументов необходимо нажать на кнопку  и добавить либо «Поле» (Поле события), либо «Значение» (Константа). Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

#### Replace

Данная функция заменяет в выбранном поле **первое вхождения** символов, указанных во втором аргументе, на символы, указанные в третьем аргументе.

Для создания переменной с функцией Replace, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции. Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события, в строках Первый аргумент и Второй аргумент ввести значения. Для завершения создания переменной необходимо нажать кнопку ОК. Данная функция регистрозависимая.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 99. Пример функции Replace

#### Replace\_all

Данная функция заменяет в выбранном поле **все вхождения** символов, указанных во втором аргументе, на символы, указанные в третьем аргументе.

Для создания переменной с функцией Replace\_all, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции. Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события, в строках Первый аргумент и Второй аргумент ввести значения. Для завершения создания переменной необходимо нажать кнопку ОК. Данная функция регистрозависимая.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

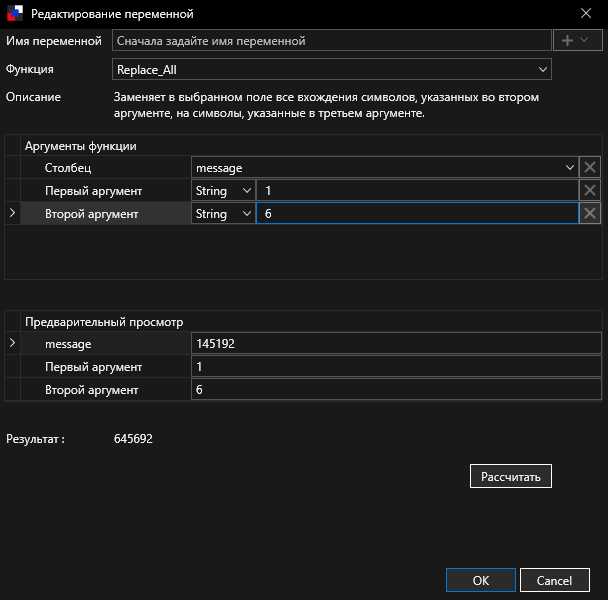


Рисунок 100. Пример функции Replace\_all

#### Split

Данная функция возвращает группу значений на основе заднего разделителя и количества групп.

Для создания переменной с функцией Split, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции. Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события, в строках Разделитель и Количество ввести значения. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

#### Substring

Данная функция возвращает часть строкового аргумента, начиная с позиции (индекс начала – отсчёт начинается с 1), указанной в первом числовом аргументе, и в количестве необходимых символов, указанном во втором числовом аргументе.

Для создания переменной с функцией Substring, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции. Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события, в строках Начальный индекс и Конечный индекс ввести значения. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 101. Пример функции Substring

#### To\_lower

Данная функция возвращает строковый аргумент, преобразованный в нижний регистр.

Для создания переменной с функцией To\_lower, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции. Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 102. Пример функции To\_lower

#### To\_upper

Данная функция возвращает строковый аргумент, преобразованный в верхний регистр.

Для создания переменной с функцией To\_upper, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции. Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 103. Пример функции To\_upper

## **Функции для работы с активными списками**

#### Get\_activeslist\_value

Данная функция возвращает значение, связанное с определённым полем указанного активного списка.

Для создания переменной с функцией Get\_activeslist\_value, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

В меню «аргументы функции» необходимо добавить нужные аргументы. При выборе функции Get\_activelist\_value необходимо выбрать активный список. Также есть возможность просмотра содержимого активного списка, для этого необходимо выбрать кнопку .

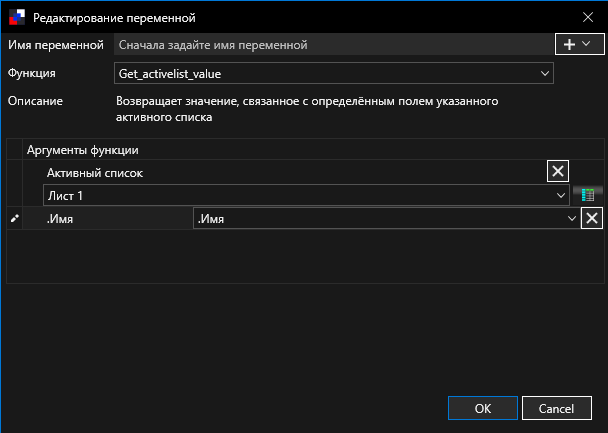


Рисунок 104. Пример функции Get\_activeslist\_value

## **Преобразование типа**

#### DateTime\_to\_UnixTime

Данная функция принимает строку в качестве аргумента в заданном формате и преобразует её значение Unixtime в формате длинное целое.

Для создания переменной с функцией DateTime\_to\_UnixTime, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции. Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

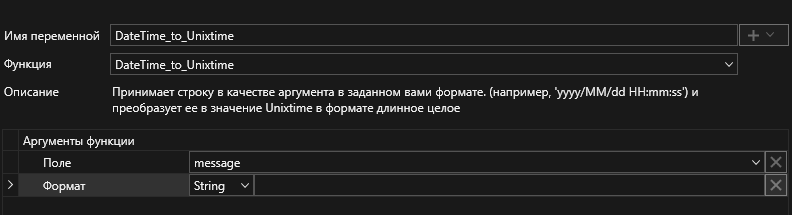


Рисунок 105. Пример функции DateTime\_to\_UnixTime

#### Ip\_to\_integer

Данная функция возвращает значение поля формата IP в формате int.

Для создания переменной с функцией Ip\_to\_int, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции. Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

#### String\_to\_float

Данная функция принимает строку в качестве аргумента и возвращает целое число в формате чиста с плавающей точкой.

Для создания переменной с функцией String\_to\_float, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции. Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

#### String\_to\_long

Данная функция принимает строку в качестве аргумента и возвращает целое число в формате длинное целое.

Для создания переменной с функцией String\_to\_long, необходимо нажать кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать соответствующую функцию.

Далее, необходимо назначить аргументы функции. Для этого в строке «Столбец» в выпадающем списке следует выбрать необходимое поле события. Для завершения создания переменной необходимо нажать кнопку ОК.

Для просмотра результата отработки функции, необходимо в разделе «Предварительный просмотр» нажать кнопку «Рассчитать».

# **ПРАВИЛА ОБОГАЩЕНИЯ**

Правила обогащения предназначены для обогащения событий ИБ до их записи в базу данных с событиями безопасности.

Для создания правил обогащения в меню ресурсов необходимо перейти на вкладку «Правила обогащения» и выбрать необходимую папку, в которой будет располагаться новое правило обогащения, или создать новую, после чего выбрать пункт меню «Создать» (см. Рисунок 102).

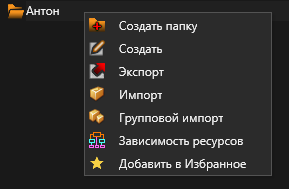


Рисунок 106. Дерево правил обогащения

Написание правил обогащения ничем не отличается от написания простых правил корреляции (см. раздел «ПРАВИЛА»). Но в правилах обогащения отсутствуют такие элементы как «Агрегированные поля», и из действий можно использовать только «Установить значение». На рисунке ниже представлен пример правила обогащения.



Рисунок 107. Пример правила обогащения

# **РЕТРОСПЕКТИВНЫЕ ПРАВИЛА**

Для выявления инциденты ИБ в исторических данных (данных, уже хранящихся в БД системы) следует воспользоваться Ретроспективными правилами. Работа с ретроспективными правилами, практически не отличается от работы с Правилами, выполняющимися в режиме реального времени.

Чтобы создать ретроспективное правило в меню ресурсов необходимо перейти на вкладку «Ретроспективные правила» и выбрать необходимую папку, в которой будет располагаться новое правило, или создать новую, после чего выбрать пункт меню «Создать» (см. Рисунок 104).

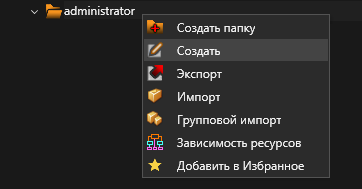


Рисунок 108. Дерево ретроспективных правил

После чего откроется окно конструктора написания ретроспективных правил (см. Рисунок 105).

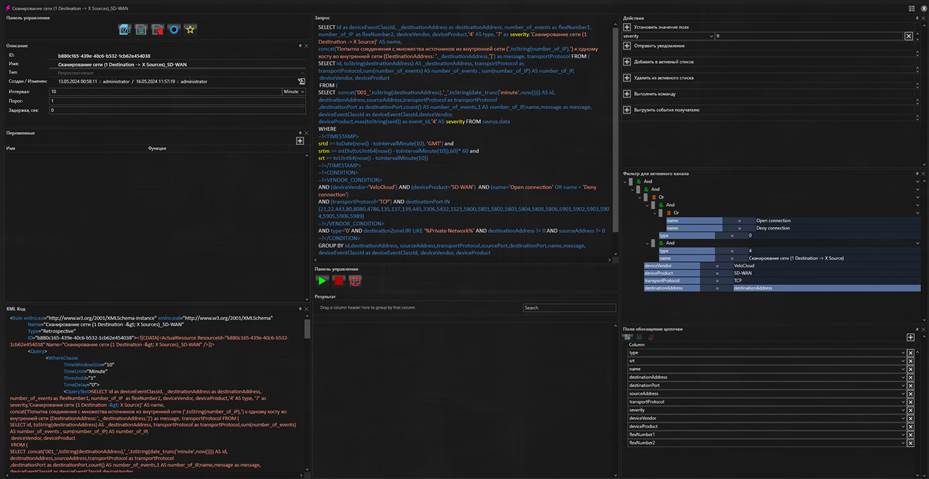


Рисунок 109. Конструктор создания ретроспективных правил

Для создания правил в первую очередь необходимо заполнить основную информацию (см. Рисунок 106), где:

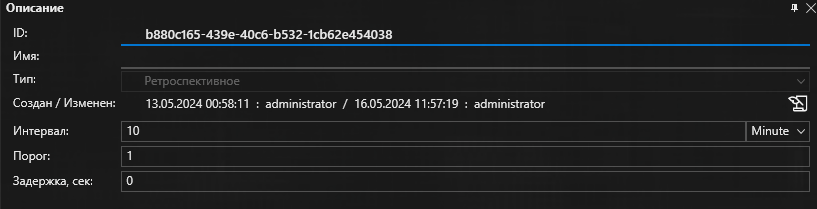


Рисунок 110. Основная информация по Правилу

* ID – уникальный идентификатор Правила присваивается автоматически;
* Имя – наименование правила;
* Дата создания/изменения – Дата и время создания/изменения правила, присваивается автоматически.
* Интервал – Количество срабатываний правила за единицу времени. Может принимать значения в секундах, минутах, часах и днях.

Для просмотра истории изменения необходимо нажать на кнопку .

В окне «Запрос» необходимо написать SQL-запрос к историческим данным, на основе которого будет производиться выборка событий. Подробнее о написании SQL-запросов можно посмотреть в разделе «».

Конструктор ретроспективных правил позволяет производить тестирование SQL-запросов. Для этого в окне «Панель управления» расположены кнопки «Запустить» – запускает SQL-запрос «Остановить» – прекращает SQL-запрос и «Отчистить таблицу» – удаляет данные из таблицы с результатами отработки запроса.

Далее при необходимости можно добавить Переменные, которые будут использоваться в правиле, а также Действия, которые будут срабатывать после его отработки. Подробнее о Переменных и Действиях можно посмотреть в разделе «ПРАВИЛА».

В меню «Панель управления» располагаются кнопки взаимодействия с правилом. Подробнее о них описано в таблице ниже.

Таблица 7. Кнопки взаимодействия с Ретроспективными правилами

|  |  |  |
| --- | --- | --- |
| Иконка | Наименование | Назначение |
|  | XML Код | Включает отображение XML Кода правила |
|  | Сохранить | Сохраняет правило |
|  | Сохранить как | Сохраняет копию правила |
|  | Включено/Выключено | Включает или выключает выполнение правила.  Красный цвет означает, что правило выключено, синий – включено. |
|  | Добавить в Избранное | Используется для добавления в «Избранное» |

На рисунке ниже представлен пример Ретроспективного правила, выявляющего сканирование сети.

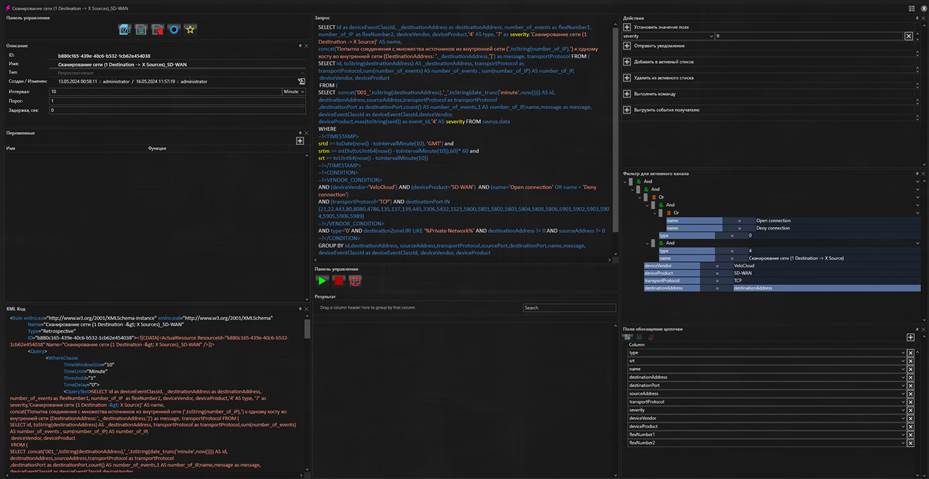


Рисунок 111. Пример ретроспективного правила

# **ФИЛЬТРЫ**

## **Создание фильтра**

Для создания нового фильтра необходимо перейти на вкладку «Фильтры». Далее, нажав правой кнопкой мыши (ПКМ) на папку, выбрать кнопку «Создать» (см. Рисунок 108).

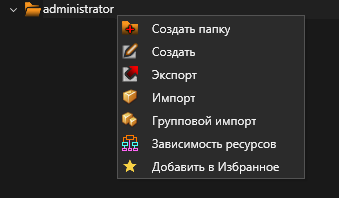


Рисунок 112. Окно создания фильтра

Далее необходимо ввести название фильтра и задать условия (см. Рисунок 109) фильтрации событий. Для сохранения фильтра необходимо нажать на кнопку .

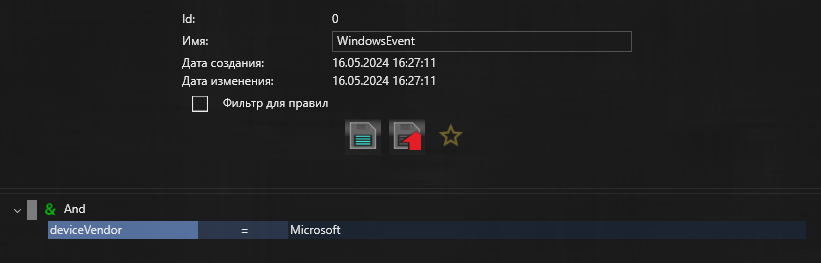


Рисунок 113. Окно настройки фильтра

## **Изменение фильтра**

Для изменения фильтра необходимо во вкладке «Фильтры» нажать ПКМ по нужному фильтру и в контекстном меню выбрать пункт «Открыть» (см. Рисунок 110).

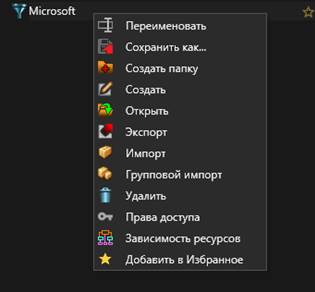


Рисунок 114. Окно взаимодействия с фильтром

В открывшемся окне следует произвести необходимые изменения (см. Рисунок 111). Для сохранения изменений необходимо нажать на кнопку .

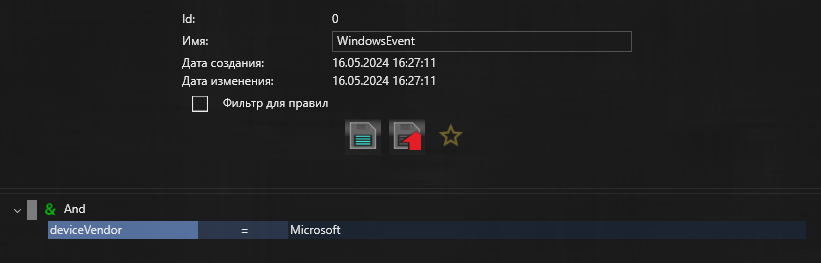


Рисунок 115. Окно редактирования фильтра

## **Удаление фильтра**

Для удаления фильтра необходимо во вкладке «Фильтры» нажать ПКМ по нужному фильтру и в контекстном меню выбрать пункт «Удалить» (Рисунок 112). После чего Фильтр будет помечен на удаление, для полного удаления необходимо повторить процедуру.

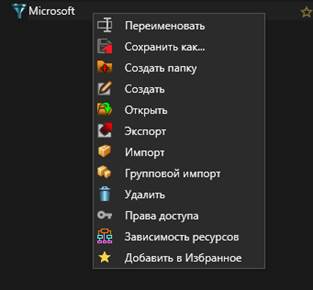


Рисунок 116. Удаление фильтра

## **Создание условий**

Для этого требуется нажать ПКМ на условие And, и выбрать пункт создания условия ЛКМ (см. Рисунок 113).

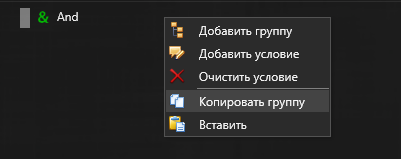


Рисунок 117. Создание условия фильтра

В открывшемся окне можно выбрать необходимые условия (см. Рисунок 114). По умолчанию в фильтре не установлена регистронезависисмость, при необходимости её можно включить в редакторе условий.



Рисунок 118. Окно создания условий

Перечень параметров условия:

* = – равно;
* != – не равно;
* contains – содержит;
* Not contains – не содержит;
* StartsWith– начинается с;
* EndsWith – оканчивается на;
* Not StartsWith – не начинается с;
* Not EndsWith – не оканчивается на;
* is – является (NULL/NOT NULL);
* In Filter – содержится в фильтре.

При необходимости можно добавить группу условий, для этого в конструкторе фильтров необходимо щёлкнуть ПКМ и в контекстном меню выбрать пункт «Добавить группу», после чего сформировать условие. На рисунке ниже представлен пример сформированного условия.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 119. Пример условия

## **Сохранение условий**

Для сохранения условия необходимо нажать ЛКМ на ОК. После этого, созданное условие высветится в списке условий фильтра (см. Рисунок 116).

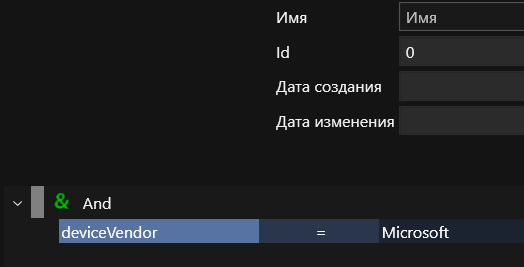


Рисунок 120. Список условий фильтра

## **Удаление условий**

Для удаления условия следует нажать ПКМ на условия и в контекстном меню выбрать «Удалить условие» (см. Рисунок 117).

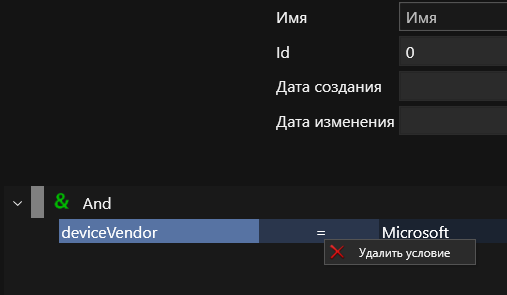


Рисунок 121. Удаление условия

## **Создание группы условий**

Также можно добавить группу условий. Для этого требуется нажать ПКМ на условие And и выбрать ЛКМ пункт создания группы условий (см. Рисунок 118).

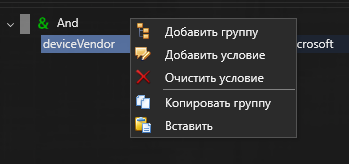


Рисунок 122. Добавление группы условий

## **Копирование и вставка условий**

Также имеется возможность копировать и вставлять эти условия. Для этого нужно нажать ПКМ в свободном поле и выбрать один из возможных пунктов (см. Рисунок 119).

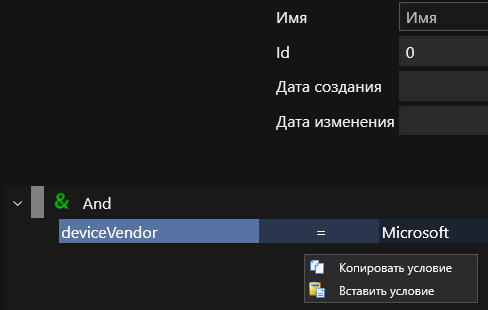


Рисунок 123. Копирование и вставка условий

# **SQL ЗАПРОСЫ**

## **Создание SQL запроса**

Для создания нового SQL запроса необходимо перейти на вкладку «SQL запросы». Далее, нажав правой кнопкой мыши (ПКМ) на папку, выбрать пункт меню «Создать» (см. Рисунок 120).

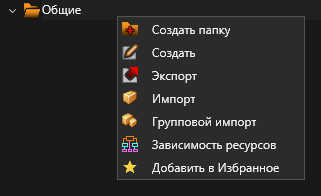


Рисунок 124. Меню взаимодействия

В левой части окна находится раздел со всеми доступными таблицами БД системы. При нажатии ЛКМ на стрелочку рядом с названием таблицы появится отображение всех находящихся в ней полей (см. Рисунок 121).



Рисунок 125. Таблицы БД

Далее необходимо ввести название и написать SQL запрос (см. Рисунок 122) для выборки данных. Для удобства написания запроса есть возможность двойным нажатием ЛКМ по названию таблицы или поля автоматически переносить их в строку запроса.



Рисунок 126. Окно создание запроса

Поля, содержащие дату и время, имеют возможность автоматического ввода диапазона дат. Для этого необходимо выбрать нужное поле нажать ПКМ и выбрать пункт меню «Clickhouse date» (см. Рисунок 123). После этого в поле запроса появится диапазон времени (см. Рисунок 123). Данный временной интервала дублируется из меню «Период» в окне создания SQL запроса. Схожий функционал доступен для поля «Severity». При выборе поля «Severity» и нажатии на него ПКМ в появившемся меню необходимо выбрать «Severity» (см. Рисунок 123). После поле «Severity» в окне запроса примет боле понятный, читаемый вид (см. Рисунок 123). Для всех полей отмеченных жёлтым цветом в поле «Запрос» доступна функция автоматического ввода функциями «Clickhouse date» и «Severity».

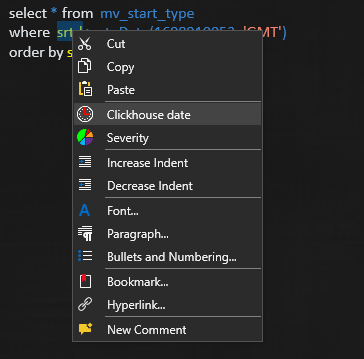


Рисунок 127. Меню взаимодействия с запросом



Рисунок 128. Пример автозаполнения диапазона

При нажатии на кнопку  в окне «Результат» произойдёт выполнение SQL запроса и вывод результата (см. Рисунок 125). Также доступен функционал раздельного выполнения запроса. Для это необходимо выделить необходимую часть запроса и нажать на кнопку .



Рисунок 129. Окно результата

## **Изменение SQL запроса**

Для изменения запроса следует во вкладке «SQL запросы» нажать ПКМ по необходимому и в контекстном меню выбрать пункт «Открыть» (см. Рисунок 126).

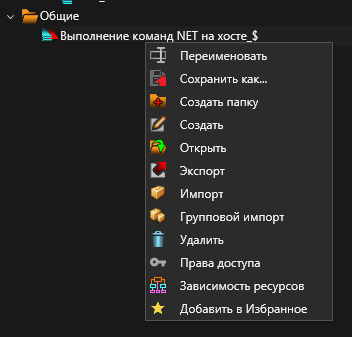


Рисунок 130. Меню взаимодействия

В открывшемся окне следует произвести необходимые изменения (см. Рисунок 127). Для сохранения изменений необходимо нажать на кнопку .

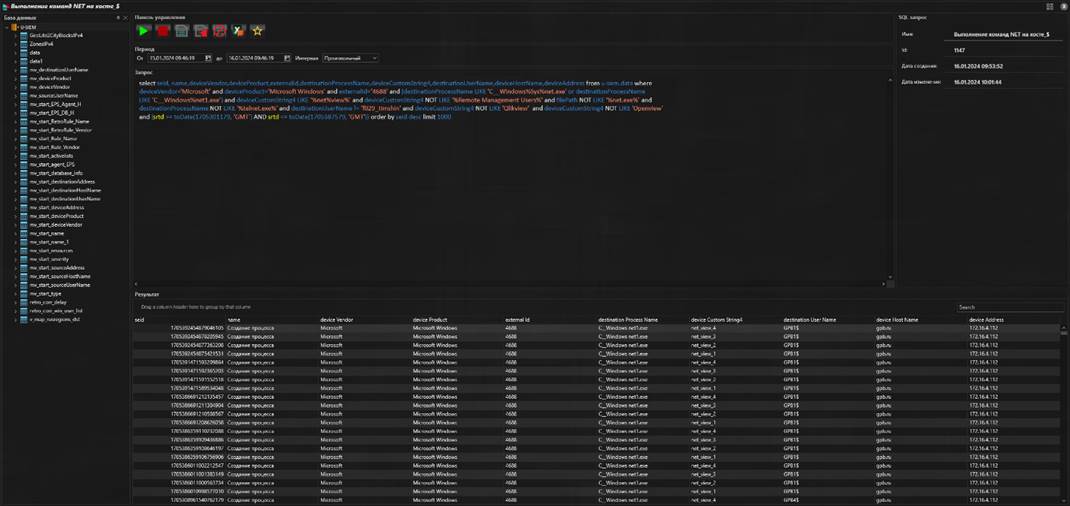


Рисунок 131. Окно редактирования запроса

## **Удаление SQL запроса**

Для удаления запроса следует во вкладке «SQL запросы» нажать ПКМ по необходимому и в контекстном меню выбрать пункт «Удалить» (см. Рисунок 128). После чего запрос будет помечен на удаление, для полного удаления необходимо повторить процедуру.

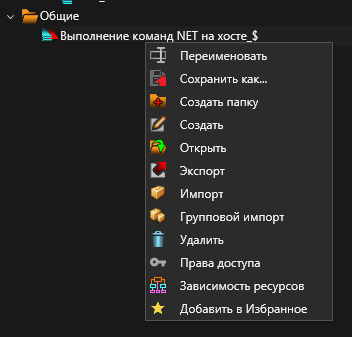


Рисунок 132. Меню взаимодействия

# **ВИЗУАЛИЗАЦИЯ ДАННЫХ**

## **Создание визуализации**

Для создания объекта визуализации данных (различные диаграммы, графики и таблицы) необходимо перейти на вкладку «Визуализации». Далее, нажав правой кнопкой мыши (ПКМ) на папку, выбрать кнопку «Создать» (см. Рисунок 129).

*Для создания объекта визуализации данных необходимо заранее создать SQL запрос в соответствующем разделе.*

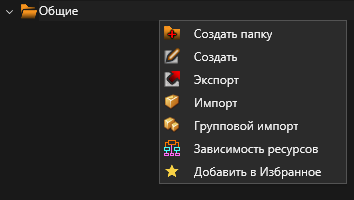


Рисунок 129. Меню взаимодействия

Далее, необходимо ввести название и описание объекта визуализации данных, выбрать необходимый запрос в разделе «База данных» (см. Рисунок 130). *В окне создания визуализации функция редактирования SQL запроса недоступна.*



Рисунок 130. Окно создания визуализации

Далее, настраивается вид визуализации. В данном меню основными настройками являются: тип диаграммы, выбор значений, внешний вид, обновление (см. Рисунок 131). В меню «Тип диаграммы» выбирается одна из доступных диаграмм. В меню «Выбор значения» необходимо вставить значения в поля координат. Только для Столбчатой диаграммы необходимо задавать диапазон значений по оси Z. В меню «Внешний вид» доступны настройки внешнего вида выбранной диаграммы. В меню «Обновление» настраивается временной период обновления данных в объекте визуализации.

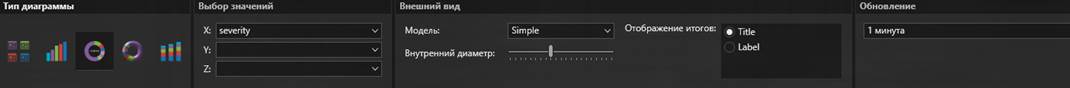


Рисунок 131. Окно редактирования вида

Для сохранения фильтра необходимо нажать на кнопку .

## **Изменение визуализации**

Для изменения объекта визуализации данных необходимо во вкладке «Визуализации» нажать ПКМ по нужному и в контекстном меню выбрать пункт «Открыть» (см. Рисунок 132).

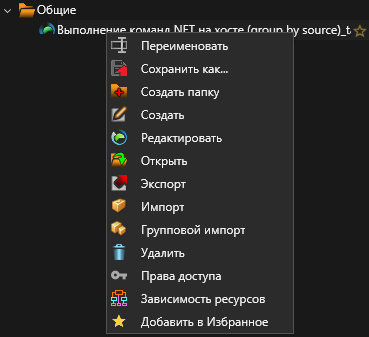


Рисунок 132. Меню взаимодействия

В открывшемся окне следует произвести необходимые изменения. Для сохранения изменений необходимо нажать на кнопку .

## **Удаление визуализации**

Для удаления объекта визуализации данных необходимо во вкладке «Визуализации» нажать ПКМ по нужному и в контекстном меню выбрать пункт «Удалить» (Рисунок 133). После чего объект визуализации данных будет помечена на удаление, для полного удаления необходимо повторить процедуру.

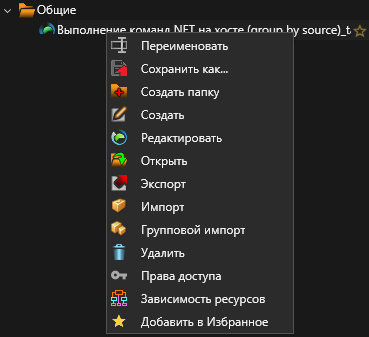


Рисунок 133. Меню взаимодействия

# **ДАШБОРДЫ**

## **Создание дашборда**

Для создания нового дашборда необходимо перейти на вкладку «Дашборды». Далее, нажав правой кнопкой мыши (ПКМ) на папку, выбрать пункт меню «Создать» (см. Рисунок 134).

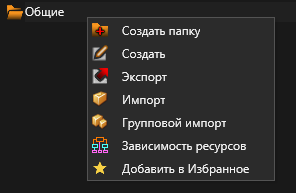


Рисунок 134. Меню взаимодействия

*Для создания дашборда необходимо заранее создать объекты визуализации данных в соответствующем разделе.*

В открывшемся меню доступен выбор заранее созданных объектов визуализации данных (различные диаграммы, графики и таблицы). В данном меню необходимо выбрать один или несколько объектов визуализации. Также есть возможность сделать выбранный дашборд стартовым. Для этого необходимо выставить соответствующую галочку рядом с кнопкой сохранения дашборда. При сохранения дашборда необходимо ввести название и нажать на кнопку .

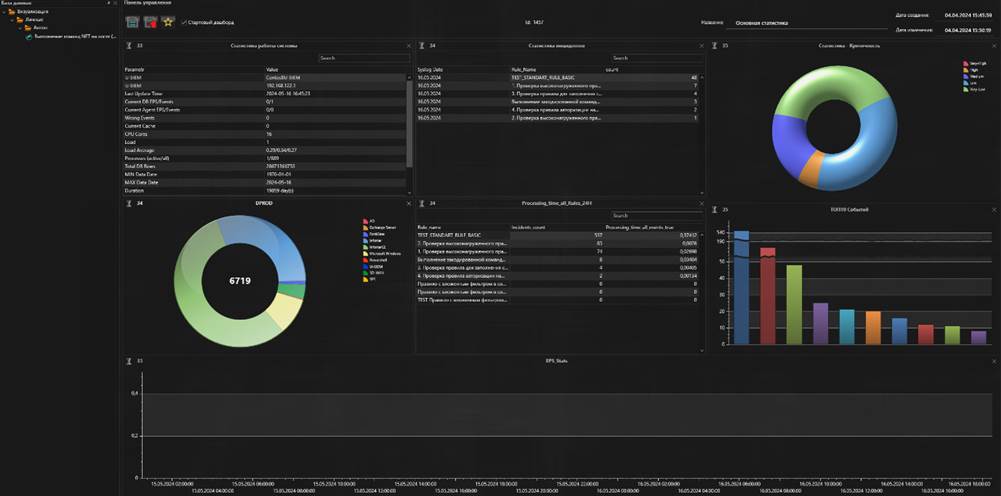


Рисунок 135. Окно создания дашборда

## **Изменение дашборда**

Для изменения дашборда необходимо во вкладке «Дашборды» нажать ПКМ по нужному дашборду и в контекстном меню выбрать пункт «Редактировать» (см. Рисунок 136).

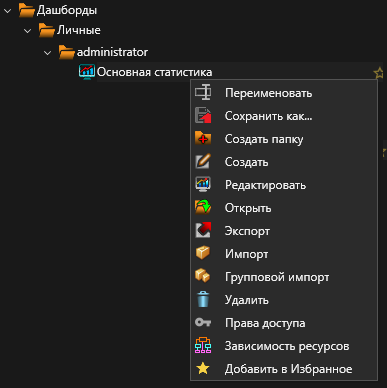


Рисунок 136. Меню взаимодействия

В открывшемся окне доступны изменения названия дашборда, выбор дополнительных объектов визуализаций данных. Для удаления уже размещенных на дашборде необходимо нажать  в правой верхней части приложения.

## **Удаление дашборда**

Для удаления дашборда необходимо во вкладке «Дашборда» нажать ПКМ по нужному дашборду и в контекстном меню выбрать пункт «Удалить» (см. Рисунок 137). После чего дашборд будет помечен на удаление, для полного удаления необходимо повторить процедуру.

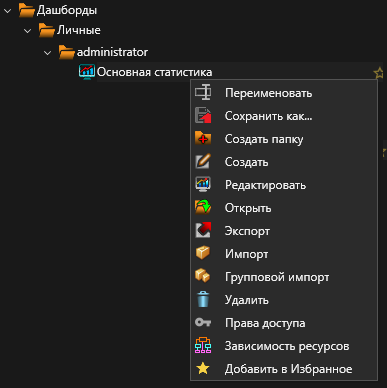


Рисунок 137. Меню взаимодействия

# **НАБОРЫ ПОЛЕЙ**

## **Создание набора полей**

Для создания набора полей необходимо перейти на вкладку «Наборы полей». Далее, нажав правой кнопкой мыши (ПКМ) на папку, выбрать кнопку «Создать» (см. Рисунок 138).

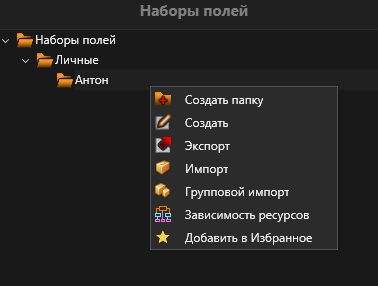


Рисунок 138. Меню взаимодействия

Далее, необходимо ввести название, перенести необходимые поля из левого списка в правый (см. Рисунок 139). Для сохранения необходимо нажать на кнопку .

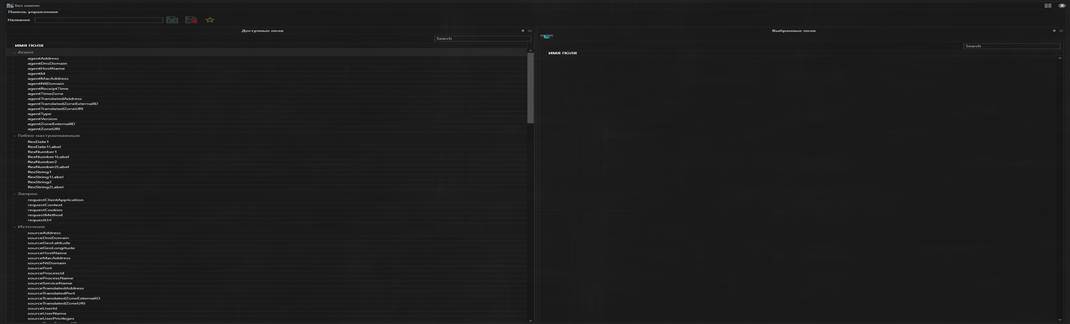


Рисунок 139. Окно создания набора полей

## **Изменение набора полей**

Для изменения набора полей необходимо во вкладке «Наборы полей» нажать ПКМ по нужному набору полей и в контекстном меню выбрать пункт «Открыть» (см. Рисунок 140).

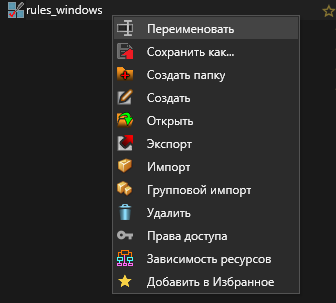


Рисунок 140. Меню взаимодействия

В открывшемся окне следует произвести необходимые изменения (см. Рисунок 141). Для сохранения изменений необходимо нажать на кнопку .

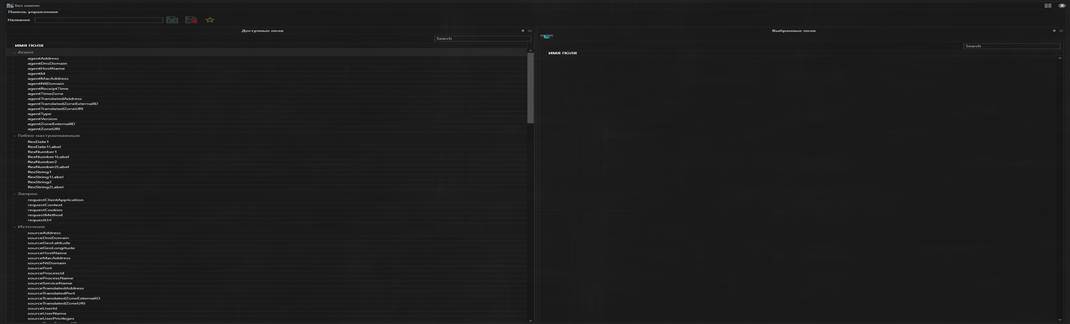


Рисунок 141. Окно редактирования набора полей

## **Удаление набора полей**

Для удаления следует во вкладке «SQL запросы» нажать ПКМ по необходимому и в контекстном меню выбрать пункт «Удалить» (см. Рисунок 142). После чего набор полей будет помечен на удаление, для полного удаления необходимо повторить процедуру.

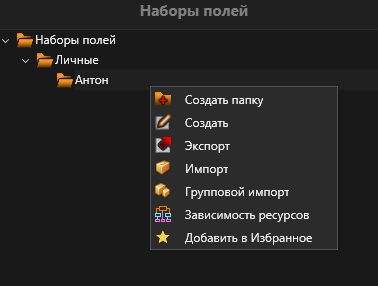


Рисунок 142. Меню взаимодействия

# **КОНТЕКСТНЫЙ ПОИСК**

Контекстный поиск предназначен для навигации между ресурсами в консоли управления. Позволяет выполнять поиск ресурсов по имени, их id в Системе, ссылкам в иных ресурсах, упоминаниям в условиях фильтрации.

Для запуска контекстного поиска необходимо:

1. Перейти на вкладку «Контекстный поиск»;
2. В открывшемся окне ввести в строку поиска необходимые значения;
3. По необходимости установить дополнительные настройки поиска «Игнорировать регистр» и «Сокращенный формат»;
4. Нажать на кнопку «Найти».
5. После чего в окне «Результаты поиска» появятся строки, соответствующие запросу.