

САВРУС

Руководство пользователя

АННОТАЦИЯ

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

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 САВРУС рекомендуется внимательно ознакомиться с настоящим руководством.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ И ТЕРМИНЫ.....	7
АВТОРИЗАЦИЯ В СИСТЕМЕ.....	8
1. Конфигурация консоли при первоначальном входе.....	8
2. Импорт настроек консоли из предыдущих инсталляций.....	9
ОСНОВНЫЕ ЭЛЕМЕНТЫ КОНСОЛИ.....	12
3. Ресурсы консоли.....	12
НАСТРОЙКА РАБОЧЕГО ПРОСТРАНСТВА.....	14
1. Взаимодействие с окнами рабочего пространства.....	14
2. Макет рабочего пространства.....	18
3. Список автозагрузки ресурсов.....	21
4. Закрепление рабочего пространства «Меню ресурсов».....	22
5. Смена темы рабочего пространства.....	22
6. Настройка параметров программы.....	23
ЭЛЕМЕНТЫ ВЗАИМОДЕЙСТВИЯ С РЕСУРСАМИ.....	26
1. Функции контекстного меню.....	26
2. Права доступа.....	27
3. Экспорт и импорт ресурсов.....	28
4. Просмотр истории изменений.....	31
ИЗБРАННОЕ.....	34
АКТИВНЫЕ КАНАЛЫ.....	35
1. Основные элементы активного канала.....	35
Радар.....	35
Таблица АК.....	36
2. Создание активного канала.....	37
3. Изменение временного интервала и количества записей.....	38
4. Добавление полей данных.....	39
5. Написание условий.....	42
6. Открытие/запуск активного канала.....	43
7. Редактирование активного канала.....	48

Фильтрация событий.....	50
Группировка событий.....	52
Выгрузка и печать.....	55
8. Локальные настройки активного канала.....	55
9. Глобальные настройки активного канала.....	56
АКТИВНЫЕ СПИСКИ.....	57
1. Создание активного списка.....	57
2. Наполнение активного списка.....	61
3. Управление активным списком.....	64
4. Удаление активного списка.....	66
УВЕДОМЛЕНИЯ.....	67
ШАБЛОНЫ УВЕДОМЛЕНИЙ.....	68
ПРАВИЛА.....	69
1. Создание правил.....	69
Стандартные правила.....	70
Агрегационные правила.....	79
2. Управление правилами.....	82
3. Редактирование правила.....	82
4. Создание АК по событиям, сгенерированным правилом.....	83
5. Удаление правила.....	83
МОНИТОРИНГ ЗАГРУЗКИ КОРРЕЛЯТОРА.....	85
1. Событие «CPU».....	85
2. Событие «rule time statistics».....	86
3. Параметры config.xml коррелятора.....	87
ФУНКЦИИ ПЕРЕМЕННЫХ.....	89
1. Создание и управление функциями переменных.....	89
2. Арифметические функции.....	89
3. Дата и время.....	94
4. Пользовательские функции.....	102
5. Строковые функции.....	106
6. Функции для работы с активными списками.....	110
7. Преобразование типа.....	111

ПРАВИЛА ОБОГАЩЕНИЯ.....	113
РЕТРОСПЕКТИВНЫЕ ПРАВИЛА.....	114
1. Ретроспективное правило.....	115
2. Ретроспективное GUI.....	117
3. Ретроспективное сравнение.....	119
ФИЛЬТРЫ.....	123
1. Создание фильтра.....	123
2. Изменение фильтра.....	123
4. Удаление фильтра.....	124
5. Создание условий.....	125
6. Сохранение условий.....	126
7. Удаление условий.....	127
8. Создание группы условий.....	127
9. Копирование и вставка условий.....	127
SQL ЗАПРОСЫ.....	129
1. Создание SQL запроса.....	129
2. Изменение SQL запроса.....	131
3. Удаление SQL запроса.....	132
4. Конструкторы запросов.....	133
ВИЗУАЛИЗАЦИЯ ДАННЫХ.....	136
1. Создание визуализации.....	136
2. Изменение визуализации.....	137
3. Удаление визуализации.....	137
ДАШБОРДЫ.....	139
1. Создание дашборда.....	139
2. Изменение дашборда.....	140
3. Удаление дашборда.....	141
4. Стартовый дашборд.....	141
НАБОРЫ ПОЛЕЙ.....	142
1. Создание набора полей.....	142
2. Изменение набора полей.....	143
3. Удаление набора полей.....	143

ОТЧЁТЫ.....	145
1. Создание отчёта.....	145
2. Добавление данных в отчёт.....	147
3. Редактирование отчёта.....	148
4. Удаление отчёта.....	148
КОНТЕКСТНЫЙ ПОИСК.....	149
ГЛОБАЛЬНЫЕ ПЕРЕМЕННЫЕ.....	150
1. Создание Глобальной переменной.....	150
2. Редактирование Глобальной переменной.....	150
3. Удаление Глобальной переменной.....	150
КОМАНДЫ ИНТЕГРАЦИИ.....	151
1. Создание Команды интеграции.....	151
2. Редактирование Команды интеграции.....	156
3. Удаление Глобальной переменной.....	156
ВЕБ-ИНТЕРФЕЙС.....	157
1. Инструкция по входу в Веб-Интерфейс.....	157
2. Основные вкладки Веб-интерфейса коррелятора.....	157
3. Описание содержания вкладок Веб-интерфейса коррелятора.....	157
4. Основные вкладки Веб-интерфейса инфортера.....	161

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

1. Конфигурация консоли при первоначальном входе

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 САВРУС 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.

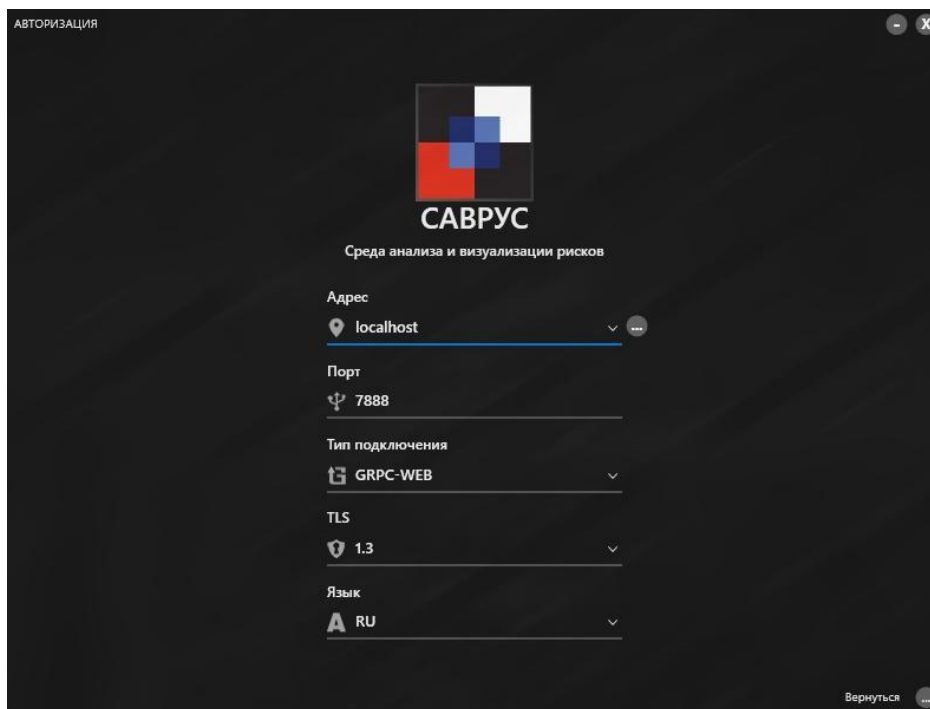


Рисунок 1. Настройки подключения

Рекомендуется обратиться к администратору САВРУС 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.

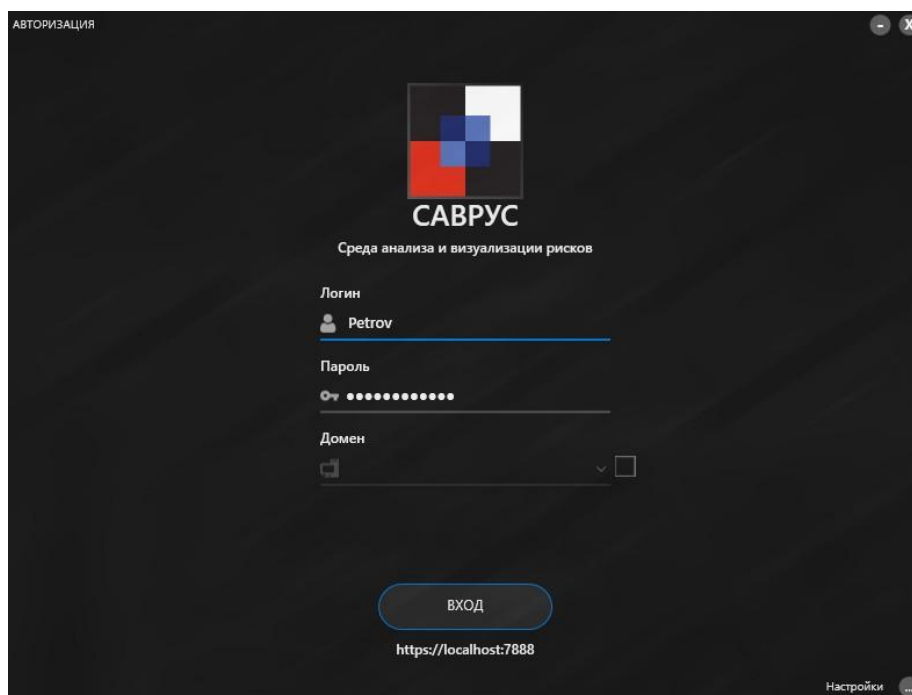


Рисунок 2. Аутентификация в системе

2. Импорт настроек консоли из предыдущих инсталляций

Функционал импорта настроек консоли из предыдущих инсталляций представляет из себя диалоговое окно, позволяющее выбрать файл настроек консоли предыдущих установленных версий, определяемых автоматически, или произвольный файл конфигурации.

Функционал призван сократить труд администратора или пользователя системы САВРУС при установке свежей версии ПО, например перенести список хостов, к которым осуществлялось подключение, настройки полей Активного канала по умолчанию.

Импортируются все доступные параметры конфигурации, в случае ошибки или отсутствия параметра – значение отбрасывается и в результирующий конфиг заносится значение по умолчанию.

Для того, чтобы импортировать настройки ранее установленной версии консоли, необходимо на стартовом экране входа в систему выбрать пункт «**Настройки**».

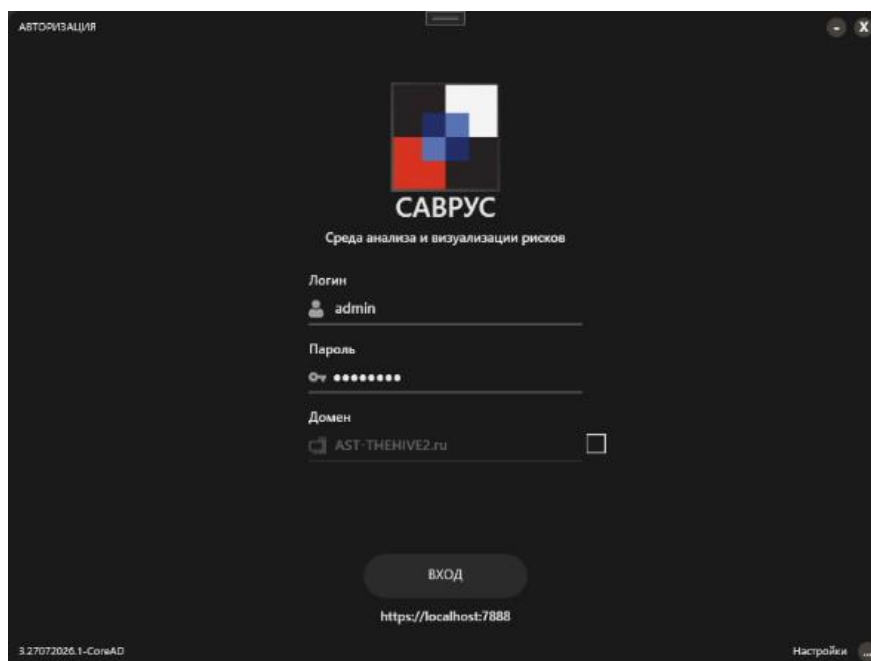


Рисунок 3. Стартовый экран входа в систему.

Затем, перейти в пункт «Импорт», находящийся в правом нижнем углу меню «Настройки».

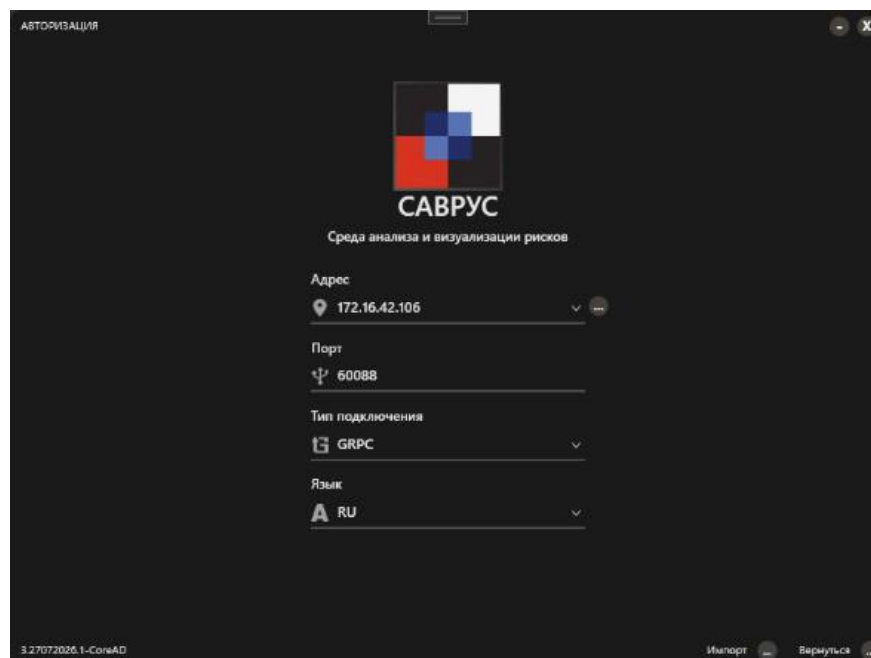


Рисунок 4. Меню "Настройки".

Далее откроется диалоговое окно, в котором отобразятся автоматически найденные файлы конфигураций предыдущих установок консоли.

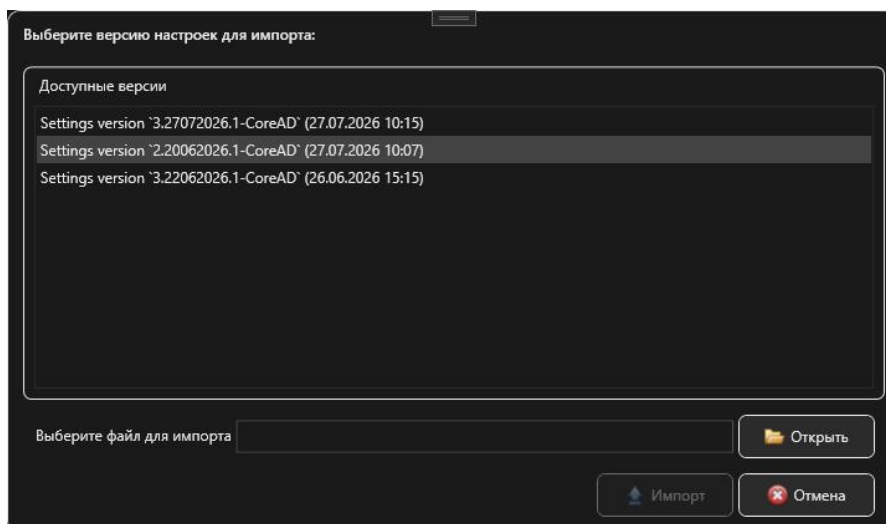


Рисунок 5. Диалоговое окно импорта файлов конфигурации.

Файлы конфигурации располагаются в системе по пути:

`C:\Users\<папка_пользователя>\AppData\Local\Savrus\Savrus_Url_<идентификатор>\1.0.0.0\ user.config`

ВАЖНО!

Конфигурация будет присутствовать в списке, если в ней содержится параметр

```
<setting name="AppVersion" serializeAs="String">  
    <value> <версия ПО></value>  
</setting>
```

С помощью кнопки «**Открыть**» можно выбрать произвольный файл конфигурации, в том числе и от версий консоли с отсутствующим параметром **AppVersion**.

После нажатия на кнопку «**Импорт**», параметры будут загружены в конфигурацию новой установки консоли.

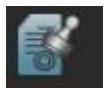
ОСНОВНЫЕ ЭЛЕМЕНТЫ КОНСОЛИ

3. Ресурсы консоли

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

Основными ресурсами являются:

Таблица 1. Ресурсы консоли

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 САВРУС.

НАСТРОЙКА РАБОЧЕГО ПРОСТРАНСТВА

Консоль САВРУС поддерживает настройку окон и сохранение внесённых изменений в макет под нужды любого специалиста. Редактировать рабочие пространства можно у любого ресурса системы. На рисунке ниже представлен пример кастомизации окон в рабочем пространстве активного канала.

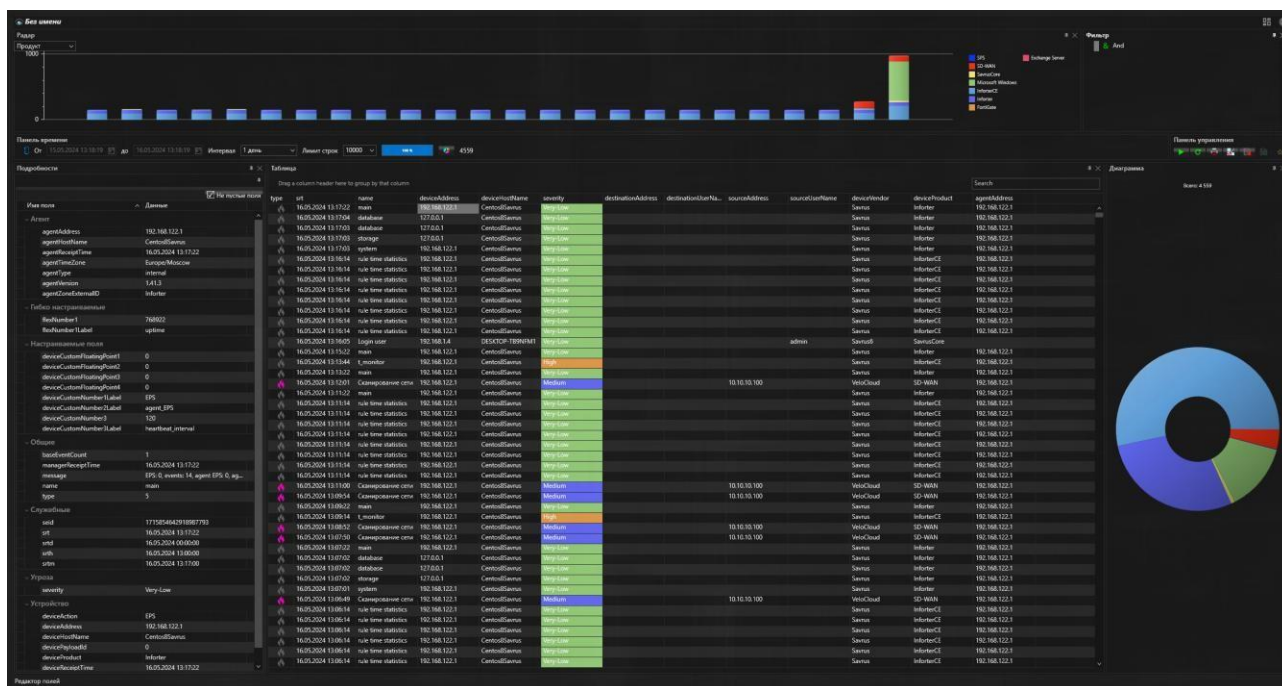


Рисунок 6. Пример изменённого положения окон в АК

1. Взаимодействие с окнами рабочего пространства

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 7). Также возможно растягивать окна. Для этого необходимо навести курсор на границу нужного окна и с зажатой «ЛКМ» потянуть в необходимую сторону.



Рисунок 7. Элемент управления для перемещения окон в рабочем пространстве

Также в консоли доступен функционал панели быстрого доступа. Данная панель становится доступна после открытия двух окон ресурсов и находится в нижней-левой части консоли и выглядит следующим образом (см. Рисунок 8).

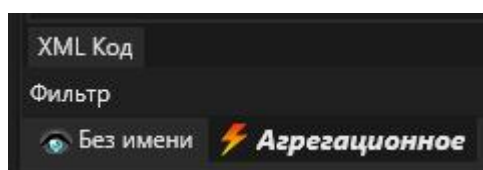


Рисунок 8. Панель быстрого доступа

В нижней части данной панели отображаются ранее открытые окна ресурсов. По середине находятся скрытые при помощи функции «Hide» элементы выбранного в данный момент ресурса. В верхней части находятся скрытые при помощи функции «Auto Hide» элементы выбранного в данный момент ресурса.

При нажатии «ПКМ» по окну ресурсов на панели быстрого доступа или по находящемуся в левом-верхнем углу заголовку раскрытого окна ресурсов откроется меню взаимодействия, которое содержит в себе следующие функции:

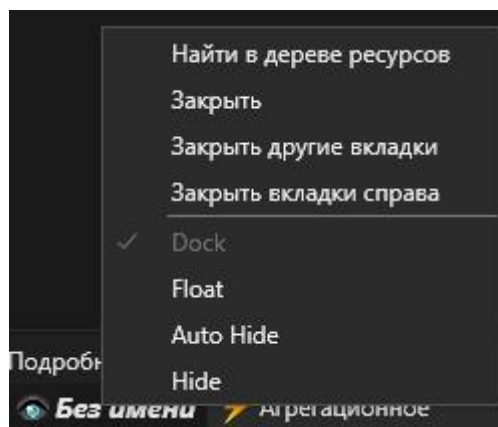


Рисунок 9. Меню взаимодействия на панели быстрого доступа

- Найти в дереве ресурсов – указывает на данный ресурс в «Меню ресурсов»

- **Заккрыть** – закрывает данное окно ресурсов, убирая его из панели быстрого доступа.
- **Заккрыть другие вкладки** – закрывает все окна кроме выбранного, убирая их с панели быстрого доступа.
- **Заккрыть вкладки справа** – закрывает все окна ресурсов, находящиеся правее от выбранного. Если правее выбранного окна нет доступных вкладок, данная функция не будет работать.
- **Dock** – позволяет вернуть ранее открепленное от интерфейса консоли окно в изначальное рабочее пространство, откуда оно было откреплено. При этом возвращая его в список окон на панели быстрого доступа.
- **Float** – позволяет открепить выбранное окно от общего рабочего пространства, открыв его в отдельном от интерфейса консоли окне. Данную функцию так же можно осуществить, если зажать «ЛКМ» на нужном окне ресурсов и вытянуть его в необходимое место за пределами рабочего пространства консоли.
- **Auto Hide** – позволяет скрыть окно, перенеся его на отдельную панель быстрого доступа в верхней-левой части рабочего пространства.
- **Hide** – позволяет скрыть окно, перенеся его на отдельную панель быстрого доступа в верхней-левой части рабочего пространства.

Вкладки окон, свёрнутых функциями «Hide» и «Auto Hide», будут размещены на разных панелях доступа (см. Рисунок 10).

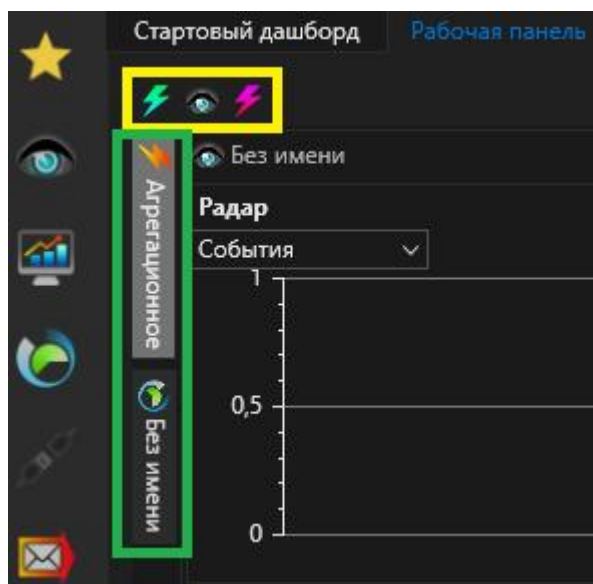


Рисунок 10. Расположение панелей доступа функций "Hide" и "Auto Hide"

На рисунке выше зелёным цветом помечена панель доступа к окнам, свёрнутым при помощи функции «Auto Hide», а жёлтым, при помощи функции «Hide».

Различие функций «Auto Hide» и «Hide» заключается в том, в каком виде будет развёрнуто скрытое окно.

Если окно было скрыто с помощью функции «Auto Hide», то при двойном нажатии «ЛКМ» по свёрнутому окну на панели быстрого доступа данное окно не будет возвращено в рабочее пространство, с которого оно было скрыто, а откроется в отдельном от интерфейса консоли окне.

Если же окно было скрыто с помощью функции «Hide», то при нажатии «ЛКМ» по свёрнутому окну на панели быстрого доступа, данное окно будет возвращено на основную панель быстрого доступа.

Функции «Dock», «Float», «Auto Hide» и «Hide» применимы к отдельным элементам рабочего пространства. Применение данных функций к отдельным элементам немного отличается от применения к окнам ресурсов.

При нажатии «ПКМ» по панели заголовка любого из элементов рабочего пространства, появится меню управления окном элемента (см. Рисунок 11).

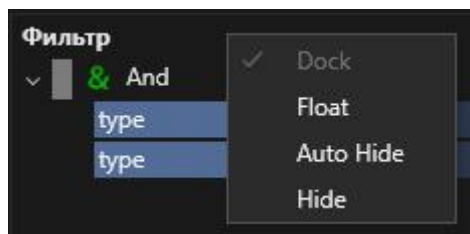


Рисунок 11. Меню управления окном

Данное меню содержит в себе следующие функции:

- Dock – позволяет вернуть ранее открепленный от интерфейса консоли элемент на его изначальную позицию в рабочем пространстве откуда оно было откреплено.
- Float – позволяет открепить выбранный элемент от общего рабочего пространства, открыв его в отдельном от интерфейса консоли окне. Данную функцию так же можно осуществить, если зажать «ЛКМ» на нужном элементе окна ресурсов и вытянуть его в необходимое место за пределами рабочего пространства консоли.
- Auto Hide – позволяет скрыть элемент, перенеся его на панель быстрого доступа в нижней-левой части рабочего пространства.

- Hide – позволяет скрыть окно, перенеся его на панель быстрого доступа в нижней-левой части рабочего пространства.

Отличие работы функций «Auto Hide» и «Hide» от ранее описанного примера с окнами ресурсов заключается в том, что развёртывание ранее свёрнутого окна при помощи функции «Hide» возвращает окно на изначальное место в рабочем пространстве. Во всех остальных аспектах они идентичны.

Функцию «Auto Hide» возможно реализовать с помощью нажатия «ЛКМ» по значку «Auto Hide» , находящегося в правом-верхнем углу каждого элемента окна ресурсов.

Для возвращения окна рабочего пространства к стандартному виду необходимо нажать «ЛКМ» на кнопку «Установить сохраненный макет»  находящуюся в правом-верхнем углу рабочего экрана.

2. Макет рабочего пространства

Консоль «САВРУС» поддерживает функцию создания макетов рабочего пространства для каждого пользователя.

Данная функция реализуется с помощью кнопки «Установить сохраненный макет»  находящуюся в правом-верхнем углу рабочего экрана.

Нажав «ПКМ» по данной кнопке, откроется меню взаимодействия с макетом (см. Рисунок 12).

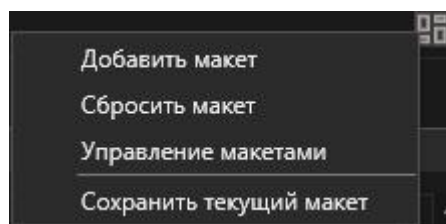


Рисунок 12. Меню взаимодействия с макетом

Меню макетов содержит в себе следующие функции:

- Добавить макет – позволяет сохранить настройки текущего макета рабочего пространства, добавляя его в меню «Управления макетами».
- Сбросить макет – сбрасывает настройки макета рабочего пространства, возвращая их к базовым (установленным при разработке).
- Управление макетами – открывает меню «Управления макетами».
- Сохранить текущий макет – сохраняет текущие настройки макета, заменяя базовые (установленные разработчиками).

Добавить макет

Нажатием «ЛКМ» по данной функции откроется окно (см. Рисунок 13) «Сохранить текущий макет».

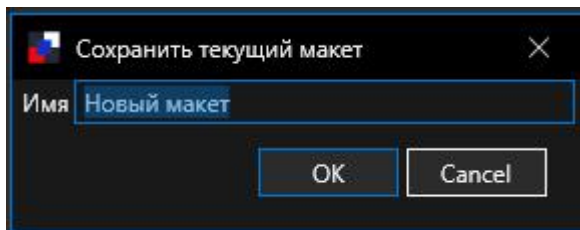


Рисунок 13. Окно "Сохранить текущий макет"

В данном окне необходимо ввести название сохраняемого макета и нажать на кнопку «ОК». После подтверждения названия данный макет будет занесён в список сохраненных макетов в меню «Управление макетами».

Сбросить макет

Нажатием «ЛКМ» по данной функции текущие настройки рабочего пространства будут сброшены до базовых (установленных при разработке) настроек макета.

Это не изменит настройки личного макета, созданного при помощи функции «Сохранить текущий макет», а также настройки ранее добавленных макетов из меню «Управление макетами», созданных с помощью функции «Добавить макет», если вы в момент сброса макета пользовались каким-то из них.

Управление макетами

При нажатии «ЛКМ» по данной функции откроется окно «Управление макетами» (см. Рисунок 14).

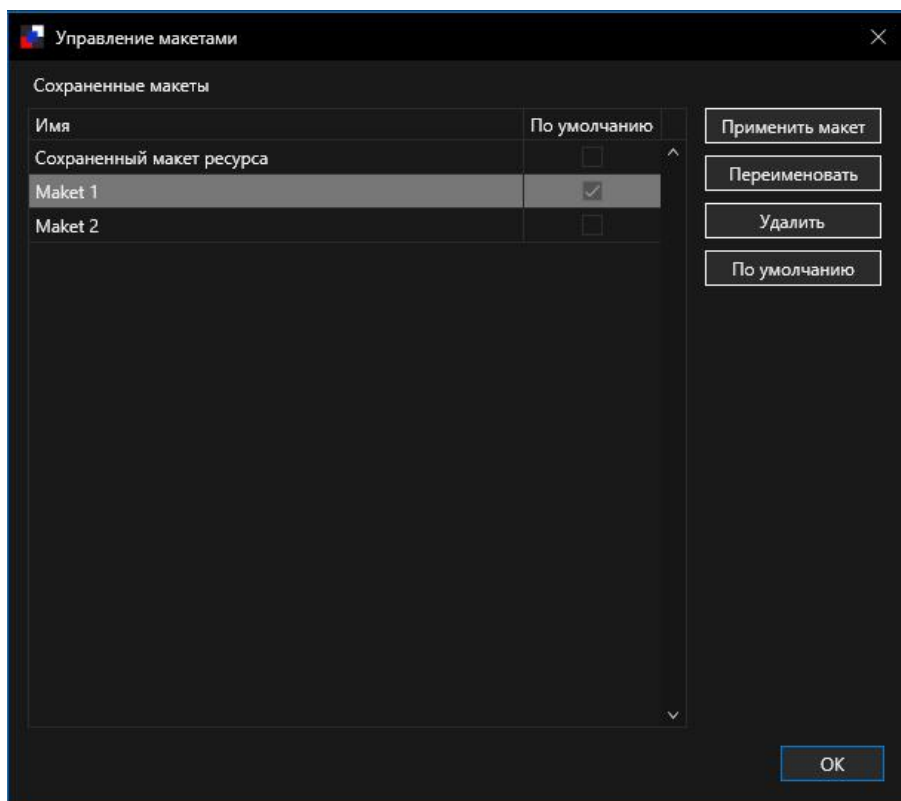


Рисунок 14. Окно "Управление макетами"

В левой части данного окна находится таблица «Сохраненные макеты», в которой отображаются все ранее добавленные макеты с помощью функции «Добавить макет». Если ранее макеты не добавлялись, то в данной таблице будет находиться только «Сохраненный макет ресурса» (подробное описание настройки данного макета находится в описании функции «Сохранить текущий макет»). В столбце «По умолчанию», галочкой отмечен макет, настройки которого будут использоваться при создании нового правила. Чтобы выдать макету статус «По умолчанию», требуется выбрать необходимый макет щёлкнув по нему «ЛКМ», далее нажать на кнопку «По умолчанию» в правой стороне окна.

Сохранить текущий макет

Данная функция сохраняет текущие настройки макета исключительно для пользователя, который вносит изменения в макет и только в конкретном выбранном ресурсе.

При использовании данной функции, настройки рабочего пространства выбранные пользователем, заменяют базовые настройки, установленные разработчиками. Теперь при нажатии «ЛКМ» по кнопке «Установить сохраненный макет» , находящейся в правом-

верхнем углу рабочего пространства, будут применяться настройки пользователя, сохраненные ранее, а не базовые настройки установленные разработчиками консоли.

Сохраненный макет будет срабатывать всегда при входе в ресурс, к которому он был применён.

Сохранённые настройки макета автоматически применяются к макету «Сохраненный макет ресурса» в окне «Управление макетами».

3. Список автозагрузки ресурсов

Функция «Автозагрузка» позволяет формировать персональный список ресурсов для автозагрузки с хранением списка в БД, что обеспечивает доступность списка, составленного определенным пользователем с любого рабочего места. Внесённые в список автозагрузки ресурсы будут автоматически открываться во вкладке «Рабочая панель» при запуске консоли.

Для открытия списка ресурсов автозагрузки необходимо, открыть вкладку «Администрирование» в дереве ресурсов и в открывшемся окне выбрать вкладку «Автозагрузка».

При открытии модуля «Автозагрузка» на экран консоли «САВРУС» выводится окно (см. Рисунок 15), содержащее список всех типов ресурсов, доступных в системе.

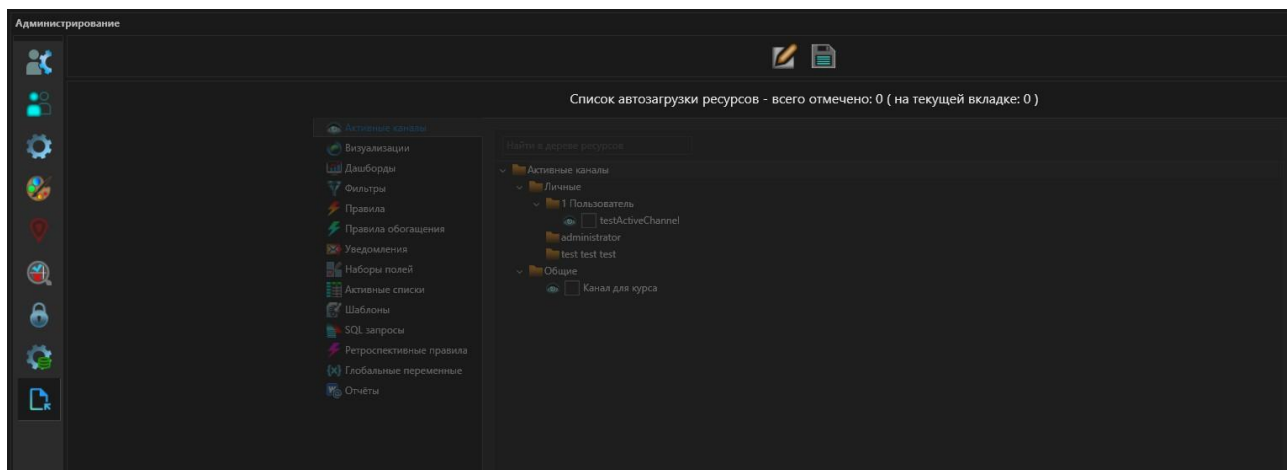


Рисунок 15. Внешний вид окна выбора ресурсов для автозагрузки.

В заголовке списка ресурсов отображается информация о выбранных ресурсах (всего и на выбранной вкладке), дополнительно, рядом с названием типа ресурса системы отображается кол-во выбранных ресурсов этого типа.

Для редактирования списка, необходимо нажать на кнопку «Режим редактирования», находящуюся в верхней части окна «Администрирование». Далее откроется доступ к списку

ресурсов, в котором нужно выбрать необходимые для автозагрузки ресурсы поставив на против них галочку.

Для сохранения списка автозагрузки необходимо нажать на кнопку «Сохранить», находящуюся в верхней части окна «Администрирование».

Для того, чтобы изменения вступили в силу необходимо перезапустить консоль.

При следующем запуске консоли «Саврус», выбранные ресурсы будут загружены и доступны во вкладке «Рабочая панель».

4. Закрепление рабочего пространства «Меню ресурсов»

Функция находится в правом-верхнем углу любого из раскрытых окон «Меню ресурсов» (см. Рисунок 16) и позволяет убрать наложение открытого окна “Меню ресурсов” на активное рабочее пространство консоли, при этом немного сузив его.

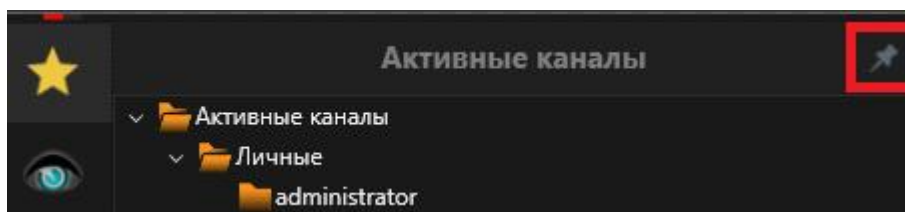


Рисунок 16. Расположение функции закрепления

Для возвращения окна в изначальное состояние повторно кликните ЛКМ по иконке закрепления .

5. Смена темы рабочего пространства

Для смены темы рабочего пространства необходимо, в дереве ресурсов открыть вкладку «Администрирование» и во внутренних вкладках окна выбрать «Настройка темы» . В левой части открывшегося окна (см. Рисунок 17) можно выбрать одну из доступных тем интерфейса.

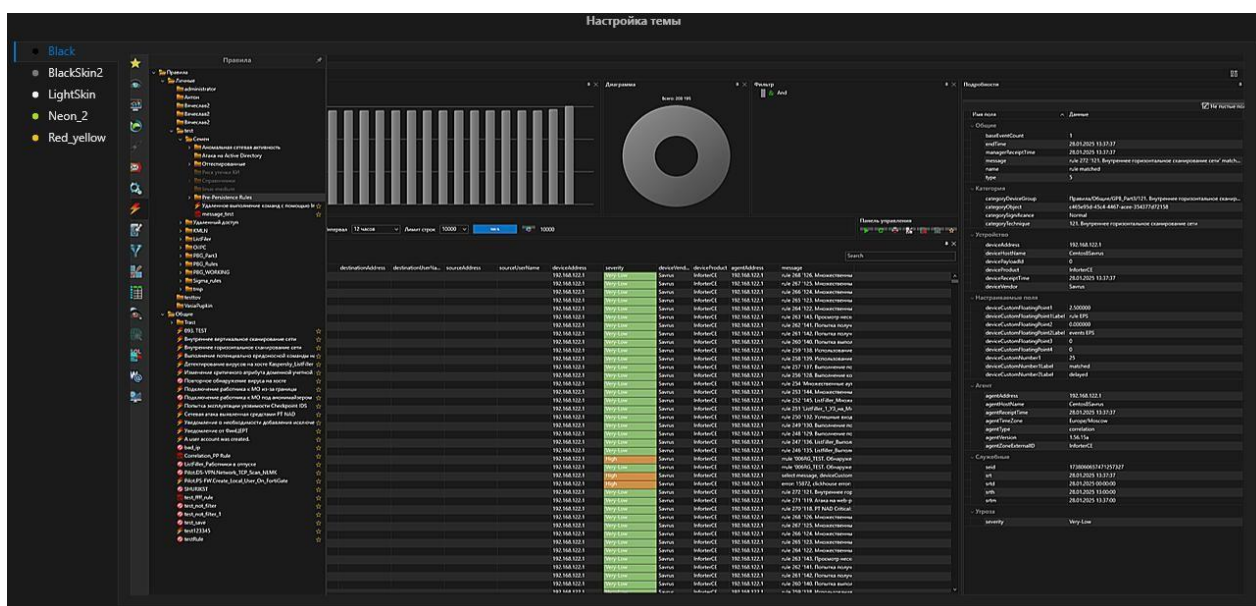
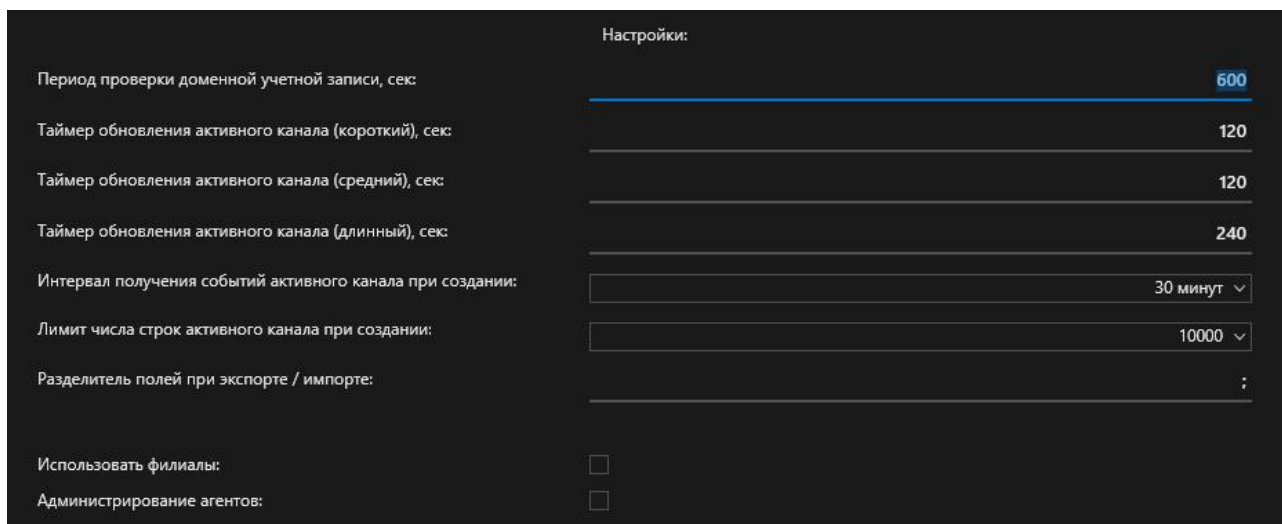


Рисунок 17. Окно "Настройка темы"

Для применения выбранной темы необходимо нажать на кнопку «Сохранить»  в верхней части окна «Администрирование».

6. Настройка параметров программы

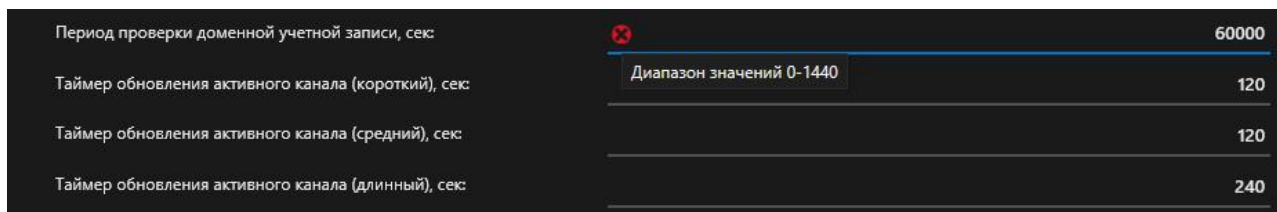
Функция "Параметры программы" предоставляет пользователю возможность настроить некоторые аспекты работы программы, оптимизируя ее производительность и удобство использования. Этот раздел содержит набор параметров, которые влияют на частоту обновления данных, ограничения объемов информации, интеграцию с другими системами.



Настройки:	
Период проверки доменной учетной записи, сек:	600
Таймер обновления активного канала (короткий), сек:	120
Таймер обновления активного канала (средний), сек:	120
Таймер обновления активного канала (длинный), сек:	240
Интервал получения событий активного канала при создании:	30 минут ▾
Лимит числа строк активного канала при создании:	10000 ▾
Разделитель полей при экспорте / импорте:	;
Использовать филиалы:	☐
Администрирование агентов:	☐

Рисунок 18. Параметры программы

При выходе за пределы допустимых значений для некоторых параметров программа будет отображать предупреждение, чтобы пользователь мог корректно скорректировать настройки. На скриншоте видно, что при вводе значения за пределами допустимого диапазона (например, 60000 вместо диапазона 0-1440) появляется красный крестик с текстовым сообщением о недопустимом значении. Это помогает избежать ошибок конфигурации и гарантирует, что все параметры установлены правильно.



Период проверки доменной учетной записи, сек:	✖ Диапазон значений 0-1440	60000
Таймер обновления активного канала (короткий), сек:		120
Таймер обновления активного канала (средний), сек:		120
Таймер обновления активного канала (длинный), сек:		240

Рисунок 19. Пример предела значения

Ниже приведены подробные описания каждого параметра:

Название	Описание	Значения по умолчанию	Предельные значения
Период проверки доменной учетной записи, сек	Эта функция позволяет установить интервал времени (в секундах), через который программа будет проверять статус доменной учетной записи пользователя.	600 секунд	0-1440
Таймер обновления активного канала (короткий), сек	Эта функция определяет частоту обновления данных в активном канале для короткого таймера.	120 секунд	0-1440
Таймер обновления активного канала (средний), сек	Эта функция устанавливает средний интервал обновления данных в активном канале.	120 секунд	0-1440
Таймер обновления активного канала (длинный), сек	Эта функция определяет длительный интервал обновления данных в активном канале.	240 секунд	0-1440
Интервал получения событий активного канала при создании	Эта функция задает периодичность получения событий из активного канала при его создании.	30 минут	
Лимит числа строк активного канала при создании	Эта функция ограничивает максимальное количество строк, которое может содержать активный канал при его создании.	10000 строк	
Разделитель полей при экспорте / импорте	Эта функция устанавливает символ, который будет использоваться для разделения полей при экспорте или импорте данных из Активного списка.	;	
Использовать филиалы	Данная функция включает режим мультитенантности		
Администрирование агентов	Данная функция включает режим управления агентами		

ЭЛЕМЕНТЫ ВЗАИМОДЕЙСТВИЯ С РЕСУРСАМИ

1. Функции контекстного меню

Взаимодействие с ресурсами консоли происходит через контекстное меню появляющееся при нажатии ПКМ. Основные функции контекстного меню:

Таблица 2. 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 на ресурс и их редактирования	
	Зависимость ресурсов	Предназначено для просмотра дерева ресурсов	
	Добавить в избранное	Предназначено для добавления в Избранное	
	Проверка ресурса	Предназначен для автоматической валидации ресурсов системы	

2. Права доступа

Система даёт возможность создать отчёт, выводящий права доступа к конкретному объекту (ресурсу) системы. Для этого достаточно нажать ПКМ по названию ресурса и в

контекстном меню выбрать пункт «Права доступа». В открывшемся диалоговом окне появиться список всех пользователей, имеющих доступ к ресурсу.

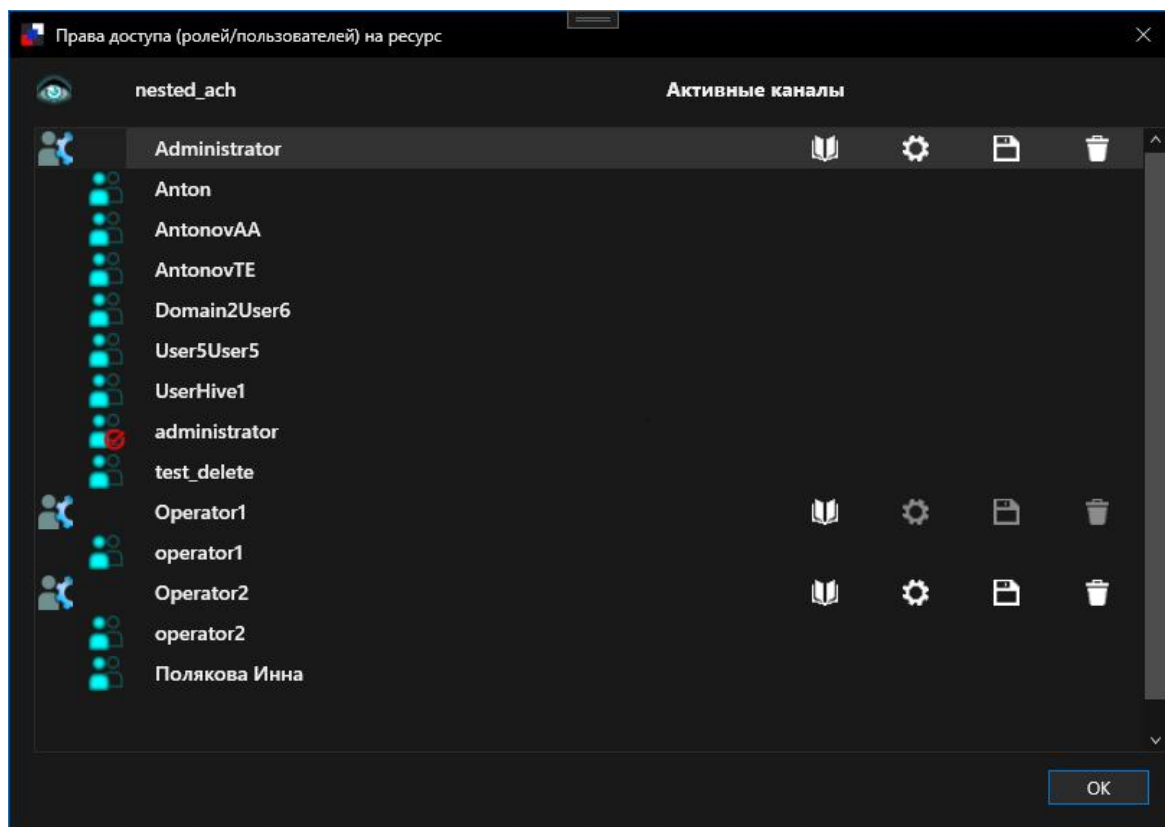


Рисунок 20. Окно настройки прав доступа

3. Экспорт и импорт ресурсов

Экспорт

Для экспорта ресурсов необходимо выбрать нужный ресурс в «Меню ресурсов», нажатием «ПКМ» по выбранному ресурсу вызвать контекстное меню и выбрать пункт меню «Экспорт» (см. Рисунок 21).

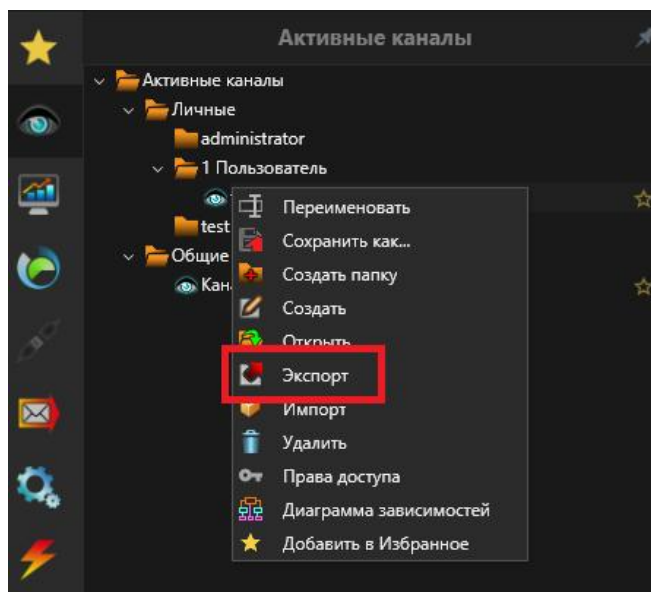


Рисунок 21. Расположение функции "Экспорт" в контекстном меню

Далее необходимо выбрать папку сохранения экспортируемого ресурса в вашей ОС и нажать кнопку «Сохранить». После сохранения ресурса, необходимо закрыть открывшееся окно «Экспорт» нажав на кнопку «ОК».

Импорт

Для импорта ресурсов необходимо вызвать контекстное меню нажатием «ПКМ» по любой из доступных папок в «Меню ресурсов» и в открывшемся меню выбрать пункт «Импорт» (см. Рисунок 22).

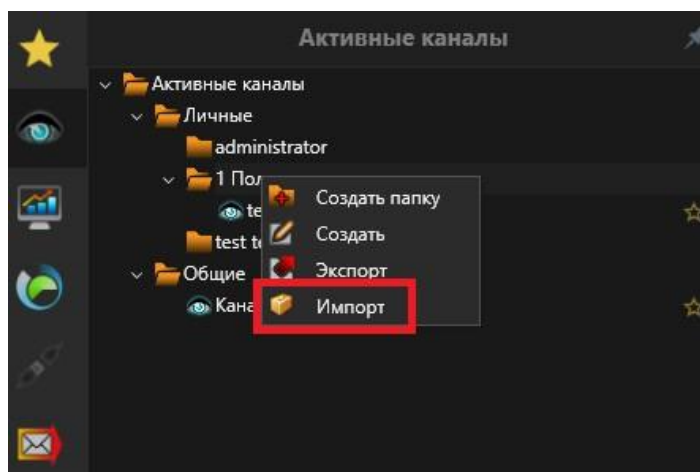


Рисунок 22. Расположение функции "Импорт" в контекстном меню

Далее необходимо выбрать ZIP архив импортируемого ресурса и нажать на кнопку «Открыть». Система самостоятельно определяет какой тип ресурса импортируется (правило, активный список и тд.) автоматически открывая директорию необходимую для сохранения данного ресурса.

В открывшемся окне (см. Рисунок 23) в правой стороне необходимо выбрать импортируемый ресурс, а в левой папку в консоли, в которую он будет сохранен.

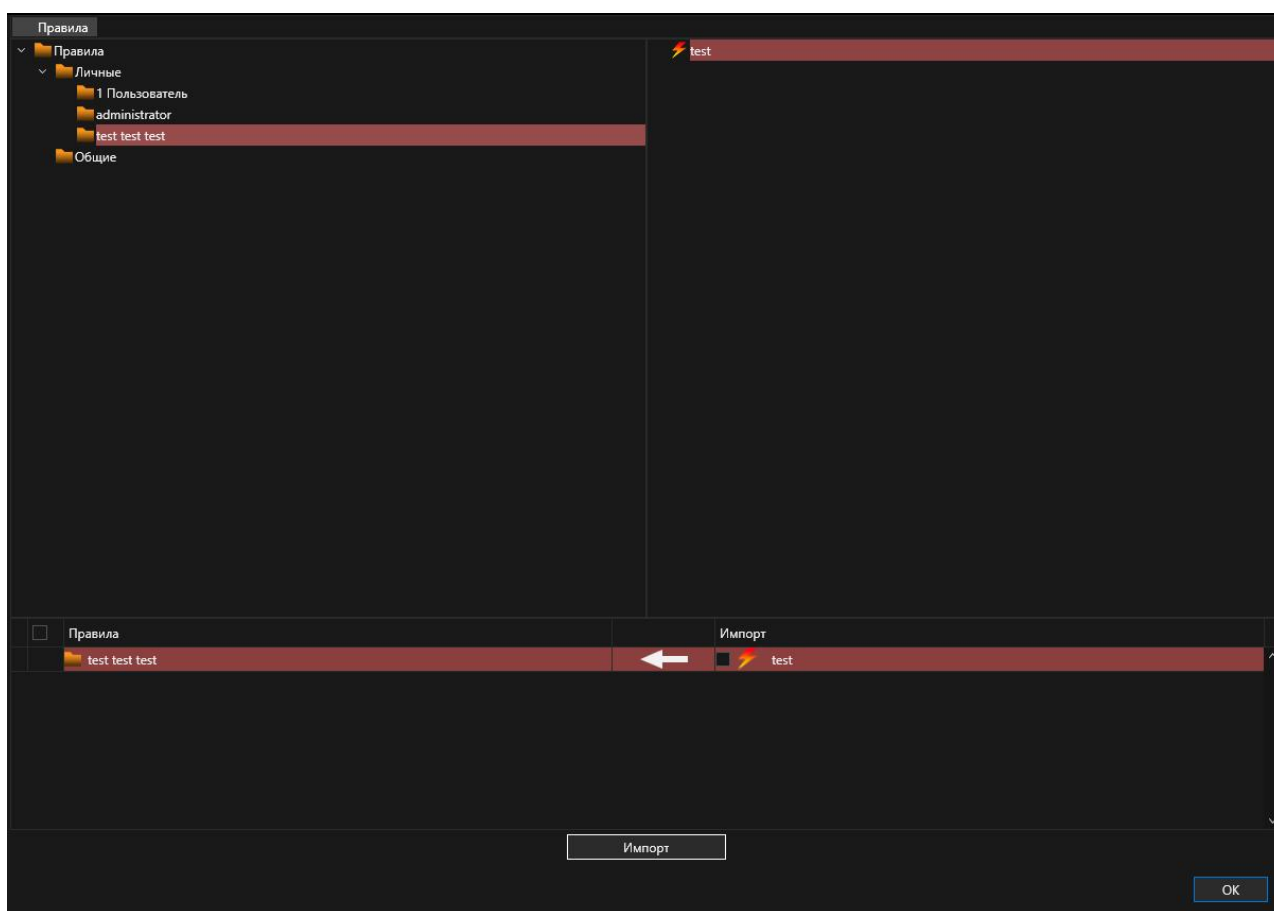


Рисунок 23. Окно импорта ресурсов

Далее нажать на кнопку «Импорт» в нижней части окна, после чего выбранный файл будет импортирован.

Если в выбранной для импорта папке содержится ресурс, совпадающий с названием импортируемого ресурса, то система отклонит импорт данного ресурса.

Для импорта ресурсов с совпадающим названием необходимо (см. Рисунок 24) в нижней части окна поставить галочку на функции «Заменить», находящуюся в столбце «Импорт» напротив импортируемого ресурса.

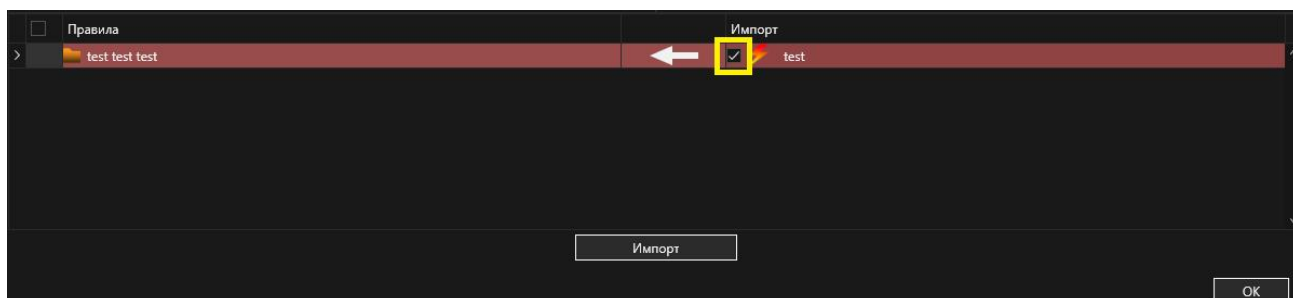


Рисунок 24. Расположение функции "Замена"

После нажать на кнопку «Импорт», тогда выбранный ресурс будет импортирован с заменой.

4. Просмотр истории изменений

В некоторых элементах консоли доступна функция «Показать историю».  Данная функция служит для просмотра сделанных ранее изменений в определённом ресурсе системы.

Эксплуатация данной функции будет описана далее на примере ресурса «Правила». В ресурсе «Правила» данная функция находится в разделе «Описание» (см. Рисунок 25). Активировать её можно нажатием ЛКМ по иконке.

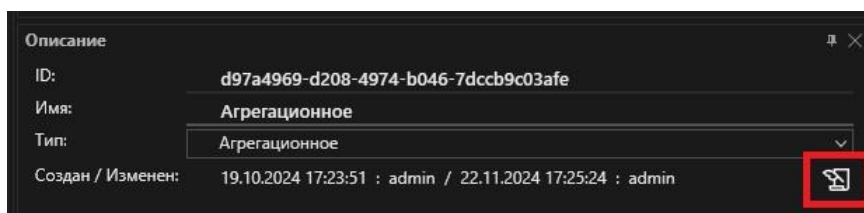
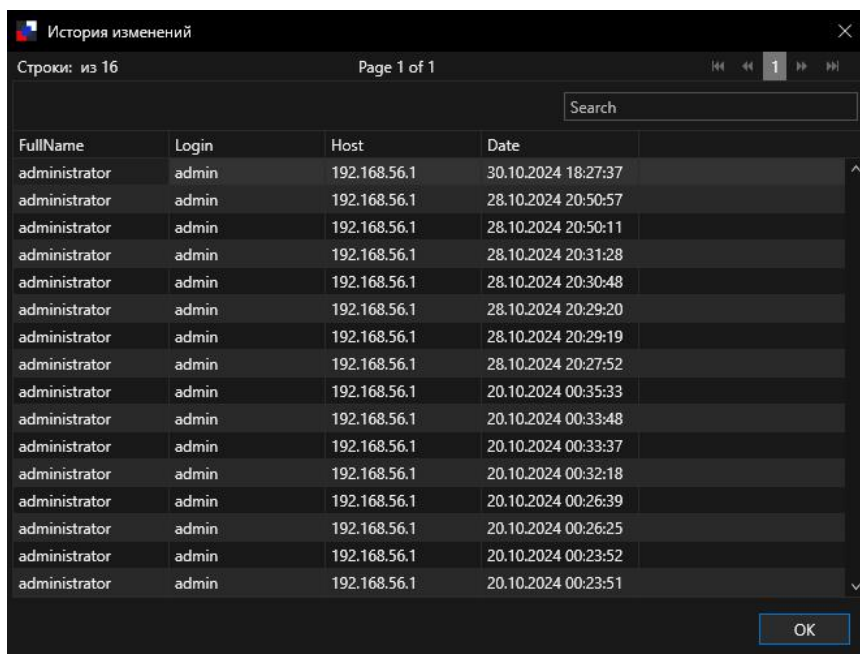


Рисунок 25. Расположение функции "Показать историю"

При активации данной функции появится окно «История изменений» (см. Рисунок 26).



FullName	Login	Host	Date
administrator	admin	192.168.56.1	30.10.2024 18:27:37
administrator	admin	192.168.56.1	28.10.2024 20:50:57
administrator	admin	192.168.56.1	28.10.2024 20:50:11
administrator	admin	192.168.56.1	28.10.2024 20:31:28
administrator	admin	192.168.56.1	28.10.2024 20:30:48
administrator	admin	192.168.56.1	28.10.2024 20:29:20
administrator	admin	192.168.56.1	28.10.2024 20:29:19
administrator	admin	192.168.56.1	28.10.2024 20:27:52
administrator	admin	192.168.56.1	20.10.2024 00:35:33
administrator	admin	192.168.56.1	20.10.2024 00:33:48
administrator	admin	192.168.56.1	20.10.2024 00:33:37
administrator	admin	192.168.56.1	20.10.2024 00:32:18
administrator	admin	192.168.56.1	20.10.2024 00:26:39
administrator	admin	192.168.56.1	20.10.2024 00:26:25
administrator	admin	192.168.56.1	20.10.2024 00:23:52
administrator	admin	192.168.56.1	20.10.2024 00:23:51

Рисунок 26. История изменений

В данном окне можно увидеть информацию о пользователях, которые вносили изменения с упоминанием адреса и точной датой изменения. Так же, в правой-верхней его части находятся: навигация по страницам и контекстный поиск (не зависимый от регистра).

При двойном нажатии ЛКМ на любую из ячеек в окне «История изменений», вас перенесёт на служебную панель с открытым окном «Сравнение ресурсов» (см. Рисунок 27). Для эксплуатации данного окна необходимо закрыть окно «История изменений».

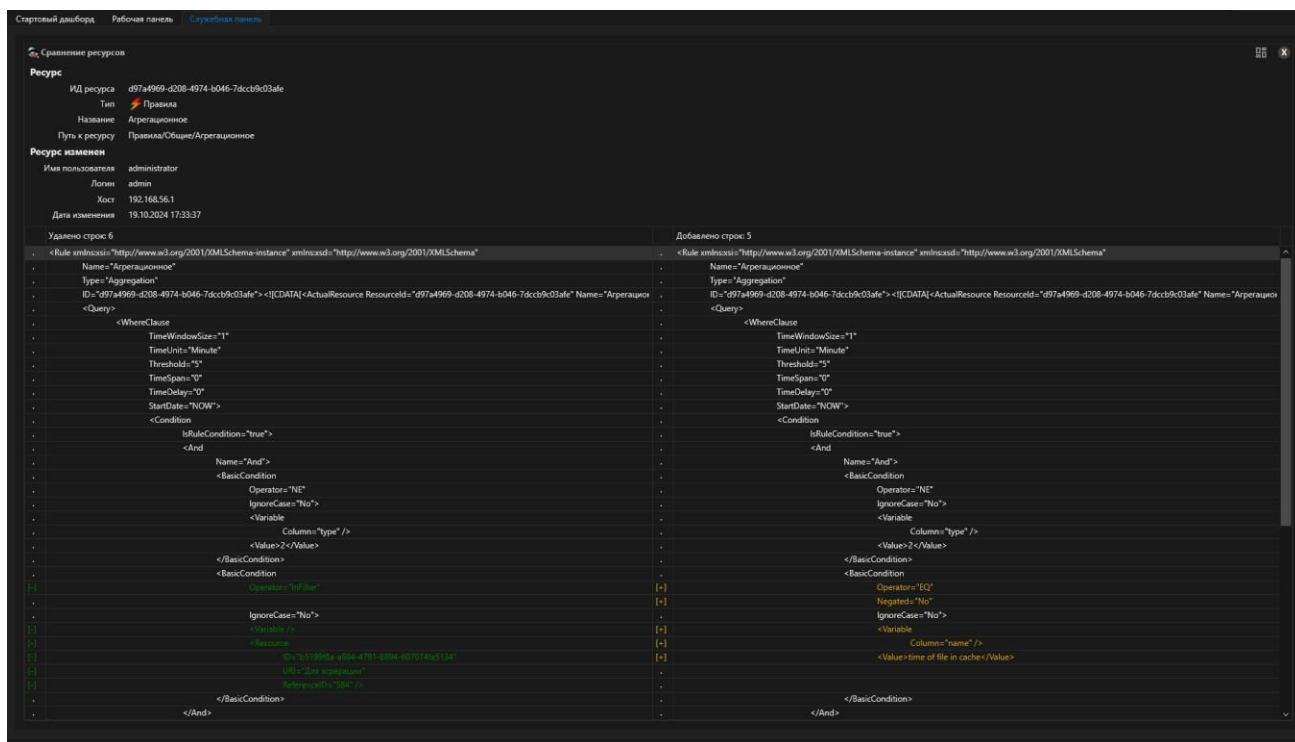


Рисунок 27. Окно "Сравнение ресурсов"

В верхней части окна находится информация о ресурсе и пользователе вносившим изменения.

В нижней, поделённой на две части, указано в каких количествах и какие именно изменения были внесены. Левая часть показывает правило до внесения в него изменений, правая – после. В заголовках обеих сторон расположена информация о кол-ве изменённых строк в данном правиле. Зелёным цветом показаны удалённые строки, жёлтым – добавленные.

Чтобы выйти из окна «Сравнение ресурсов», необходимо: либо перейти на рабочую панель в левом верхнем углу консоли, либо закрыть окно нажатием ЛКМ на иконку закрытия в правом верхнем углу служебной панели (см. Рисунок 28).

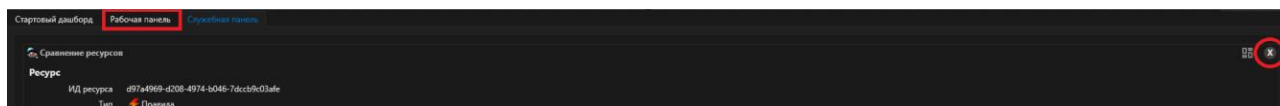


Рисунок 28. Способы закрытия окна "Сравнение ресурсов"

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 в появившемся меню выбрать «Добавить в Избранное» или нажать ЛКМ на кнопку . После чего выбранные ресурсы появятся в списке во вкладке «Избранное», а так же будет отмечен знаком  в общем древе ресурсов.

Управлять статусом избранного ресурса можно и из окна редактирования ресурса. При нажатии на кнопку «Избранное» в открытом окне редактирования ресурса у данного ресурса сменится статус членства в списке «Избранное», но это не приведет к сохранению открытого ресурса.

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

АКТИВНЫЕ КАНАЛЫ

1. Основные элементы активного канала

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

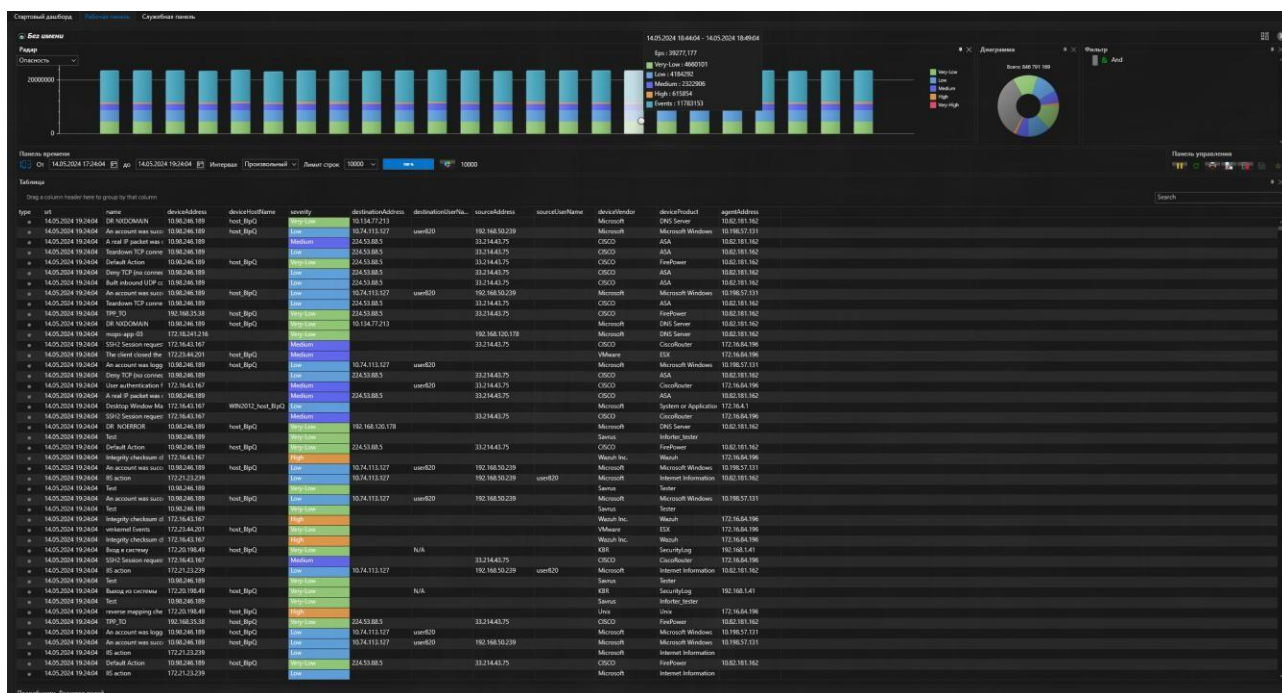


Рисунок 29. Пример Активного канала

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 30), Производитель (по производителям см. Рисунок 31), Продукт (по продуктам), Тип (по типам событий). Для смены типа группировки радара следует в верхнем левом углу выбрать необходимый в выпадающем списке.

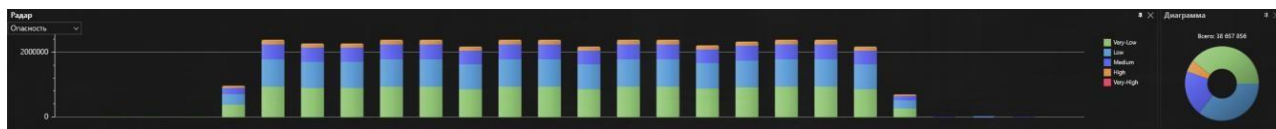


Рисунок 30. Пример Радара по уровню опасности

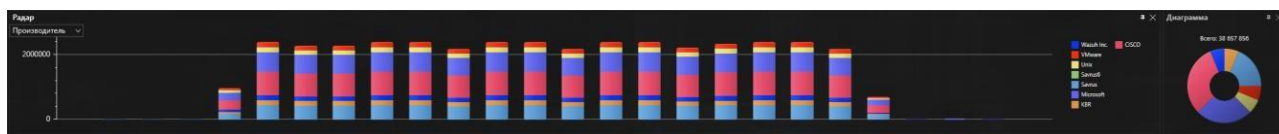


Рисунок 31. Пример Радара по производителям

Таблица АК

Основной элемент отображения событий — это таблица, в которую выводятся все необходимые поля событий ИБ (см. Рисунок 32).

type	deviceName	severity	src	destinationAddress	sourceUser	name	destinationUser	sourceAddress	deviceAddress	deviceProduct	deviceVendor	agentAddress
DESKTOP-RT04LD	192.168.1.1047	12.01.2024 19:10:47	admin	Open object	192.17.253.1	Samsung	Samsung					
DESKTOP-RT04LD	192.168.1.1047	12.01.2024 19:10:47	admin	Login subsystem	192.17.253.1	Samsung	Samsung					
DESKTOP-RT04LD	192.168.1.1047	12.01.2024 19:10:47	admin	Unlogon subsystem	192.17.253.1	Samsung	Samsung					
DESKTOP-RT04LD	192.168.1.1047	12.01.2024 19:10:47	admin	Open object	192.17.253.1	Samsung	Samsung					
DESKTOP-RT04LD	192.168.1.1047	12.01.2024 19:10:47	admin	Unlogon subsystem	192.17.253.1	Samsung	Samsung					
DESKTOP-RT04LD	192.168.1.1047	12.01.2024 19:10:47	admin	Login subsystem	192.17.253.1	Samsung	Samsung					
DESKTOP-RT04LD	192.168.1.1047	12.01.2024 19:10:47	admin	Unlogon subsystem	192.17.253.1	Samsung	Samsung					
CentosServer	192.168.1.1039	12.01.2024 19:10:39	main	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1038	12.01.2024 19:10:38	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1037	12.01.2024 19:10:37	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1037	12.01.2024 19:10:37	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1037	12.01.2024 19:10:37	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1036	12.01.2024 19:10:36	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1036	12.01.2024 19:10:36	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1036	12.01.2024 19:10:36	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1035	12.01.2024 19:10:35	rule time statistics	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1035	12.01.2024 19:10:35	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1035	12.01.2024 19:10:35	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1034	12.01.2024 19:10:34	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1034	12.01.2024 19:10:34	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1034	12.01.2024 19:10:34	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1034	12.01.2024 19:10:34	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1033	12.01.2024 19:10:33	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1033	12.01.2024 19:10:33	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1033	12.01.2024 19:10:33	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1033	12.01.2024 19:10:33	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1032	12.01.2024 19:10:32	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1032	12.01.2024 19:10:32	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1032	12.01.2024 19:10:32	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1032	12.01.2024 19:10:32	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1031	12.01.2024 19:10:31	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1031	12.01.2024 19:10:31	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1031	12.01.2024 19:10:31	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1031	12.01.2024 19:10:31	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1030	12.01.2024 19:10:30	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1030	12.01.2024 19:10:30	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1030	12.01.2024 19:10:30	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1030	12.01.2024 19:10:30	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1029	12.01.2024 19:10:29	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1029	12.01.2024 19:10:29	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1029	12.01.2024 19:10:29	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1029	12.01.2024 19:10:29	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1028	12.01.2024 19:10:28	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1028	12.01.2024 19:10:28	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1028	12.01.2024 19:10:28	Microsoft Windows	CPH45	192.168.1.12	Microsoft Windows	Microsoft	192.168.1.12	192.168.1.12			
CentosServer	192.168.1.1028	12.01.2024 19:10:28	rule matched	192.168.1.12	Infected	Infected	192.168.1.12	192.168.1.12	192.168.1.12			

Рисунок 32. Активный канал в табличном представлении

Также возможно отображения событий ИБ в виде различного рода сгруппированных диаграмм и таблиц (см. Рисунок 33) для этого необходимо нажать на кнопку , для отмены кнопки — .



Рисунок 33. Активный канал в виде диаграмм

2. 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 34).

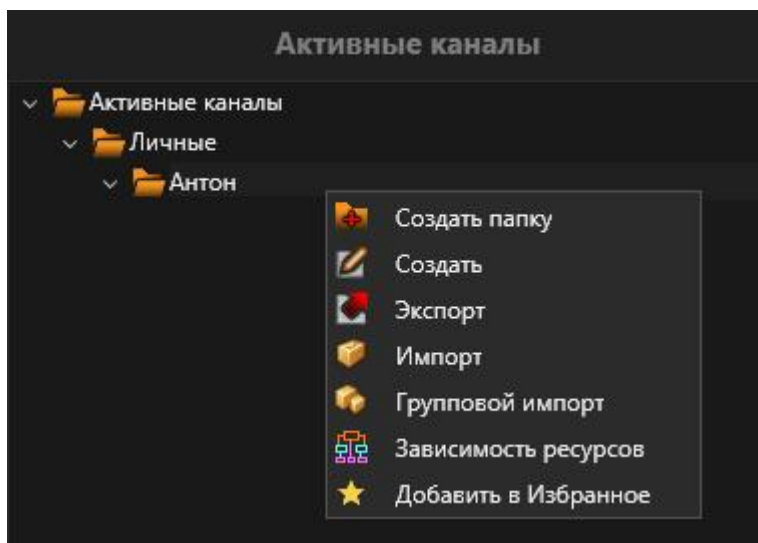


Рисунок 34. Меню Активного канала

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 3. 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 произвольном 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 «ОК». 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 .

3. Изменение временного интервала и количества записей

В АК можно менять временной диапазон и количество записей, для этого используется Панель времени (см. Рисунок 35).



Рисунок 35. 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 независимости от выбранного временного диапазона доступна функция выбора количества 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.

4. 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 36). 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.

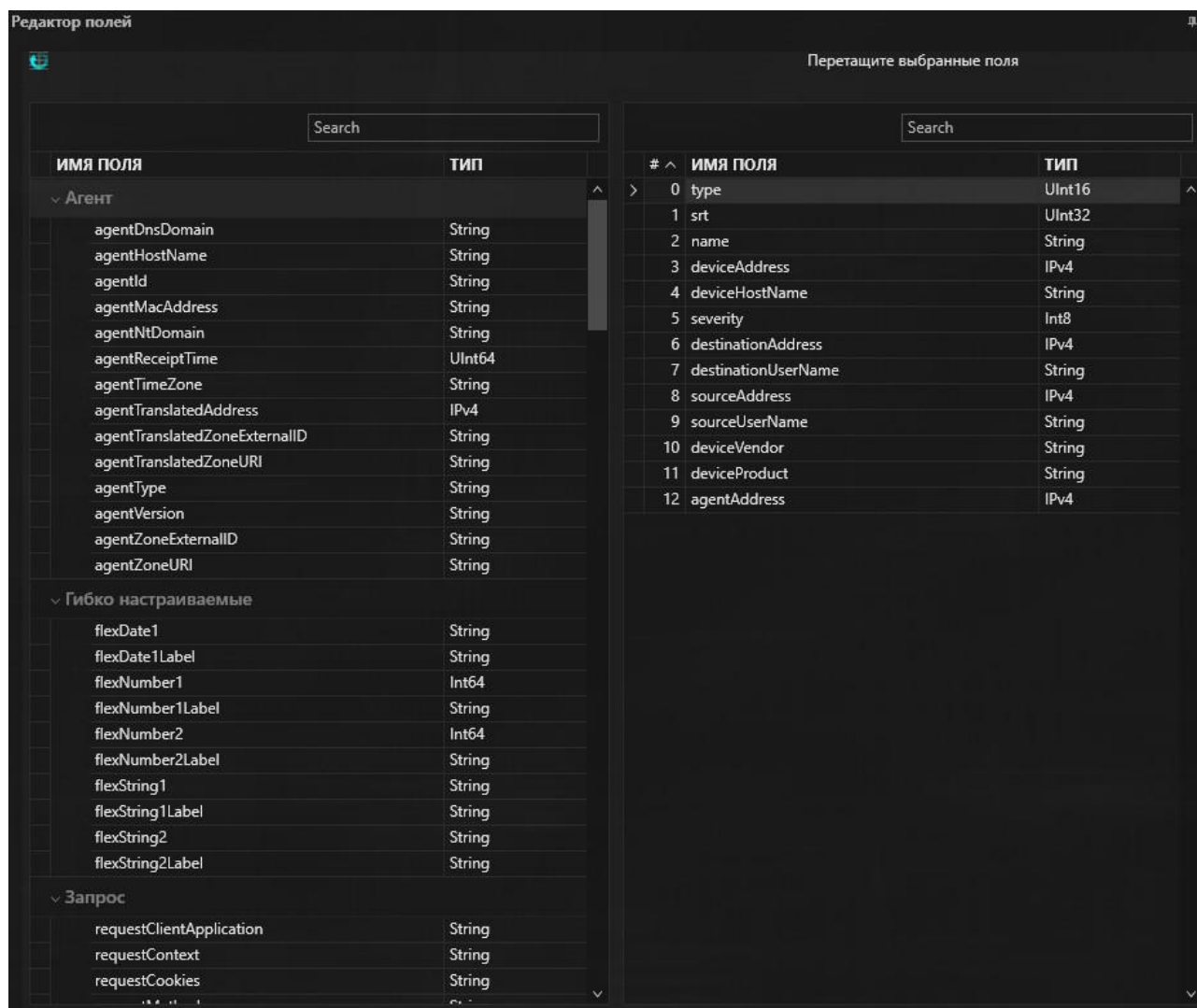


Рисунок 36. Редактор полей

В верхней части редактора запросов расположен элемент поиска полей данных по названию (см. Рисунок 37). Поисковые запросы полей не чувствительны к регистру.

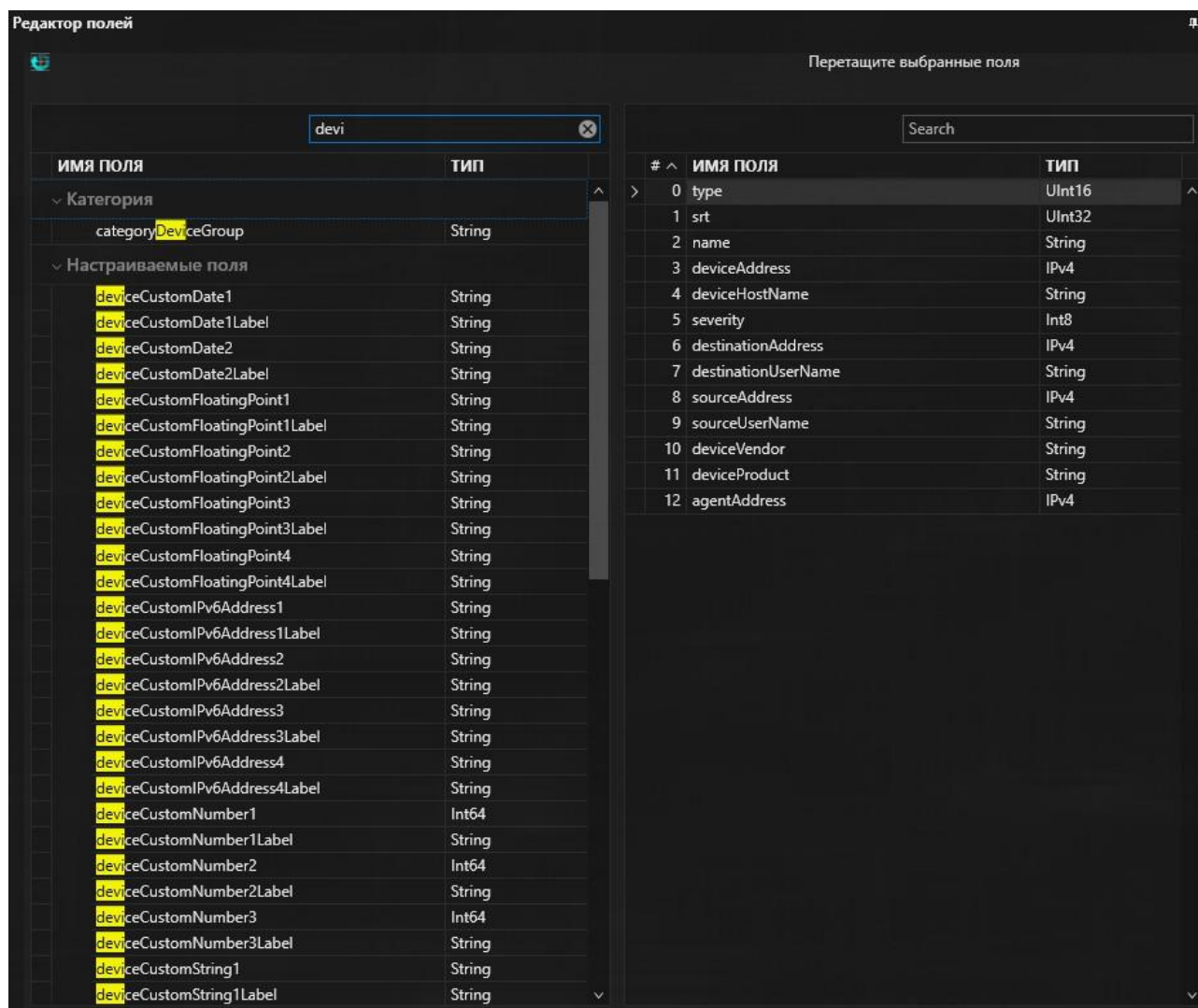


Рисунок 37. Пример поиска

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



При работе с активным каналом стоит обратить внимание на поле «type». В активном канале оно отображается в числовых значениях. Каждому событию присваивается свое число. Список постепенно расширяется. Ниже представлено соотношение чисел и типов событий.

- 0 – базовое
- 1 – сегрегированное из ArcSight
- 2 – корреляционное (online)

- 4 – корреляционное (retrospective)
- 5 – служебное событие

5. 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 38), и дважды щёлкнуть ЛКМ по полю условия.

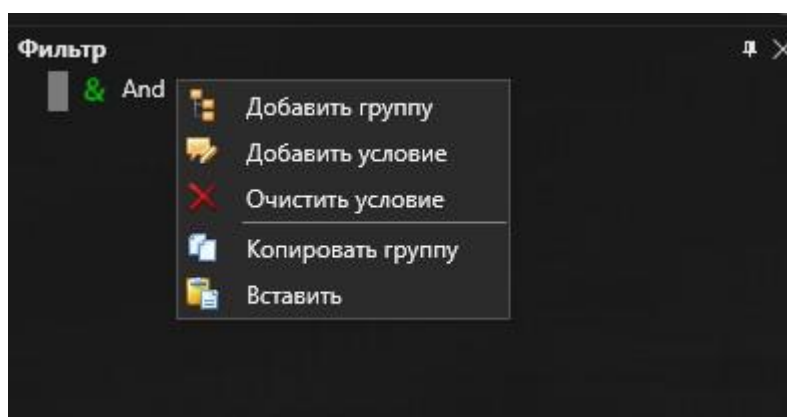


Рисунок 38. Контекстное меню редактора условий

После чего откроется диалоговое окно «Редактирования условий» (см. Рисунок 39) 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 «ОК». Для удаления условия необходимо нажать по нему ПКМ и в контекстном меню выбрать пункт «удалить условие».

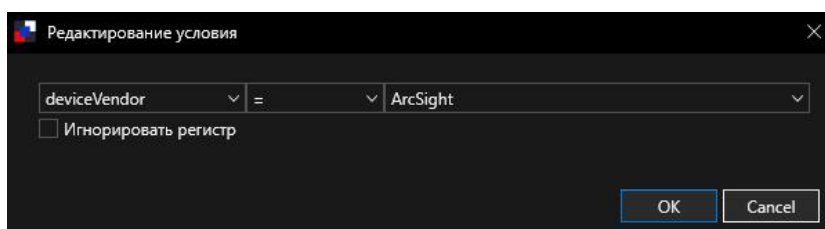


Рисунок 39. Редактирование условий

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.



Рисунок 40. Пример условия

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

6. 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 41) представлен с открытыми АК для быстрого переключения между ними.

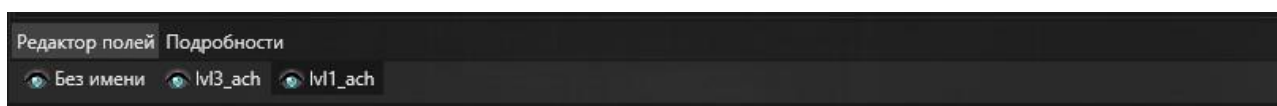
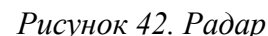


Рисунок 41. Перечень вкладок

Инфографика событий/радар (см. Рисунок 42). 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.



A screenshot of the Windows 10 taskbar. On the left is the Start button. Next to it are several pinned taskbar icons: a green play button, a green circular arrow, a printer, a document with a pencil, a document with a red X, a document with a magnifying glass, a document with a list, and a yellow star. On the right side of the taskbar is the system tray, which includes a speaker icon, a close button (X), and a search bar with the text "Search".

Рисунок 43. Поиск в таблице АК

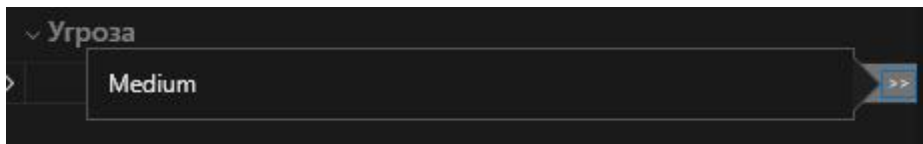
The screenshot displays the Windows Task Manager Performance tab. At the top, a bar chart shows the usage of various system resources over time, with a legend indicating CPU (blue), Memory (orange), Disk (green), Network (red), and GPU (purple). Below the chart, a circular progress indicator shows the overall system health. The main area is a table of running processes, with columns for Name, PID, Session Name, Description, Company Name, Architecture, and Status. The table lists various system processes, including System, smss.exe, csrss.exe, explorer.exe, and many others, along with their respective PIDs and session names.

Name	PID	Session Name	Description	Company Name	Architecture	Status
System	4	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System	System	Microsoft Windows	x64	Running
explorer.exe	160	System	System	Microsoft Windows	x64	Running
System	160	System	System	Microsoft Windows	x64	Running
smss.exe	160	System	System	Microsoft Windows	x64	Running
csrss.exe	160	System				

Рисунок 44. Пример активного канала с разделом "Подробности"

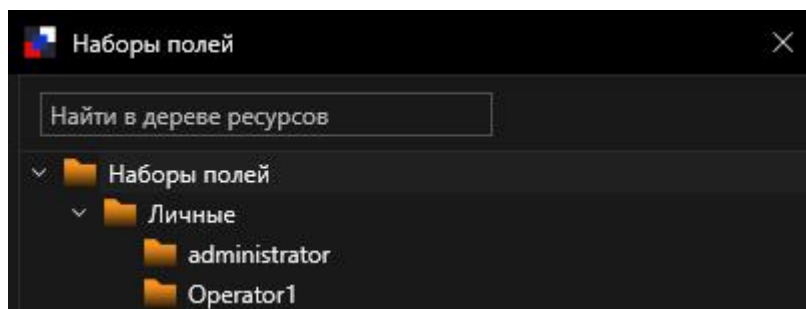
Для детального просмотра события необходимо дважды щёлкнуть по событию, представленному в таблице. Поля события объединены по логическим группам и отсортированы по алфавиту (см. Рисунок 45). При нажатии на кнопку  открывается

полное содержимое поля. Эта функция предназначена для удобной работы с данными, содержащими большое количество символов, а также упрощает копирование информации из поля.



Так же в правом-верхнем углу окна «Подробности» можно убрать галочку с функции «Не пустые поля». После выключения данной функции в окне отобразятся все доступные поля.

В окне «Подробности события» доступна возможность применить ранее созданный набор полей. Для этого следует нажать кнопку  «Добавить набор полей» и в открывшемся окне выбрать нужный набор.



Подробности

☒ Не пустые поля

Search

Имя поля	Данные
Общие	
baseEventCount	1
endTime	02.08.2025 15:24:59.071
managerReceiptTime	02.08.2025 15:24:59.071
message	remove old file '/opt/inforter/data/1754136834_...
name	check_old_files
type	5
Устройство	
deviceAddress	172.16.42.187
deviceHostName	ad.savrus
deviceProduct	Inforter
deviceReceiptTime	02.08.2025 15:24:59.071
deviceVendor	Savrus
Агент	
agentAddress	172.16.42.187
agentHostName	ad.savrus
agentName	Inforter
agentReceiptTime	02.08.2025 15:24:59.071
agentTimeZone	Europe/Moscow
agentType	correlation
agentVersion	2.4.3
Служебные	
seid	1754137511139276173
srt	02.08.2025 15:25:11.000
srtid	08.02.2025 00:00:00
srth	02.08.2025 15:00:00.000
srtm	02.08.2025 15:25:00.000
Угроза	
severity	Medium

Рисунок 45. Описание события

На представленном ниже скриншоте показано контекстное меню для взаимодействия с событиями, которое отображается при нажатии правой кнопкой мыши (ПКМ) на событие. Меню предоставляет пользователю гибкие возможности для фильтрации, анализа и экспорта данных события. Оно предназначено для быстрой настройки обработки информации без необходимости перехода в дополнительные окна или разделы системы.

Интерфейс структурирован логически: сначала идут условия фильтрации, затем действия по созданию каналов обработки событий, и далее операции по экспорту или отправке данных. Это позволяет специалисту эффективно реагировать на события, быстро настраивать правила их обработки и интегрировать с другими системами.

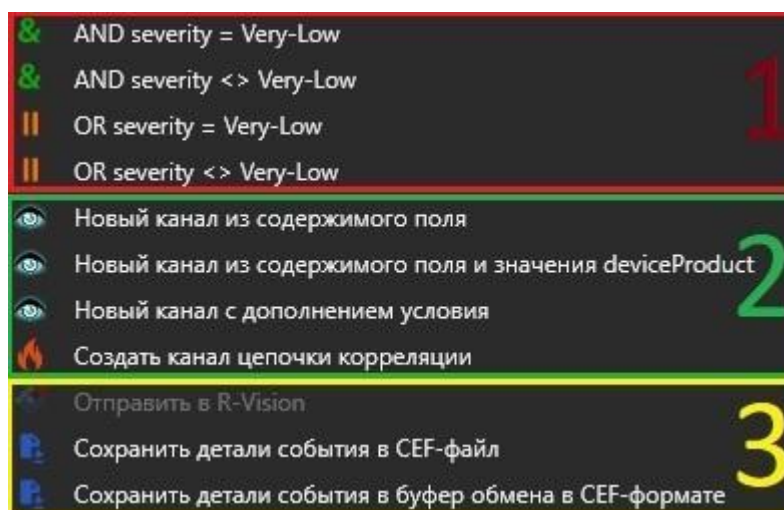


Рисунок 46. Меню взаимодействия

Ниже описаны основные функции данного меню:

1. Фильтрация событий

Фильтры позволяют выбирать события на основе определённых критериев. Доступные условия можно комбинировать с помощью логических операторов AND и OR. Выбранное условие автоматически отобразится в конструкторе условий.

- AND «поле» = «значение»

Добавляет в параметры фильтра условие «И», при котором поле будет равно значению.

- AND «поле» $\neq$ «значение»

Добавляет в параметры фильтра условие «И», при котором поле будет не равно значению.

- OR «поле» = «значение»

Добавляет в параметры фильтра условие «ИЛИ», при котором поле будет равно значению.

- OR «поле» $\diamond$ «значение»

Добавляет в параметры фильтра условие «ИЛИ», при котором поле будет не равно значению.

2. Создание новых каналов

Раздел предлагает инструменты для создания динамических каналов обработки событий потоков данных, основанных на значениях полей событий.

- Новый канал из содержимого поля

Автоматически создаёт канал, разделяющий события по уникальным значениям выбранного поля.

- Новый канал из содержимого поля и значения deviceProduct

Создаёт более точный канал, используя комбинацию поля и значения deviceProduct.

- Новый канал с дополнением условия

Позволяет создать канал, дополнив текущее условие новыми критериями.

- Создать канал цепочки корреляции

3. Экспорт и отправка данных

- Отправить в R-Vision

Отправка инцидентов в системы класса SOAR

- Сохранить детали события в CEF-файл

Экспортирует полную информацию о событии в файл формата CEF.

- Сохранить детали события в буфер обмена в CEF-формате

Копирует данные события в буфер обмена в формате CEF.

7. Редактирование активного канала

Для редактирования АК необходимо открыть нужный канал, подробное описание открытия представлено в разделе «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 47). Данный фильтр отображает значения в данной колонке уже созданного канала.

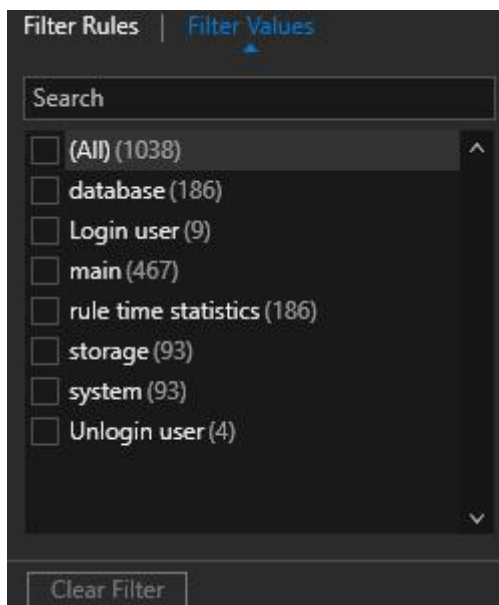


Рисунок 47. Диалоговое окно фильтра

В случае необходимости сохранения изменений следует нажать на кнопку .

Для фильтрации и сортировки событий в АК, необходимо ПКМ щёлкнуть по названию полей и в контекстном меню выбрать необходимую функцию (см. Рисунок 48).

Перечень функций для сортировки/фильтрации событий:

- Sort Ascending – сортировка по алфавиту от А до Z;
- Sort Descending – сортировка по алфавиту от Z до А;
- 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.

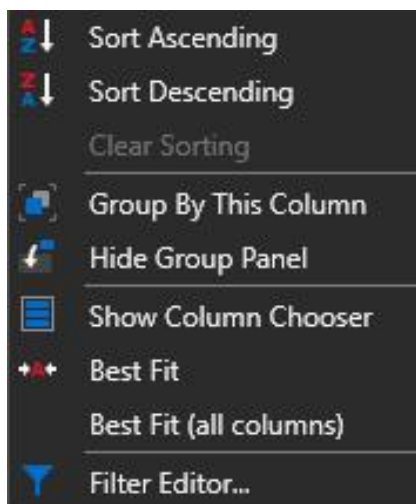


Рисунок 48. Фильтрация и сортировка

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 49). Принцип создания фильтра похож на создание условия, необходимо выбрать логический оператор, а после чего в выпадающем списке выбрать пункт «Добавить условие».

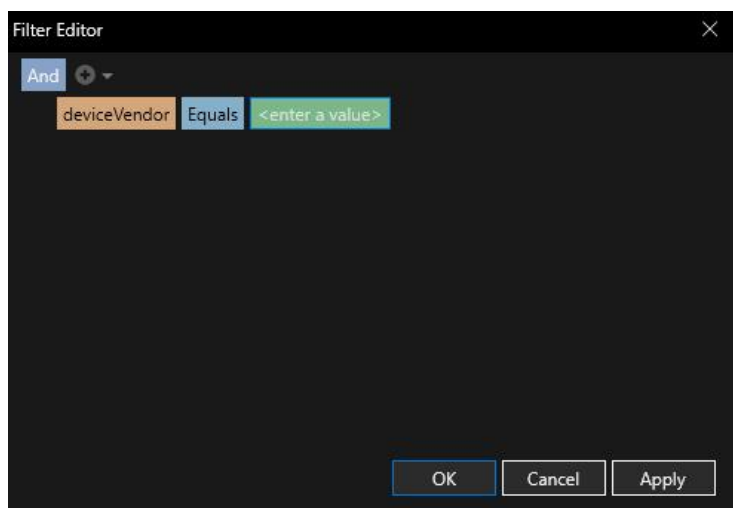


Рисунок 49. Диалоговое окно создание фильтра

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 50).

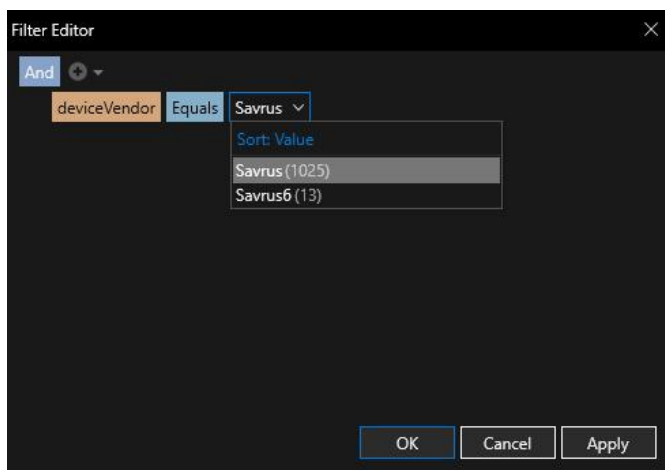


Рисунок 50. Выбор значения из предложенных вариантов

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 51) и в новой группе сменить оператора.

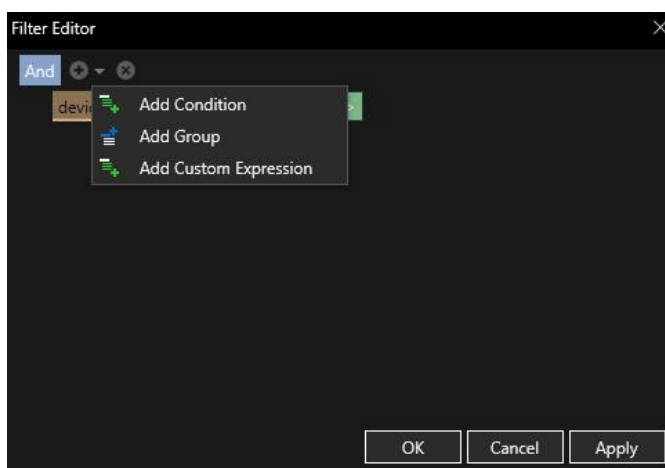


Рисунок 51. Выпадающий список

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

Для отмены фильтрации нажать на кнопку «Cancel», 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 52). Если необходимо группировать события внутри уже сгруппированных событий, следует повторить процедуру и события перейдут на следующий уровень группировки.

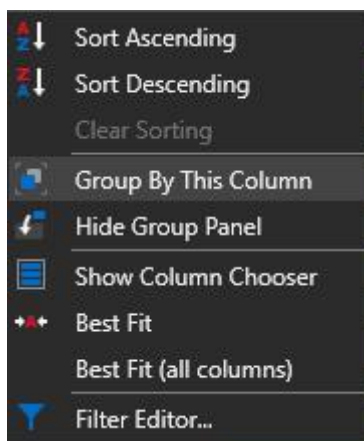


Рисунок 52. Контекстное меню группировки

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.

Таблица

deviceVendor ^

type	srt	deviceHostName	severity	sourceUserName
> deviceVendor: Savrus				
> deviceVendor: Savrus6				

Рисунок 53. 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 Expand» 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 А до Z, а при повторном нажатии сортировка от Z до А.

«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 54).

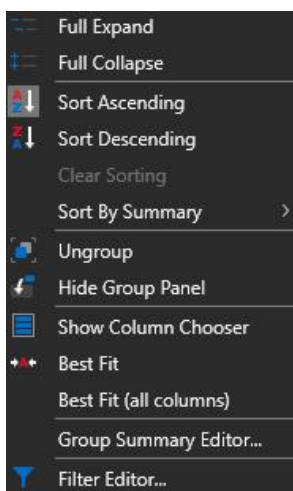


Рисунок 54. Контекстное меню элемента панели группировки

После чего откроется окно «Group Summaries», в котором необходимо поставить галочку у поля «Show row count» и нажать кнопку «ОК» (см. Рисунок 55).

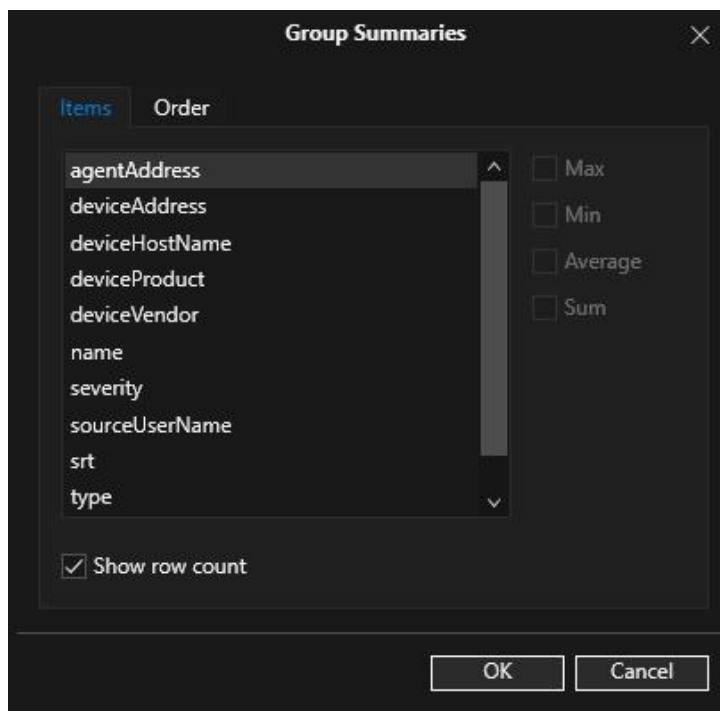


Рисунок 55. Окно редактора группировки

Пример группировки с подсчётом количества событий представлен на рисунке ниже.

Таблица									
severity	^								
type	srt	name		deviceAddress	deviceHostName	severity	^	destinationAddr...	destinationUser...
severity: Low									Count=80
severity: Medium									Count=483
severity: Very-High									Count=3
severity: Very-Low									Count=9434

Рисунок 56. 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 57).

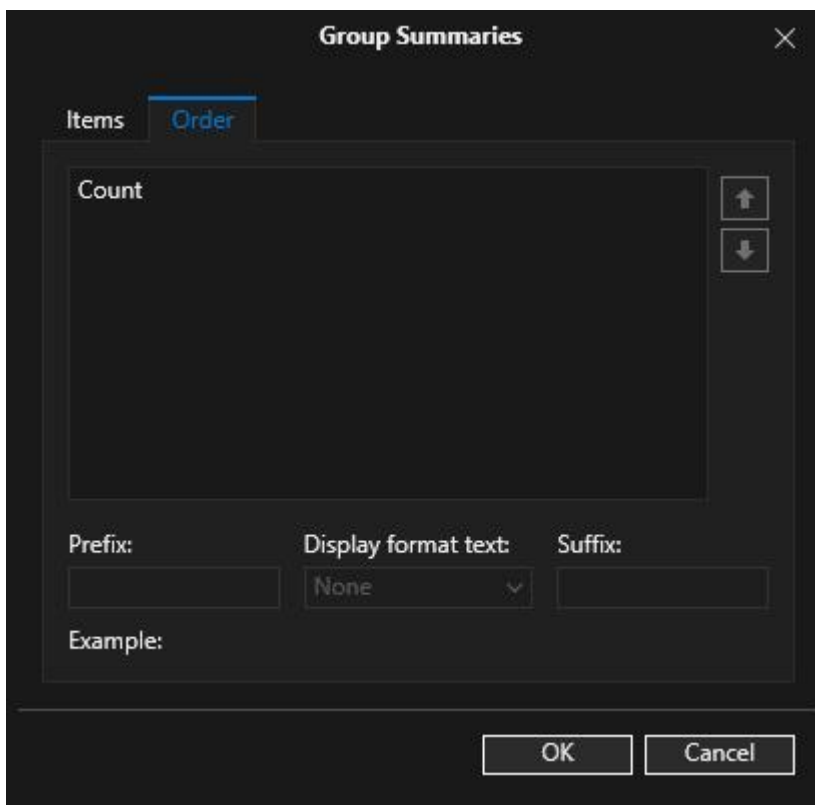


Рисунок 57. Редактор группировки

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.*

8. 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 58). После внесения изменений в настройки АК необходимо нажать на кнопку .

Настройки:	
Период проверки доменной учетной записи, сек:	600
Таймер обновления активного канала (короткий), сек:	120
Таймер обновления активного канала (средний), сек:	120
Таймер обновления активного канала (длинный), сек:	240
Интервал получения событий активного канала при создании:	30 минут ▾
Лимит числа строк активного канала при создании:	10000 ▾

Рисунок 58. Локальные настройки

9. 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 59). После внесения изменений в настройки АК необходимо нажать на кнопку .

Параметры сервера:	
Максимальное количество строк в активном списке:	10000
Таймаут бездействия пользователя, мин:	120

Рисунок 59. Глобальные настройки

АКТИВНЫЕ СПИСКИ

1. Создание активного списка

Для создания нового активного списка необходимо перейти на вкладку «Активные списки». Далее, нажав ПКМ на папку, выбрать кнопку «Создать» (см. Рисунок 60).

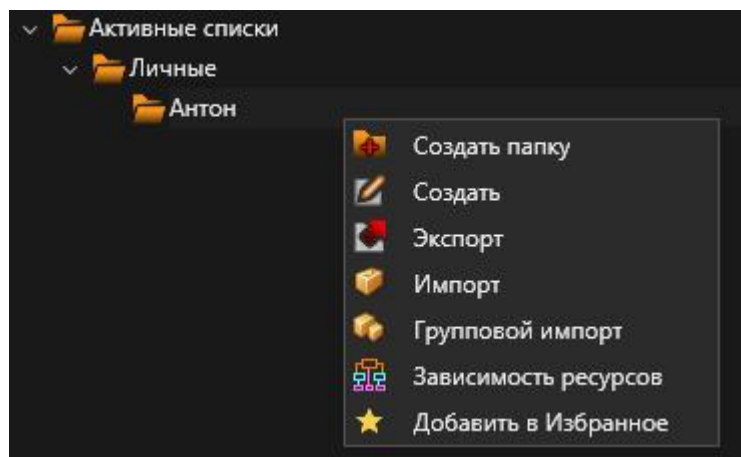
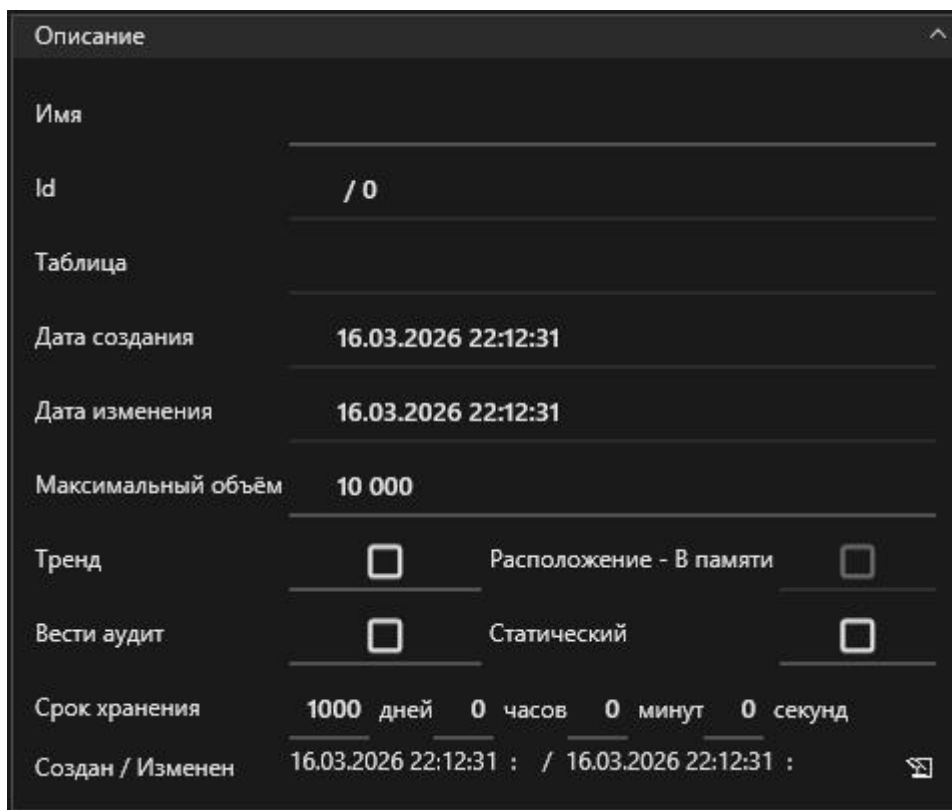


Рисунок 60. Дерево ресурсов АС

Далее, необходимо ввести параметры активного списка (см. Рисунок 61) в соответствии с Таблица 4. Параметры активного списка и создать его структуру.



Описание

Имя: _____

Id: _____ / 0

Таблица: _____

Дата создания: 16.03.2026 22:12:31

Дата изменения: 16.03.2026 22:12:31

Максимальный объем: 10 000

Тренд: ☐ Расположение - В памяти: ☐

Вести аудит: ☐ Статический: ☐

Срок хранения: 1000 дней 0 часов 0 минут 0 секунд

Создан / Изменен: 16.03.2026 22:12:31 : / 16.03.2026 22:12:31 : 

Рисунок 61. Параметры АС

Параметры активного списка указаны в таблице Таблица 4. Параметры активного списка.

Таблица 4. 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.	Расположение – В памяти	Размещение АС в оперативной памяти. Используется в АС, где важна высокая скорость обработки, но длительное хранение данных не требуется	Опционально

8.	Тренд	Таблица, которая обеспечивает длительное хранение данных.	При включении данной функции доступно только добавление записей вручную или с помощью правил корреляции. Удаление выборочных записей обеспечивается только по TTL средствами «ClickHouse». Место хранения трендов – таблицы «ClickHouse»
9.	Вести аудит	Ведение аудита АК	Опционально
10.	Статистический	Статистические списки предназначены для объёмных, редко изменяемых АС. Это позволяет меньше нагружать модуль корреляции	
11.	Срок хранения (сек)	Время хранения данных до ротации	По окончании периода данные стираются
12.	Создан/Изменен	Дата создания и последнего изменения Активного списка	

Для создания структуры активного списка необходимо в разделе «Создание» нажать ПКМ по свободному месту и выбрать «Добавить строку» (см. Рисунок 62).

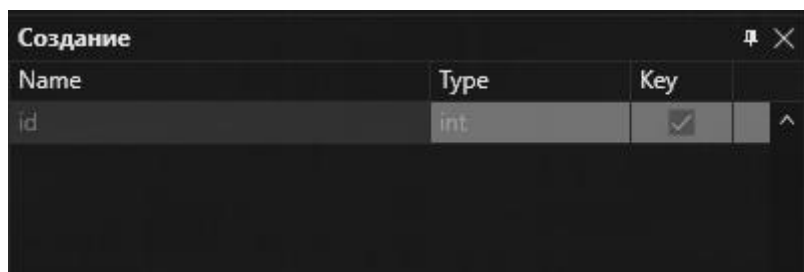


Рисунок 62. Окно добавления столбцов в активный список

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 63).



Рисунок 63. Настройка строки активного списка

Для удаления столбца из активного списка необходимо нажать ПКМ по созданному столбцу и нажать «Удалить» (см. Рисунок 64).

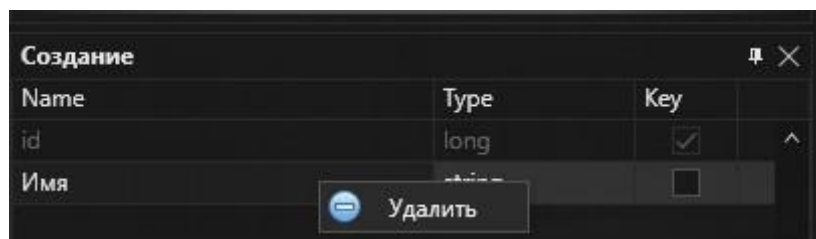


Рисунок 64. Удаление столбца

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 65).

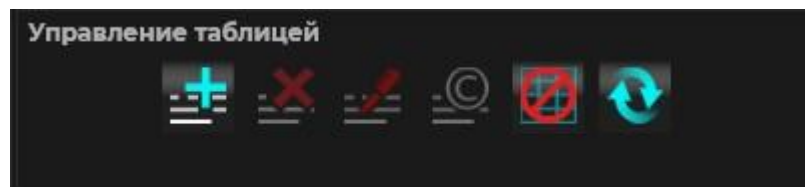


Рисунок 65. Редактирование активного списка

В открывшемся окне следует заполнить столбец «Value» необходимыми значениями. После заполнения активного списка данными необходимо нажать кнопку «ОК» (см. Рисунок 66).

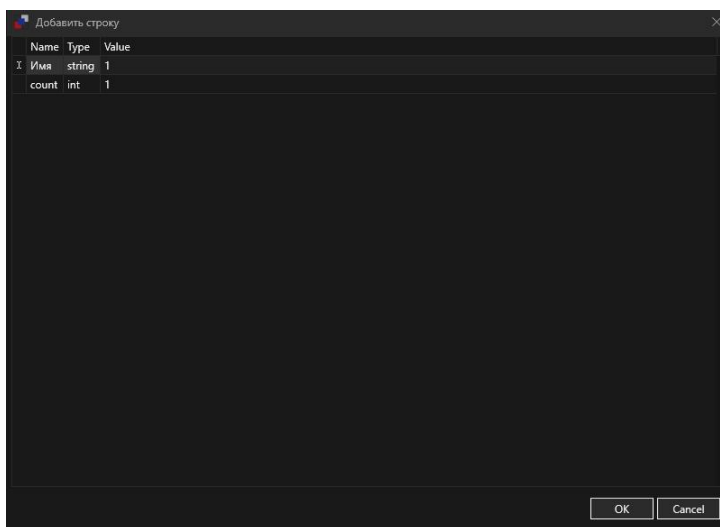


Рисунок 66. Окно изменения строки

2. Наполнение активного списка

При нажатии ПКМ на строку в таблице активного списка появляется контекстное меню взаимодействия со строками (см. Рисунок 67). Меню предназначено для работы с логическими условиями. Также меню предоставляет пользователю возможности редактирования, копирования и удаления сток в активном списке. Меню также включает функции "Копировать ячейку в буфер обмена" и "Копировать строку в буфер обмена", которые обеспечивают удобство работы с данными. Эти опции позволяют пользователю быстро скопировать как отдельные элементы (ячейки), так и целые строки из активного списка. Это особенно полезно при необходимости переноса информации в другие части интерфейса или внешние программы для дальнейшего использования или анализа. Оно интуитивно понятно благодаря использованию значков и четкому разделению функционала.

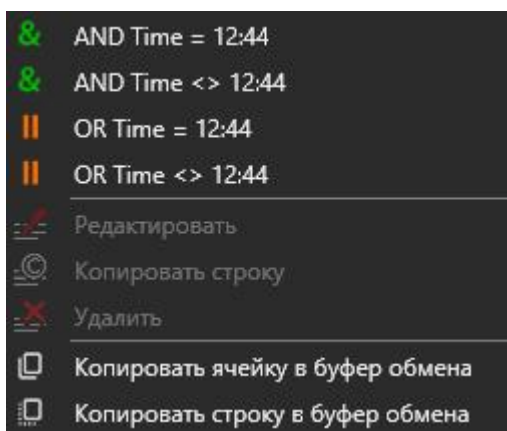


Рисунок 67. Меню взаимодействия со строкой

Для удаления строки из активного списка необходимо нажать ПКМ на строку и выбрать пункт меню «Удалить» затем подтвердить удаление (см. Рисунок 68). Или выделить необходимые строки и в разделе «Управление таблицей» нажать «Удалить строку» и после чего подтвердить удаление (см. Рисунок 69).

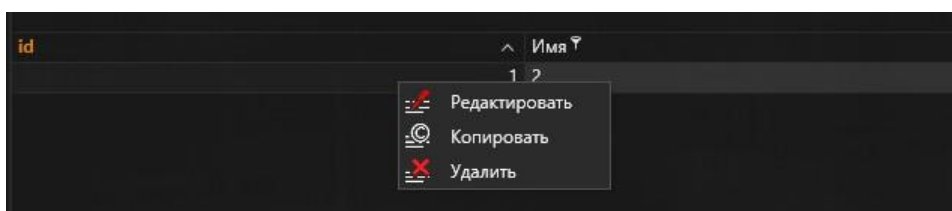


Рисунок 68. Удаление строки

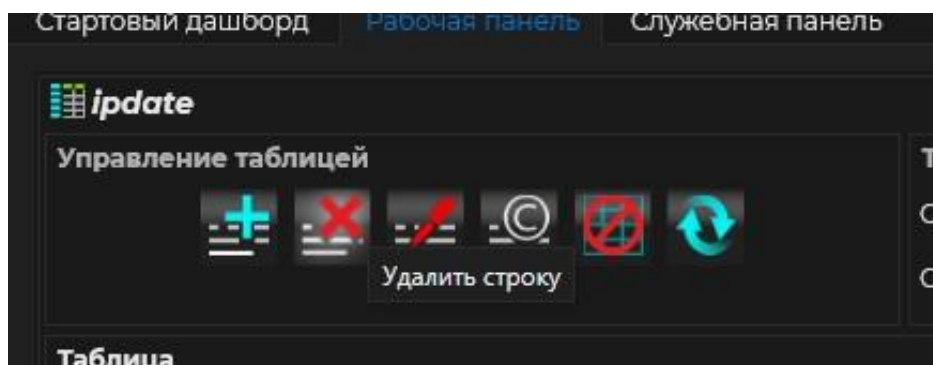


Рисунок 69. Удаление строки

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 70). Также есть возможно быстрой фильтрации схожей по функционалу с быстрой фильтрацией Активного канала (см. **Ошибка! Источник ссылки не найден.**) для этого необходимо нажать ПКМ по записи в АС и выбрать соответствующий фильтр (см. Рисунок 67)

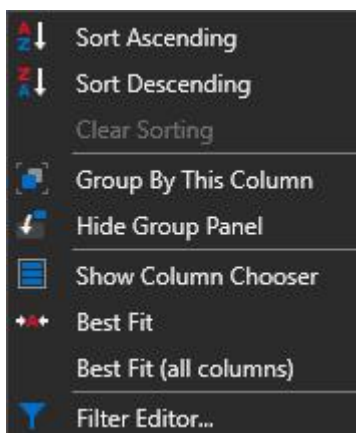


Рисунок 70. Добавление фильтра

В появившемся окне выставляем необходимые настройки и нажимаем «ОК» (см. Рисунок 71). Подробнее про настройку фильтров описано в разделе «Фильтрация событий».

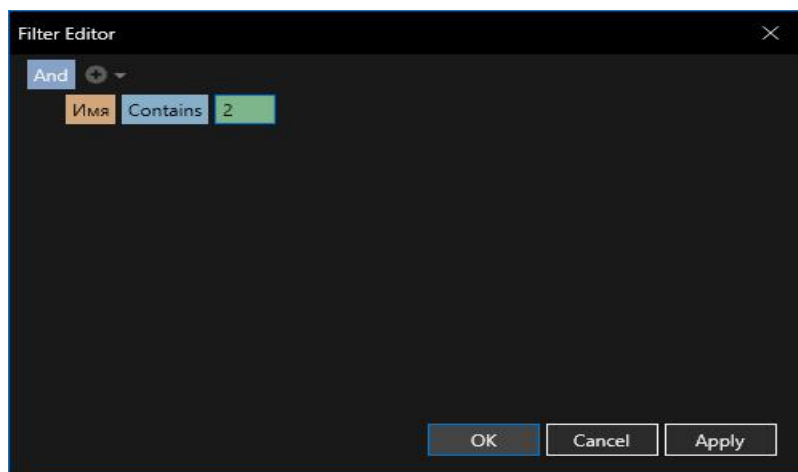


Рисунок 71. Окно настройки фильтра

Взаимодействовать с созданными фильтрами можно в нижней части АС. Фильтры отображаются в виде одной строки. При необходимости фильтрацию можно временно включать или отключать, нажав на галочку (см. Рисунок 72). Меню управления фильтром находятся в правой части строки и включают три кнопки   . Ниже описан функционал данного меню:

- Для редактирования фильтра нажмите кнопку .
- Чтобы просмотреть историю созданных фильтров, нажмите кнопку .
- Для полной очистки фильтра используйте кнопку .

Чтобы удалить отдельное условие, нажмите на кнопку крестика рядом с ним (см. Рисунок 70). Также можно удалить ненужную часть условия в редакторе фильтров «Filter Editor».



Рисунок 72. Окно удаления фильтра

В таблице активного списка можно настроить объём отображаемых строк. Для этого установите соответствующий лимит в разделе «Табличная информация» в АС. Для перемещения между страницами в таблице используются соответствующие кнопки (см. Рисунок 73). Также в АС доступен функционал сортировки колонок. Работа с этим функционалом описана в разделе Группировка событий.



Рисунок 73. Кнопки переключения страниц

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

3. Управление активным списком

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

Таблица 5. Элементы управления АЛ

Иконка	Наименование	Назначение
	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 6. 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 строку	Используется для копирования строк в АС
	Отчистить таблицу	Используется для мгновенной отчистки таблицы от всех значений
	Обновить активный список	Используется для обновления данных в АС

4. 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 74). После подтверждения удаления активный список будет помечен на удаление. Для полного удаления необходимо нажать «Удалить» повторно и подтвердить удаление.

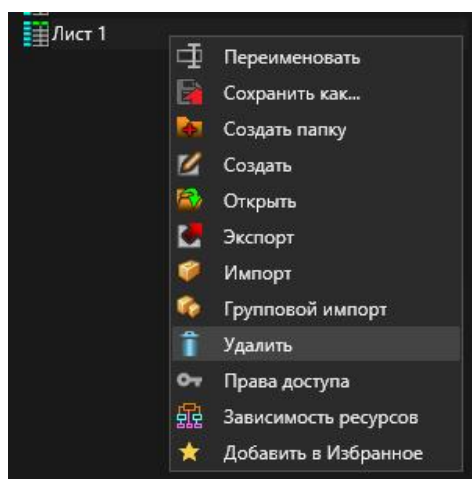


Рисунок 74. Удаление активного списка

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 75).

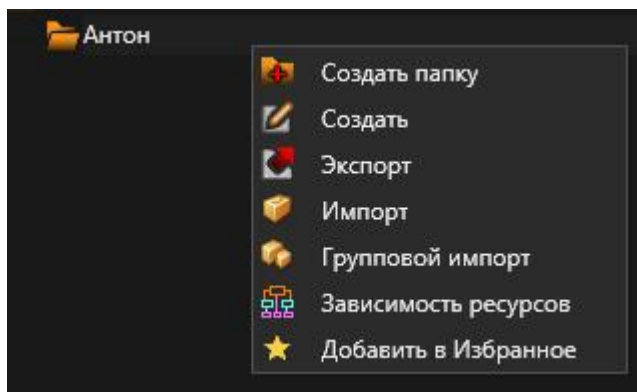


Рисунок 75. Дерево правил

В открывшемся окне создания Получателя (см. Рисунок 76) 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.

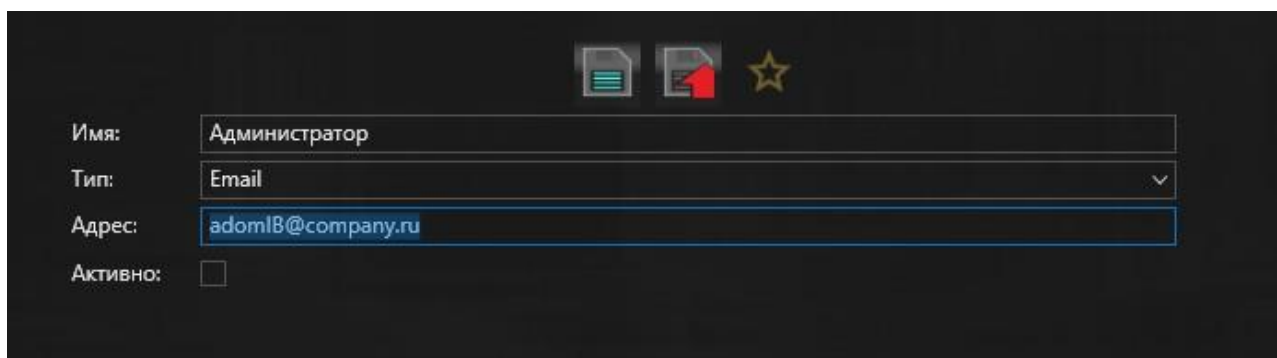


Рисунок 76. Окно создания получателя

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 77).

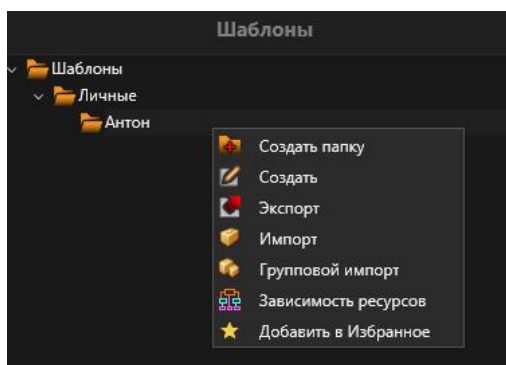


Рисунок 77. Дерево Шаблонов

После чего откроется окно создания Шаблона (см. Рисунок 78). В данном окне в поле «Имя» необходимо задать название Шаблона, в поле «Имя» добавить необходимое описание уведомления 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 .

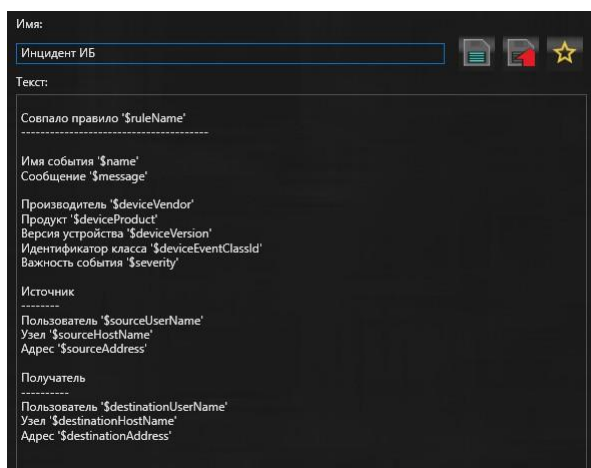


Рисунок 78. Пример Шаблона

ПРАВИЛА

1. 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 79).

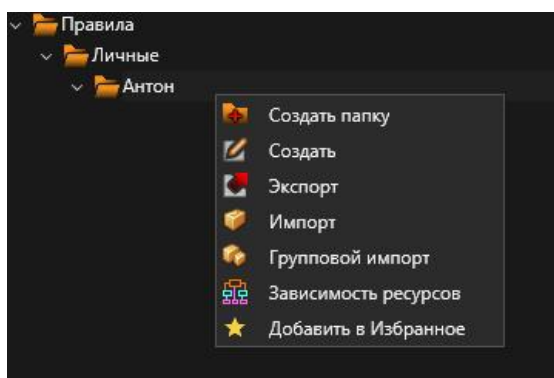


Рисунок 79. Дерево правил

После чего откроется окно конструктора написания правил корреляции (см. Рисунок 80).

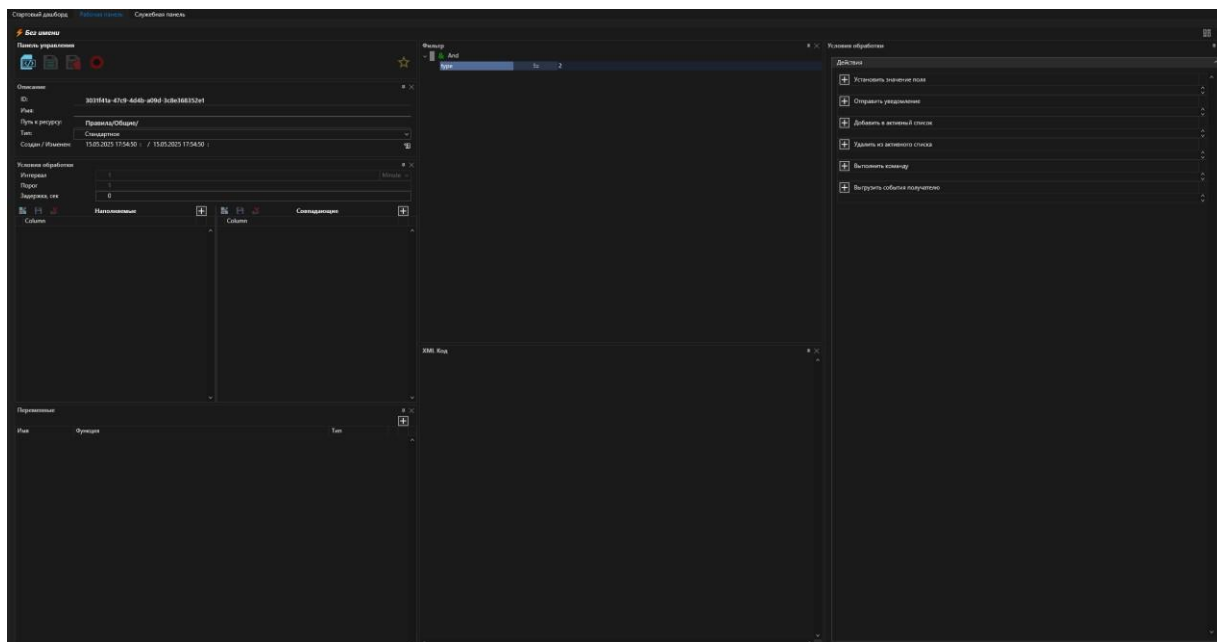
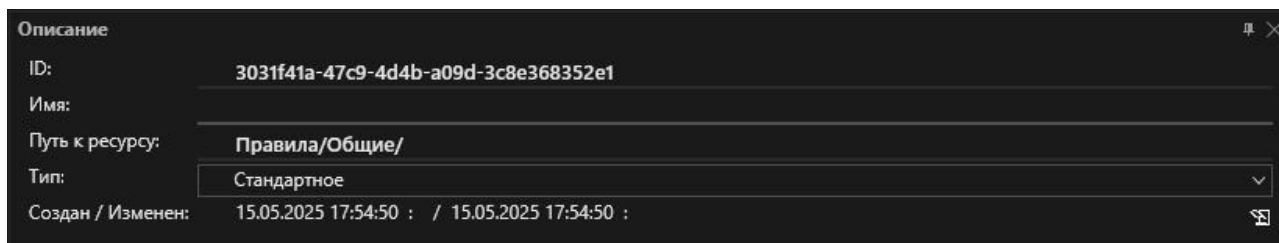


Рисунок 80. Конструктор создания правил

Для создания правил в первую очередь необходимо заполнить основную информацию (см. Рисунок 81), где:



Описание	
ID:	3031f41a-47c9-4d4b-a09d-3c8e368352e1
Имя:	
Путь к ресурсу:	Правила/Общие/
Тип:	Стандартное
Создан / Изменен:	15.05.2025 17:54:50 : / 15.05.2025 17:54:50 :

Рисунок 81. Основная информация по Правилу

- ID – уникальный идентификатор Правила присваивается автоматически;
- Имя – наименование правила;
- Путь к ресурсу (URI) – путь по которому можно найти данное правило в системе.
- 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 82). В данном поле «Задержка» указывает период времени, в котором правило не будет реагировать на повторные события, также есть возможность настроить наполняемые и совпадающие поля.

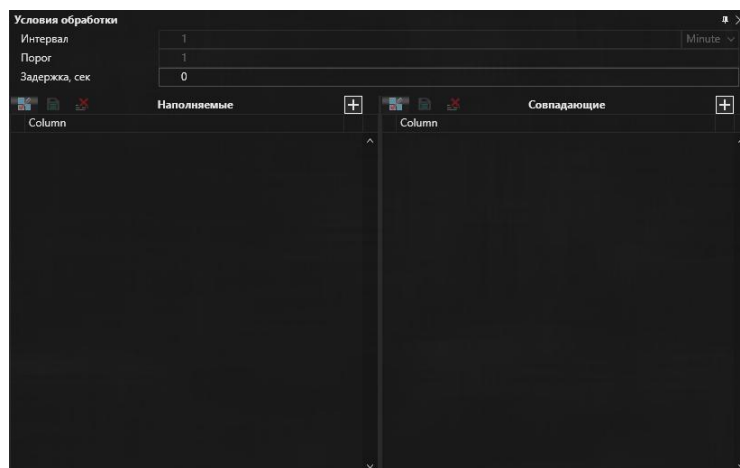


Рисунок 82. Условия обработки

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 83)

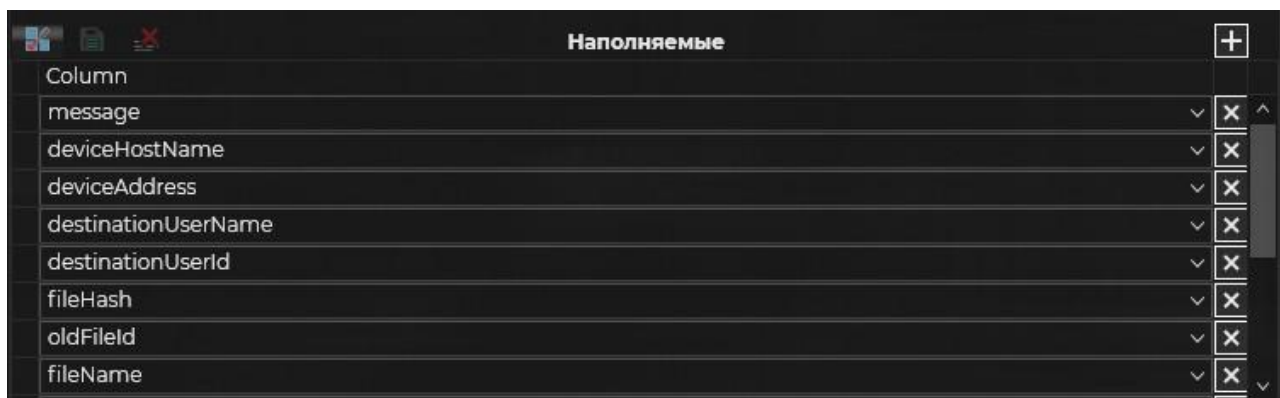


Рисунок 83. Окно агрегированных полей

Совпадающие поля

Совпадающие поля – предназначены для определения ключевых критериев группировки и идентификации связанных событий. Для корректной корреляции необходимо в раздел «Совпадающие поля» выбрать поля, значения которых должны совпадать у нескольких событий для их объединения в единую корреляционную цепочку.

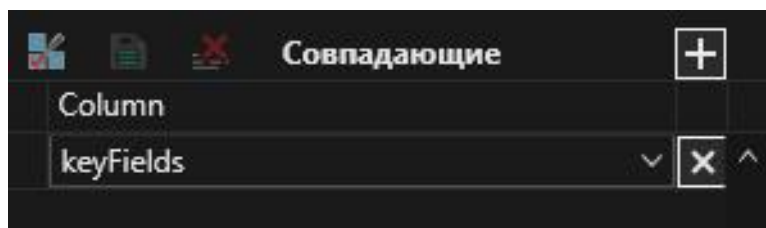


Рисунок 84. Окно совпадающих полей.

Фильтры

После добавления основной информации по Правилу следует добавить условия в разделе «Фильтр» (см. Рисунок 85). 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 85), и дважды щёлкнуть ЛКМ по полю условия.

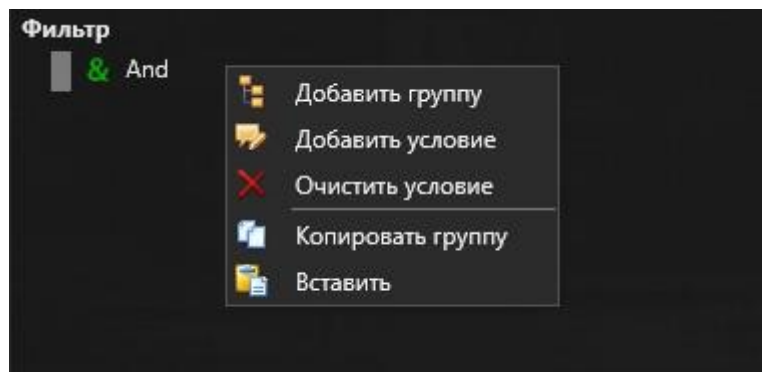


Рисунок 85. Контекстное меню редактора условий

После чего откроется диалоговое окно «Редактирования условия» (см. Рисунок 86), 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 «ОК». Для удаления условия необходимо нажать по нему ПКМ и в контекстном меню выбрать пункт «удалить условие».

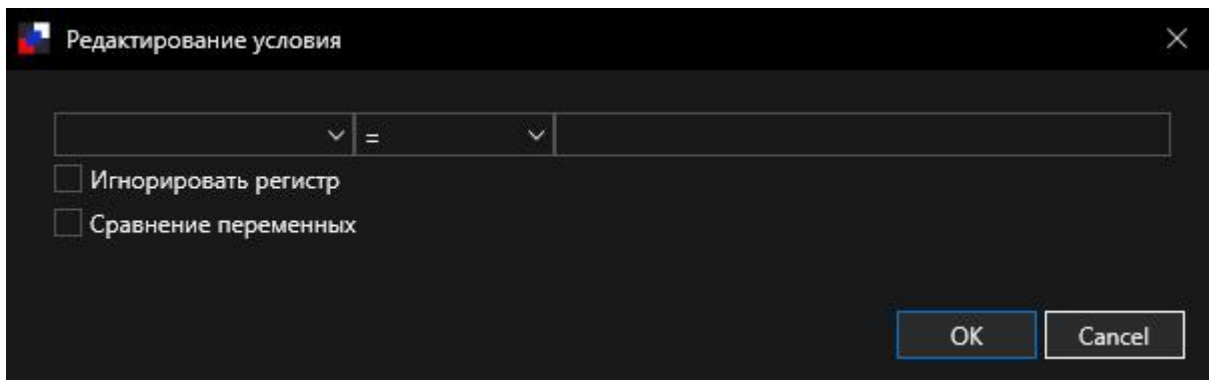


Рисунок 86. Редактирование условий

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 87).

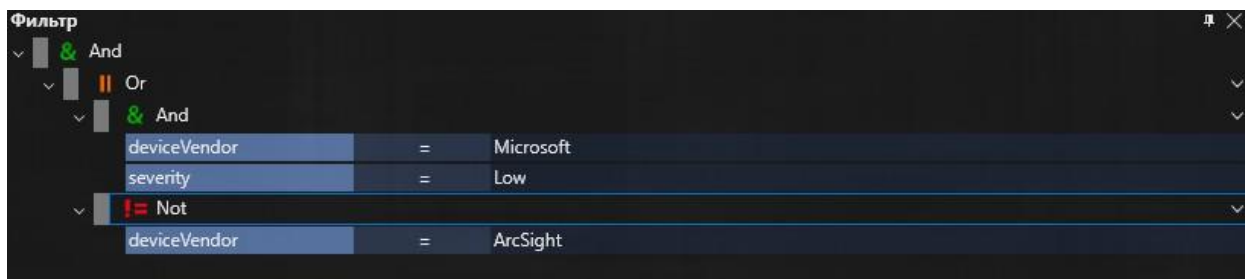


Рисунок 87. Пример условия

Обработка и порядок добавления условий

Правила в системе хранятся в виде XML. Ниже представлено описание и пример структуры XML-кода правила

```
<Rule
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  Name="тест описания xml"
  Type="Normal"
  ID="8884e349-2bf3-4419-a7ba-ae56ad1794a5">&lt;ActualResource
ResourceId="8884e349-2bf3-4419-a7ba-ae56ad1794a5" Name="тест описания xml" /&gt;]]&gt;
  &lt;Query&gt;
  &lt;Actions&gt;
  &lt;DependentVariables&gt;
  &lt;ChainCondition
    IsRuleCondition="true"&gt;
  &lt;ChainFieldSet /&gt;
&lt;/Rule&gt;</pre>
</div>
<div data-bbox="553 583 928 600" data-label="Caption">
<p>Рисунок 88. Структура XML-кода правила</p>
</div>
<div data-bbox="174 612 497 629" data-label="Text">
<p>Значение тегов в XML-коде правила:</p>
</div>
<div data-bbox="145 642 917 867" data-label="List-Group">
<ul>
<li>• &lt;Rule&gt; – описывает общую информацию о правиле и его основные составляющие.</li>
<li>• &lt;Query&gt; – описывает условия обработки правила (тег &lt;WhereClause&gt;), наполняемые, совпадающие и уникальные поля (теги &lt;GroupByClause&gt;, &lt;CommonClause&gt; и &lt;SelectClause&gt;), а также фильтр (тег &lt;Condition&gt;).</li>
<li>• &lt;Actions&gt; – описывает перечень действий, которые будут отрабатывать в ходе работы правила. Каждое действие описывается в отдельном теге &lt;Action&gt;.</li>
<li>• &lt;DependentVariables&gt; – описывает перечень переменных, используемых в правиле, каждая переменная в отдельном теге &lt;DependentVariable&gt;.</li>
<li>• &lt;ChainCondition&gt; – используется для ретроспективных правил и описывает фильтр запроса/</li>
<li>• &lt;ChainFieldSet /&gt; – используется для ретроспективных правил и описывает Поля обогащения цепочки.</li>
</ul>
</div>
<div data-bbox="902 913 930 928" data-label="Page-Footer">
<p>74</p>
</div>
```

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

```
<Condition
  IsRuleCondition="true">
  <And
    Name="And">
    <BasicCondition
      Operator="NE"
      IgnoreCase="No">
      <Variable
        Column="type" />
      <Value>2</Value>
    </BasicCondition>
    <BasicCondition
      Operator="EQ"
      Negated="No"
      IgnoreCase="No">
      <Variable
        Column="deviceVendor" />
      <Value>Microsoft</Value>
    </BasicCondition>
    <BasicCondition
      Operator="EQ"
      Negated="No"
      IgnoreCase="No">
      <Variable
        Column="deviceProduct" />
      <Value>Microsoft Windows</Value>
    </BasicCondition>
    <BasicCondition
      Operator="EQ"
      Negated="No"
      IgnoreCase="No">
      <Variable
        Column="externalId" />
      <Value>4688</Value>
    </BasicCondition>
    <BasicCondition
      Operator="InActiveList"
      IgnoreCase="No">
      <Variable
        Column="dst4"
        ColumnName="d1" />
      <Resource
        ID="46358c30-6e5e-4420-9d6e-213384022e7b"
        URI="Windows_Enumeration_Commands"
        ReferenceID="2670" />
      </BasicCondition>
    </And>
```

Рисунок 89. Порядок условий в xml-коде

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



Рисунок 90. Порядок добавления условий.

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

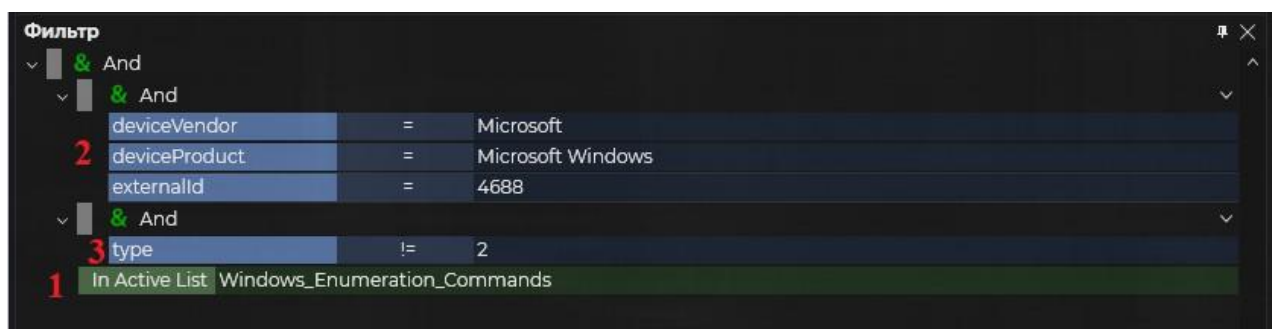


Рисунок 91. Некорректный порядок условий

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 обрабатывало и не нагружало систему. На рисунке ниже представлено оптимизированное условие, которое имеет следующий порядок отработки:



Рисунок 92. Корректный порядок условий

1. Первым отработывает 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 93) – система во вновь созданном корреляционном событии присвоит выбранным полям назначенные параметры. Кнопка  предназначена для добавления нового поля, кнопка  предназначена для удаления добавленного поля.

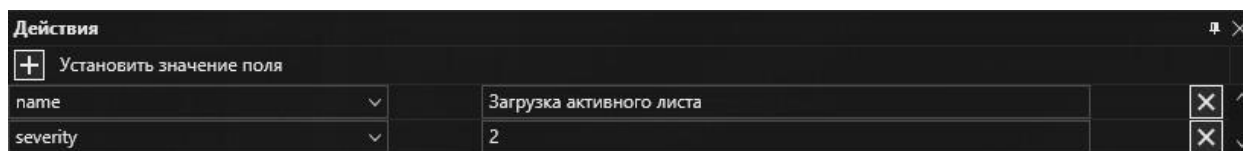


Рисунок 93. Окно установки значений полям

Отправить уведомление (см. Рисунок 94) – 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. В случае необходимости отправки уведомлений нескольким пользователям в списке «Получатель» необходимо выбрать папку с пользователями.

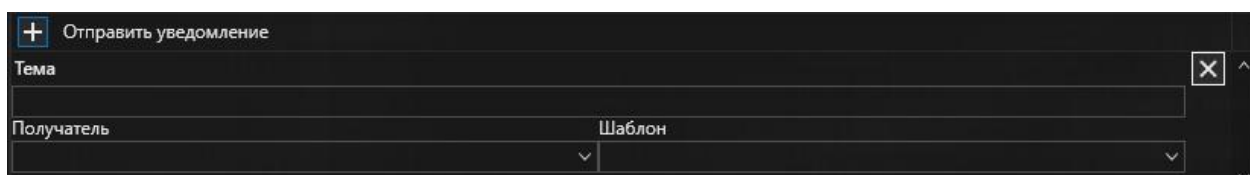


Рисунок 94. Окно настройки отправки уведомлений

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 95). Данной иконкой  обозначаются ключевые поля в активных списках.

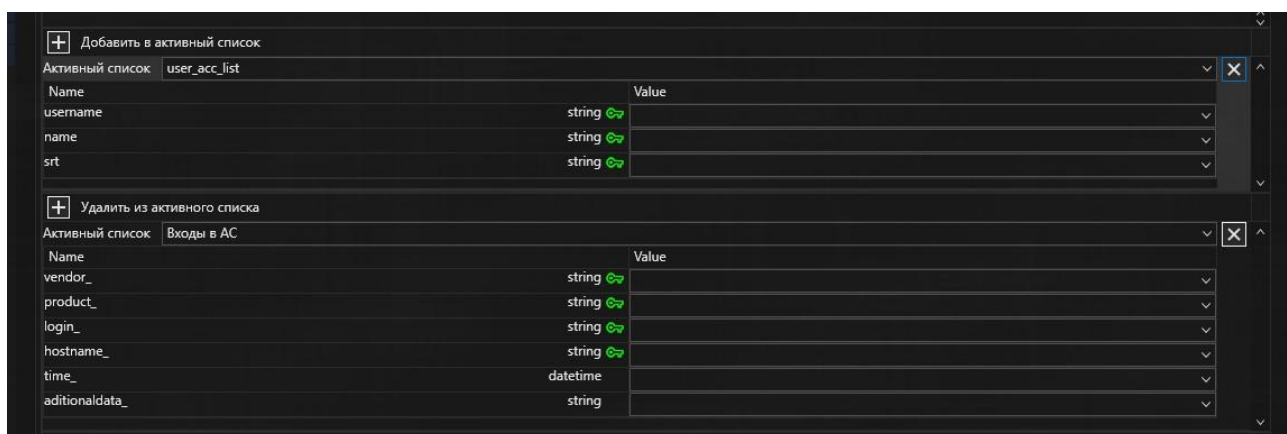


Рисунок 95. Окно обновления данных в АС

Переменные

Переменные – при необходимости в Правила можно добавлять различные переменные (см. Рисунок 96). **В рамках одного правила нельзя создавать переменные с одинаковыми названиями.**

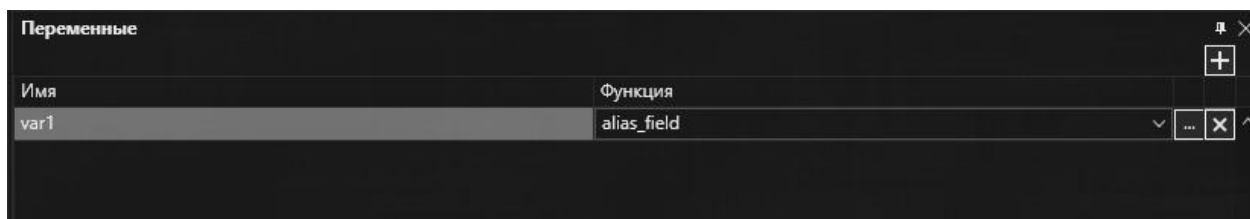


Рисунок 96. Окно добавления Переменных

Полный перечень поддерживаемых функций переменных представлен в разделе «ФУНКЦИИ ПЕРЕМЕННЫХ».

После завершения создания правила необходимо нажать кнопку «Сохранить» .

Агрегационные правила

Условия обработки

Для создания правил Агрегации необходимо выбрать условия обработки (см. Рисунок 97).

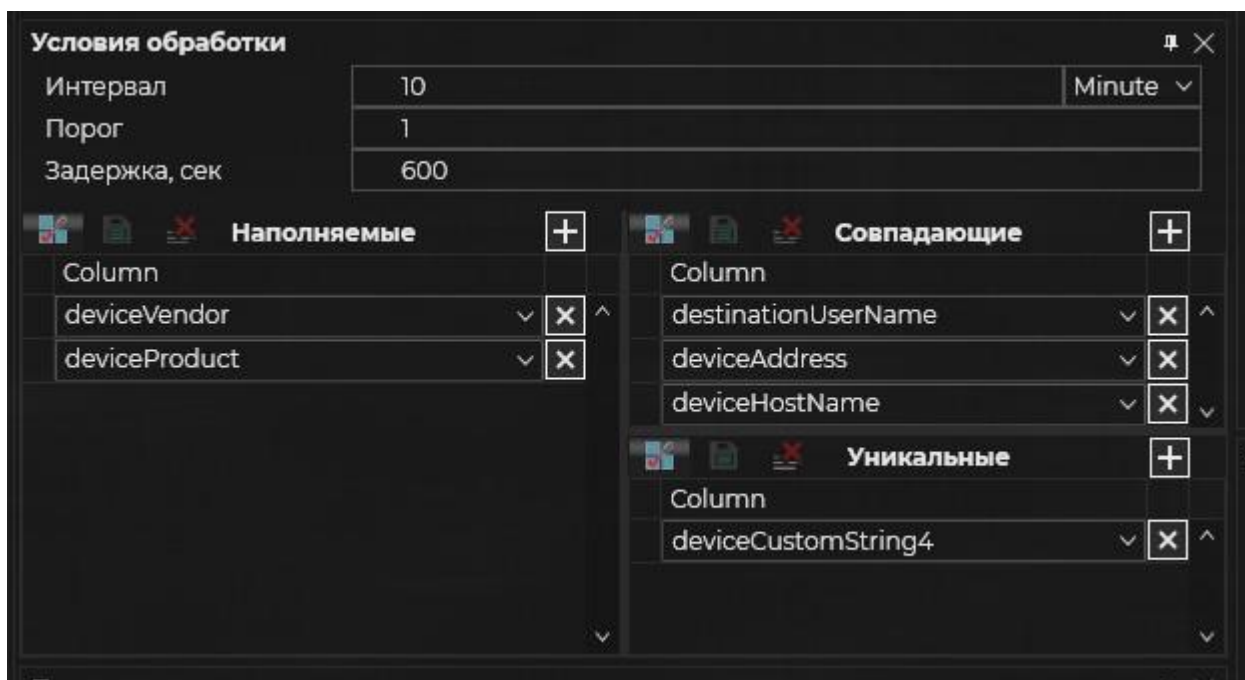


Рисунок 97. Условия обработки

- 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 98). По этим полям высчитывается хэш.

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

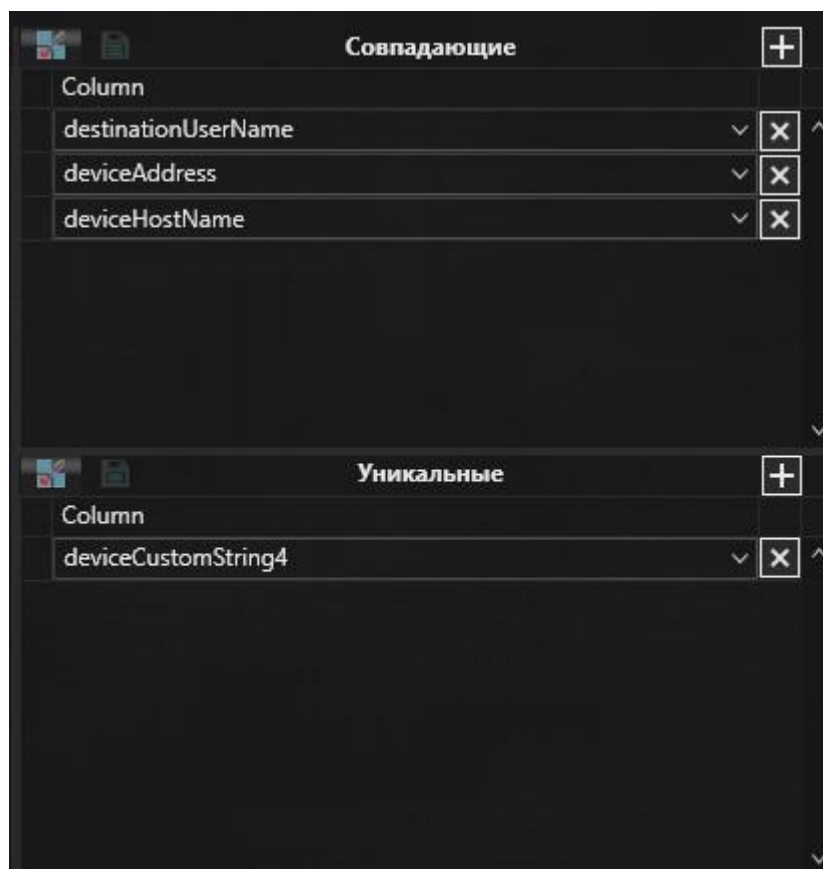


Рисунок 98. Поля агрегирования

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 99). 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 99. Поля обогащения цепочки

Также для Агрегационных правил доступен функционал «In memory list». Данный функционал представляет собой активный лист, в котором хранятся значения полей правила корреляции. Подробнее о данном функционале можно узнать в подразделе «Rules» раздела «ВЕБ-ИНТЕРФЕЙС».

2. 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

3. 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 100).

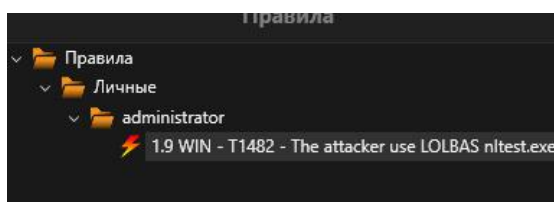


Рисунок 100. Дерево правил

После завершения редактирования правила необходимо нажать кнопку «Сохранить»



4. Создание АК по событиям, сгенерированным правилом

Для создания АК по событиям, сгенерированным правилом необходимо в дереве ресурсов кликнуть ПКМ по правилу и выбрать пункт меню «Создать канал по событиям, сгенерированным правилом» (см. Рисунок 101).

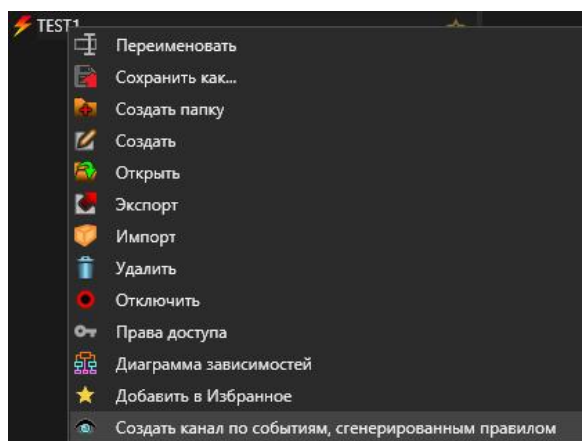


Рисунок 101. Выпадающее меню управления правилами

После активации данной функции автоматически будет создан АК, включающий в себя события, отработанные по выбранному правилу.

Для сохранения данного АК необходимо нажать на кнопку «Сохранить»  на панели управления АК.

5. Удаление правила

Для удаления Правил в меню ресурсов необходимо перейти на вкладку «Правила» и выбрать необходимое Правило, после чего выбрать «Удалить» (см. Рисунок 102). После подтверждения удаления правило деактивируется и пометится как ресурс на удаление. Для полного удаления необходимо нажать «Удалить» повторно и подтвердить удаление.

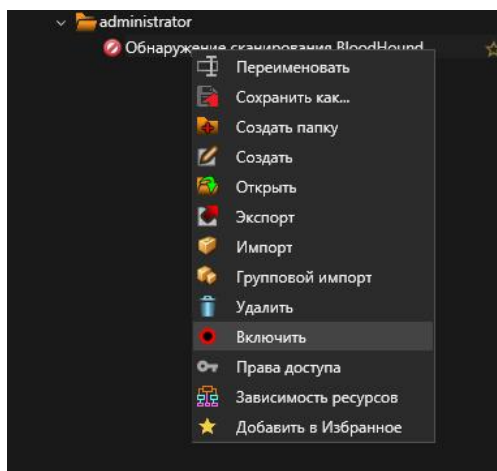


Рисунок 102. Управление правилами

МОНИТОРИНГ ЗАГРУЗКИ КОРРЕЛЯТОРА

В данном разделе приведены примеры событий от коррелятора, которые отображают степень его загруженности.

1. Событие «CPU»

Данное событие отображает степень загрузки CPU правилами и выглядит следующим образом (см. Рисунок 103).

Имя поля	Данные
Общие	
baseEventCount	1
endTime	12.12.2024 10:55:38
managerReceiptTime	12.12.2024 10:55:38
message	current CPU usage 31.000000%, average: 11.400000%
name	cpu
type	5
Категория	
categoryDeviceGroup	Правила/Личные/Vasia/067. Запуск процесса из нестандартной директории
categoryObject	cd75cf59-bab2-4db7-b81a-5eabbf8edf7f
categorySignificance	Normal
categoryTechnique	067. Запуск процесса из нестандартной директории
Устройство	
deviceAddress	172.16.42.106
deviceHostName	ST-Jatoba-Sert
devicePayloadId	0
deviceProduct	InfoterCE
deviceReceiptTime	12.12.2024 10:55:38
deviceVendor	Savrus
Настраиваемые поля	
deviceCustomFloatingPoint1	31.000000
deviceCustomFloatingPoint1Label	CPU usage
deviceCustomFloatingPoint2	11.400000
deviceCustomFloatingPoint2Label	Average CPU usage
deviceCustomFloatingPoint3	0.000000
deviceCustomFloatingPoint3Label	Time of true match, interval 120 sec.
deviceCustomFloatingPoint4	0.000333
deviceCustomFloatingPoint4Label	Time of false match, interval 120 sec.
deviceCustomNumber1Label	Events matched true
deviceCustomNumber2	236
deviceCustomNumber2Label	Events matched false
deviceCustomNumber3	120
deviceCustomNumber3Label	Interval
deviceCustomString1	067. Запуск процесса из нестандартной директории
Гибко настраиваемые	

Рисунок 103. Пример заполненных полей события «CPU»

Описание (наиболее ключевых показателей для оценки нагрузки):

1. Событие возвращается раз в интервал, выставленный в корреляторе heartbeat_interval (deviceCustomNumber3)
2. Показывает максимальный (CPU usage) и средний уровень (Average CPU usage) значения загрузки процессора правилами (типа «Стандартное», «Агрегационное») за указанный интервал (message | deviceCustomFloatingPoint1+ deviceCustomFloatingPoint2) – усредненное значение интервала высчитывается из 5 предыдущих замеров и участвует далее в отключении правил (типа «Стандартное», «Агрегационное»).

2. Событие «rule time statistics»

Данное событие отображает определённые статистические данные по отработке правил и выглядит следующим образом (см. Рисунок 104).

Общие	
baseEventCount	1
endTime	17.12.2024 13:45:43
managerReceiptTime	17.12.2024 13:45:43
message	rule 163 'New Service Installation Detected' matched true(15): 0.000649, matched false(13111): 0.000002
name	rule time statistics
type	5
Категория	
categoryDeviceGroup	Правила/Общие/New Service Installation Detected
categoryObject	c78be347-b4dc-48d0-b630-c26f226d97ab
categorySignificance	Normal
categoryTechnique	New Service Installation Detected
Устройство	
deviceAddress	172.16.42.106
deviceHostName	ST-Jatoba-Sert
devicePayloadId	0
deviceProduct	InforterCE
deviceReceiptTime	17.12.2024 13:45:43
deviceVendor	Savrus
Настраиваемые поля	
deviceCustomFloatingPoint1	1.411507
deviceCustomFloatingPoint1Label	load percentage
deviceCustomFloatingPoint2	0.000651
deviceCustomFloatingPoint2Label	Average time of match
deviceCustomFloatingPoint3	0.009737
deviceCustomFloatingPoint3Label	Time of true match, interval 120 sec.
deviceCustomFloatingPoint4	0.029427
deviceCustomFloatingPoint4Label	Time of false match, interval 120 sec.
deviceCustomNumber1	15
deviceCustomNumber1Label	Events matched true
deviceCustomNumber2	13111
deviceCustomNumber2Label	Events matched false
deviceCustomNumber3	120
deviceCustomNumber3Label	Interval
deviceCustomString1	New Service Installation Detected

Рисунок 104. Пример заполненных полей события «rule time statistics»

В таблице ниже приведено описание метрик.

Таблица 7. Описание метрик

№	Наименование поля	Описание значения
1.	deviceCustomFloatingPoint1	Среднее время, затраченное на одно атомарное событие при успешном срабатывании правила (за диапазон CustomNumber3)
2.	deviceCustomFloatingPoint1 Lable	Load percentage – объем загрузки коррелятора, генерируемый правилом за указанный heartbeat_interval (deviceCustomNumber3) от общего объема загрузки активных правил (типа «Стандартное», «Агрегационное») за указанный heartbeat_interval (deviceCustomNumber3)
3.	deviceCustomFloatingPoint2	Среднее время, затраченное на одно срабатывание правила (за диапазон CustomNumber3)
4.	deviceCustomFloatingPoint3	Суммарное время, затраченное на все события при успешном срабатывании правила (за диапазон CustomNumber3)
5.	deviceCustomFloatingPoint4	Суммарное время, затраченное на все события при неуспешном срабатывании правила (за диапазон CustomNumber3)
6.	deviceCustomNumber1	Кол-во событий при успешном срабатывании правила (за диапазон CustomNumber3)
7.	deviceCustomNumber2	Кол-во событий, находящихся в обработке при неуспешном срабатывании правила (за диапазон CustomNumber3)
8.	deviceCustomNumber3	Параметр heartbeat_interval из конфигурационного файла InforterCE отвечающий за интервал сообщений о состоянии inforter CE

Если
$$\frac{(\text{deviceCustomFloatingPoint3} + \text{deviceCustomFloatingPoint4})}{\text{CustomNumber3}} >$$
 значения rules_disable_threshold, указанного в конфигурационного файла InforterCE и отвечающее за ограничение отключения правил, то правило будет отключено.

3. Параметры config.xml коррелятора

Данные параметры участвуют в процессе контроля и снижения загрузки коррелятора.

```
<?xml version="1.0"?>
<inforter_ce threads="64" vendor="Savrus">
```

```
<logging logging_level="1" size="5" heartbeat_interval="120"
splitting_logs="false" max_string_size="16384" />
<ce folder="/opt/inforter/data/" rules_matches="200"
rules_disable_threshold="3" rules_optimization="false"
max_cpu_usage_percentage="50"
rules_action_colleration_event_fields="false"
```

1. rules_matches="200" – кол-во сработок конкретных правил корреляции за 1 сек., после которых конкретное правило отключается.
2. rules_disable_threshold="3" – параметр отключения правила по потребляемому времени на обработку, рассчитывается по формуле параметров, выдаваемых по каждому правилу в событии 'rule time statistics'.

Если $\frac{(\text{deviceCustomFloatingPoint3} + \text{deviceCustomFloatingPoint4})}{\text{CustomNumber3}} > \text{значения rules_disable_threshold}$, указанного в конфигурационного файла InforteCE и отвечающее за ограничение отключения правил, то правило будет отключено.

3. max_cpu_usage_percentage="50" - параметр отключения правила по нагрузке на CPU (сервера с коррелятором) – в случае, если 5 последовательных замеров события Average CPU usage (события «CPU») будет больше выставленного параметра max_cpu_usage_percentage будет отключаться при каждом heartbeat_interval по одному правилу (типа Стандартное / Агрегационное) с максимальным значением Load percentage (события 'rule time statistics').

Для правил типа «Ретроспективное», «Ретроспективное GUI» пока реализовано ограничение по времени, затрачиваемому на выполнение правила, если на выполнение конкретного правила потребуется более 120 сек – оно будет отключено. Реализовано также отключение правил типа «Ретроспективное», «Ретроспективное GUI», в случаях превышения времени выполнения правила за рамки установленной частоты выполнения конкретного правила – оно будет отключено.

ФУНКЦИИ ПЕРЕМЕННЫХ

1. Создание и управление функциями переменных

Для создания переменной с необходимой функцией, требуется нажать на кнопку  в окне «Переменные». В открывшемся диалоговом окне следует ввести название переменной и выбрать необходимую функцию.

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».

2. Арифметические функции

Absolute

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

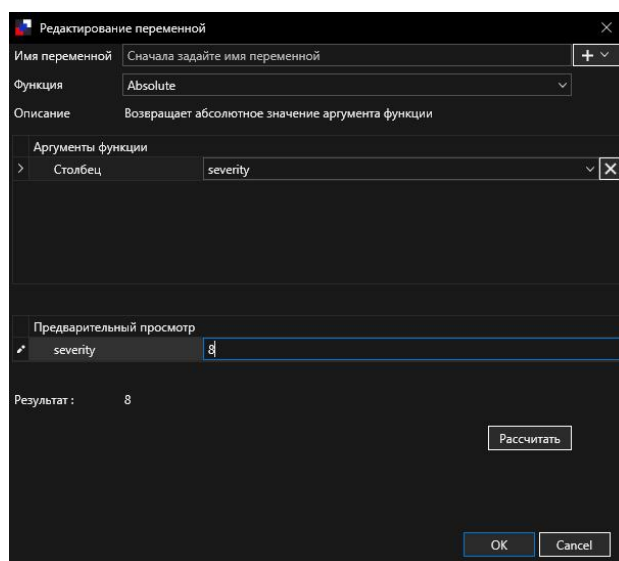
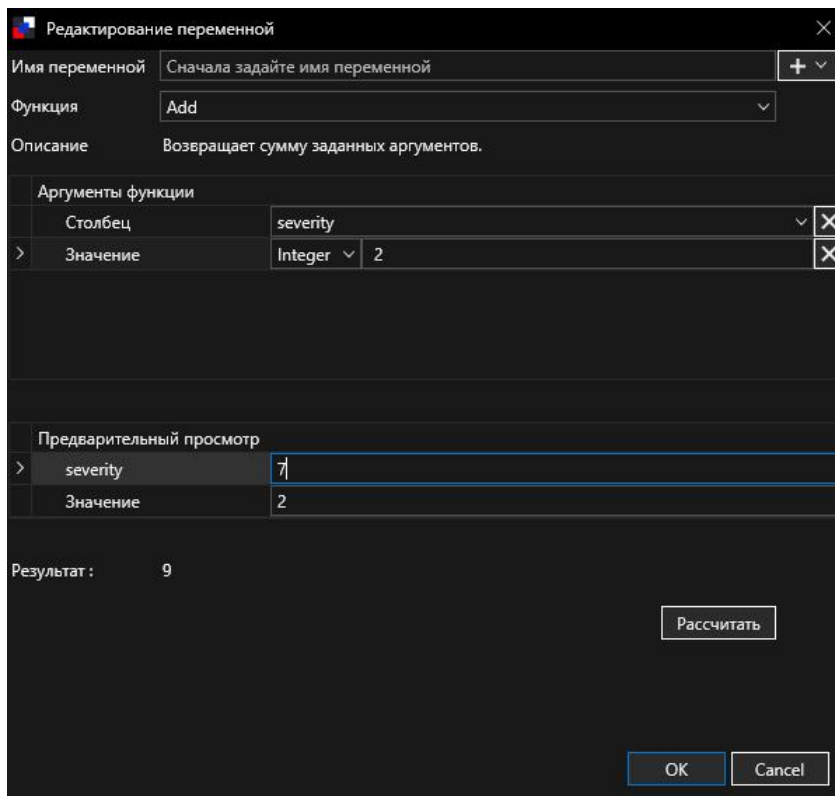


Рисунок 105. Пример функции Absolute

Add

Данная функция возвращает результат сложения числовых аргументов.



Аргументы функции	
Столбец	Значение
severity	Integer
	2

Предварительный просмотр	
Столбец	Значение
severity	7
	2

Результат : 9

Рассчитать

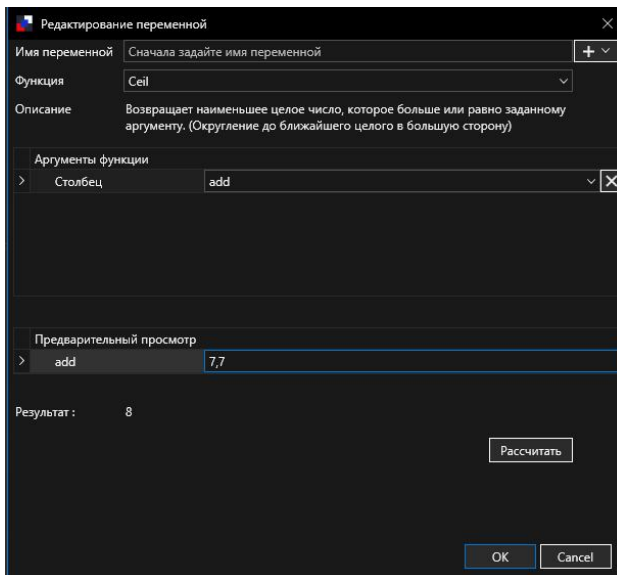
OK Cancel

Рисунок 106. Пример функции Add

Ceil

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

в большую сторону).



Редактирование переменной

Имя переменной: Сначала задайте имя переменной

Функция: Ceil

Описание: Возвращает наименьшее целое число, которое больше или равно заданному аргументу. (Округление до ближайшего целого в большую сторону)

Аргументы функции

Столбец	
	add

Предварительный просмотр

add	7,7

Результат: 8

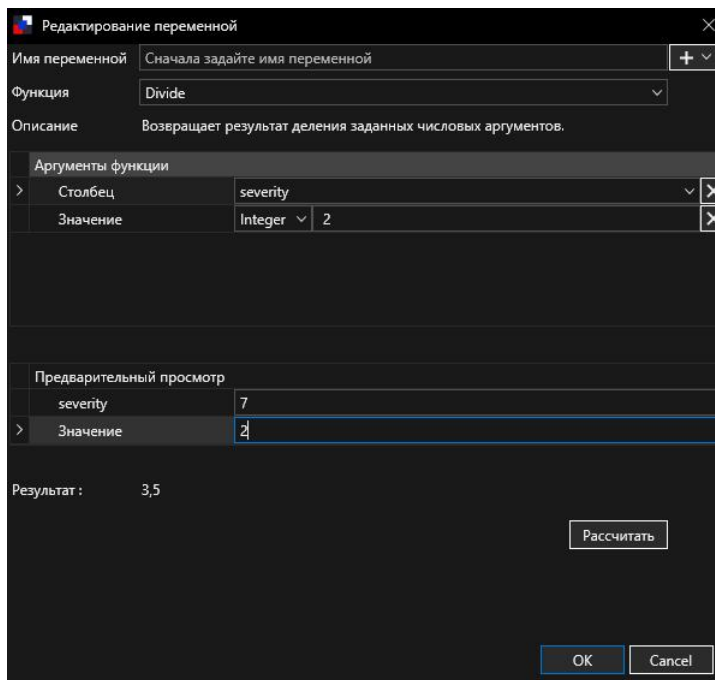
Рассчитать

OK Cancel

Рисунок 107. Пример функции Celi

Divide

Данная функция возвращает результат деления числовых аргументов.



Редактирование переменной

Имя переменной: Сначала задайте имя переменной

Функция: Divide

Описание: Возвращает результат деления заданных числовых аргументов.

Аргументы функции

Столбец	
Значение	severity
	Integer
	2

Предварительный просмотр

severity	7
Значение	2

Результат: 3,5

Рассчитать

OK Cancel

Рисунок 108. Пример функции Divide

Floor

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

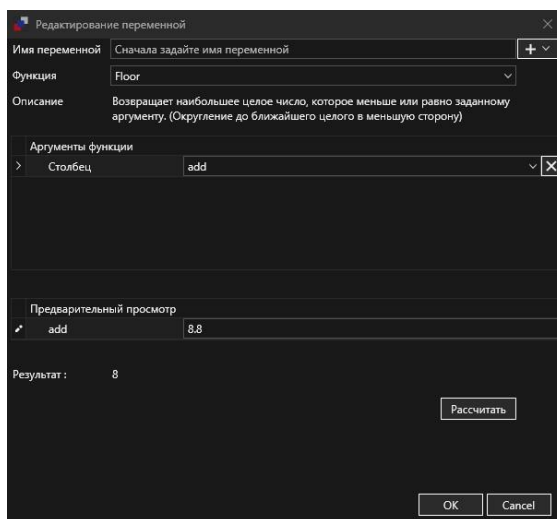


Рисунок 109. Пример функции Floor

Multiply

Данная функция возвращает произведение числовых аргументов.

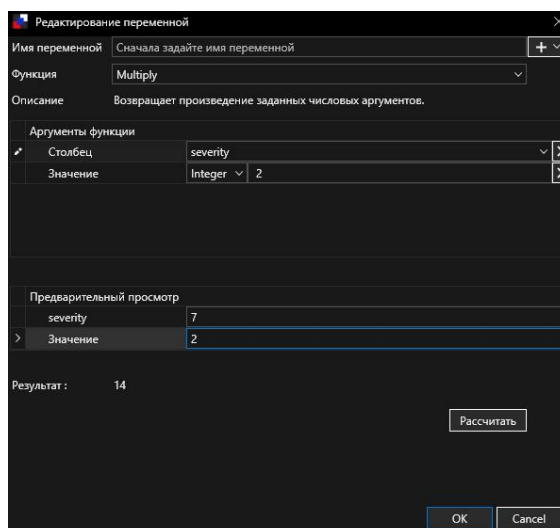


Рисунок 110. Пример функции Multiply

Round

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

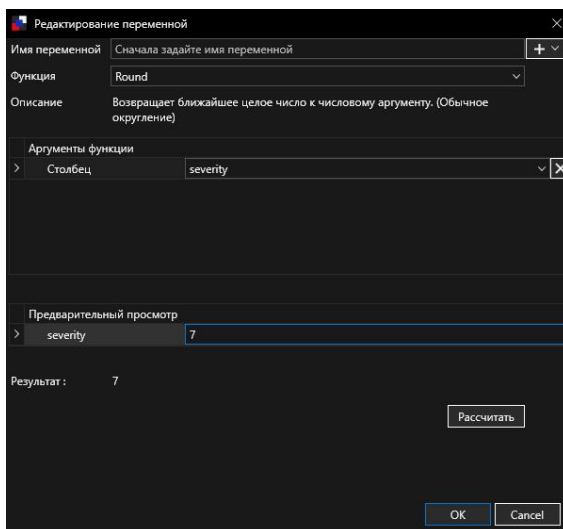


Рисунок 111. Пример функции Round

RoundN

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

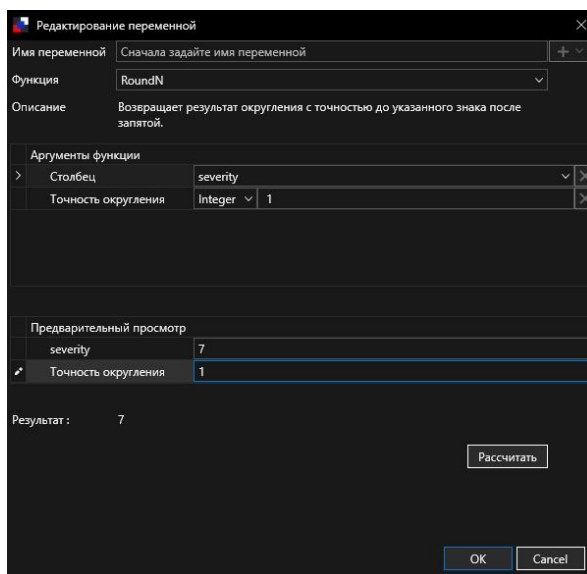


Рисунок 112. Пример функции RoundN

Subtract

Данная функция возвращает результат вычитания числовых аргументов.

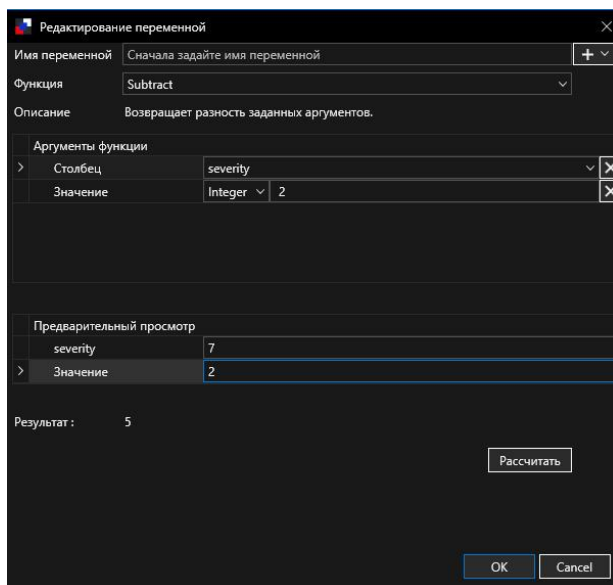


Рисунок 113. Пример функции Subtract

3. Дата и время

При взаимодействии с функциями в данном разделе необходимо использовать даты в формате UnixTime.

Get_current_time

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

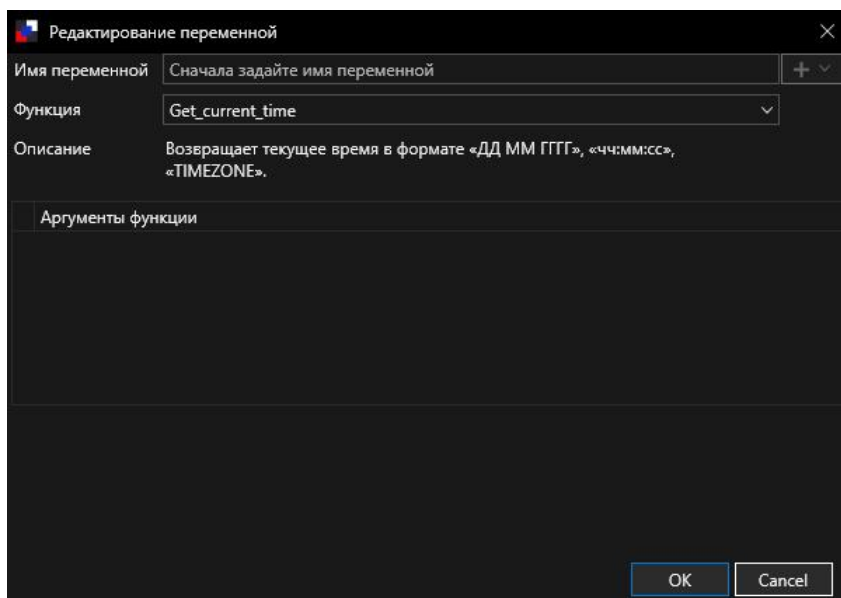


Рисунок 114. Пример функции `Get_current_time`

Get_day_of_month

Данная функция возвращает целое число от 1 до 31 для представления дня месяца, на основе выбранной метки времени.

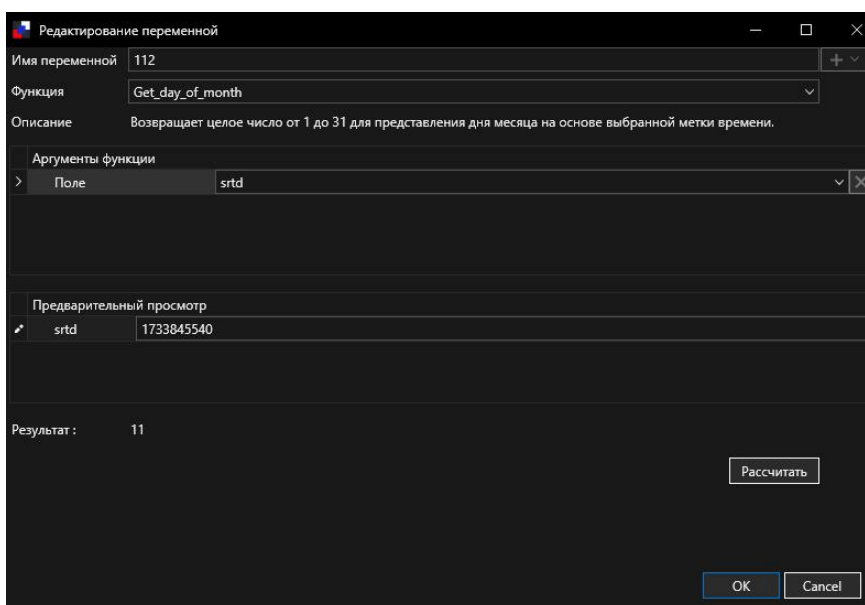


Рисунок 115. Пример функции `Get_day_of_month`

Get_day_of_week

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

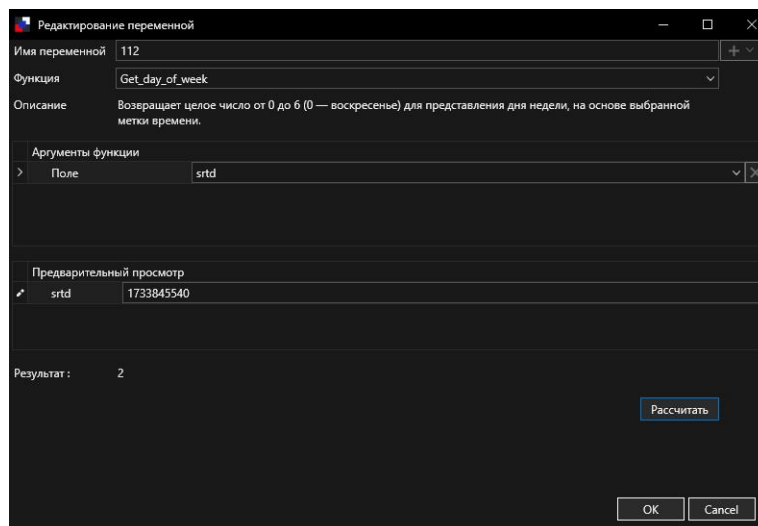


Рисунок 116. Пример функции Get_day_of_week

Get_day_of_year

Данная функция возвращает целое число от 0 до 365 (366) для представления дня года, на основе выбранной метки времени.

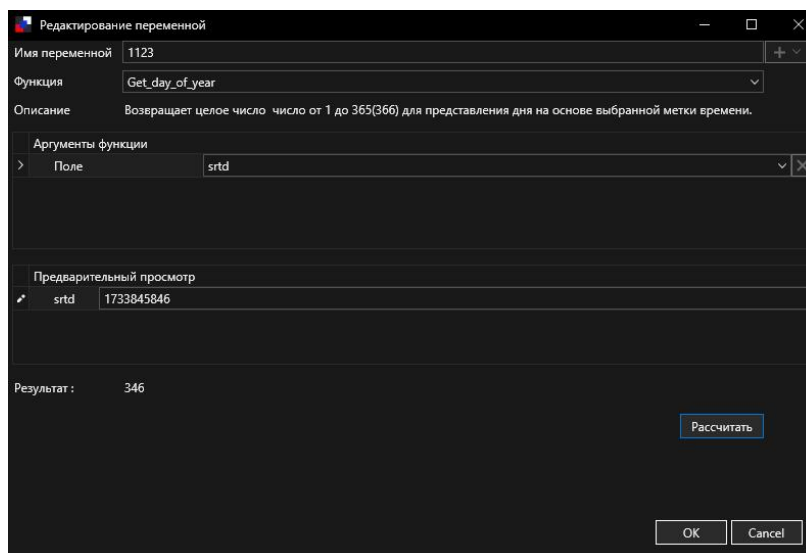


Рисунок 117. Пример функции Get_day_of_year

Get_format_time

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

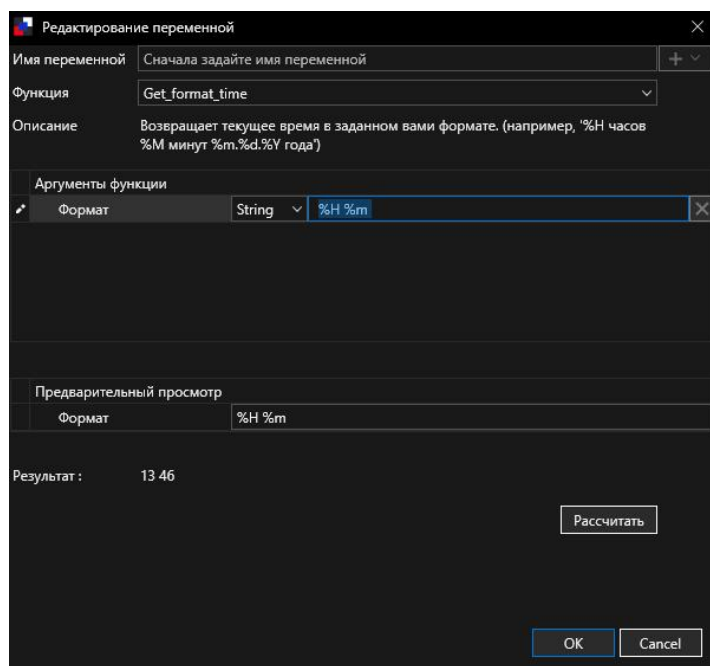


Рисунок 118. Пример функции Get_format_time

Get_hour_of_day

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

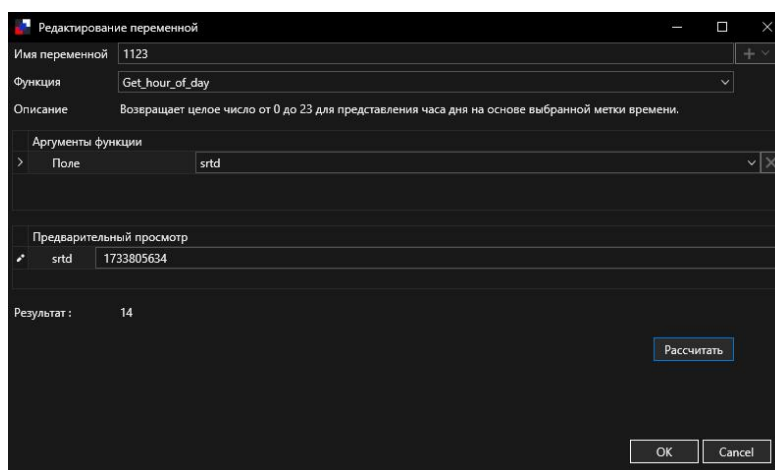


Рисунок 119. Пример функции Get_hour_of_day

Get_minute_of_hour

Данная функция возвращает целое число от 0 до 59 для представления минуты в часе, на основе выбранной метки времени.

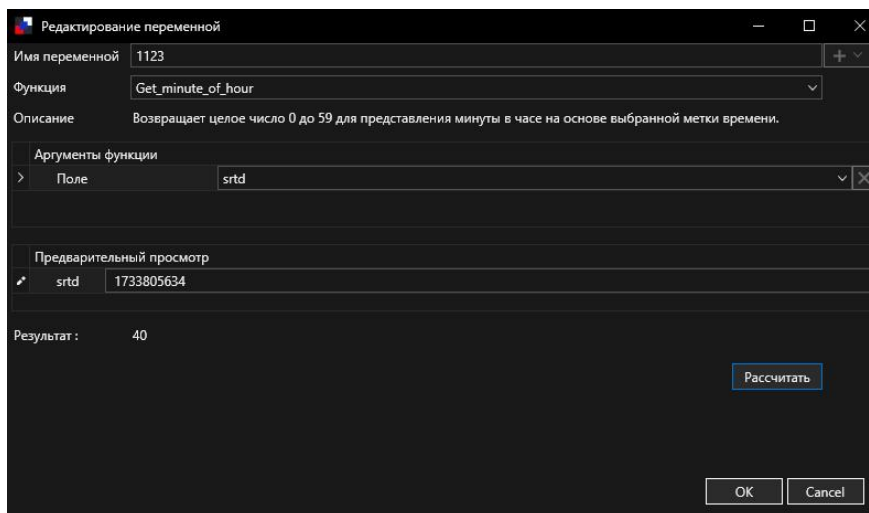


Рисунок 120. Пример функции Get_minute_of_hour

Get_month_of_year

Данная функция возвращает целое число от 1 до 12 для представления месяца, на основе выбранной метки времени.

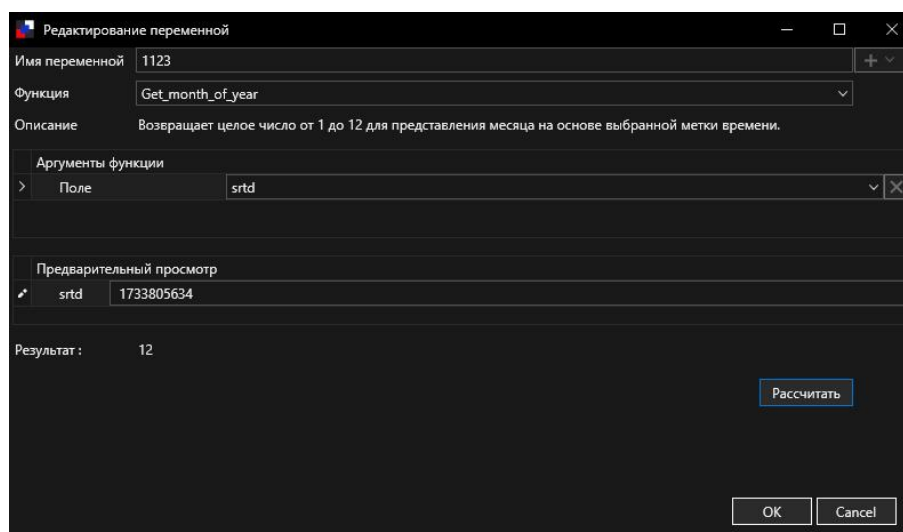


Рисунок 121. Пример функции Get_month_of_year

Get_year

Данная функция возвращает целое число для представления года, на основе выбранной метки времени.

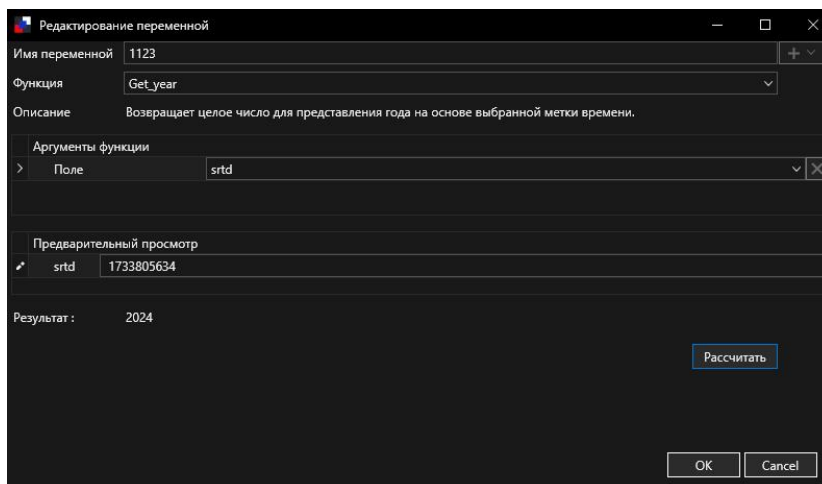


Рисунок 122. Пример функции Get_year

Time_Offset

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

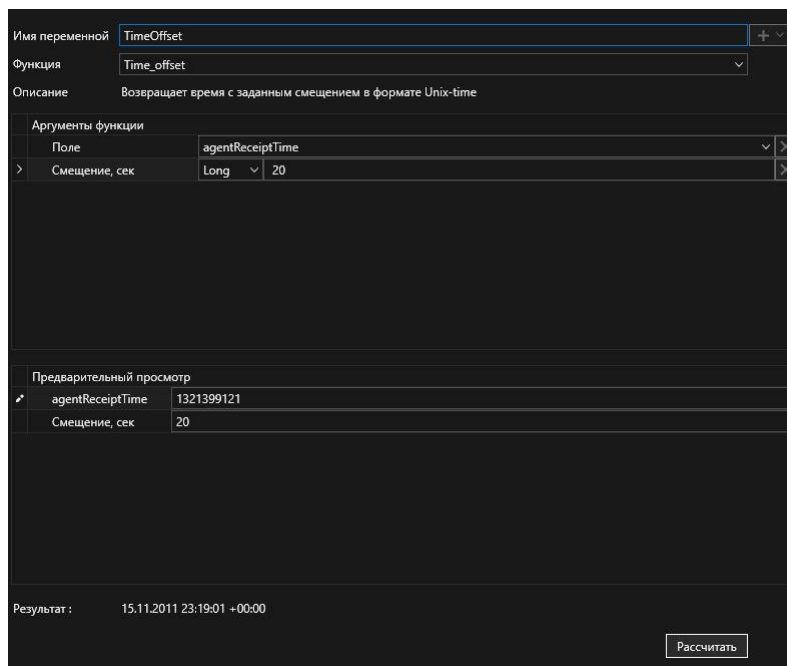
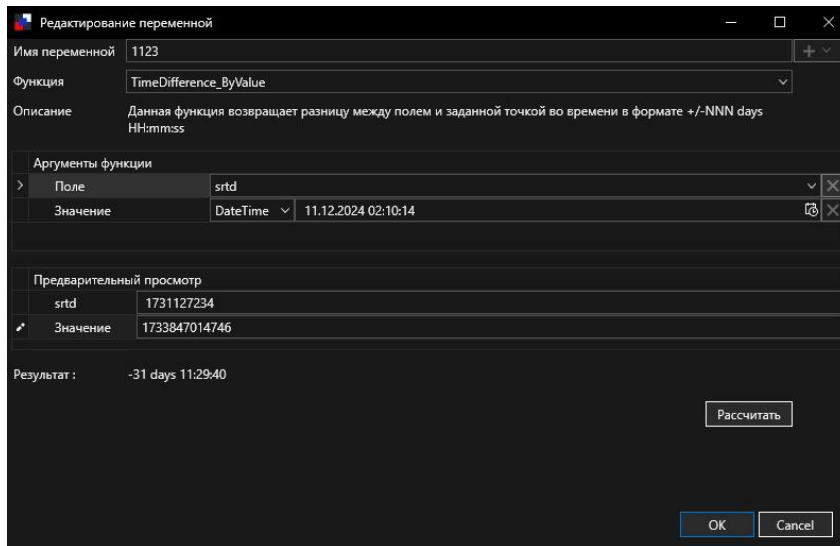


Рисунок 123. Пример функции Time_offset

TimeDifference_ByValue

Данная функция возвращает разницу между полем и заданной точкой во времени в формате +/- NNN days HH:mm:ss



Редактирование переменной

Имя переменной: 1123

Функция: TimeDifference_ByValue

Описание: Данная функция возвращает разницу между полем и заданной точкой во времени в формате +/-NNN days HH:mm:ss

Аргументы функции

Аргумент	Значение
Поле	srtld
Значение	DateTime 11.12.2024 02:10:14

Предварительный просмотр

Аргумент	Значение
srtld	1731127234
Значение	1733847014746

Результат: -31 days 11:29:40

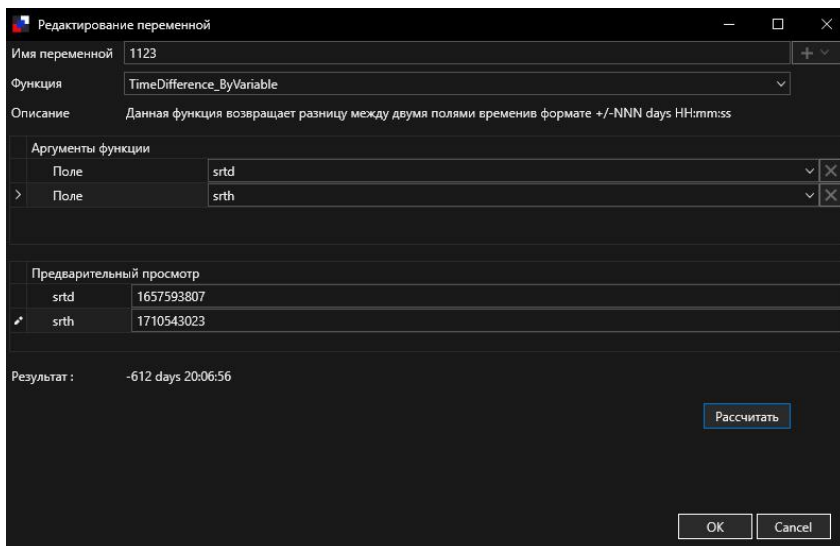
Рассчитать

OK Cancel

Рисунок 124. Пример функции TimeDifference_ByValue

TimeDifference_ByVariable

Данная функция возвращает разницу между двумя полями времени в формате +/- NNN days HH:mm:ss.



Редактирование переменной

Имя переменной: 1123

Функция: TimeDifference_ByVariable

Описание: Данная функция возвращает разницу между двумя полями времени в формате +/-NNN days HH:mm:ss

Аргументы функции

Аргумент	Значение
Поле	srtld
Поле	srth

Предварительный просмотр

Аргумент	Значение
srtld	1657593807
srth	1710543023

Результат: -612 days 20:06:56

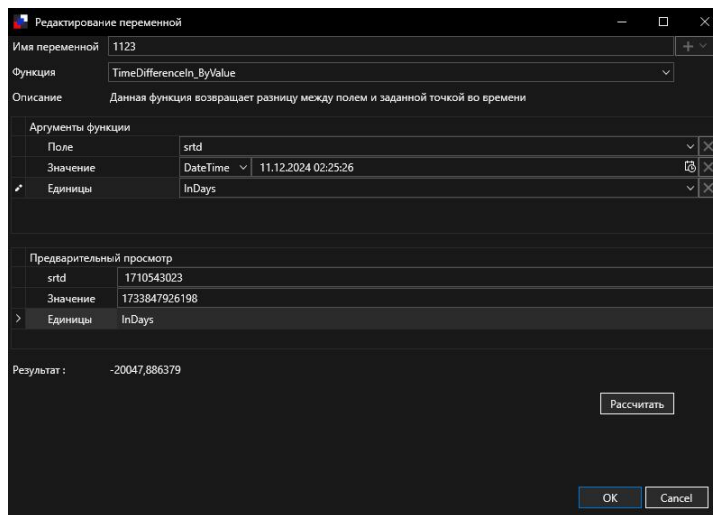
Рассчитать

OK Cancel

Рисунок 125. Пример функции TimeDifference_ByVariable

TimeDifferenceln_ByValue

Данная функция возвращает разницу между полем и заданной точкой во времени.



Редактирование переменной

Имя переменной: 1123

Функция: TimeDifferenceln_ByValue

Описание: Данная функция возвращает разницу между полем и заданной точкой во времени

Аргументы функции

Поле	Значение	Единицы
srtid	DateTime 11.12.2024 02:25:26	InDays

Предварительный просмотр

Поле	Значение	Единицы
srtid	1710543023	InDays
srt	1733847926198	InDays

Результат: -20047,886379

Рассчитать

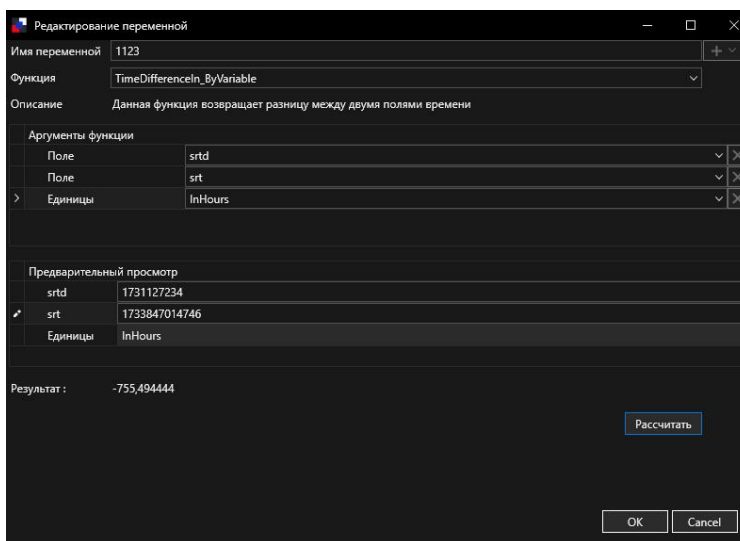
OK Cancel

Рисунок 126. Пример функции TimeDifferenceln_ByValue

TimeDifferenceln_ByVariable

Данная функция возвращает разницу между двумя полями времени.

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



Редактирование переменной

Имя переменной: 1123

Функция: TimeDifferenceln_ByVariable

Описание: Данная функция возвращает разницу между двумя полями времени

Аргументы функции

Поле	Значение	Единицы
srtid	1731127234	InHours
srt	1733847014746	InHours

Предварительный просмотр

Поле	Значение	Единицы
srtid	1731127234	InHours
srt	1733847014746	InHours

Результат: -755,494444

Рассчитать

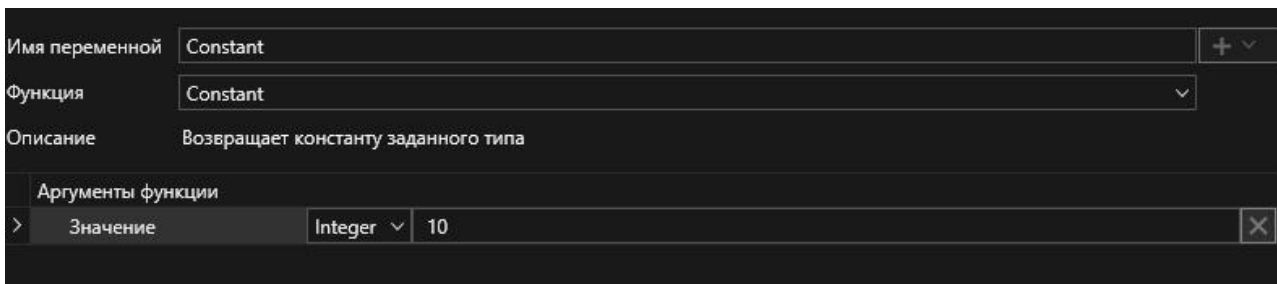
OK Cancel

Рисунок 127. Пример функции TimeDifferenceln_ByVarriable

4. Пользовательские функции

Constant

Данная функция возвращает константу заданного типа.

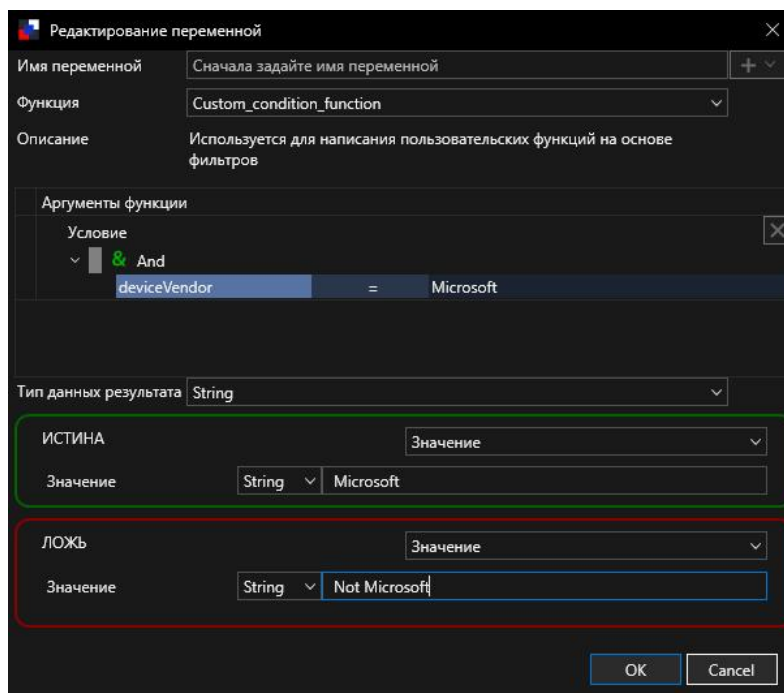


Имя переменной	Constant
Функция	Constant
Описание	Возвращает константу заданного типа
Аргументы функции	
> Значение	Integer 10

Рисунок 128. Пример функции Constant

Custom_condition_function

Данная функция используется для написания пользовательских функций на основе фильтров.



Имя переменной	Сначала задайте имя переменной
Функция	Custom_condition_function
Описание	Используется для написания пользовательских функций на основе фильтров
Аргументы функции	
Условие	deviceVendor = Microsoft
Тип данных результата String	
ИСТИНА	Значение String Microsoft
ЛОЖЬ	Значение String Not Microsoft

Рисунок 129. Пример функции Custom_condition_function

Get_array_value

Данная функция ищет ключ в поле(массиве) ключей и возвращает соответствующее значение элемента (по порядковому номеру) из поля(массива) значений.

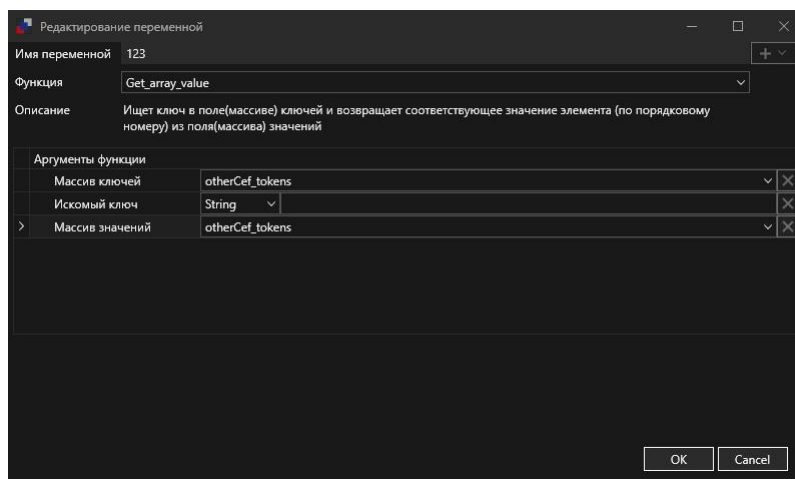


Рисунок 130. Пример функции `Get_array_value`

Match_True

Данная функция возвращает результат функции Match в виде 1 или 0 – соответствие/не соответствие значения поля (переменной) заданному значению.

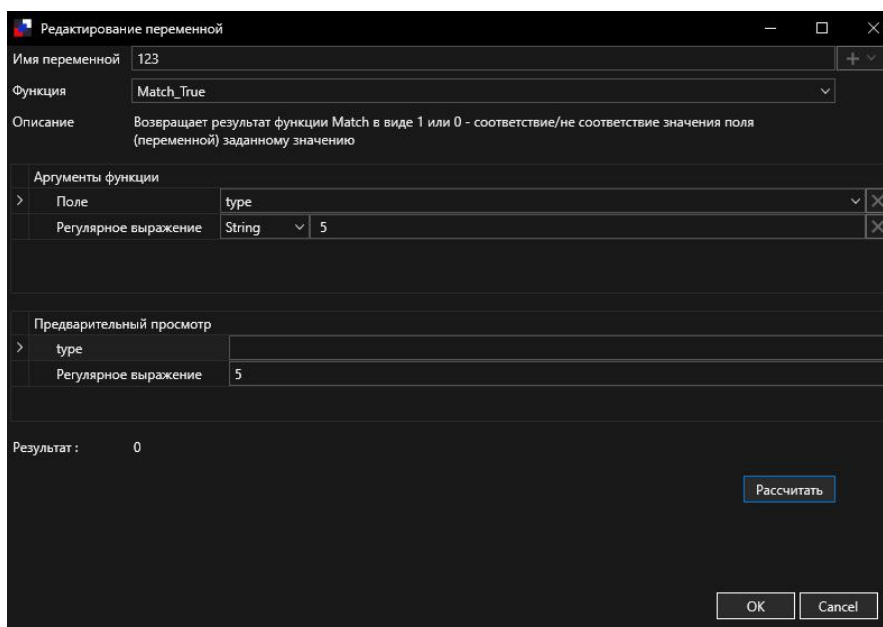
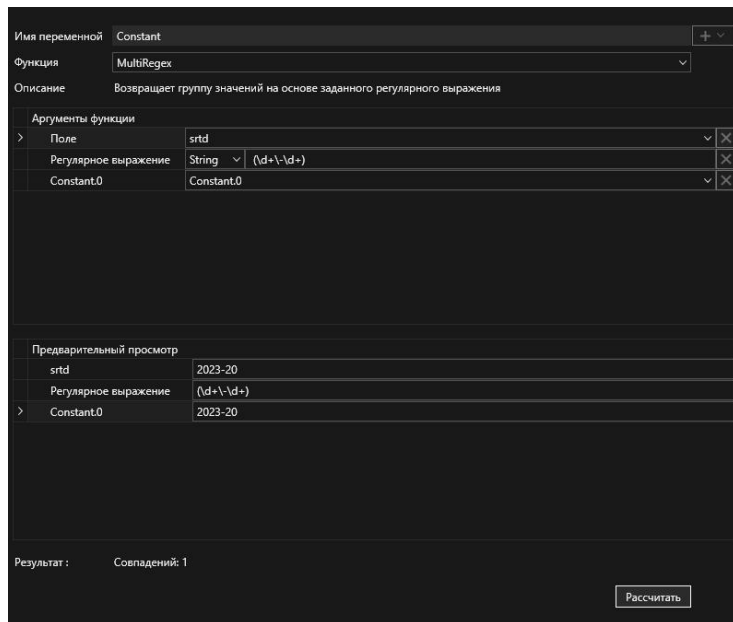


Рисунок 131. Пример функции `Match_True`

MultiRegex

Данная функция возвращает группу значений на основе заданного регулярного выражения.



Имя переменной: Constant

Функция: MultiRegex

Описание: Возвращает группу значений на основе заданного регулярного выражения

Аргументы функции:

Поле	Значение
srtid	srtid
Регулярное выражение	String (ld+~\ld+)
Constant 0	Constant 0

Предварительный просмотр:

Поле	Значение
srtid	2023-20
Регулярное выражение	(ld+~\ld+)
Constant 0	2023-20

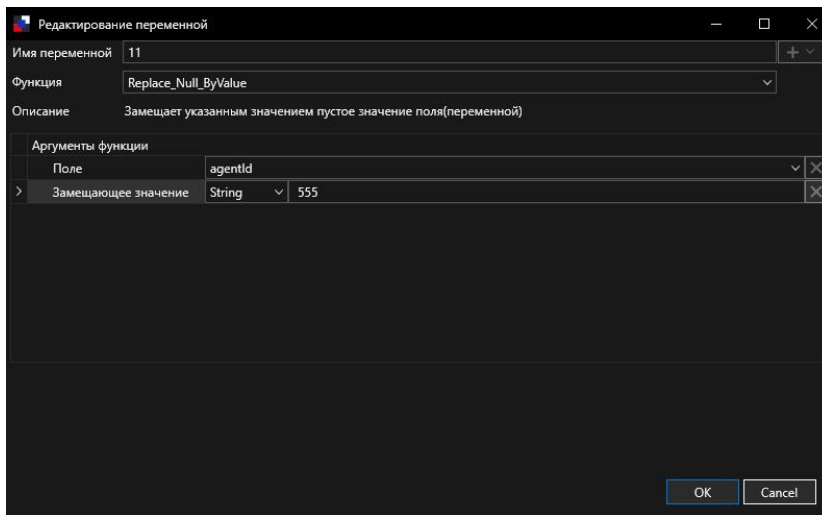
Результат: Совпадений: 1

Рассчитать

Рисунок 132. Пример функции MultiRegex

Replace_Null_ByValue

Данная функция замещает указанное значение поля (переменной)



Редактирование переменной

Имя переменной: 11

Функция: Replace_Null_ByValue

Описание: Замещает указанным значением пустое значение поля(переменной)

Аргументы функции:

Поле	Значение
agentId	agentId
Замещающее значение	String 555

OK Cancel

Рисунок 133. Пример функции Replace_Null_ByValue

Replace_Null_ByVariable

Данная функция замещает указанное значение поля (переменной)

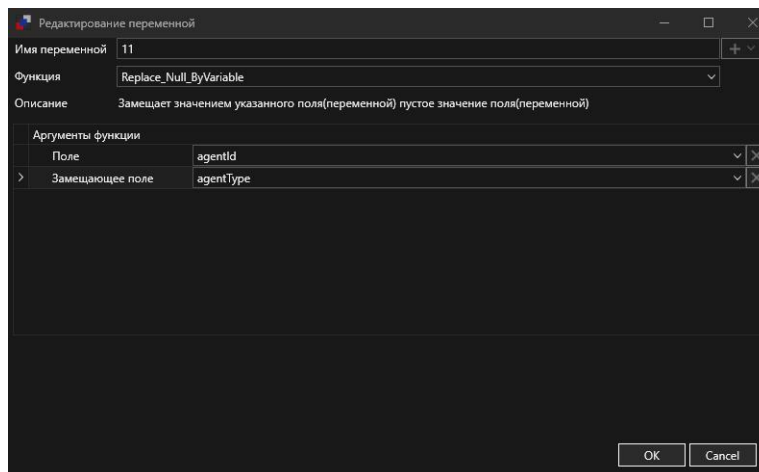


Рисунок 134. Пример функции Replace_Null_ByVariable

Regex

Данная функция возвращает значение на основе заданного регулярного выражения.

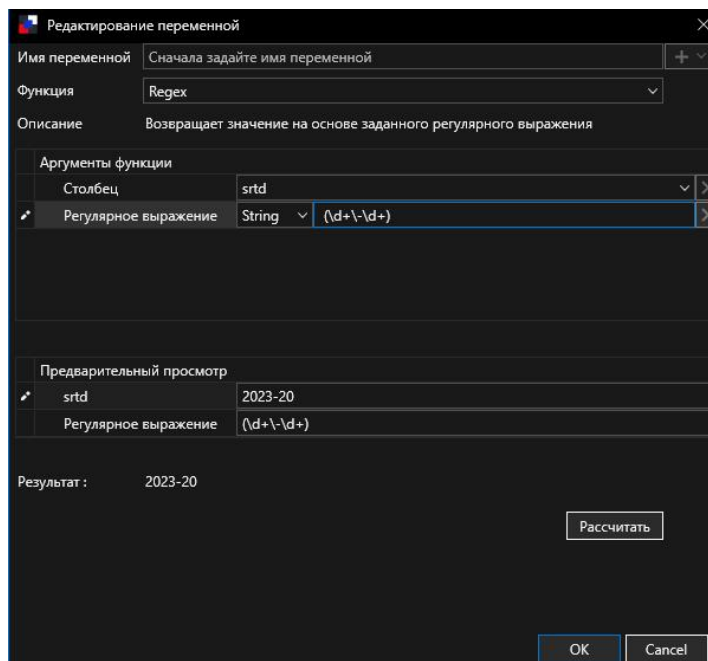


Рисунок 135. Пример функции Regex

5. Строковые функции

Alias_field

Данная функция создаёт альтернативное имя для указанного поля.

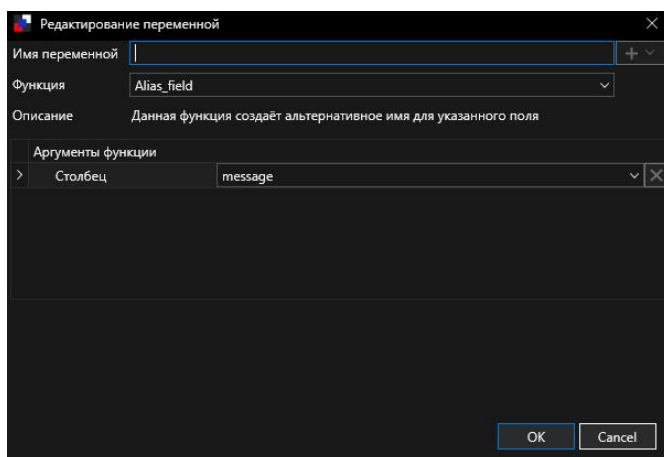


Рисунок 136. Пример функции Alias_field

Concat

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

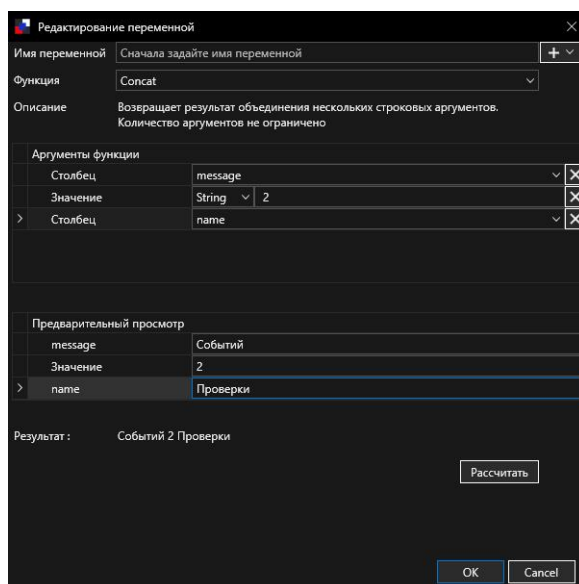


Рисунок 137. Пример функции Concat

Replace

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

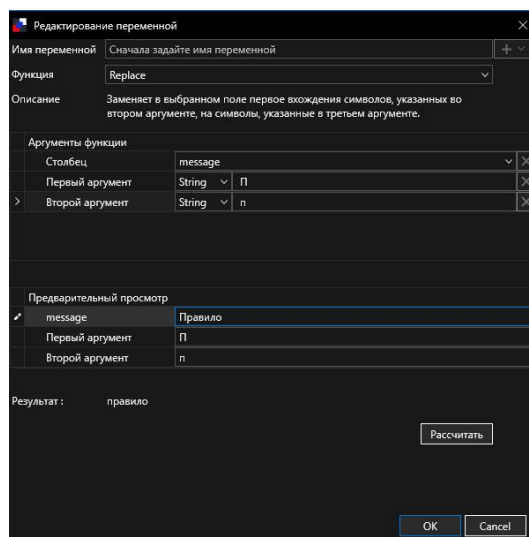
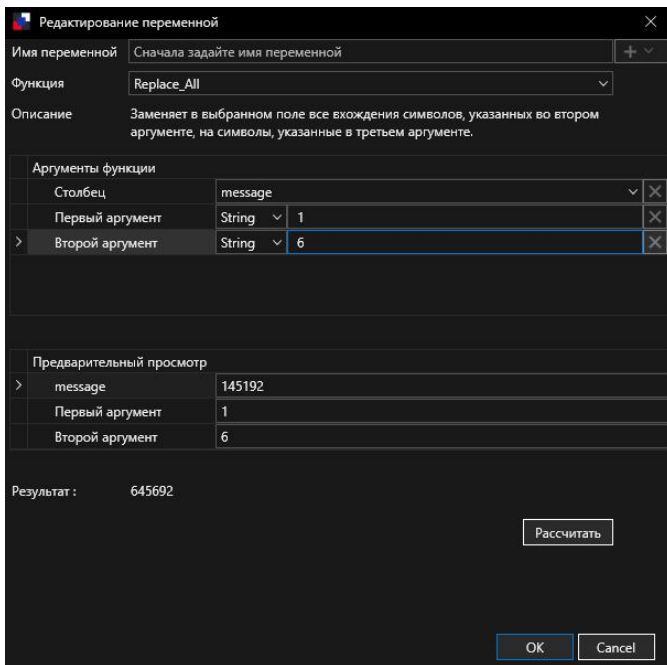


Рисунок 138. Пример функции Replace

Replace_all

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

регистрозависимая.



Редактирование переменной

Имя переменной: Сначала задайте имя переменной

Функция: Replace_All

Описание: Заменяет в выбранном поле все вхождения символов, указанных во втором аргументе, на символы, указанные в третьем аргументе.

Аргументы функции	
Столбец	message
Первый аргумент	String 1
Второй аргумент	String 6

Предварительный просмотр

message	
Первый аргумент	1
Второй аргумент	6

Результат: 645692

Рассчитать

OK Cancel

Рисунок 139. Пример функции `Replace_all`

Split

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

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.

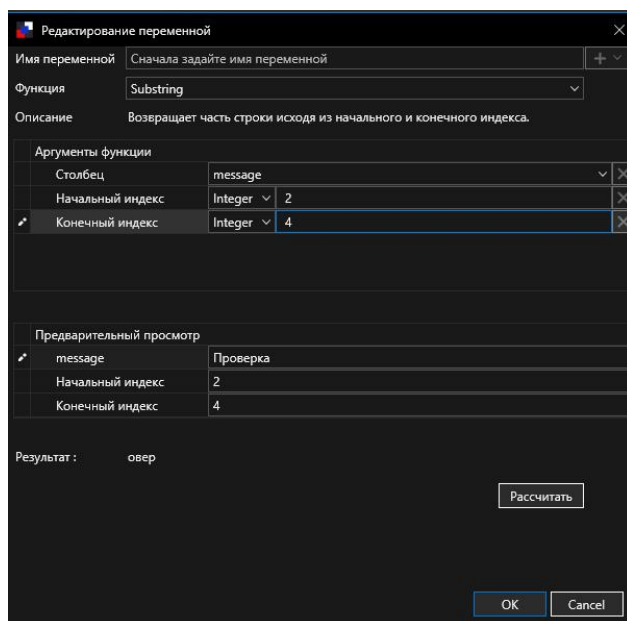


Рисунок 140. Пример функции Substring

To_lower

Данная функция возвращает строковый аргумент, преобразованный в нижний регистр.

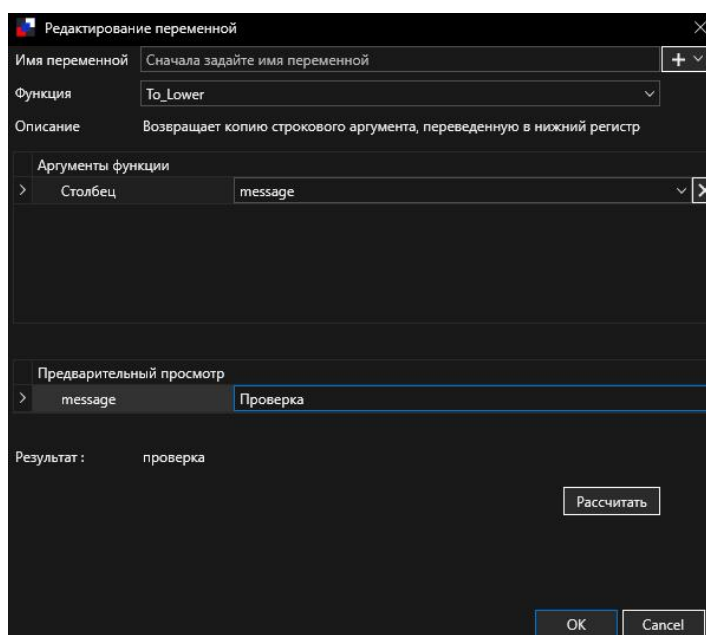


Рисунок 141. Пример функции To_lower

To_upper

Данная функция возвращает строковый аргумент, преобразованный в верхний регистр.

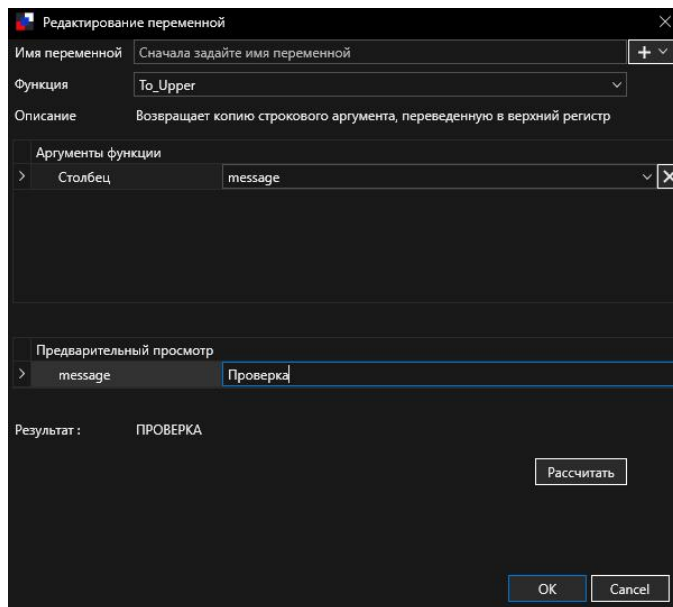


Рисунок 142. Пример функции To_upper

6. Функции для работы с активными списками

Get_activeslist_value

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

В меню «аргументы функции» необходимо добавить нужные аргументы (см. Рисунок 143). При выборе функции Get_activeslist_value необходимо выбрать активный список. Также есть возможность просмотра содержимого активного списка, для этого необходимо выбрать кнопку .

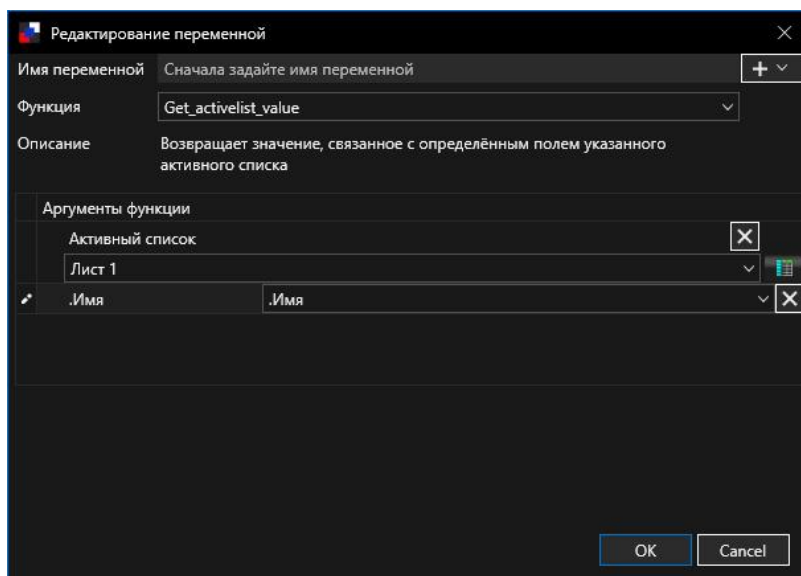


Рисунок 143. Пример функции `Get_activelist_value`

7. Преобразование типа

`DateTime_to_UnixTime`

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

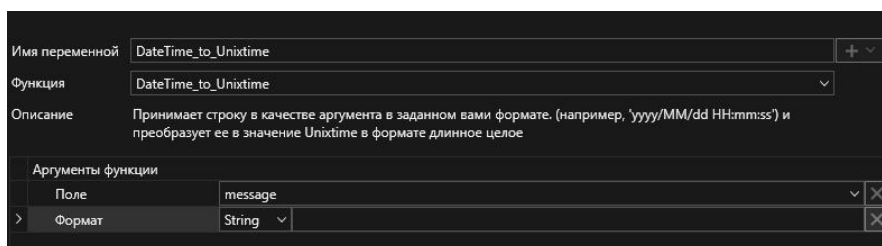


Рисунок 144. Пример функции `DateTime_to_UnixTime`

`Ip_to_integer`

Данная функция возвращает значение поля формата IP в формате int.

`Ip_to_String`

Данная функция возвращает значение поля формата IP в формате string.

Number_to_String

Данная функция возвращает значение поля формата Number в формате string.

String_to_Date

Данная функция принимает строку в качестве аргумента в заданном вами формат, (например 'уууу/ММ/дд НН:мм:сс') и преобразует ее в значение Unixtime в формате длинное целое.

String_to_integer

Данная функция возвращает значение поля формата string в формате int.

String_to_Ip

Данная функция возвращает значение поля формата string в формате IPv4.

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.

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 145).

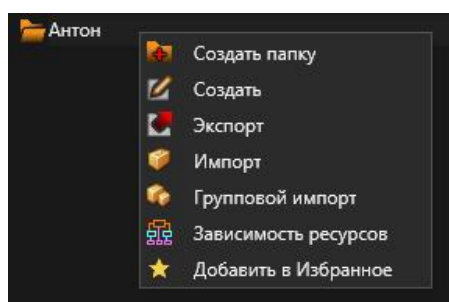


Рисунок 145. Дерево правил обогащения

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.

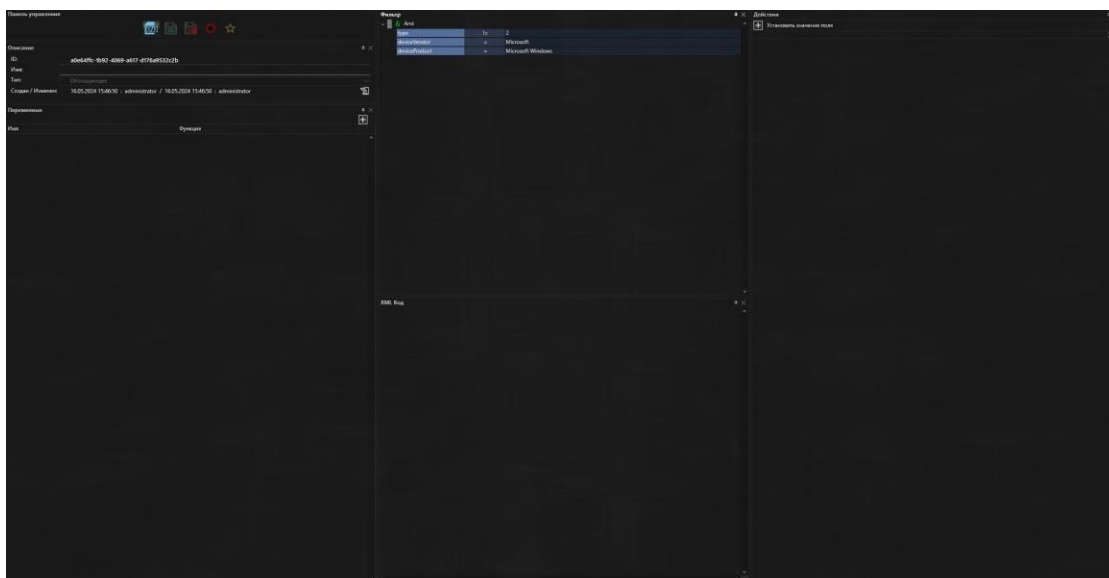


Рисунок 146. Пример правила обогащения

РЕТРОСПЕКТИВНЫЕ ПРАВИЛА

Для выявления инцидентов 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 147).

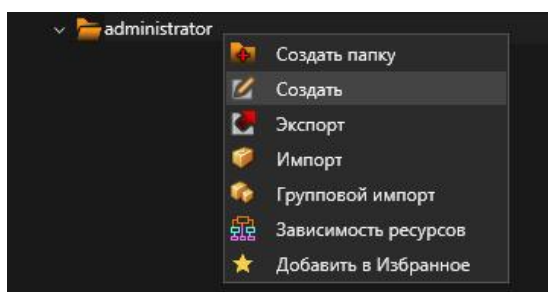


Рисунок 147. Дерево ретроспективных правил

После чего откроется окно конструктора написания ретроспективных правил (см. Рисунок 148).

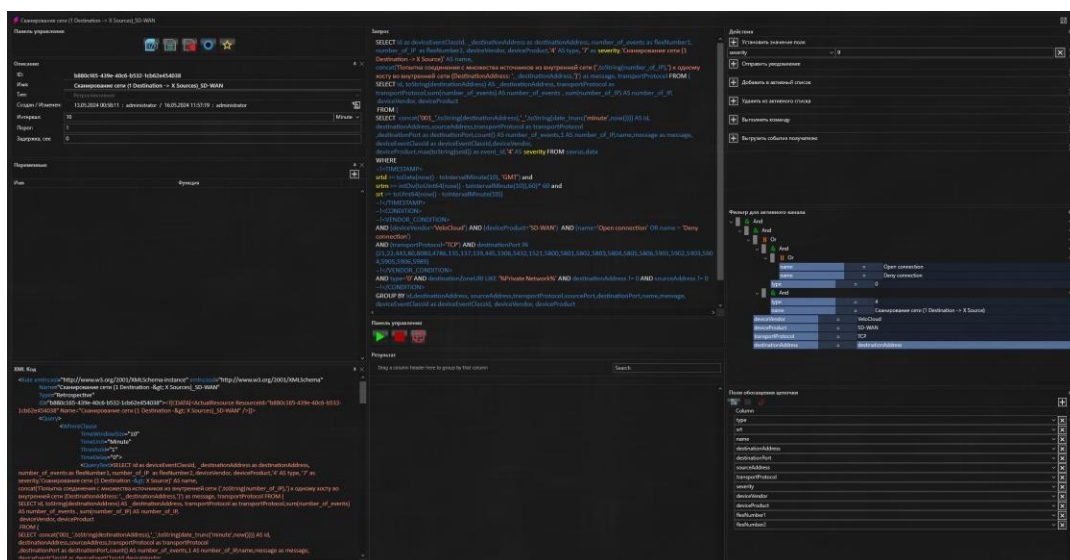


Рисунок 148. Конструктор создания ретроспективных правил

Для создания правил в первую очередь необходимо заполнить основную информацию (см. Рисунок 149), где:

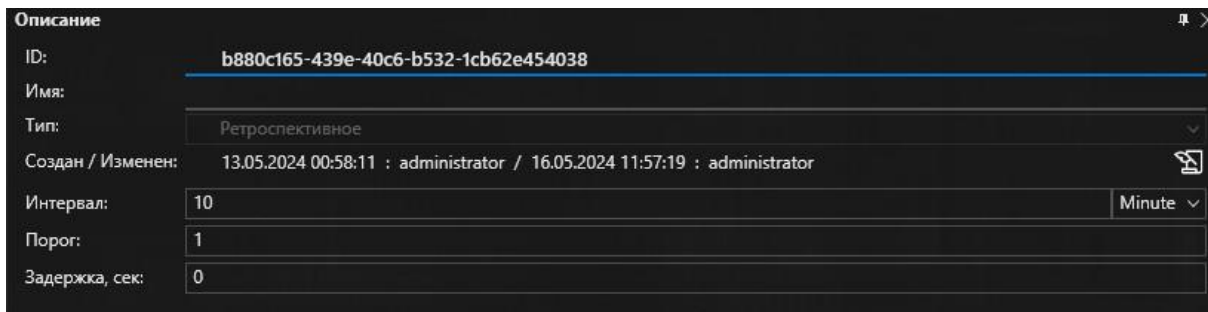


Рисунок 149. Основная информация по Правилу

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

Для просмотра истории изменения необходимо нажать на кнопку  (подробнее см. раздел «Просмотр истории изменений»).

Система поддерживает 2 типа правил: Ретроспективное и Ретроспективное GUI

- ретроспективное правило формируется при помощи ввода SQL-запроса;
- ретроспективное GUI правило формируется при помощи графического интерфейса консоли.

1. Ретроспективное правило

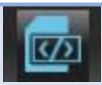
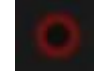
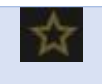
В окне «Запрос» необходимо написать SQL-запрос к историческим данным, на основе которого будет производиться выборка событий. Подробнее о написании SQL-запросов можно посмотреть в разделе «SQL ЗАПРОСЫ».

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 8. 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.

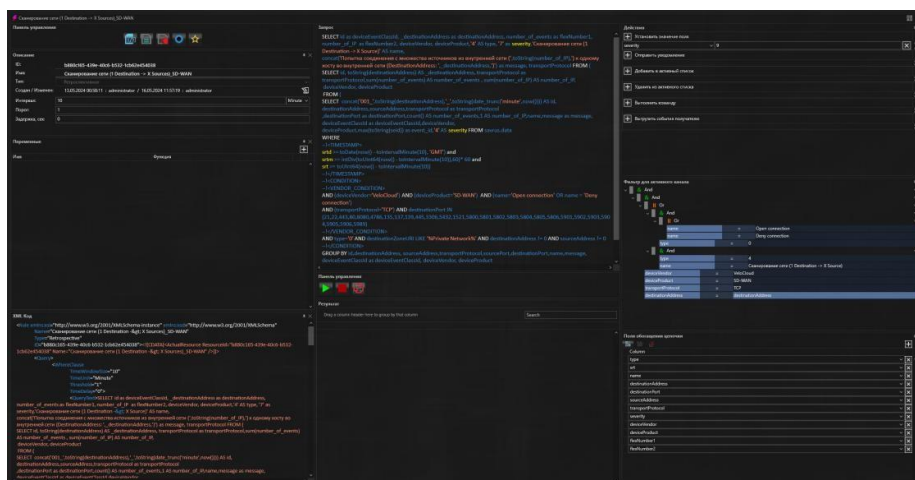


Рисунок 150. Пример ретроспективного правила

2. Ретроспективное GUI

При выборе типа правила «Ретроспективное GUI» в окне «Описание» добавятся дополнительные строки: начальная дата, лимит и порог.

- Начальная дата – указывается порог времени, от которого будет происходить запрос к историческим данным. Правее от поля с датой расположено активное поле «Now». При активации данного поля начальная дата синхронизируется с вашим реальным временем.
- Порог – указывается кол-во событий для срабатывания правила.
- Лимит – указывается максимальное кол-во событий, отображаемых при применении данного правила.

Все настроенные параметры в окне «Описание» будут накладываться на отработку верхнего условия And в окне «Фильтр запроса».

При помощи окна «Фильтр запроса» необходимо составить условие исполнения правила. В данном окне находятся два условия And. Согласно верхнему условию And выполняется запрос в БД (данное условие отвечает за составление SQL-запроса), на основе которого выгружается список записей, к которым далее применяется потоковая обработка данных согласно нижнему условию And.

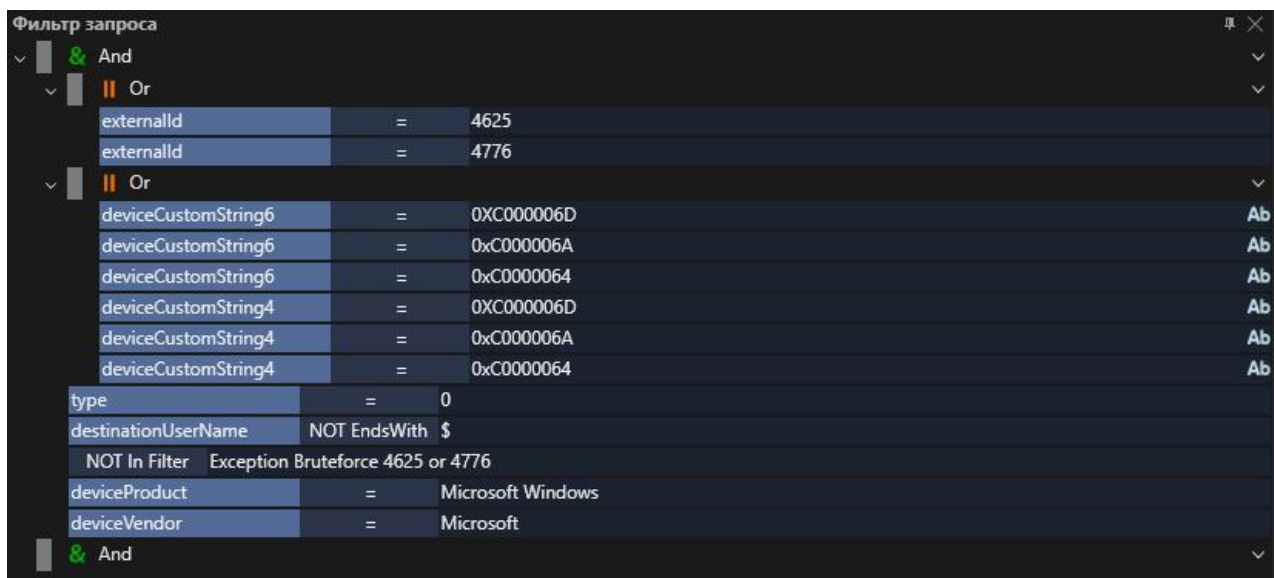


Рисунок 151. Пример условий правила "Ретроспективное GUI"

В окне «Панель управления» расположены кнопки: «SQL-запрос» - формирует SQL-запрос по ранее составленным условиям в окне «Фильтр запроса», который отобразится в окне «Запрос», «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 соответствующих подпунктах раздела «ПРАВИЛА».

[illegible]

Рисунок 152. Пример правила "Ретроспективное GUI"

3. Ретроспективное сравнение

Правила типа «Ретроспективное сравнение» следует использовать, если необходимо построить цепочку корреляции с двумя событиями. Например, когда необходимы выявить инцидент, где сначала наступило одно событие, а потом второе. Главной особенностью данного вида правил является конструктор для написания сложного запроса.

Данный вид правил поддерживает обработку только двух разных событий с общими полями.

Для создания правила в первую очередь необходимо заполнить основную информацию, где:

- ID – уникальный идентификатор Правила присваивается автоматически;
- Имя – наименование правила;
- Source – таблица, из которой будет производится выборка событий с помощью запроса. Запросы можно писать ко всем таблицам, которые есть в ClickHouse, а также к Активным спискам;
- Путь к ресурсу – расположение правила;
- Тип – тип правила;
- Создан/Изменен – дата и время создания/изменения правила, присваивается автоматически;
- Частота выполнения – это количество раз за единицу времени, которое будет выполняться запрос, например, раз в 5 минут или 2 раза в час и т.д. Единица времени может принимать следующие значения: секунды, минуты, дни;
- Начальная дата – Дата, с которой начинается выборка событий в запросе.
- Лимит – это максимальное кол-во записей, выводимых в запросе.

Далее необходимо выбрать поля, которые будут перенесены из базового события в корреляционное. Кол-во полей не ограничено.



Column	Field
endTime	endTime
destinationHostName	
deviceEventClassId	

Поле сравнения: endTime

☒ Match IN

Interval (sec): 120

Рисунок 153. Пример "Выбранных полей"

После этого из выбранных полей необходимо определить одно, по которому будет проводиться сравнение события, на рисунке выше это поле «endTime». Т. е. то поле, которое будет совпадать у обоих событий. Выбрать режим работы параметра Match IN, если галочка установлена, то это означает что 1-е и 2-е событие произошли, если галочки нет – то 1-е событие произошло, а 2-е – нет. И указать временной интервал (в секундах), в течение которого должно случиться или не случиться событие 2.

Далее при помощи окна «Фильтр запроса» необходимо составить условие выполнения правила. В данном окне находятся три фильтра:

- первый фильтр накладывает условия на запрос к первому событию;
- второй фильтр накладывает условия на запрос ко второму событию;
- третий фильтр является уточняющим и накладывает условие на результат объединённого запроса (тот запрос, который формируется из Выбранных полей и фильтров на события и расположенный в блоке «Запрос»).

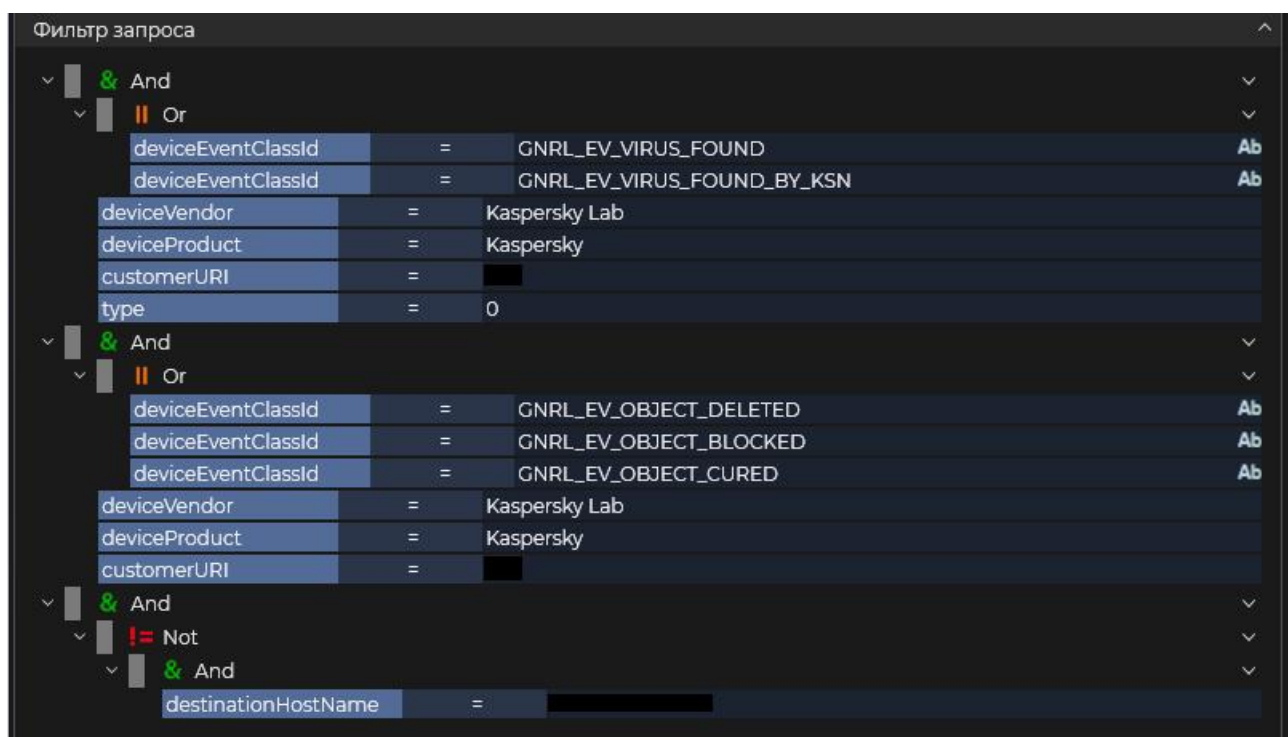


Рисунок 154. Пример условий правила "Ретроспективное сравнение"

После выбора полей и написания фильтра, рекомендуется отобразить SQL запрос и выполнить его, чтобы убедиться в его корректности.

Ниже предоставлен пример сформированного запроса, где t1 – это событие 1, а t2 – это событие 2. Система автоматически назначает переменной t1 максимальные значения полям srt и seid, а переменной t2 – минимальные значения.

```
SELECT
    t1.srt_max AS `t1.srt_max`,
    t2.srt_min AS `t2.srt_min`,
    t1.seid_max AS `t1.seid_max`,
    t2.seid_min AS `t2.seid_min`,
    t1.endTime AS `t1.endTime`,
    t2.endTime AS `t2.endTime`,
    t1.destinationHostName AS `t1.destinationHostName`,
    t2.destinationHostName AS `t2.destinationHostName`,
    t1.deviceEventClassId AS `t1.deviceEventClassId`,
    t2.deviceEventClassId AS `t2.deviceEventClassId`
FROM
    ( SELE
CT
    endTime,
    destinationHostName,
    deviceEventClassId,
    max (toDateTime(srt)) AS srt_max,
    max (seid) AS seid_max
FROM savrus.data
WHERE srt > toUnixTimestamp(now() - INTERVAL 120 SECOND, 'UTC')
    AND ( ( ( deviceVendor = 'Kaspersky Lab'
    AND deviceProduct = 'Kaspersky'
    AND customerURI = 'test'
    AND type = '0' )
    AND ( deviceEventClassId ILIKE 'GNRL_EV_VIRUS_FOUND'
    OR deviceEventClassId ILIKE 'GNRL_EV_VIRUS_FOUND_BY_KSN' ) ) )
GROUP BY
    endTime,
    destinationHostName,
    deviceEventClassId) t1, (
SELECT
    endTime,
    destinationHostName,
    deviceEventClassId,
    min (toDateTime(srt)) AS srt_min,
    min (seid) AS seid_min
FROM savrus.data
WHERE srt > toUnixTimestamp(now() - INTERVAL 120 SECOND, 'UTC')
    AND ( ( ( deviceVendor = 'Kaspersky Lab'
    AND deviceProduct = 'Kaspersky'
    AND customerURI = 'test' )
    AND ( deviceEventClassId ILIKE 'GNRL_EV_OBJECT_DELETED'
    OR deviceEventClassId ILIKE 'GNRL_EV_OBJECT_BLOCKED'
    OR deviceEventClassId ILIKE 'GNRL_EV_OBJECT_CURED' ) ) ) )
```

```
GROUP BY
    endTime,
    destinationHostName,
    deviceEventClassId) t2
WHERE t1.endTime = t2.endTime
LIMIT 1000
```

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 соответствующих подпунктах раздела «ПРАВИЛА».

Но для сохранения и включения правила, должно быть создано, хотя бы одно любое действие. Рекомендуем устанавливать любое цифровое значение в диапазоне (0-10) для поля severity.

На рисунке ниже представлен пример сформированного правила «Ретроспективное сравнение», которое выявляет обнаружение и удаление файла антивирусом Kaspersky.

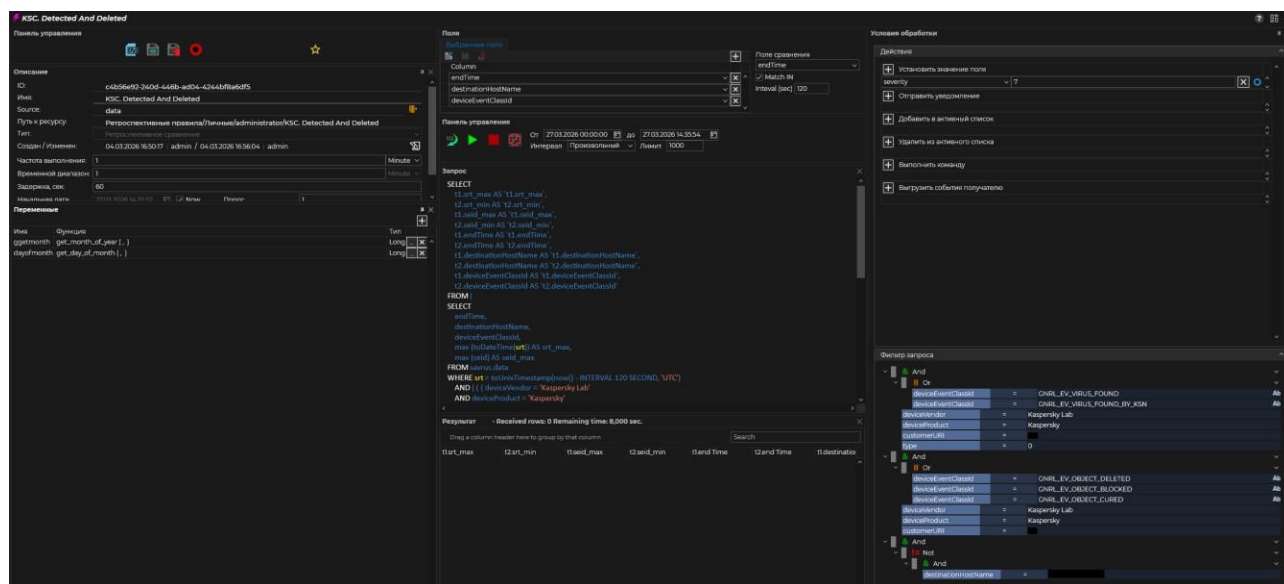


Рисунок 155. Пример правила "Ретроспективное сравнение"

ФИЛЬТРЫ

1. Создание фильтра

Для создания нового фильтра необходимо перейти на вкладку «Фильтры». Далее, нажав правой кнопкой мыши (ПКМ) на папку, выбрать кнопку «Создать» (см. Рисунок 156).

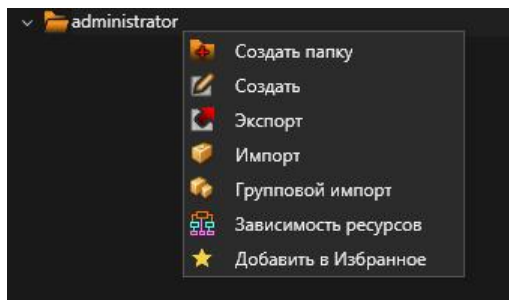


Рисунок 156. Окно создания фильтра

Далее необходимо ввести название фильтра и задать условия (см. Рисунок 157) фильтрации событий. Для сохранения фильтра необходимо нажать на кнопку .

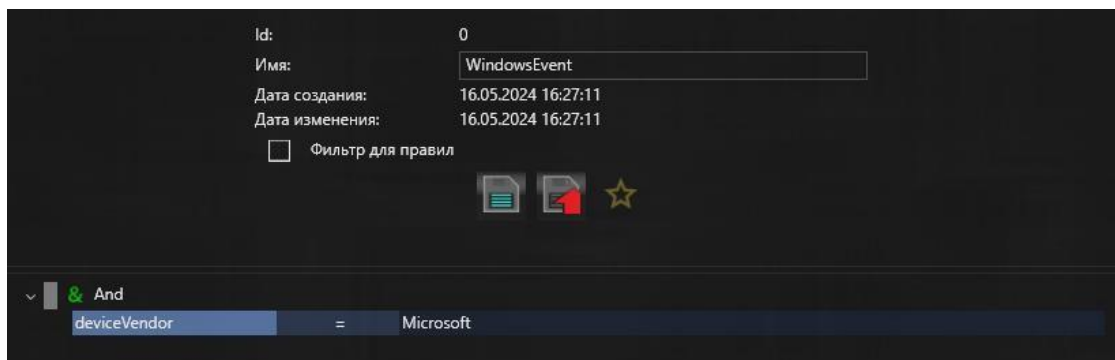


Рисунок 157. Окно настройки фильтра

2. Изменение фильтра

Для изменения фильтра необходимо во вкладке «Фильтры» нажать ПКМ по нужному фильтру и в контекстном меню выбрать пункт «Открыть» (см. Рисунок 158).

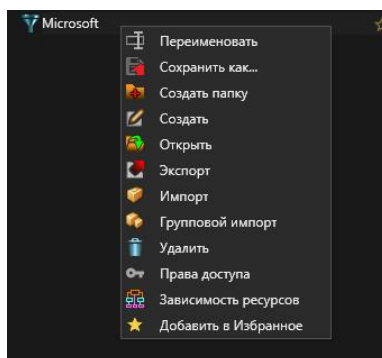


Рисунок 158. Окно взаимодействия с фильтром

В открывшемся окне следует произвести необходимые изменения (см. Рисунок 159). Для сохранения изменений необходимо нажать на кнопку .

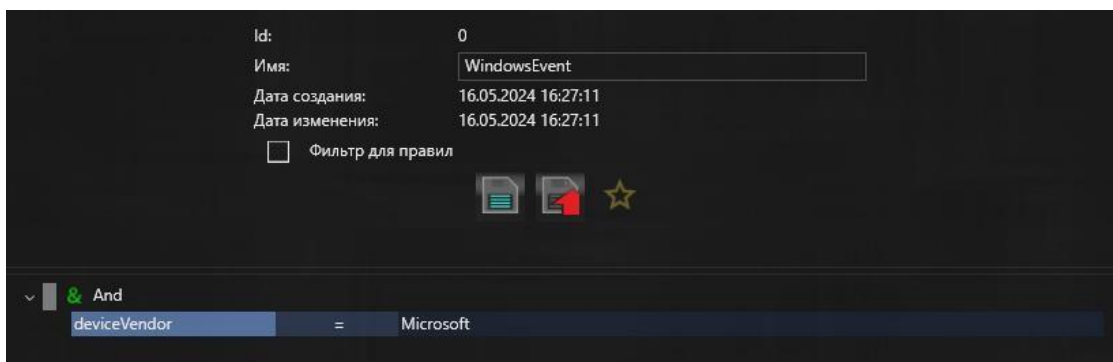


Рисунок 159. Окно редактирования фильтра

4. Удаление фильтра

Для удаления фильтра необходимо во вкладке «Фильтры» нажать ПКМ по нужному фильтру и в контекстном меню выбрать пункт «Удалить» (Рисунок 160). После чего Фильтр будет помечен на удаление, для полного удаления необходимо повторить процедуру.

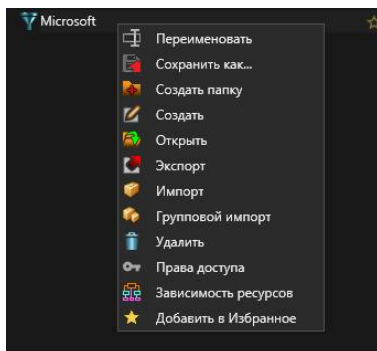


Рисунок 160. Удаление фильтра

5. Создание условий

Для этого требуется нажать ПКМ на условие And, и выбрать пункт создания условия ЛКМ (см. Рисунок 161).

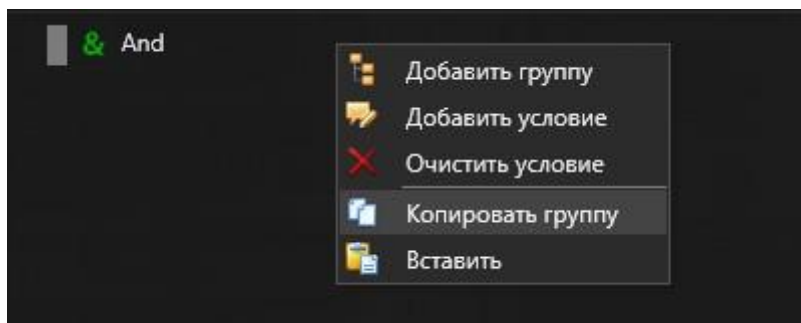


Рисунок 161. Создание условия фильтра

В открывшемся окне можно выбрать необходимые условия (см. Рисунок 162). По умолчанию в фильтре не установлена регистронезависимость, при необходимости её можно включить в редакторе условий.

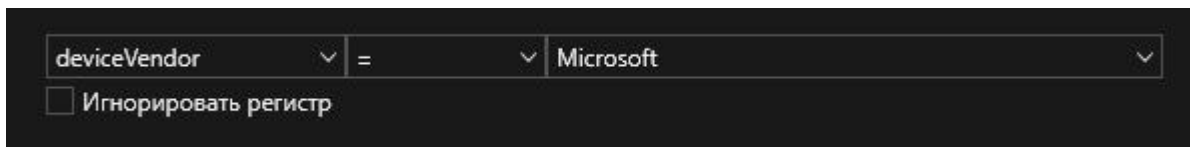


Рисунок 162. Окно создания условий

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.



Рисунок 163. Пример условия

6. Сохранение условий

Для сохранения условия необходимо нажать «ЛКМ» на «ОК». После этого, созданное условие высветится в списке условий фильтра (см. Рисунок 164).

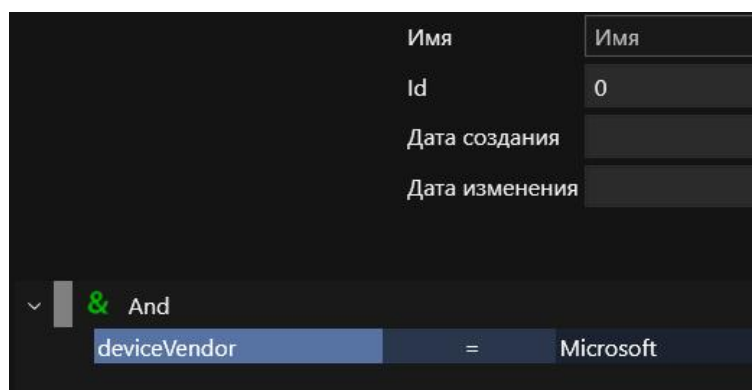


Рисунок 164. Список условий фильтра

7. Удаление условий

Для удаления условия следует нажать ПКМ на условия и в контекстном меню выбрать «Удалить условие» (см. Рисунок 165).

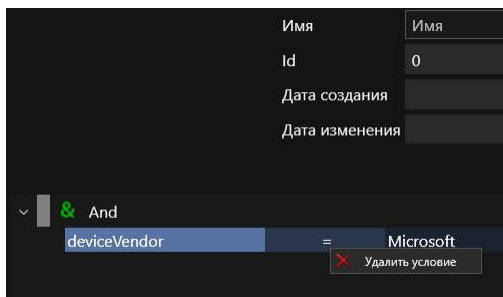


Рисунок 165. Удаление условия

8. 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 166).

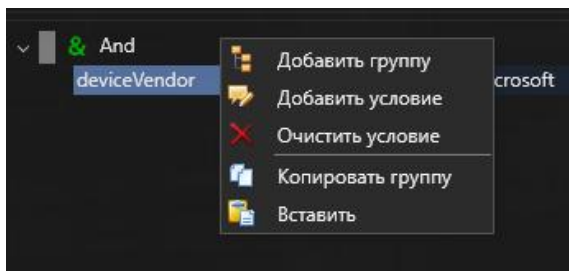


Рисунок 166. Добавление группы условий

9. Копирование и вставка условий

Также имеется возможность копировать и вставлять условия. Для этого нужно нажать ПКМ в свободном поле и выбрать один из возможных пунктов (см. Рисунок 167).

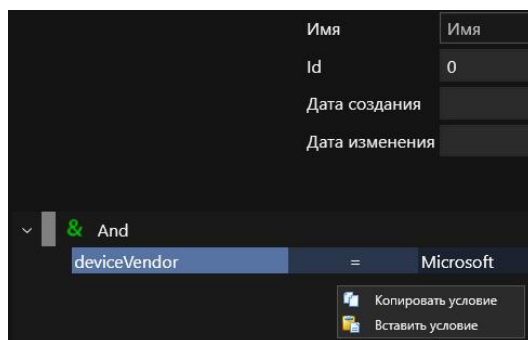


Рисунок 167. Копирование и вставка условий

SQL ЗАПРОСЫ

1. 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 168).

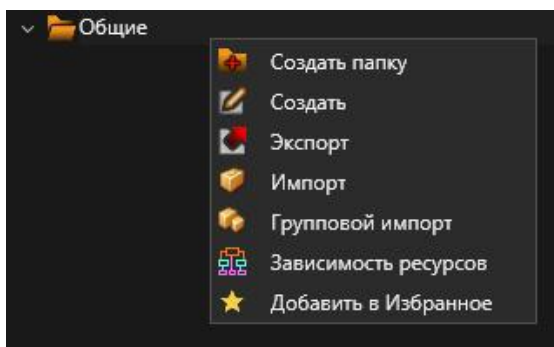


Рисунок 168. Меню взаимодействия

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 169).



Рисунок 169. Таблицы БД

Далее необходимо ввести название и написать SQL запрос (см. Рисунок 170) для выборки данных. Для удобства написания запроса есть возможность двойным нажатием ЛКМ по названию таблицы или поля автоматически переносить их в строку запроса.

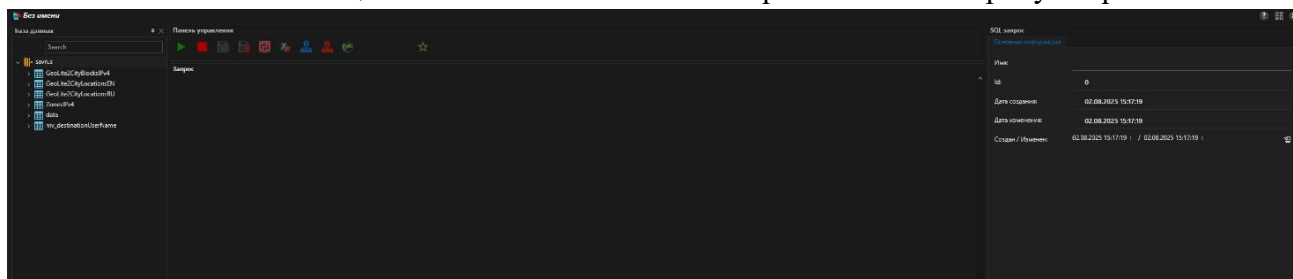


Рисунок 170. Окно создание запроса

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 171). После этого в поле запроса появится диапазон времени (см. Рисунок 170). 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 171). После поле «Severity» в окне запроса примет более понятный, читаемый вид. Для всех полей отмеченных жёлтым цветом в поле «Запрос» доступна функция автоматического ввода функциями «Clickhouse date» и «Severity».

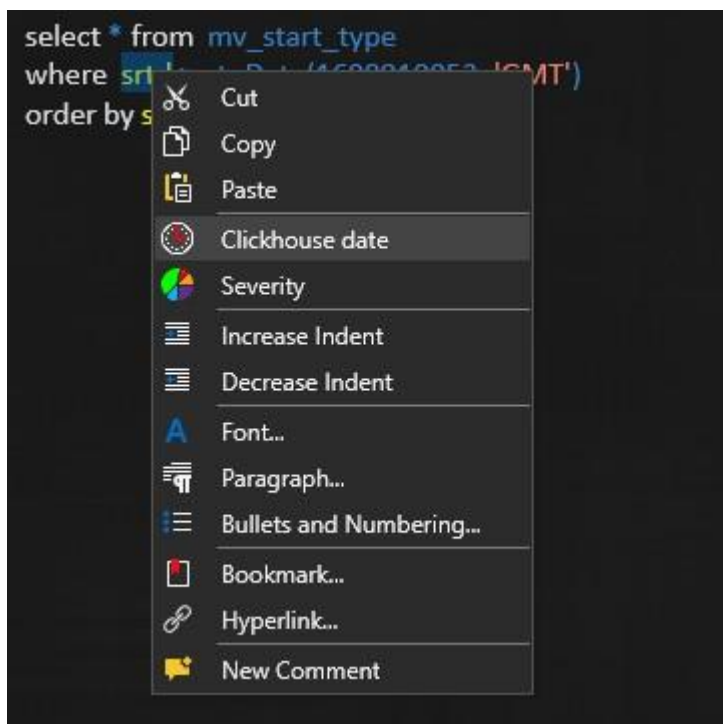


Рисунок 171. Меню взаимодействия с запросом

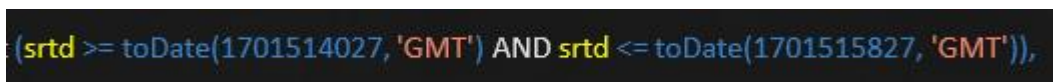


Рисунок 172. Пример автозаполнения диапазона

При нажатии на кнопку  в окне «Результат» произойдёт выполнение SQL запроса и вывод результата (см. Рисунок 173). Также доступен функционал отдельного выполнения запроса. Для это необходимо выделить необходимую часть запроса и нажать на кнопку .



Рисунок 173. Окно результата

2. Изменение SQL запроса

Для изменения запроса следует во вкладке «SQL запросы» нажать ПКМ по необходимому и в контекстном меню выбрать пункт «Открыть» (см. Рисунок 174).

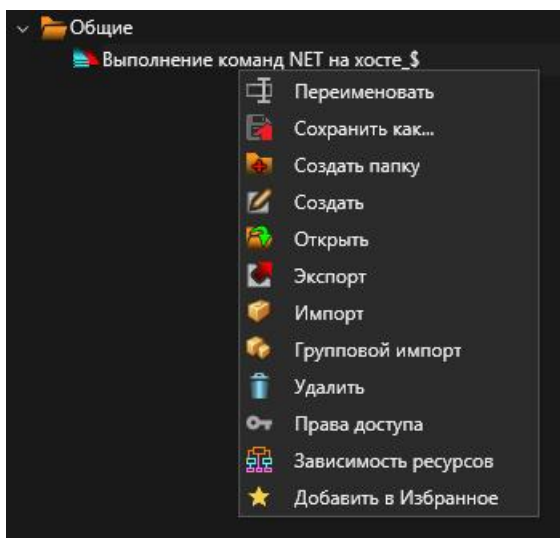


Рисунок 174. Меню взаимодействия

В открывшемся окне следует произвести необходимые изменения (см. Рисунок 175).
Для сохранения изменений необходимо нажать на кнопку .

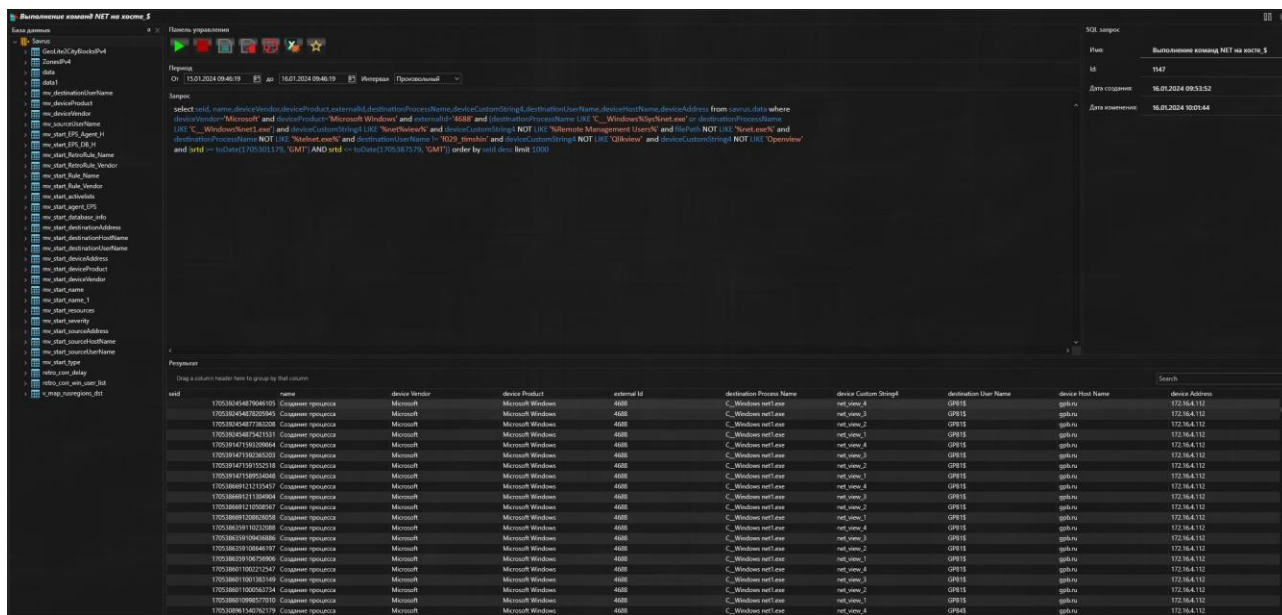


Рисунок 175. Окно редактирования запроса

3. Удаление SQL запроса

Для удаления запроса следует во вкладке «SQL запросы» нажать ПКМ по необходимому и в контекстном меню выбрать пункт «Удалить» (см. Рисунок 176). После

чего запрос будет помечен на удаление, для полного удаления необходимо повторить процедуру.

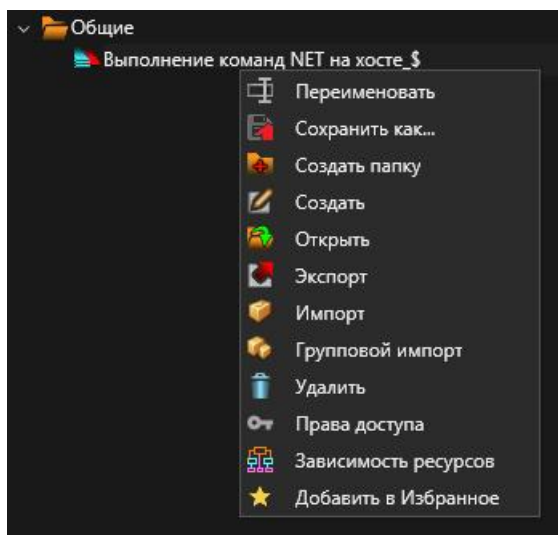


Рисунок 176. Меню взаимодействия

4. Конструкторы запросов

Консоль САВРУС поддерживает функцию графического создания SQL запросов. Для того чтобы войти в графический конструктор, необходимо нажать на кнопку  «Конструктор запросов» на панели управления.

В открывшемся окне конструктора запросов, (см. Рисунок 177) в левой части находится список всех доступных таблиц БД системы. В правой части список операторов и функций для написания SQL запроса.

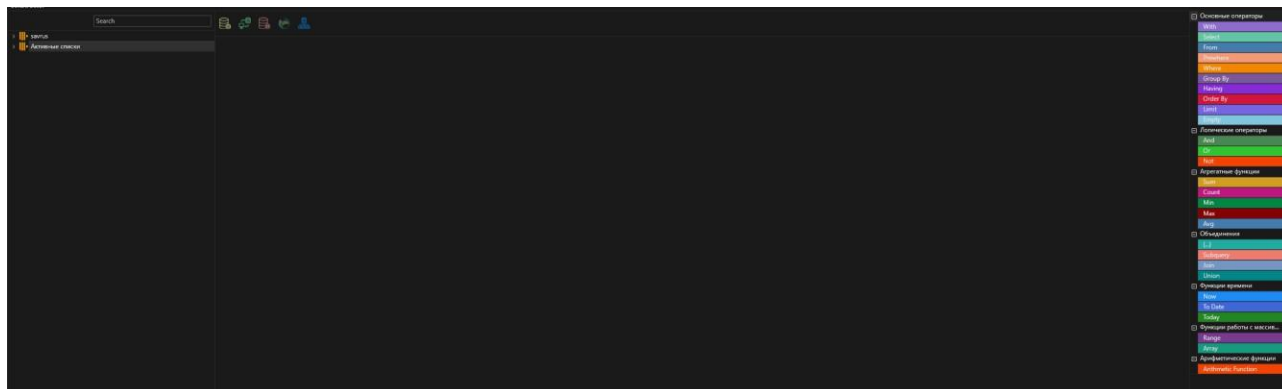


Рисунок 177. Окно "Конструктор запросов"

В нижней части находится скрываемый блок (см. Рисунок 178), который активируется нажатием на  находящуюся в правом-нижнем углу окна, либо же при создании или запуске SQL запроса, сконструированного с помощью графических модулей. В левой части данного блока отображается SQL запрос в текстовом формате, а в правой результат SQL запроса.

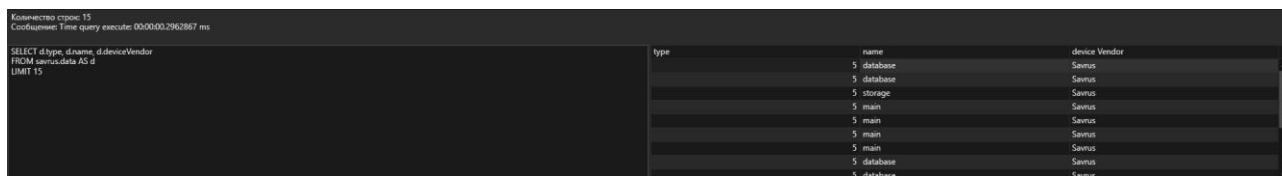


Рисунок 178. Окно данных SQL запроса

В верхней части окна конструктора запросов находится панель управления.

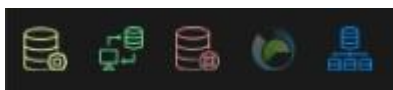


Рисунок 179. Панель управления окна "Конструктор запросов"

Кнопка  «создать SQL запрос» переводит сконструированный при помощи графических модулей SQL запрос в текстовый формат, который будет отображаться в скрываемом блоке интерфейса (см. Рисунок 178). При активации данной функции, запрос не будет запущен и данные не будут сгенерированы.

Кнопка  «Запустить» отвечает за генерацию данных по сконструированному при помощи графических модулей SQL запросу. Сгенерированные данные будут отображаться в скрываемом блоке интерфейса (см. Рисунок 178).

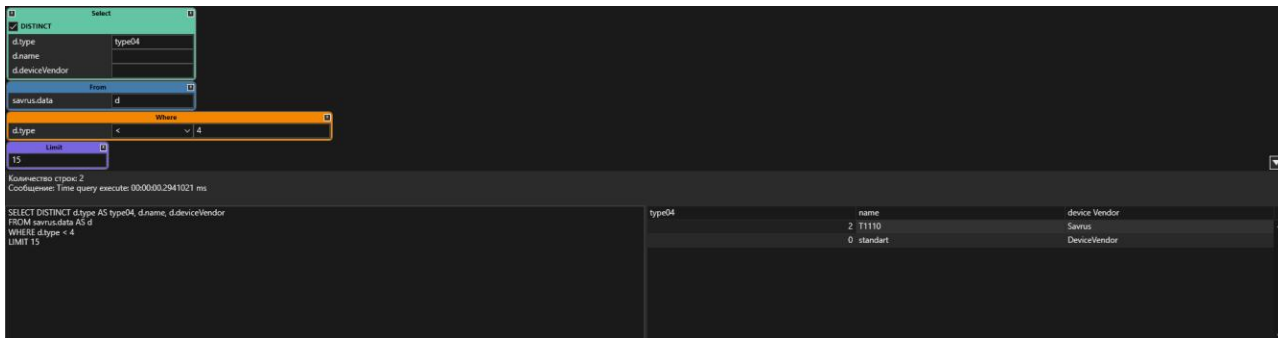
Кнопка  «Очистить» удаляет все блоки операторов и функций, ранее размещённых в рабочем пространстве окна конструктора запросов.

Кнопка  «Вернуться» сворачивает конструктор запросов перенося пользователя в интерфейс SQL запросов.

После сворачивания конструктора запросов, ранее созданный в нём SQL запрос будет отображаться в окне «Запрос». Для того, чтобы вернуться в меню графического создания SQL запроса необходимо повторно нажать на  «Конструктор запросов» на панели управления.

Для создания SQL запроса при помощи графических блоков необходимо перетянуть требуемые блоки из меню операторов и функций в рабочее пространство окна. Для наполнения выбранных блоков операторов или функций данными из доступных полей таблиц БД, необходимо, из списка доступных полей данных, перетащить выбранное поле на шапку блока оператора или функции находящегося в рабочем пространстве.

Пример сформированного SQL запроса представлен ниже.



Скриншот интерфейса конструктора запросов. В меню операторов и функций выбраны следующие блоки:

- Select:** DISTINCT, type04, d.name, d.deviceVendor
- From:** savrusdata, d
- Where:** d.type < 4
- Limit:** 15

Вывод SQL запроса:

```
SELECT DISTINCT d.type AS type04, d.name, d.deviceVendor
FROM savrusdata AS d
WHERE d.type < 4
LIMIT 15
```

Количество строк: 2
Сообщение: Time query executor: 00:00:00.2941021 ms

type04	name	device Vendor
2	T1110	Savrus
0	standart	DeviceVendor

Рисунок 180. Внешний вид SQL запроса, созданного в конструкторе запросов

ВИЗУАЛИЗАЦИЯ ДАННЫХ

1. 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 181).

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

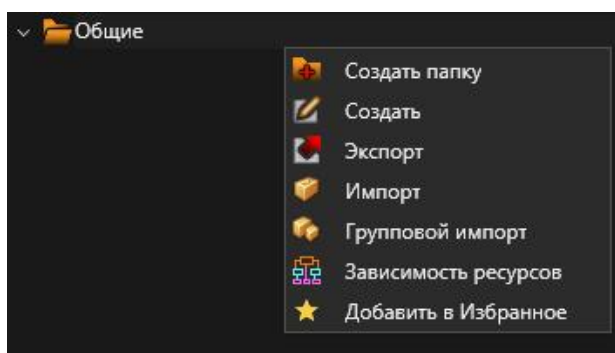


Рисунок 181. Меню взаимодействия

Далее, необходимо ввести название и описание объекта визуализации данных, выбрать необходимый запрос в разделе «База данных» (см. Рисунок 182). *В окне создания визуализации функция редактирования SQL запроса недоступна.*



Рисунок 182. Окно создания визуализации

Далее, настраивается вид визуализации. В данном меню основными настройками являются: тип диаграммы, выбор значений, внешний вид, обновление (см. Рисунок 183). В меню «Тип диаграммы» выбирается одна из доступных диаграмм. В меню «Выбор значения» необходимо вставить значения в поля координат. Только для Столчатой 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.

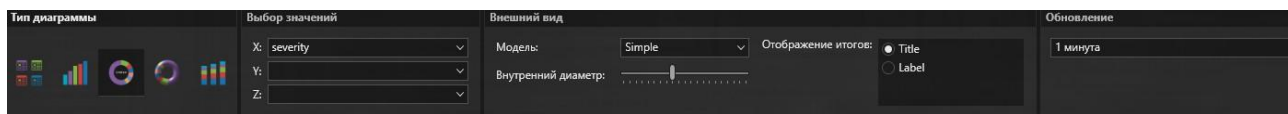


Рисунок 183. Окно редактирования вида

Для сохранения необходимо нажать на кнопку .

Для обновления данных в объектах визуализации можно также использовать клавишу F5.

2. Изменение визуализации

Для изменения объекта визуализации данных необходимо во вкладке «Визуализации» нажать ПКМ по нужному и в контекстном меню выбрать пункт «Открыть» (см. Рисунок 184).

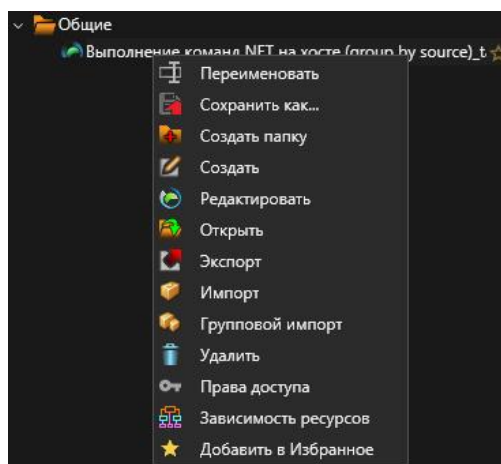


Рисунок 184. Меню взаимодействия

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

3. Удаление визуализации

Для удаления объекта визуализации данных необходимо во вкладке «Визуализации» нажать ПКМ по нужному и в контекстном меню выбрать пункт «Удалить» (Рисунок 185). После чего объект визуализации данных будет помечена на удаление, для полного удаления необходимо повторить процедуру.

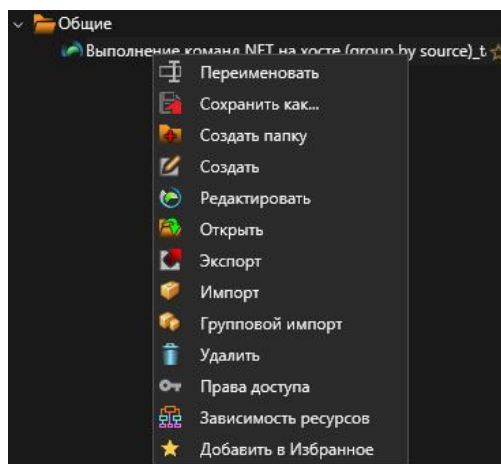


Рисунок 185. Меню взаимодействия

ДАШБОРДЫ

1. 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 186).

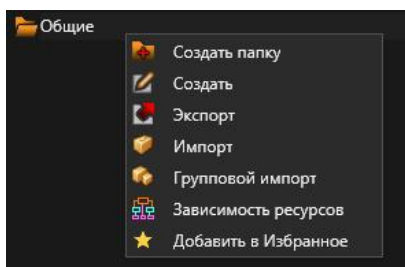


Рисунок 186. Меню взаимодействия

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 сохранении дашборда необходимо ввести название и нажать на кнопку .

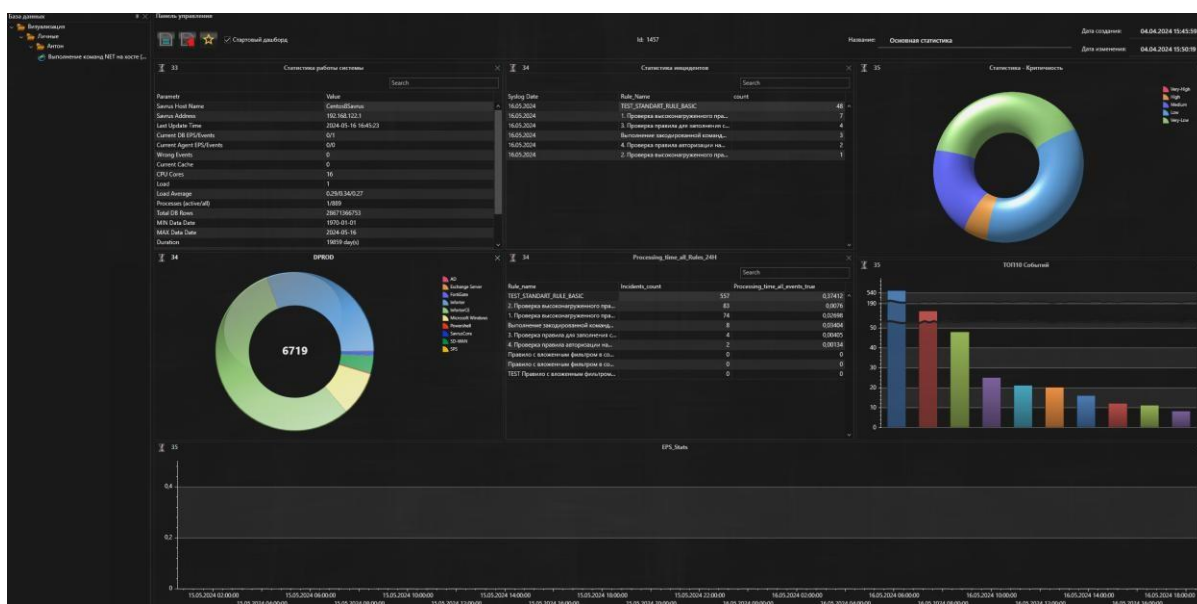


Рисунок 187. Окно создания дашборда

2. Изменение дашборда

Для изменения дашборда необходимо во вкладке «Дашборды» нажать ПКМ по нужному дашборду и в контекстном меню выбрать пункт «Редактировать» (см. Рисунок 188).

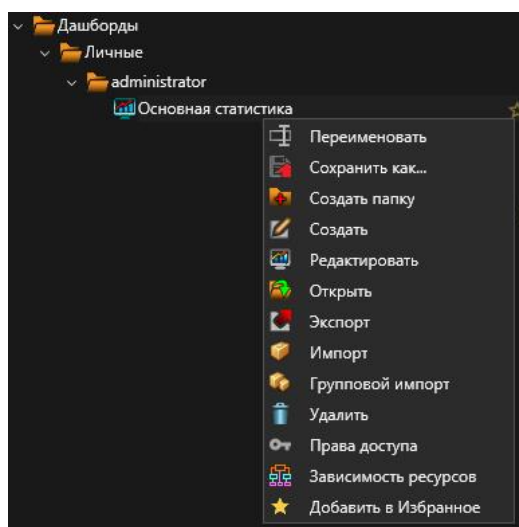


Рисунок 188. Меню взаимодействия

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.

3. Удаление дашборда

Для удаления дашборда необходимо во вкладке «Дашборда» нажать ПКМ по нужному дашборду и в контекстном меню выбрать пункт «Удалить» (см. Рисунок 189). После чего дашборд будет помечен на удаление, для полного удаления необходимо повторить процедуру.

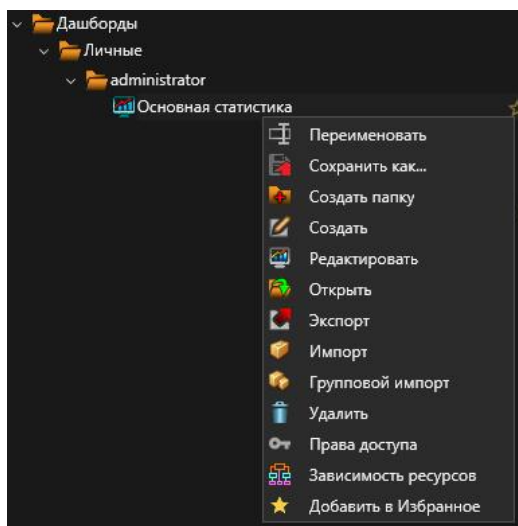


Рисунок 189. Меню взаимодействия

4. Стартовый дашборд

Любой созданный в системе дашборд можно установить в качестве стартового. Для этого необходимо открыть в режиме редактирования нужный дашборд и в Панели управления включить галочку напротив «Стартовый дашборд». **Важно: Стартовым дашбордом можно сделать только те дашборды, которые расположены в папке пользователя, под которым произведён вход в консоль САВРУС.** Если дашборд будет расположен в папке «Общие» или любой другой чужой папке, то даже при поставленной галочке «Стартовый дашборд», он не установится как стартовый.

2. 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 192).

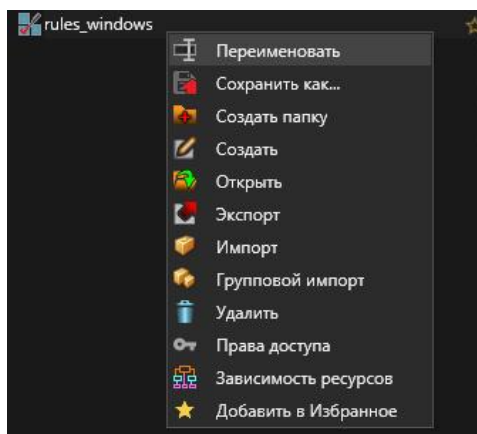


Рисунок 192. Меню взаимодействия

В открывшемся окне следует произвести необходимые изменения (см. Рисунок 193). Для сохранения изменений необходимо нажать на кнопку .

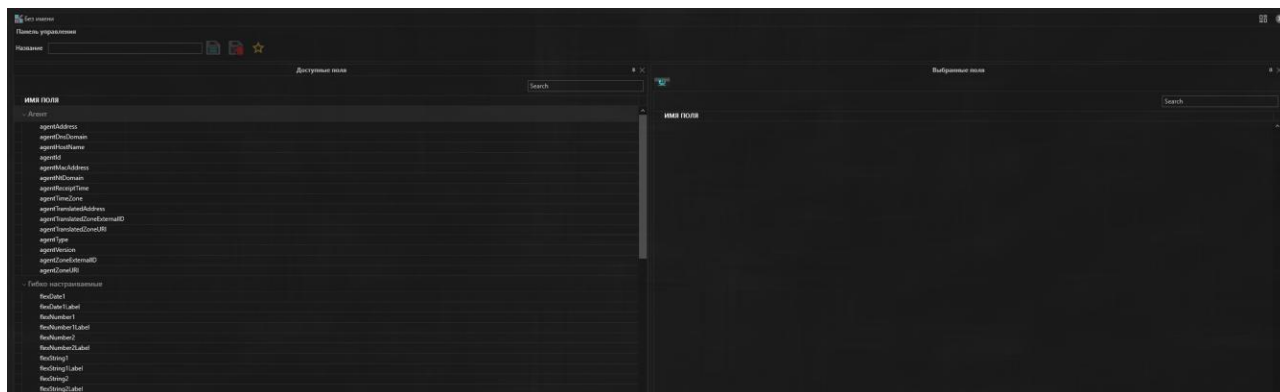


Рисунок 193. Окно редактирования набора полей

3. Удаление набора полей

Для удаления следует во вкладке «SQL запросы» нажать ПКМ по необходимому и в контекстном меню выбрать пункт «Удалить» (см. Рисунок 194). После чего набор полей будет помечен на удаление, для полного удаления необходимо повторить процедуру.

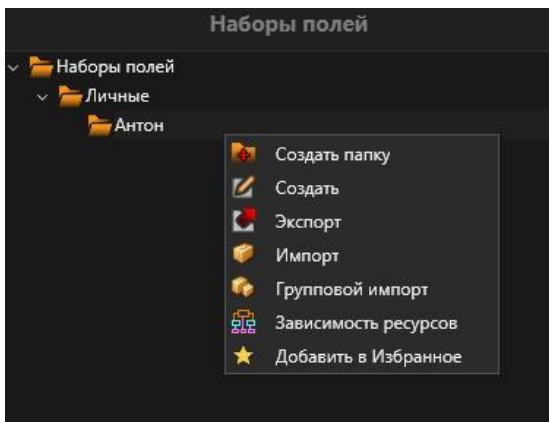


Рисунок 194. Меню взаимодействия

ОТЧЁТЫ

1. Создание отчёта

Отчёты позволяют на базе ранее созданных элементов визуализации данных составить подробный отчёт.

Для создания отчёта необходимо перейти на вкладку «Отчеты». Далее выбрать необходимую папку для разрешения в ней отчёта или же создать новую. Нажать ПКМ на папку и в контекстном меню выбрать кнопку «Создать». Откроется окно с конструктором создания отчётов.

В панели управления настраиваются параметры отправки отчёта.

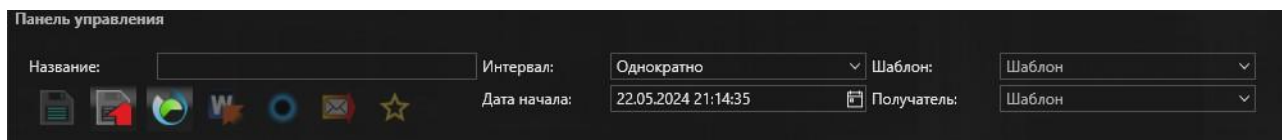


Рисунок 195. Панель управления отчётами

Таблица 9. Настройки панели управления отчетами

Наименование	Назначение
Интервал	Частота отправки отчёта получателю. Система поддерживает следующие интервалы: • однократно; • каждый час; • каждый день.
Дата начала	Дата, с которой начнётся отправка первого отчёта.
Шаблон	Шаблон письма, которое будет уходить на почту получателю.
Получатель	Пользователь, на чью электронную почту будет направлен отчёт.

Шаблон настраивается на вкладке «Шаблоны», где «Имя» будет темой письма, а «Текст» – телом.

Имя:

FastReport

Текст:

Надеюсь, наши письма окажутся для вас полезными. Тем не менее, дайте знать, если не хотите их получать.

Рисунок 196. Пример шаблона

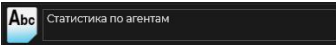
Кнопки панели управления.

Таблица 10. Кнопки панели управления.

Иконка	Наименование	Назначение
	Сохранить	Сохраняет отчёт
	Сохранить как	Сохраняет копию отчёта
	Показать диаграммы	Включает отображение диаграмм, добавленных в отчёт в окне конструктора.
	Сохранить в Word	Сохраняет отчёт в формате .docx на локальном компьютере.
	Включить/Отключить	Включает или отключает работу отчёта. Красный цвет означает, что отправка выключена, синий – включена.

	Отправить отчёт	Сразу отправляет созданный отчёт.
	Добавить в Избранное	Используется для добавления в «Избранное».

2. Добавление данных в отчёт

Для добавления данных в отчёт необходимо использовать раздел «Шаблон отчёта» в окне конструктора. Для добавления текстовых полей в отчёт, для описания объектов визуализации необходимо нажать на кнопку «Добавить текст» . После чего в окне добавиться поле для ввода текстовых данных . В него рекомендуется ввести информацию, раскрывающую данные, предоставленные в объектах визуализации.

Для добавления объектов визуализации необходимо дважды нажать по их названию в дереве ресурсов в левой части окна конструктора отчётов. Объекты визуализации должны быть заранее созданы в системе (подробнее см. раздел «ВИЗУАЛИЗАЦИЯ ДАННЫХ» настоящего руководства).

На рисунке ниже предоставлен пример окна конструктора отчёта с данными.

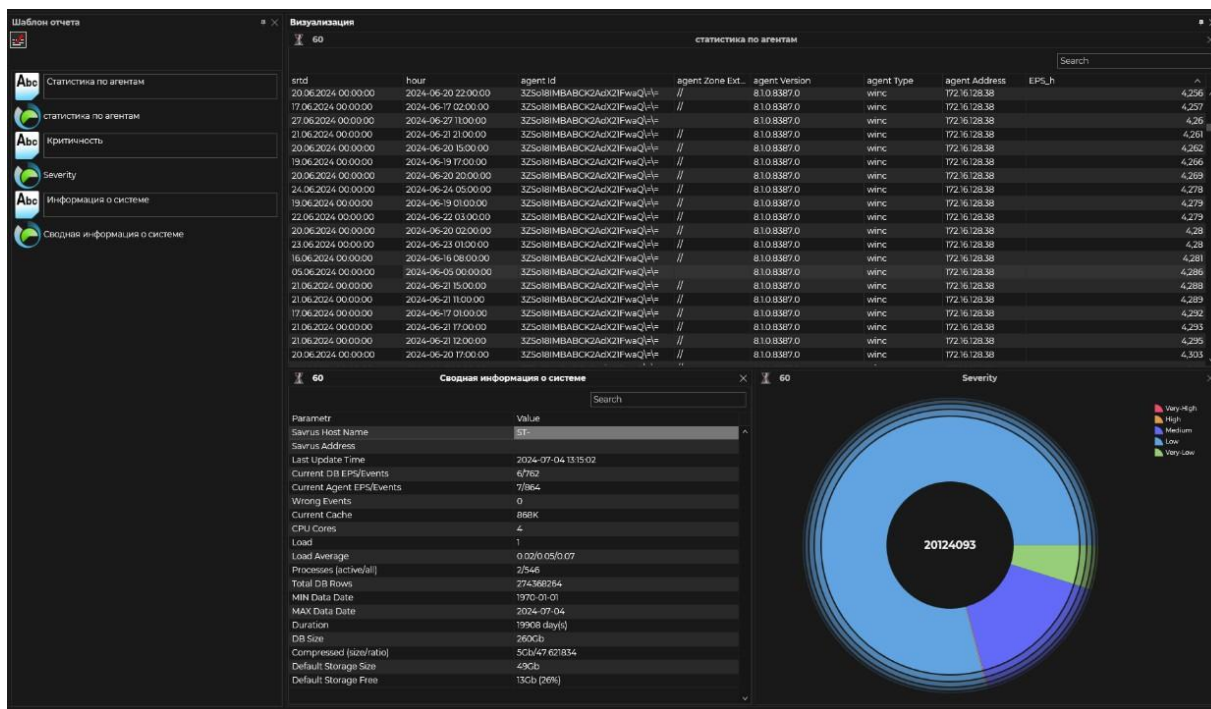


Рисунок 197. Пример отчёта в конструкторе

Для просмотра созданного отчёта необходимо выгрузить его в word файл.

3. Редактирование отчёта

Для редактирования отчёта во вкладке «Отчёты» нажать ПКМ по необходимому и в контекстном меню выбрать пункт «Открыть» или два раза кликнуть ЛКМ по названию. Далее необходимо внести все необходимые изменения и кликнуть кнопку «Сохранить» или «Сохранить как...».

4. Удаление отчёта

Для удаления следует во вкладке «Отчёты» нажать ПКМ по необходимому и в контекстном меню выбрать пункт «Удалить». После чего отчёт будет помечен на удаление, для полного удаления необходимо повторить процедуру.

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 во вкладку «Контекстный поиск» или с помощью комбинации клавиш ctrl+f;
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.

ГЛОБАЛЬНЫЕ ПЕРЕМЕННЫЕ

Глобальные переменные предназначены для создания переменных доступных к вызову в разнообразных ресурсах системы.

1. Создание Глобальной переменной

Для создания Глобальной переменной необходимо перейти во вкладку «Глобальные переменные», выбрать папку для создания переменной, нажать ПКМ по папке выбрать пункт меню «Создать».

Далее, в открывшемся окне необходимо ввести название переменной и выбрать функцию, также присутствует возможность ссылаться на ранее созданные локальные переменные. Подробнее о переменных можно узнать в разделе «ФУНКЦИИ ПЕРЕМЕННЫХ» настоящего руководства.

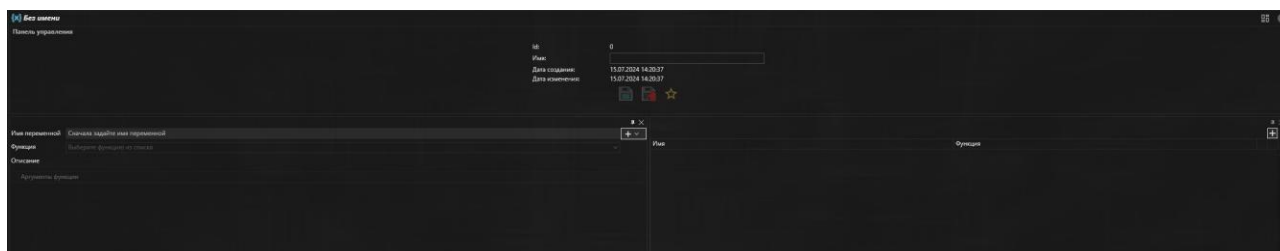


Рисунок 198. Меню создания глобальной переменной

2. Редактирование Глобальной переменной

Для редактирования Глобальной переменной во вкладке «Глобальные переменные» нажать ПКМ по необходимой переменной и в контекстном меню выбрать пункт «Открыть» или два раза кликнуть ЛКМ по названию. Далее необходимо внести все необходимые изменения и кликнуть кнопку «Сохранить» или «Сохранить как...».

3. Удаление Глобальной переменной

Для удаления Глобальной переменной следует во вкладке «Глобальные переменные» нажать ПКМ по необходимой переменной и в контекстном меню выбрать пункт «Удалить». После чего переменная будет помечена на удаление, для полного удаления необходимо повторить процедуру.

КОМАНДЫ ИНТЕГРАЦИИ

Модуль «**Команды интеграции**» предназначен для расширения функционала элементов отображения данных системы «САВРУС» путем добавления в контекстное меню объектов (сущностей системы) «Команда интеграции» различных типов.

Команды интеграции являются сущностями системы «САВРУС», подчиняются правилам общей ролевой модели, используют общий интерфейс создания и редактирования.

Команды интеграции позволяют вызывать внешние приложения (веб-браузер, консоль CMD), используя значения полей элементов отображения данных в качестве параметров или составных частей команд, осуществлять действия с сущностями системы «САВРУС».

На данный момент реализованы три типа команд: **URL**, **Script** и **SystemObject**.

Команды **URL** позволяют вызвать веб-браузер с сформированной командой адресной строкой.

Команды **Script** позволяют запустить приложение ОС в отдельном окне рабочей станции, на которой запущена консоль «САВРУС». С использованием SSH появляется возможность выполнять команды на удаленных серверах.

Команды **SystemObject** предназначены для выполнения действий с сущностями системы «САВРУС», например – получить данные ячейки Активного канала и открыть предопределенный Активный список с установленным фильтром по значению этой ячейки на выбранное заранее поле списка.

1. Создание Команды интеграции

Для создания Команды интеграции необходимо перейти во вкладку «Команды интеграции» , выбрать папку для создания команды, нажать ПКМ по папке выбрать пункт меню «Создать».

Далее необходимо задать ее имя, тип и аргументы. Для большей информативности можно задать «Описание» команды, которое будет отображено во всплывающей подсказке (ToolTip) пункта контекстного меню, содержащего команды.

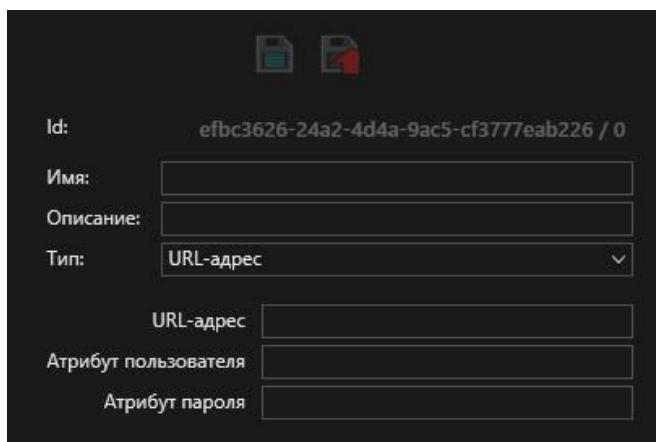


Рисунок 199. Внешний вид вкладки "Команды интеграции".

Далее, необходимо выбрать нужный тип команды: **URL**, **Script** или **SystemObject** и заполнить поля команды, отвечающие за выполнение.

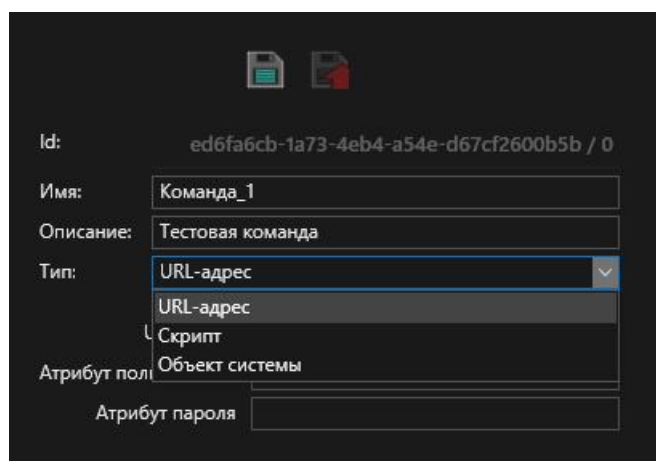


Рисунок 200. Выпадающее меню типов Команды интеграции.

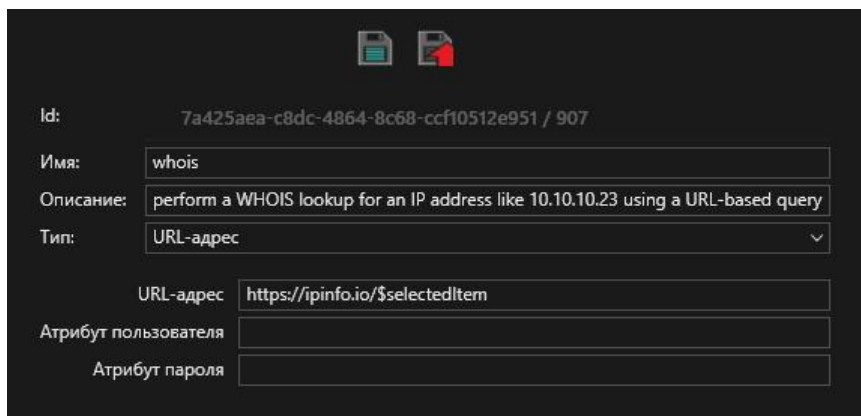
URL-адрес

Для типа команд **URL**, поля команд, отвечающие за выполнение – это «**URL-адрес**», «**Атрибут пользователя**» и «**Атрибут пароля**». При формировании итоговой строки команды будут выполнены следующие преобразования:

- плейсхолдер **\$selectedItem**, будет заменен на значение ячейки элемента отображения данных, для которой было вызвано контекстное меню
- плейсхолдер **\$user** будет заменен значением поля «**Атрибут пользователя**»
- плейсхолдер **\$pass** будет заменен значением поля «**Атрибут пароля**»

Использование плейсхолдеров возможно только в поле «**URL-адрес**».

Пример Команды интеграции типа URL, выполняющей запрос WHOIS с содержимым выбранной ячейки Активного канала и результат ее выполнения – открытое окно веб-браузера с сформированной командой адресной строкой.



The screenshot shows a configuration window for a command. At the top, there are two icons: a document and a red arrow. Below them, the 'Id' is '7a425aea-c8dc-4864-8c68-ccf10512e951 / 907'. The 'Имя:' (Name) field contains 'whois'. The 'Описание:' (Description) field contains 'perform a WHOIS lookup for an IP address like 10.10.10.23 using a URL-based query'. The 'Тип:' (Type) is set to 'URL-адрес' (URL address) with a dropdown arrow. Below this, the 'URL-адрес' (URL address) field contains 'https://ipinfo.io/\$selectedItem'. There are also empty fields for 'Атрибут пользователя' (User attribute) and 'Атрибут пароля' (Password attribute).

Рисунок 201. Пример готовой Команды интеграции типа URL-адрес.

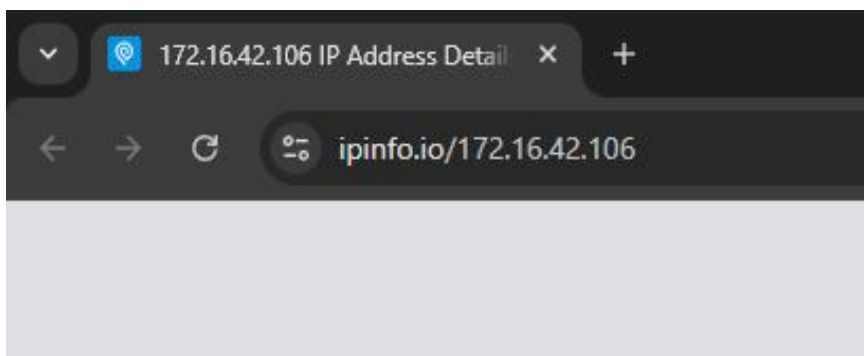
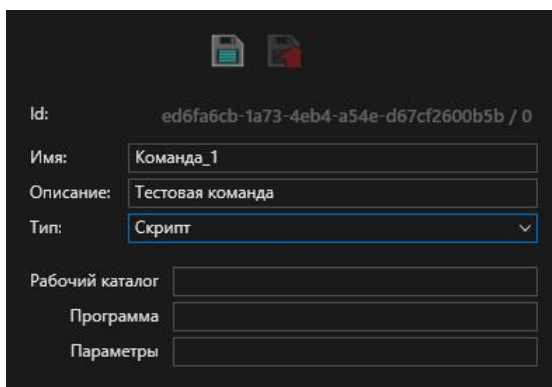


Рисунок 202. Пример срабатывания Команды интеграции типа URL-адрес.

Скрипт

Для команды типа **Script** необходимо заполнить поля «Рабочий каталог», «Программа» и «Параметры». В этом типе команд поддерживается использование только плейсхолдера \$selectedItem. Если «Рабочий каталог» не задан – скрипт будет выполняться в каталоге консоли «САВРУС».



Id: ed6fa6cb-1a73-4eb4-a54e-d67cf2600b5b / 0

Имя: Команда_1

Описание: Тестовая команда

Тип: Скрипт

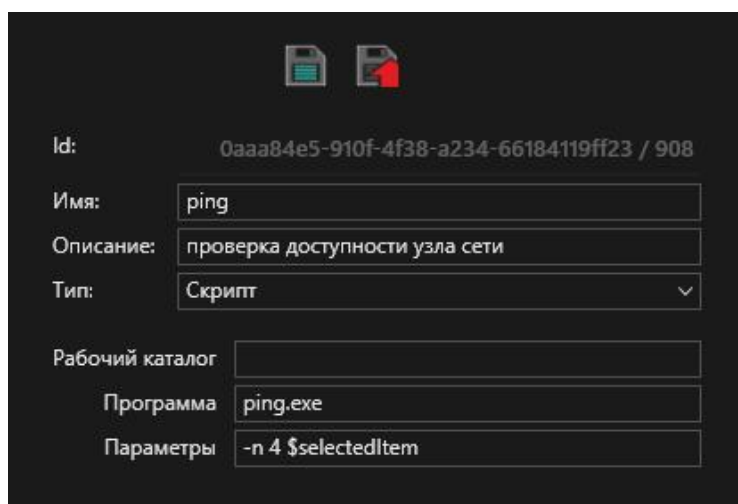
Рабочий каталог:

Программа:

Параметры:

Рисунок 203. Меню параметров Команды интеграции типа Скрипт.

Пример Команды интеграции типа Script, выполняющей команду PING с содержимым выбранной ячейки Активного канала и результат ее выполнения – открытое окно консоли CMD с сформированной командой и результатом ее выполнения.



Id: 0aaa84e5-910f-4f38-a234-66184119ff23 / 908

Имя: ping

Описание: проверка доступности узла сети

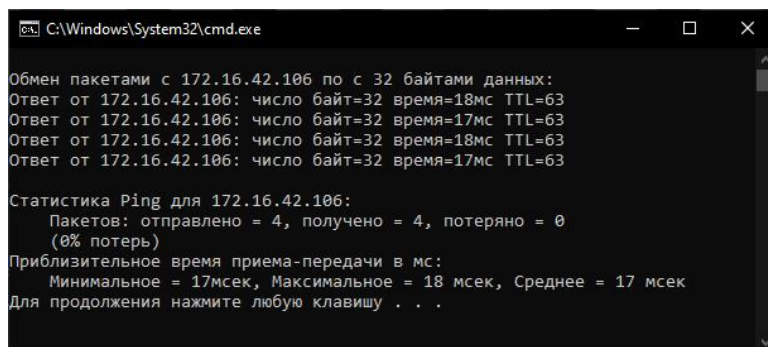
Тип: Скрипт

Рабочий каталог:

Программа: ping.exe

Параметры: -n 4 \$selectedItem

Рисунок 204. Пример готовой Команды интеграции типа Скрипт.



```
C:\Windows\System32\cmd.exe

Обмен пакетами с 172.16.42.106 по 32 байтами данных:
Ответ от 172.16.42.106: число байт=32 время=18мс TTL=63
Ответ от 172.16.42.106: число байт=32 время=17мс TTL=63
Ответ от 172.16.42.106: число байт=32 время=18мс TTL=63
Ответ от 172.16.42.106: число байт=32 время=17мс TTL=63

Статистика Ping для 172.16.42.106:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потеря)
    Приблизительное время приема-передачи в мс:
    Минимальное = 17мсек, Максимальное = 18 мсек, Среднее = 17 мсек
    Для продолжения нажмите любую клавишу . . .
```

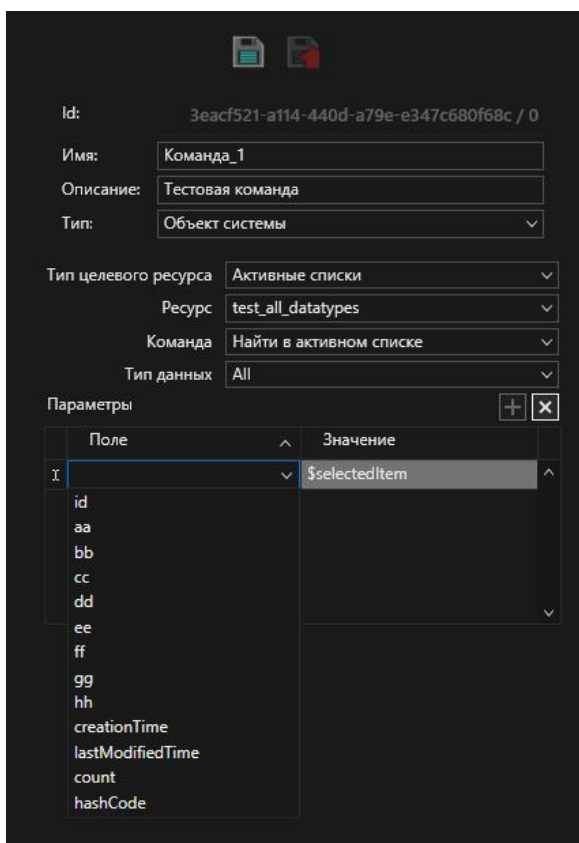
Рисунок 205. Пример срабатывания Команды интеграции типа Скрипт.

Объект системы

Для команды типа **SystemObject** необходимо:

- выбрать «Тип целевого ресурса» - тип ресурса, над которым будет выполняться действие команды (пока поддерживаются только Активные списки)
- из выпадающего дерева ресурсов «Ресурс» выбрать конкретный ресурс выбранного типа
- из списка «Команда» - выбрать действие, которое необходимо произвести с выбранным выше ресурсом
- при необходимости, определить допустимый «Тип данных» для работы команды – в данном случае он накладывает ограничение на список доступных полей списка в параметрах команды и будет влиять на доступность команды в контекстном меню, в зависимости от типа данных выбранной ячейки
- добавить параметры команды

В параметрах команды допустимо использование плейсхолдера **\$selectedItem**



Id: 3eacf521-a114-440d-a79e-e347c680f68c / 0

Имя: Команда_1

Описание: Тестовая команда

Тип: Объект системы

Тип целевого ресурса: Активные списки

Ресурс: test_all_datatypes

Команда: Найти в активном списке

Тип данных: All

Параметры

Поле	Значение
id	\$selectedItem
aa	
bb	
cc	
dd	
ee	
ff	
gg	
hh	
creationTime	
lastModifiedTime	
count	
hashCode	

Рисунок 206. Меню параметров Команды интеграции типа Объект системы.

Контекстное меню **Активного канала**, предоставляющее доступ к Командам интеграции, для выделенной ячейки будет выглядеть следующим образом:

Таблица

Drag a column header here to group by that column

type	srt	name	deviceAddress	deviceHostName	severity	destinationAddress	destinationUserNa...	sourceAddress
cpu	06.01.2026 10:23:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:23:44	cpu	172.16.42.106	ST-42.106	Very-Low			
database	06.01.2026 10:22:16	database	127.0.0.1	ST-42.106	Very-Low			
system	06.01.2026 10:22:16	system	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:21:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:20:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:20:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:18:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:18:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:16:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:16:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:14:45	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:14:45	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:12:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:12:44	cpu	172.16.42.106	ST-42.106	Very-Low			
database	06.01.2026 10:12:15	database	127.0.0.1	ST-42.106	Very-Low			
system	06.01.2026 10:12:15	system	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:11:45	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:11:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:10:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:09:45	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:09:45	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:08:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:07:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:07:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:06:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:02:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:02:44	cpu	172.16.42.106	ST-42.106	Very-Low			
database	06.01.2026 10:02:14	database	127.0.0.1	ST-42.106	Very-Low			
system	06.01.2026 10:02:13	system	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:01:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:00:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 10:00:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 09:58:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 09:58:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 09:57:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 09:56:45	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 09:55:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 09:55:44	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 09:53:45	cpu	172.16.42.106	ST-42.106	Very-Low			
cpu	06.01.2026 09:53:44	cpu	172.16.42.106	ST-42.106	Very-Low			

Контекстное меню:

- AND deviceAddress = 172.16.42.106
- AND deviceAddress <> 172.16.42.106
- OR deviceAddress = 172.16.42.106
- OR deviceAddress <> 172.16.42.106
- Новый канал из содержимого поля
- Новый канал из содержимого поля и значения deviceProduct
- Новый канал с дополнением условия
- Создать канал цепочки корреляции
- Отправить в R-Vision
- Сохранить детали события в CEF-файл
- Сохранить детали события в буфер обмена в CEF-формате
- Команды интеграции
 - test
 - test_url
 - test_script
 - test_object
 - test_object_saveas
 - whois
 - ping
 - set_filter_test1.dd
 - set_filter_test3.string
 - set_filter_test3.int
 - set_filter_test3.long
 - set_filter_test3.ip
 - set_filter_test3.data
 - Команда_1
- Тестовая команда

Рисунок 207. Контекстное меню Активного канала, предоставляющее доступ к Командам интеграции.

2. Редактирование Команды интеграции

Для редактирования Глобальной переменной во вкладке «Команды интеграции» нажать ПКМ по необходимой переменной и в контекстном меню выбрать пункт «Открыть» или два раза кликнуть ЛКМ по названию. Далее необходимо внести все необходимые изменения и кликнуть кнопку «Сохранить» или «Сохранить как...».

3. Удаление Глобальной переменной

Для удаления Команды интеграции следует во вкладке «Команда интеграции» нажать ПКМ по необходимой переменной и в контекстном меню выбрать пункт «Удалить». После чего команда будет помечена на удаление, для полного удаления необходимо повторить процедуру.

ВЕБ-ИНТЕРФЕЙС

1. Инструкция по входу в Веб-Интерфейс.

Для того, чтобы попасть в Веб-Интерфейс 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 САВРУС.

2. Основные вкладки Веб-интерфейса коррелятора.

Веб-интерфейс коррелятора представлен на рисунке ниже (см. Рисунок 208) и содержит в себе такие вкладки, как:

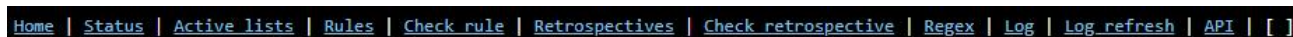


Рисунок 208. Веб-интерфейс коррелятора.

- Home – домашняя страница Веб-интерфейса.
- Status – страница отображающая служебную информацию.
- Active lists – страница с описанием активных списков.
- Rules – страница с описанием правил типа «Стандартное».
- Check rules – страница тестирования правил типа «Стандартное», «Агрегационное».
- Retrospectives – страница с описанием правил типа «Ретроспективное».
- Check retrospectives – страница тестирования правил типа «Ретроспективное».
- Regex – содержит функционал проверки Регулярных Выражений
- Log – не обновляемая страница логов коррелятора.
- Log refresh – обновляемая страница логов коррелятора.
- API – страница с описанием методов API содержащихся в корреляторе.

В ячейке **[]** будет находиться название открытой в данный момент вкладки.

Во вкладках «Rules» и «Retrospectives» отображаются только активные правила.

3. Описание содержания вкладок Веб-интерфейса коррелятора.

Active lists

На данной вкладке содержатся активные списки и их описание.

Нажав «ЛКМ» по активному списку, откроется окно с его содержимым.

Rules

На данной вкладке отображаются только включенные правила типа «Стандартное», «Агрегационное», «Корреляционное».

Столбцы на панели ниже содержат в себе информацию о:

Rule	Conds	Vars	Threshold	TimeUnit	WindowSize	WindowSeconds	MatchedTrue	MatchedFalse	LastMatchedTime	Delay	Granulation
------	-------	------	-----------	----------	------------	---------------	-------------	--------------	-----------------	-------	-------------

Рисунок 209. Столбцы параметров правил во вкладке "Rules"

- Rule – название правила.
- Conds – кол-во условий содержащихся в правиле.
- Vars – кол-во переменных содержащихся в правиле.
- Threshold – кол-во событий необходимых для срабатывания правила типа «Агрегационное»
- TimeUnit – показатель измерения времени.
- WindowSize – размер измерения окна в минутах.
- WindowSeconds – размер измерения окна в секундах.
- MatchedTrue – кол-во успешных срабатываний правила.
- MatchedFalse – кол-во не успешных срабатываний правила.
- LastMatchedTime – Последнее время сработки правила.
- Delay – отсрочка срабатывания правила.
- Granulation – Параметр отвечающий за быструю обработку и фильтрацию правил. Если правило прошло грануляцию, то в данном столбце будет находится название условия, по которому правило попало под грануляцию. Данное название будет выделено зелёным цветом. Если правило не попало под условия грануляции, то в данном столбце будет находиться запись «FALSE» красного цвета.

При нажатии ЛКМ на любое правило в столбце «Rule», откроется страница с деталями выбранного правила.

Также для Агрегационных правил доступен функционал «In memory list». Данный функционал представляет собой активный лист, в котором хранятся значения полей правила корреляции.

Чтобы воспользоваться данной функцией необходимо в столбце «LastMatchedTime» кликнуть по уникальному для агрегационных правил показателю «hash: ...». Далее откроется «in memory list» (см. Рисунок 210).

Данный лист очищается в указанный при создании агрегационного правила интервал. В случае, если сервер будет отключен, то данные листа также будут очищены. Просмотр in memory list доступен только в веб-интерфейсе коррелятора.

Identical	Unique	hashI	hashU	lastModifiedTime	count	seid	lastMatchedTime
	net_view_1	-2006249425541467853	2997779686877689	2024-01-12 19:07:18	2	1705075635739066270	2024-01-12 19:10:37
	net_view_1	3418436791463226322	2997779686877689	2024-01-12 19:05:55	1	1705075552711336253	2024-01-12 19:10:37
	net_view_1	8843123008467920497	2997779686877689	2024-01-12 19:05:55	1	1705075552712142046	2024-01-12 19:10:38
	net_view_1	-4178934848236936944	2997779686877689	2024-01-12 19:05:55	1	1705075552712918476	2024-01-12 19:10:38
	net_view_2	-2006249425541467853	2997779686877690	2024-01-12 19:10:38	2689	1705075735617355227	2024-01-12 19:10:37
	net_view_3	-2006249425541467853	2997779686877691	2024-01-12 19:10:38	2689	1705075735618179348	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:07:18	1	1705075635742758462	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725767020694	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725769618450	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725772107547	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725774633010	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725777627850	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725780055353	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725782547328	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725784998969	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725787471645	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725789979937	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725792508895	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725794924545	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725797425866	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725799952754	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725802360695	2024-01-12 19:10:37
	net_view_4	-2006249425541467853	2997779686877692	2024-01-12 19:08:58	1	1705075725804889786	2024-01-12 19:10:37

Рисунок 210. in memory list

Check rules

Для тестирования правила необходимо (см. Рисунок 211) в верхнее пустое окно вставить код события в формате «CEF». Далее в нижнем выпадающем меню выбрать правило, которое необходимо протестировать. После нажать кнопку «Send CEF», которая запустит тест правила.



Рисунок 211 Интерфейс вкладки "Check rules"

Если правило сработало корректно, то на странице появятся следующие данные (см. Рисунок 212).

Рисунок 212. Результат теста правила во вкладке "Check rules"

Retrospectives

С содержанием в столбцах информацией можно ознакомиться в разделе Rules

Check retrospective

Рисунок 213. Интерфейс вкладки "Check retrospective"

Выпадающее меню «Limit» отвечает за кол-во отображаемых строк при выполнении теста.

Выпадающее меню «Show all events» отвечает за отображение только совпадающих с фильтром событий, если выбрано «No» и всех событий по запросу, если выбрано «Yes».

Чтобы отобразить результаты теста необходимо нажать на кнопку «Execute».

При выбранном параметре «Yes», события, подходящие под условия выбранного правила, будут отображаться зелёным цветом (см. Рисунок 214).

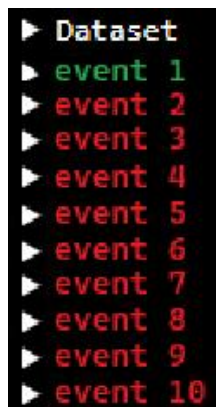


Рисунок 214. Список событий

Нажатие «ЛКМ» по любому из событий, раскроет детали данного события, которая будет выглядеть таким же образом, как и на (см. Рисунок 212).

Regex

На данной вкладке доступен функционал проверки Регулярных Выражений (regex).

Log

На данной вкладке показан Log всех событий коррелятора.

Данная вкладка является не обновляемой в реальном времени. События в данной вкладке формируются в момент перехода на вкладку.

Log refresh

На данной вкладке показан Log всех событий коррелятора.

Данная вкладка обновляется в реальном времени с интервалом в 2 сек.

4. Основные вкладки Веб-интерфейса инфортера.

Веб-интерфейс инфортера представлен на рисунке ниже (см. Рисунок 215) и содержит в себе такие вкладки, как:

[Home](#) | [Status](#) | [Active lists](#) | [Assets](#) | [PPRules](#) | [Check_pprule](#) | []

Рисунок 215. Веб-интерфейс инфортера

- Home – домашняя страница Веб-интерфейса.
- Status – страница отображающая служебную информацию.
- Active lists – страница с описанием активных списков.
- Assets – страница содержащая различные ассеты для обогащения событий.
- PPRules – страница с описанием правил типа «Pre-persistence», предназначенных для обогащения событий.
- Check pprules – страница тестирования правил типа «Pre-persistence».

В ячейке [] будет находиться название открытой в данный момент вкладки.

Взаимодействие с функционалом на вкладках «PPRules» и «Check pprules» осуществляется аналогично ранее описанному функционалу в подразделах «Rules» и «Check rules», соответственно.