САВРУС

Руководство пользователя

ООО «САВРУС»

125445, г. Москва, ул. Смольная, д. 24А, этаж 10, офис № 1029
ИНН/КПП 7743266740/774301001, ОГРН 1187746699546

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

Сокращение	Расшифровка
АК	Активный канал
ПКМ	Правая кнопка мыши
ЛКМ	Левая кнопка мыши
ИБ	Информационная безопасность
ПМ	Пункт меню
АЛ	Активный лист
Правила	Правила корреляции событий в режиме реального времени

АВТОРИЗАЦИЯ В СИСТЕМЕ

При первоначальном входе в консоль потребуется сконфигурировать её для дальнейшей работы. Для этого необходимо перейти в окно авторизации с менеджером САВРУС с помощью кнопки ... . В открывшемся диалоговом окне необходимо ввести следующие настройки (см. Рисунок 1):

- IP адрес хоста с менеджером САВРУС;
- порт авторизации с менеджером (по умолчанию используется 7889);
- тип подключения: GRPC и GRPC-WEB, при выборе GRPC необходимо будет выбрать версию TLC (по умолчанию рекомендуется использовать GRPC и TLS 1.2).

Рекомендуется обратиться к администратору САВРУС для получения данных по конфигурации системы. Для сохранения конфигурации и продолжения работы необходимо нажать кнопку «Сохранить».

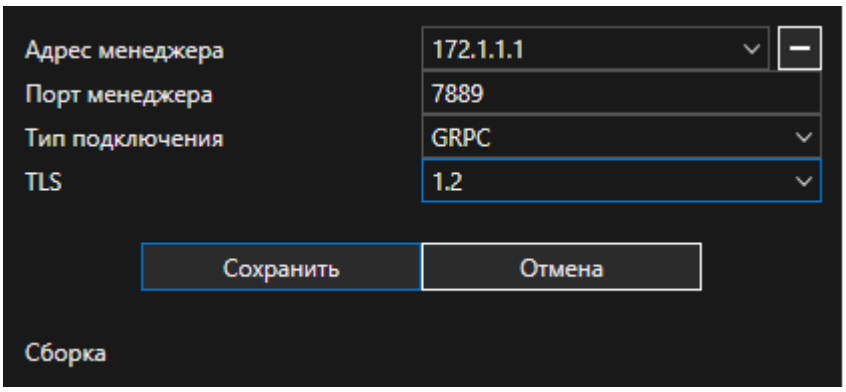


Рисунок 1. Окно авторизации с менеджером

Система поддерживает 2 типа аутентификации пользователей:

- по логину и паролю;
- доменная аутентификация.

Рекомендуется обратиться к администратору САВРУС для уточнения какой тип аутентификации к системы следует использовать.

Аутентификация по логину и паролю

Для входа в систему в окне авторизации необходимо заполнить поля: «Имя пользователя» и «Пароль» своими данными, а в поле «Адрес» выбрать необходимый IP- адрес менеджера, по умолчанию стоит адрес, который использовался при последнем входе (см. Рисунок 2). При необходимости выбрать язык интерфейса системы (поддерживается русский и

английский). После заполнения полей необходимо нажать на кнопку «Вход», которая станет активной, для отмены входа нажать на кнопку «Отмена».

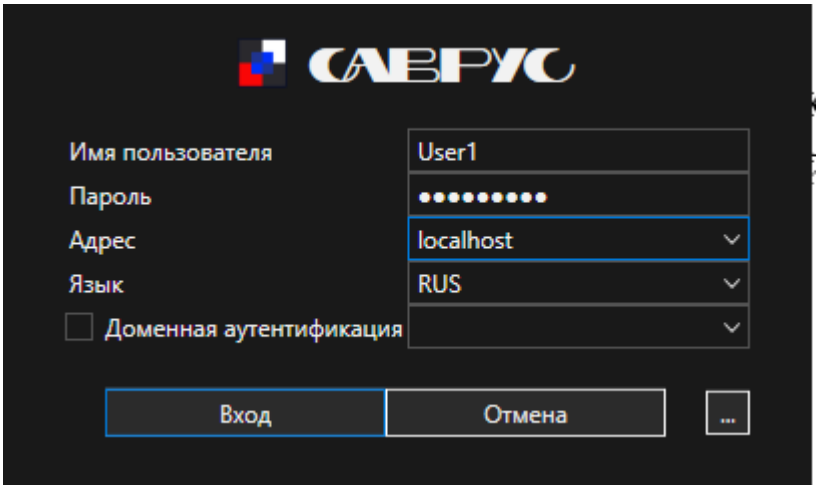


Рисунок 2. Окно авторизации

Доменная аутентификация

Для доменной аутентификации необходимо поставить галочку и выбрать из выпадающего списка необходимых домен. Рекомендуется обратиться к администратору САВРУС для уточнения домена.

ОСНОВНЫЕ ЭЛЕМЕНТЫ КОНСОЛИ

1. Стартовый экран

После авторизации в консоли пользователь попадает на стартовый экран (см. Рисунок 3). В шапке окна консоли отображаются данные об IP-адресе менеджера, лицензии и активном пользователе.

На стартовом экране располагаются 4 основные области (см. Рисунок 3):

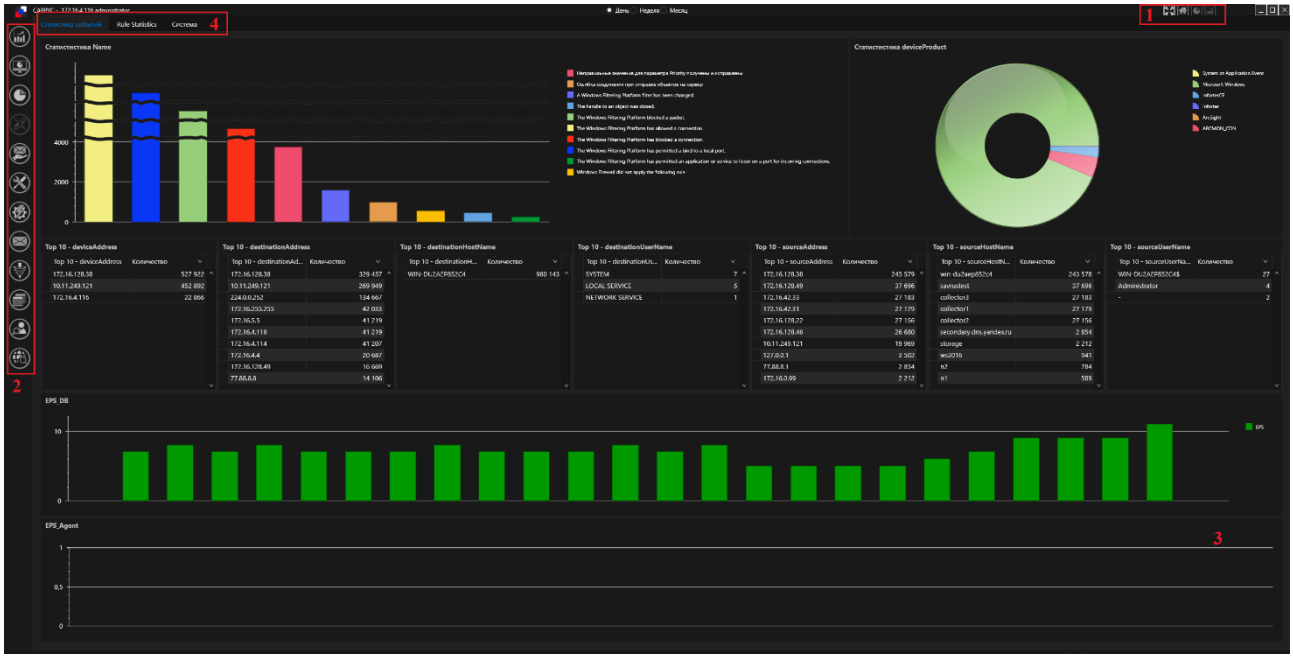


Рисунок 3. Стартовый экран

Элементы, обозначенные цифрой 1 на рисунке выше, представляют собой область рабочих пространств, между которыми можно переключаться во время работы. По умолчанию активно рабочее пространство стартового экрана ( ), на котором размещается стартовый дашборд, и настройка масштабирования (иконка), предназначенная для оптимизации рабочего экрана под любые размеры монитора. Дополнительные рабочие (Активные каналы, правила, дашборды и прочее) пространства активируются по мере использования ресурсов консоли (подробнее в разделе 2. Ресурсы консоли).

Элементы, обозначенные цифрой 3 (см. Рисунок 3), представляют собой «Стартовый дашборд», предназначенный для визуализации наиболее важных данных.

2. Ресурсы консоли

Элементы, обозначенные цифрой 2 (см. Рисунок 3), представляют собой «Меню ресурсов», посредством которого осуществляется выбор и работа с ресурсами. Основными ресурсами являются:

Иконка	Название	Описание
	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 размещения ресурсов визуализации на информационных панелях
	Визуализация	Предназначена для отображения статистики и сводных данных по событиям/инцидентам в графическом виде, по заданным фильтрам и параметрам
	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
	Фильтры	Предназначены для разграничения доступа пользователей к ресурсам
	Шаблоны	Предназначены для создания типовых шаблонов уведомлений об обнаружении инцидентов ИБ
	Активные листы	АЛ – 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 быстрого поиска по наиболее часто используемым параметрам (по итогам отработки контекстного поиска создаётся АК)
	Инциденты	Предназначены для мониторинга компонентов системы и инцидентов при распределённой инсталляции на интерактивной географической карте РФ

При неактивности одного или нескольких из перечисленных ресурсов следует обратиться к администратору САВРУС.

РАБОТА С АКТИВНЫМИ КАНАЛАМИ

1. Основные элементы активного канала

АК предназначены для отображения и работы с событиями, хранящимися в БД, их поиска и анализа. На рисунке 4 представлен пример АК.

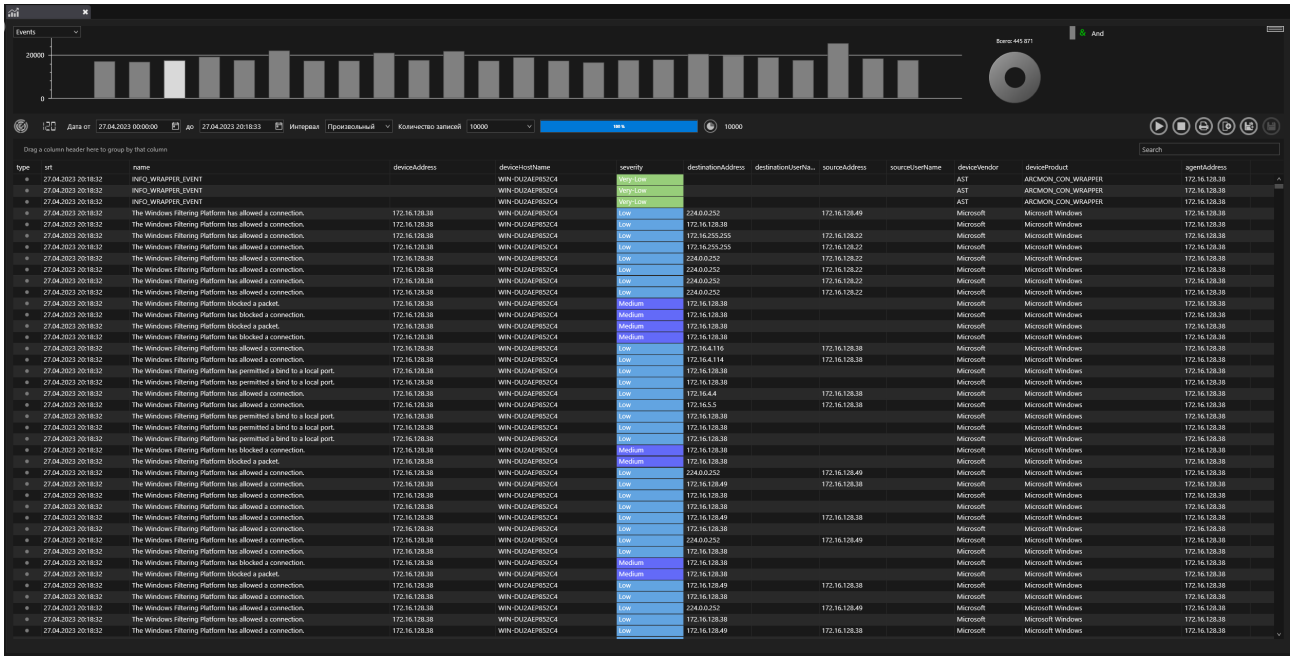


Рисунок 4. Пример Активного канала

Рассмотрим подробнее основные элементы АК.

Радар

Предназначен для графического отображения событий ИБ в различных разрезах. Можно задать следующие параметры группировки событий в радаре event (по количеству событий), severity (по критичности см. Рисунок 5), deviceVendor(по вендорам см. Рисунок 6), deviceProduct (по продуктам), type (по типам событий). Для смены типа группировки радара следует вверхнем левом углу выбрать необходимый в выпадающем списке.

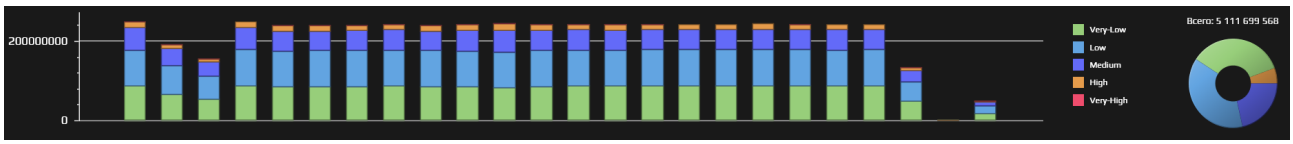


Рисунок 5. Пример Радара по уровню критичности

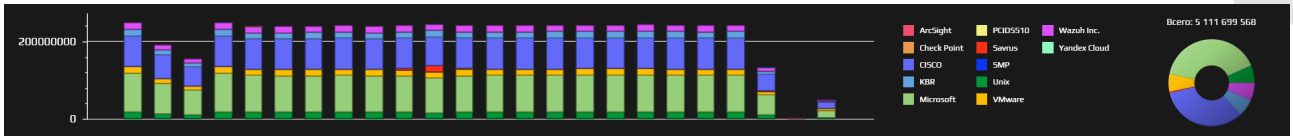


Рисунок 6. Пример Радара по вендорам

Таблица АК

Основной элемент отображения событий — это таблица, в которую выводятся все необходимые поля событий ИБ (см. Рисунок 7).

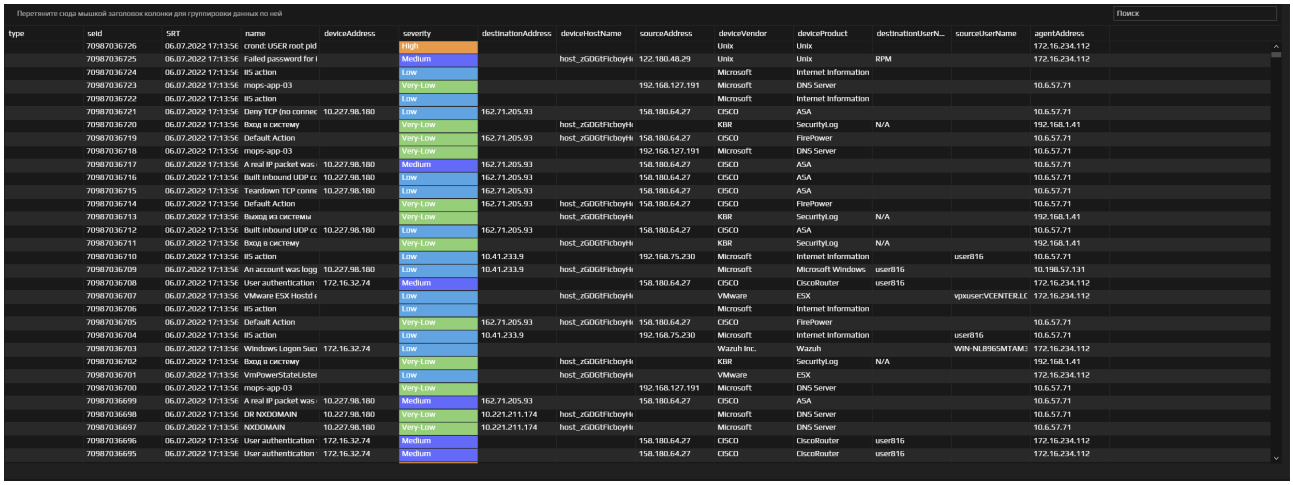


Рисунок 7.Активный канал в табличном представлении

Также возможно отображения событий ИБ в виде различного рода сгруппированных диаграмм и таблиц (см. Рисунок 8) для этого необходимо нажать на кнопку  .

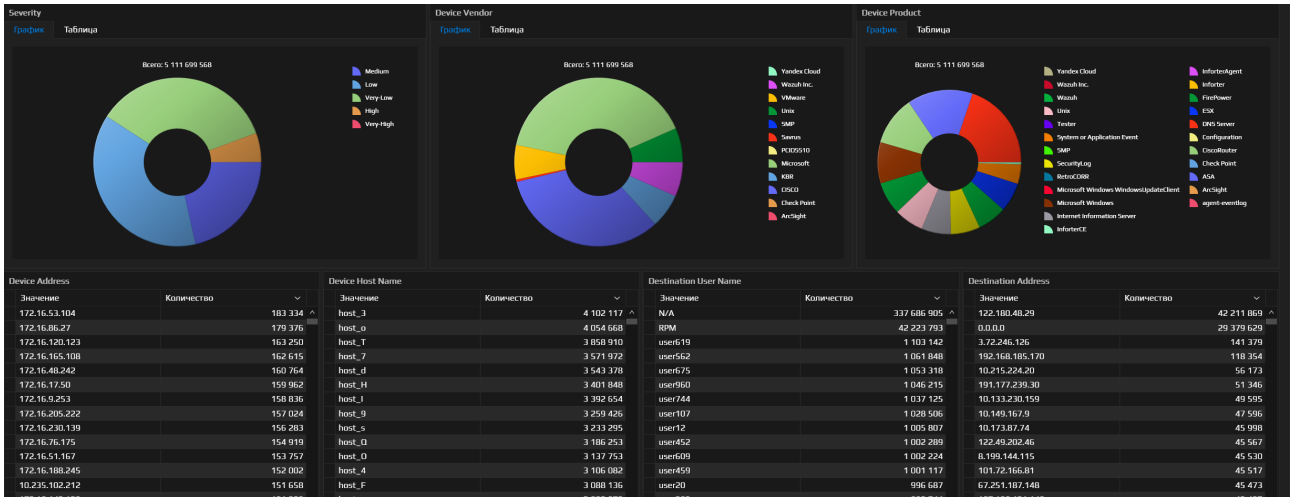


Рисунок 8. Активный канал в виде диаграмм

2. Создание активного канала

Для создания АК необходимо в меню ресурсов перейти на вкладку «Активные каналы» выбрать необходимую папку, в которой будет новый канал или создать новую папку и выбрать ПМ «Создать» (см. Рисунок 9).

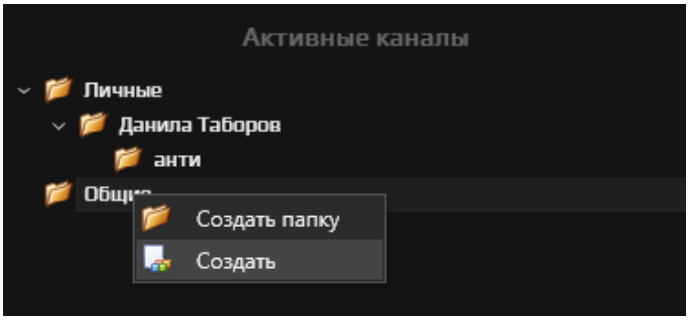


Рисунок 9. Меню Активного канала

Откроется интерфейс управления АК. По умолчанию появится АК со стандартными параметрами (см. Рисунок 10), 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»).

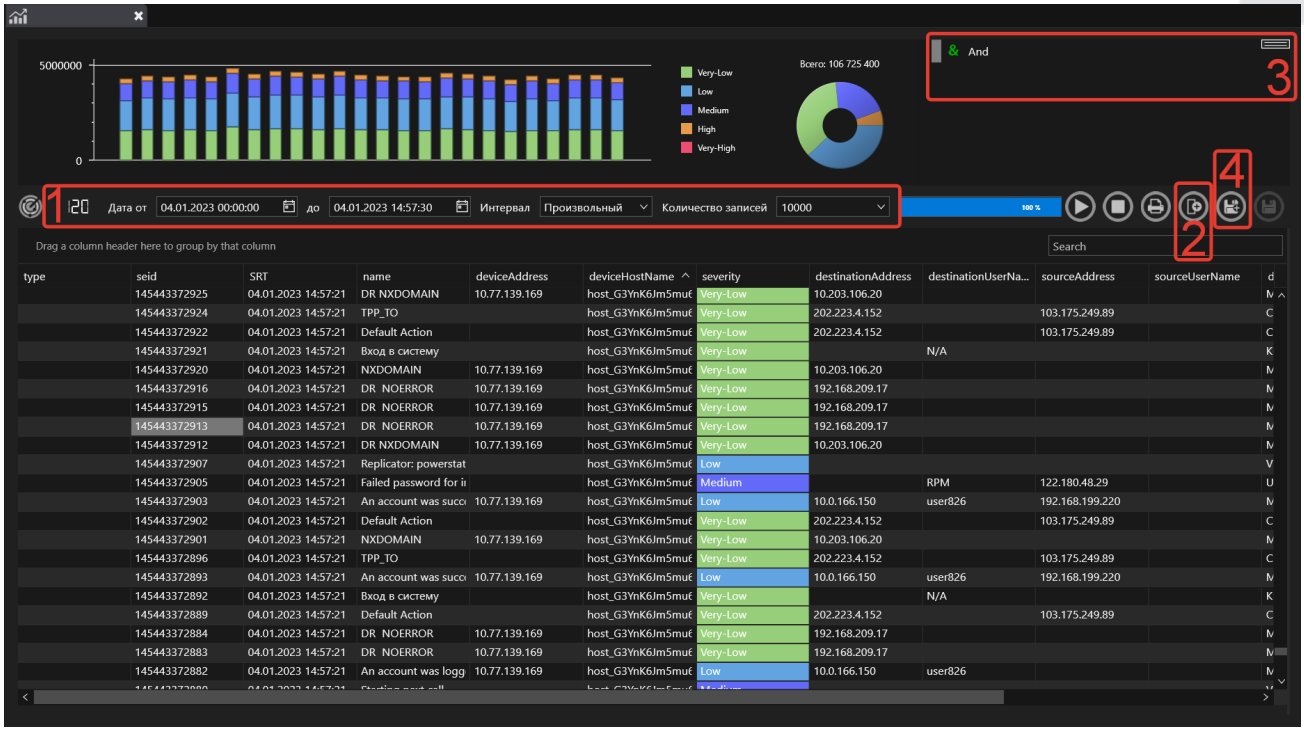


Рисунок 10. Стандартный АК

Подробное описание элементов АК см. в Таблица 1. В произвольном режиме для запуска загрузки данных необходимо нажать кнопку , в непроизвольном режиме загрузка данных будет осуществляться периодически по таймеру (согласно системным настройкам).

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

Таблица 1. Описание полей окна создания АК

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

3. Изменение временного интервала и количества записей

В АК можно менять временной диапазон и количество записей, для этого используется область под цифрой 1 (см. Рисунок 10). Временной диапазон может быть 8-ми 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).

При выборе не произвольного режима временного диапазона в левой части области под цифрой 1 (см. Рисунок 10) включается таймер, который ведёт отсчёт до следующего запроса на обновление данных.

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

- 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  и откроется диалоговое окно редактора полей (см. Рисунок 11). 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.

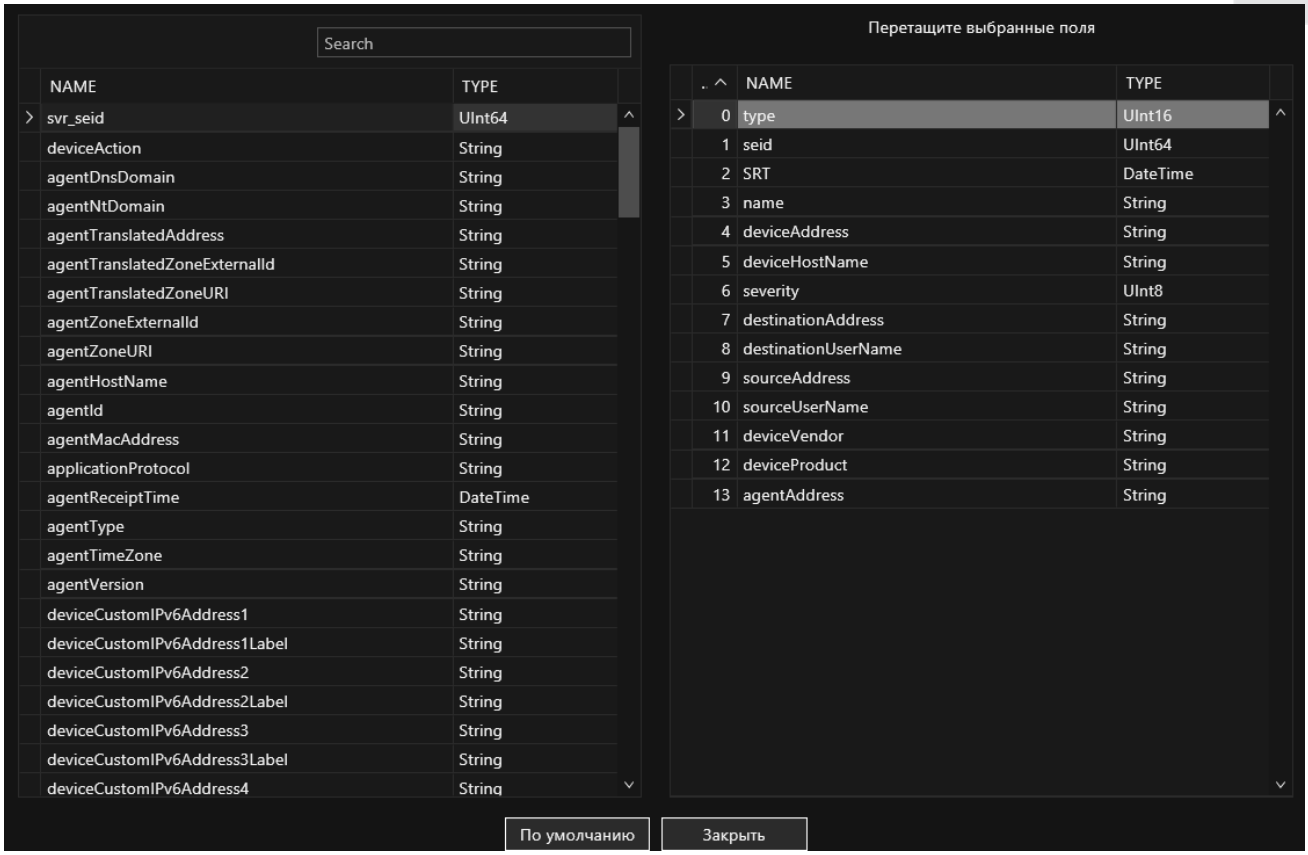


Рисунок 11. Редактор полей

В верхней части редактора запросов расположен элемент поиска полей данных по названию (см. Рисунок 12). Поисковые запросы полей не чувствительны к регистру.

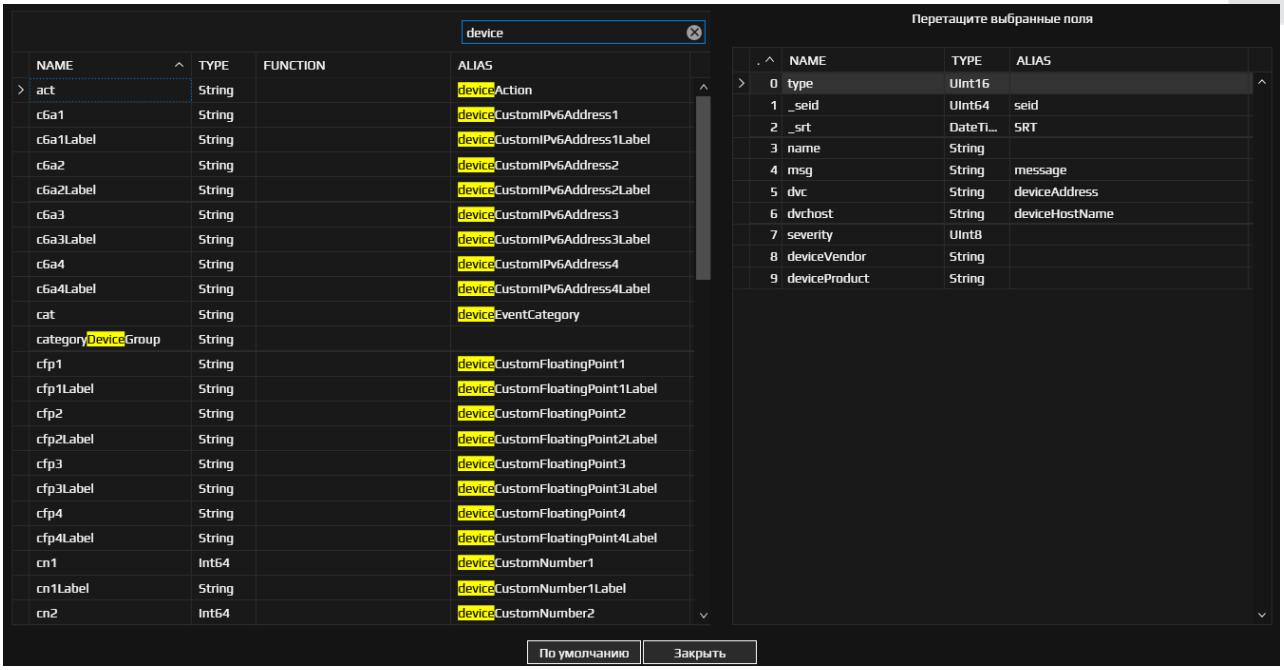


Рисунок 12. Пример поиска

5. Написание условий

При необходимости в запрос можно добавить различные условия (фильтры), для этого используется конструктор условий (см. цифра 3 Рисунок 10). Для добавления условия необходимо щёлкнуть ПКМ по условию And, и в контекстном меню пункт «Добавить условие» (см. Рисунок 13), и дважды щёлкнуть ЛКМ по полю условия.

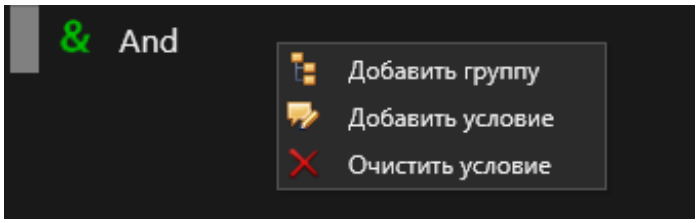


Рисунок 13. Контекстное меню редактора условий

После чего откроется диалоговое окно «Редактирования условий» (см. Рисунок 14, 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».

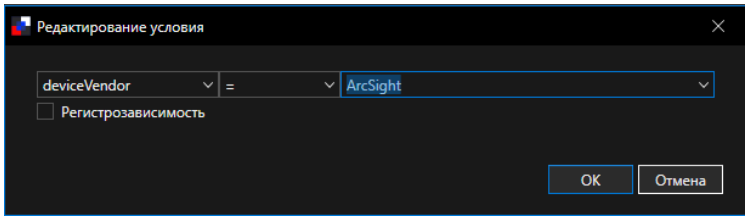


Рисунок 14. Редактирование условий

Перечень параметров условия:

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

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.

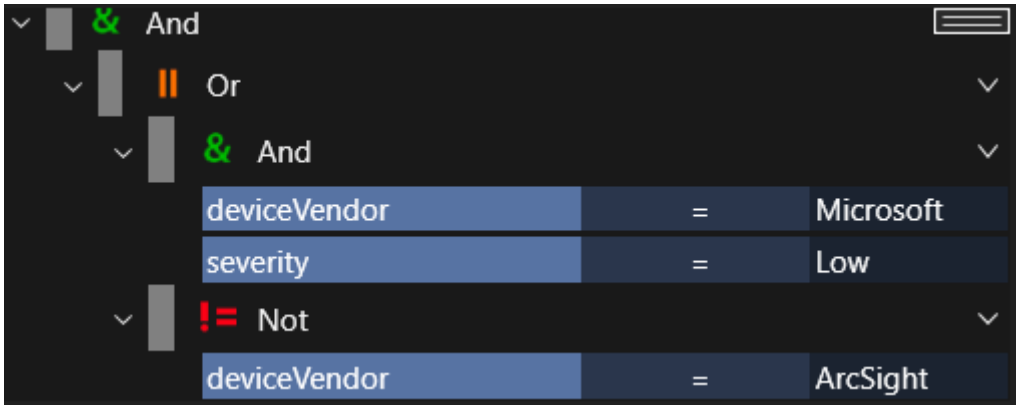


Рисунок 15. Пример условия

Также необходимо сохранить изменения в канале. Для этого нужно нажать на кнопку «Сохранить» или «Сохранить как», если необходим данный канал как основа для других каналов.

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». А для удаления АК, необходимо выбрать «Удалить», при необходимости можно переименовать АК, выбрав пункт «Переименовать».

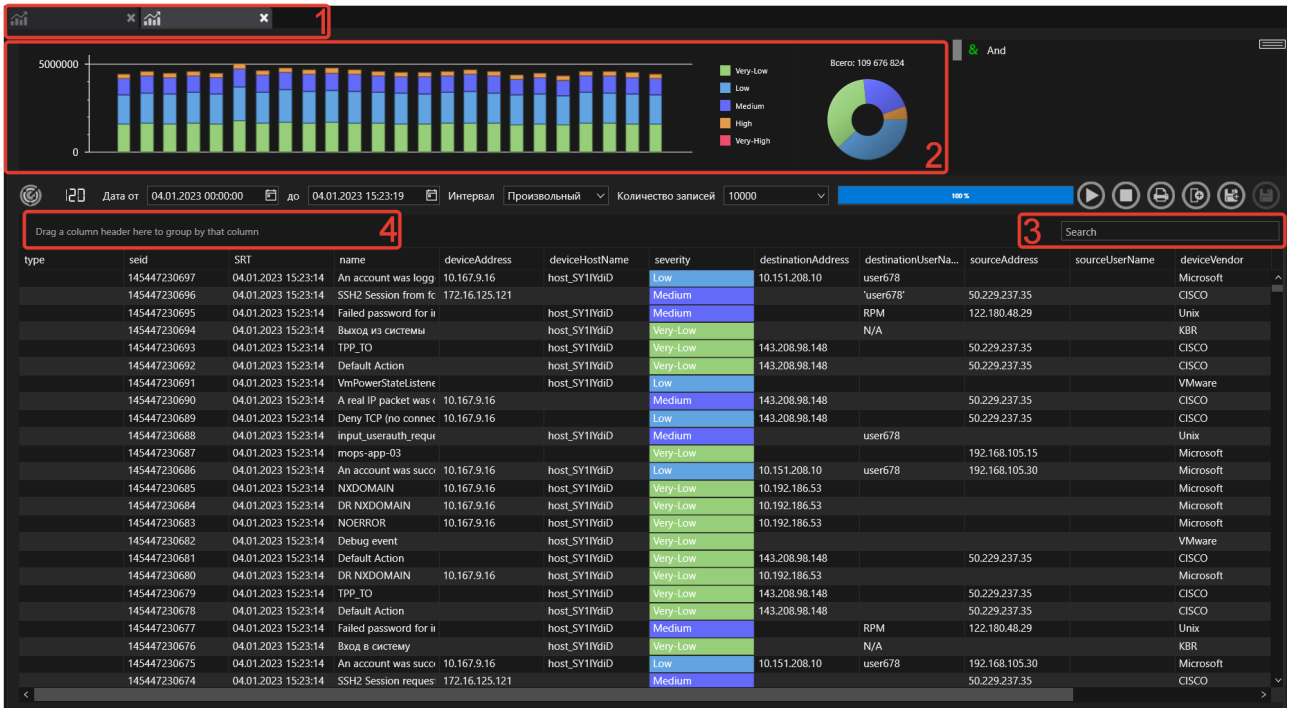
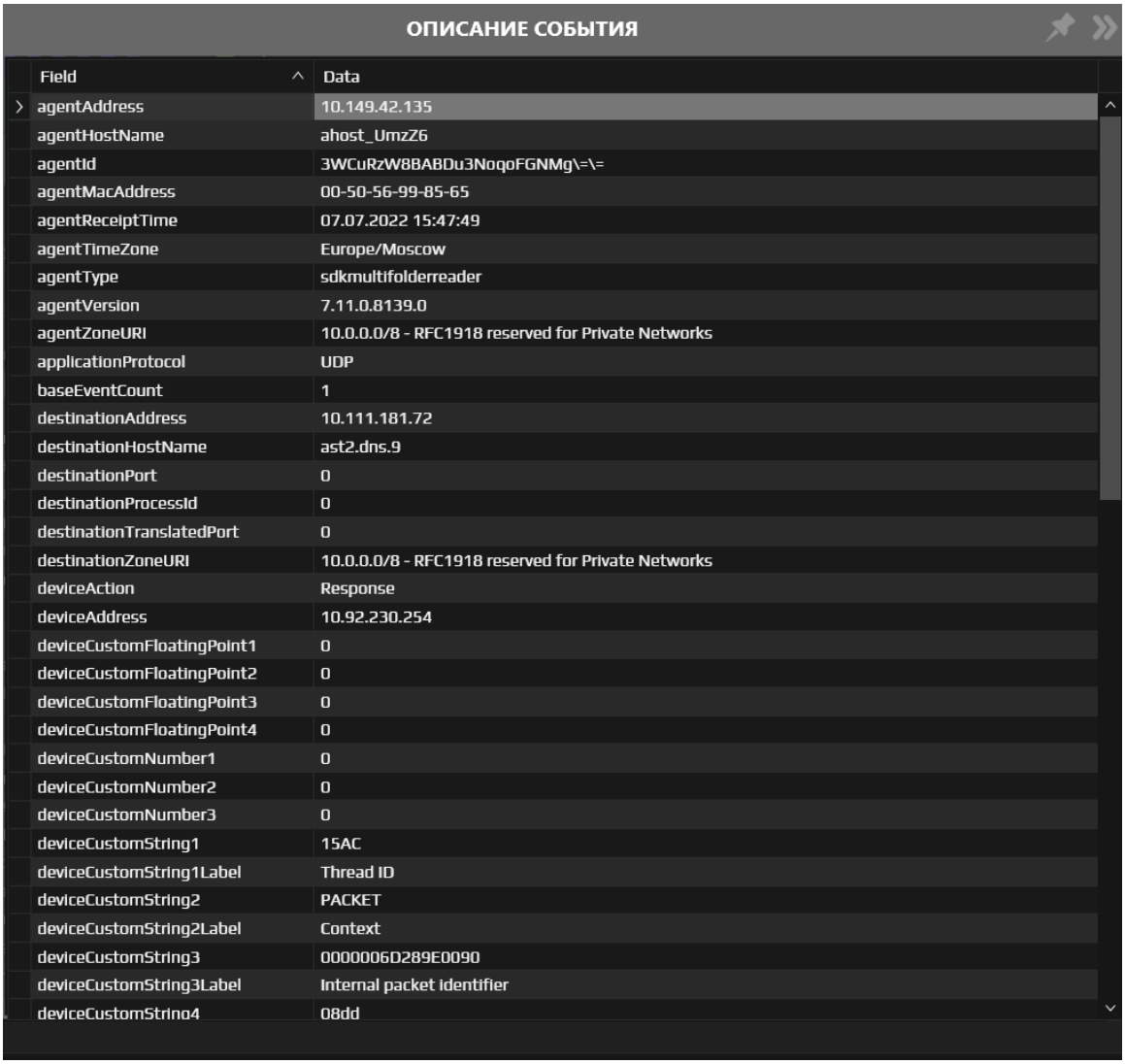


Рисунок 16. Окно АК

В области под цифрой 1 (см. Рисунок 16) представлен перечень вкладок с открытыми АК для быстрого переключения между ними. В области под цифрой 2 (см. Рисунок 16) представлена инфографика событий/радар. При наведении курсора на любую из диаграмм можно просмотреть детали событий, такие как промежуток времени, отображаемый частью радара, и кол-во событий, и их критичность. Также если дважды щёлкнуть ЛКМ в диаграмму на радаре, то построится АК за тот промежуток, что указан на радаре.

При необходимости быстрого поиска конкретного значения можно использовать поиск, расположенный в области под цифрой 3 (см. Рисунок 16).

Для детального просмотра события необходимо дважды щёлкнуть по событию, представленному в таблице. В открывшемся окне есть возможность просмотра деталей события, для закрытия окна необходимо нажать на кнопку (см. Рисунок 17).



ОПИСАНИЕ СОБЫТИЯ

Field	Data
agentAddress	10.149.42.135
agentHostName	ahost_UmzZ6
agentId	3WCuRzW8BABDu3NoqoFGNMg\=\=
agentMacAddress	00-50-56-99-85-65
agentReceiptTime	07.07.2022 15:47:49
agentTimeZone	Europe/Moscow
agentType	sdkmultifolderreader
agentVersion	7.11.0.8139.0
agentZoneURI	10.0.0.0/8 - RFC1918 reserved for Private Networks
applicationProtocol	UDP
baseEventCount	1
destinationAddress	10.111.181.72
destinationHostName	ast2.dns.9
destinationPort	0
destinationProcessId	0
destinationTranslatedPort	0
destinationZoneURI	10.0.0.0/8 - RFC1918 reserved for Private Networks
deviceAction	Response
deviceAddress	10.92.230.254
deviceCustomFloatingPoint1	0
deviceCustomFloatingPoint2	0
deviceCustomFloatingPoint3	0
deviceCustomFloatingPoint4	0
deviceCustomNumber1	0
deviceCustomNumber2	0
deviceCustomNumber3	0
deviceCustomString1	15AC
deviceCustomString1Label	Thread ID
deviceCustomString2	PACKET
deviceCustomString2Label	Context
deviceCustomString3	0000006D289E0090
deviceCustomString3Label	Internal packet identifier
deviceCustomString4	08dd

Рисунок 17. Описание события

При необходимости окно с детальным просмотром события можно закрепить в правой части области таблицы АК. Для этого следует открыть окно «Описание события» и нажать на кнопку , для открепления нажать на кнопку (см. Рисунок 18).

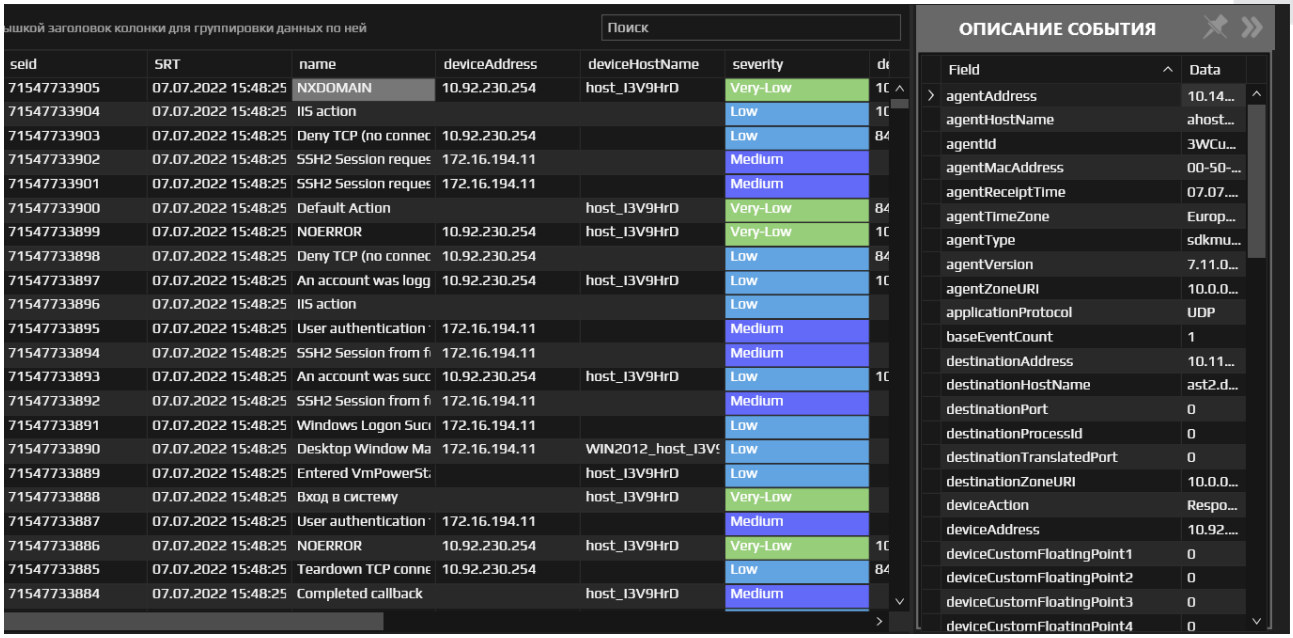


Рисунок 18. Привязка окна "Описание события"

7. Редактирование активного канала

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

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

Также в шапке полей АК можно установить фильтр. ЛКМ щёлкнуть по иконке фильтра в названии столбца и установить галочки напротив искомых значений (см. Рисунок 19). Данный фильтр отображается значения в данной колонки уже созданного канала.

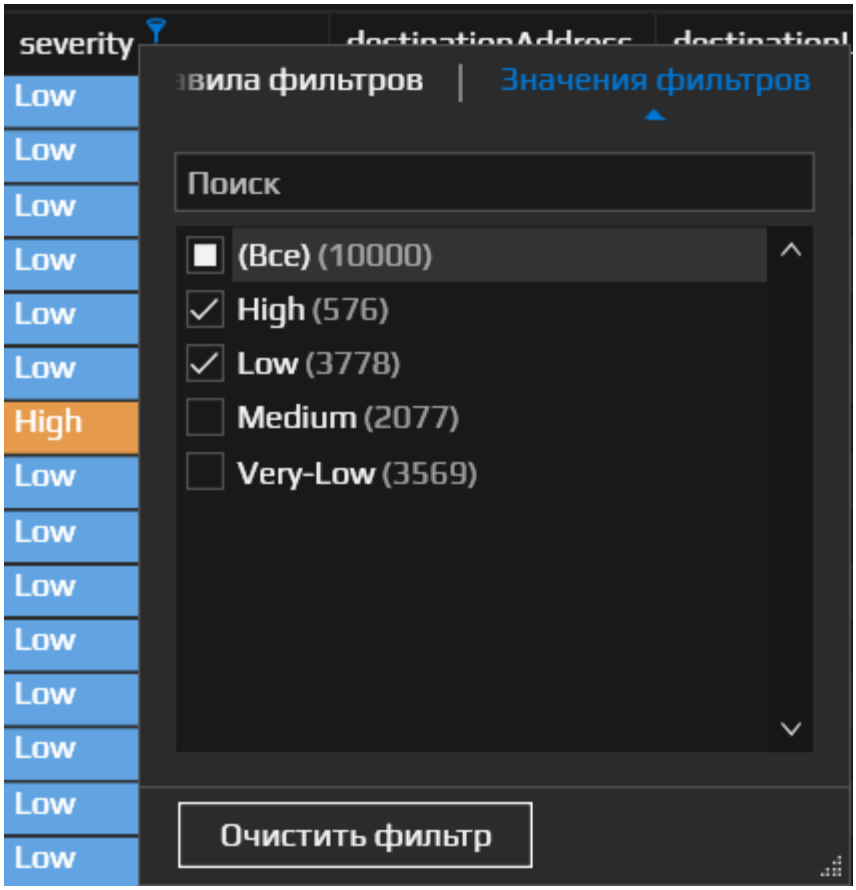


Рисунок 19. Диалоговое окно фильтра

В случае необходимости сохранения изменений следует нажать на кнопку .

Добавлять фильтры, можно с использованием контекстного меню (см. Рисунок 20) в канале, щёлкнув ПКМ по интересующему столбцу события. Выбранное условие автоматически отобразится в конструкторе условий.

Перечень параметров:

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

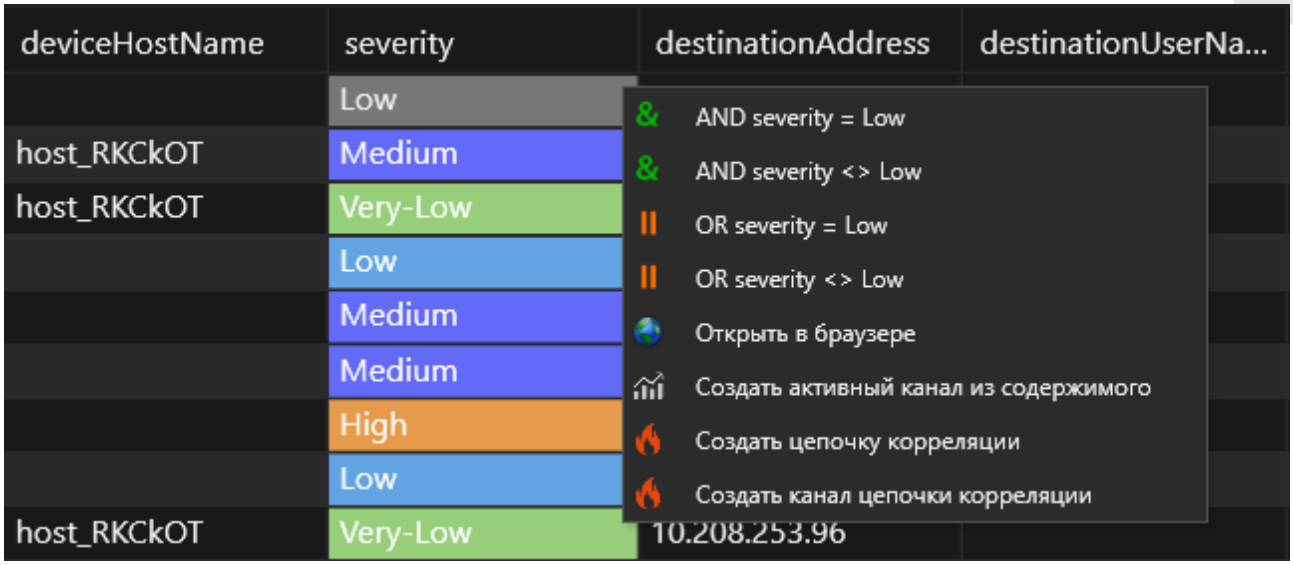


Рисунок 20. Условия / фильтры

Для фильтрации и сортировки событий в АК, необходимо ПКМ щёлкнуть по названию полей и в контекстном меню выбрать необходимую функцию (см. Рисунок 21).

Перечень функций для сортировки/фильтрации событий:

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

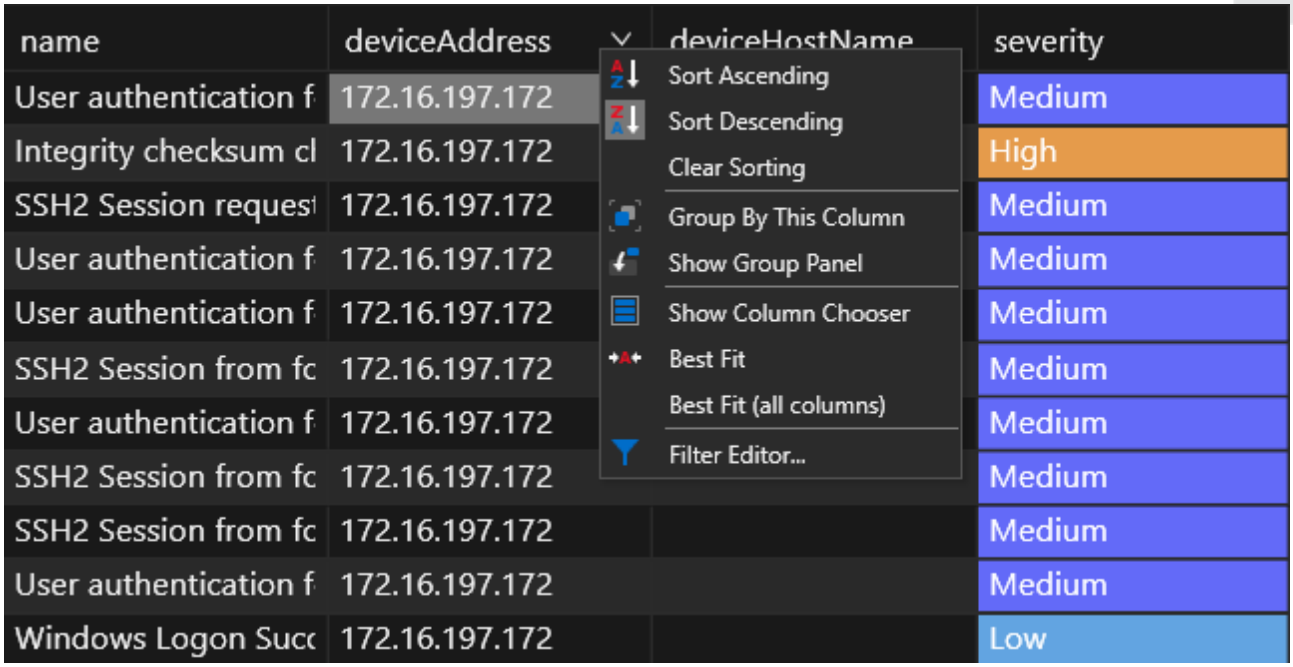


Рисунок 21. Фильтрация и сортировка

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

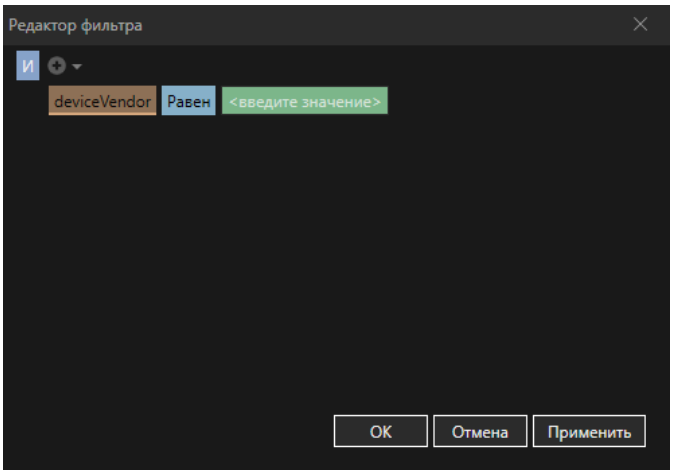


Рисунок 22. Диалоговое окно создание фильтра

В появившейся конструкции deviceAddress Equals <enter a value> 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.

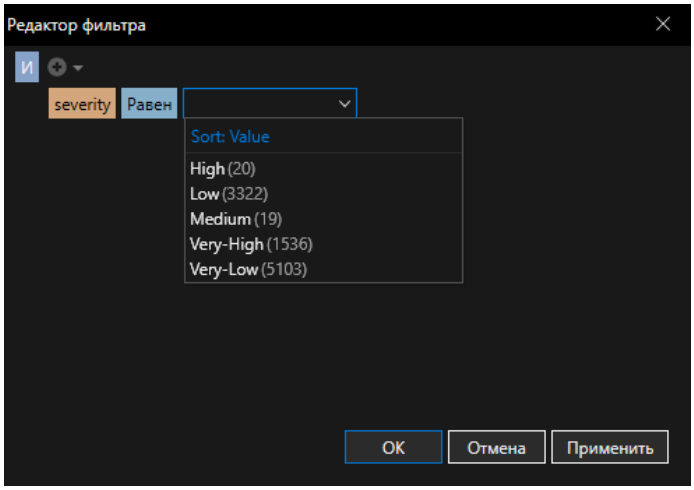


Рисунок 23. Выбор значения из предложенных вариантов

Пример: колонка severity содержит значение. И на выбор то, что уже есть в колонке открывается при наведении на стрелочку рядом с полем. Либо, значение можно внести вручную (см. Рисунок 23).

Для добавления ещё одного условия необходимо нажать на кнопку .

Если необходимо добавить условие с другим оператором, следует открыть выпадающее меню и выбрать ПМ «Add Group» (см. Рисунок 24) и в новой группе сменить оператора.

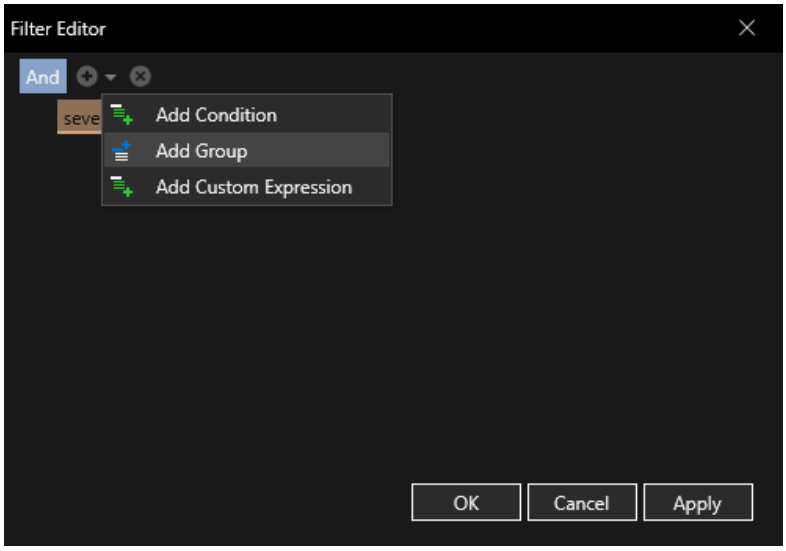


Рисунок 24. Выпадающий список

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

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

Группировка событий

Группировать события в системе можно 2-мя способами:

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

Для группировки полей с помощью контекстного меню столбца, в АК следует нажать ПКМ по нужной колонке и в контекстном меню выбрать пункт «Сгруппировать по этой колонке» (см.Рисунок 25). Если необходимо группировать события внутри уже сгруппированных событий, следует в контекстном меню нужного столбца выбрать пункт «Group By This Column» и события перейдут на следующий уровень группировки. Открыть описание событий, можно нажатием на кнопку .

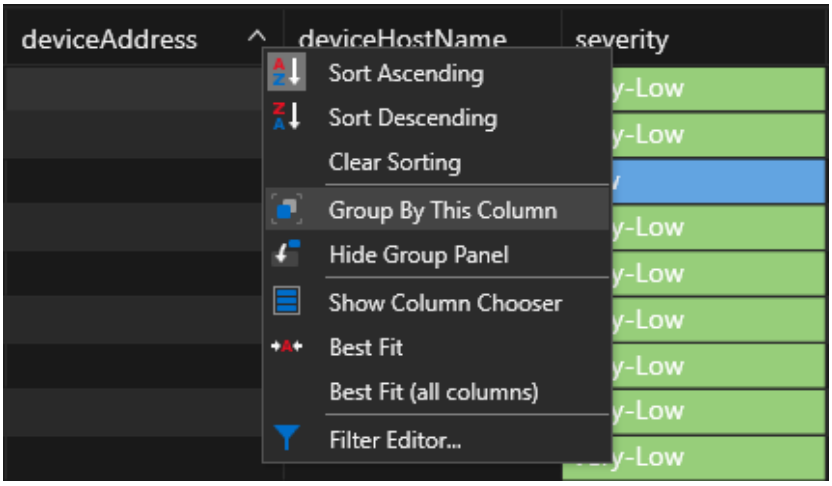


Рисунок 25. Контекстное меню группировки

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 (см. Рисунок 26 область под цифрой 1). Если необходимо группировать события внутри уже сгруппированных событий, то следует перетащить необходимый столбец в панель группировки.

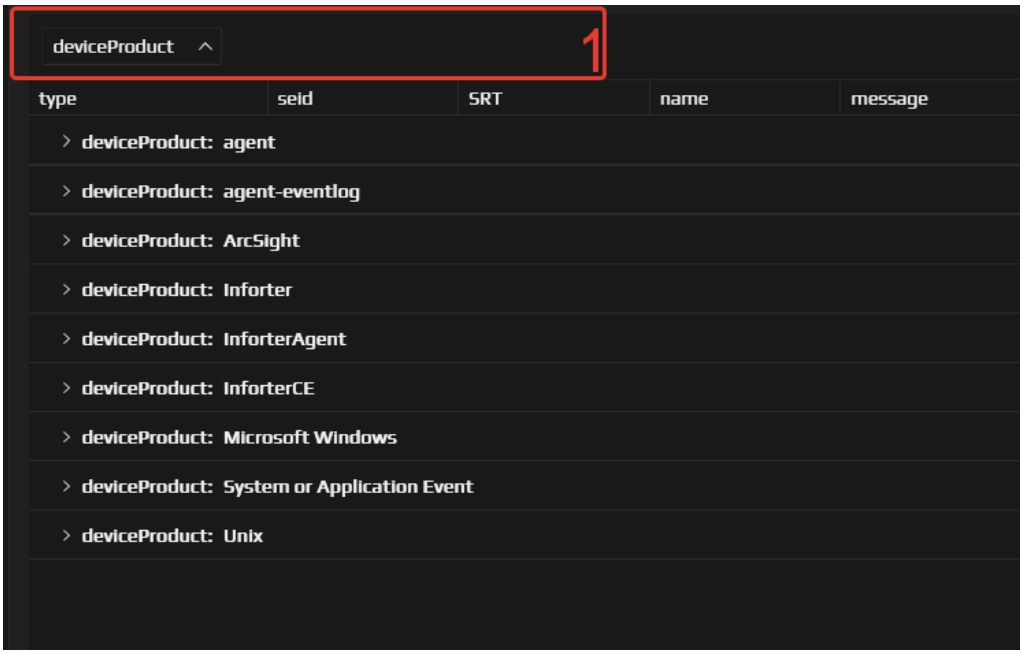


Рисунок 26. Группировка событий

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 Expande» предназначены для развёртывания и скрытия всех событий, во всех блоках группировки соответственно. При нажатии на имя столбца в панели группировки происходит сортировка группировки по алфавиту от A до Z, а при повторном нажатие сортировка от Z до Z.

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 27).

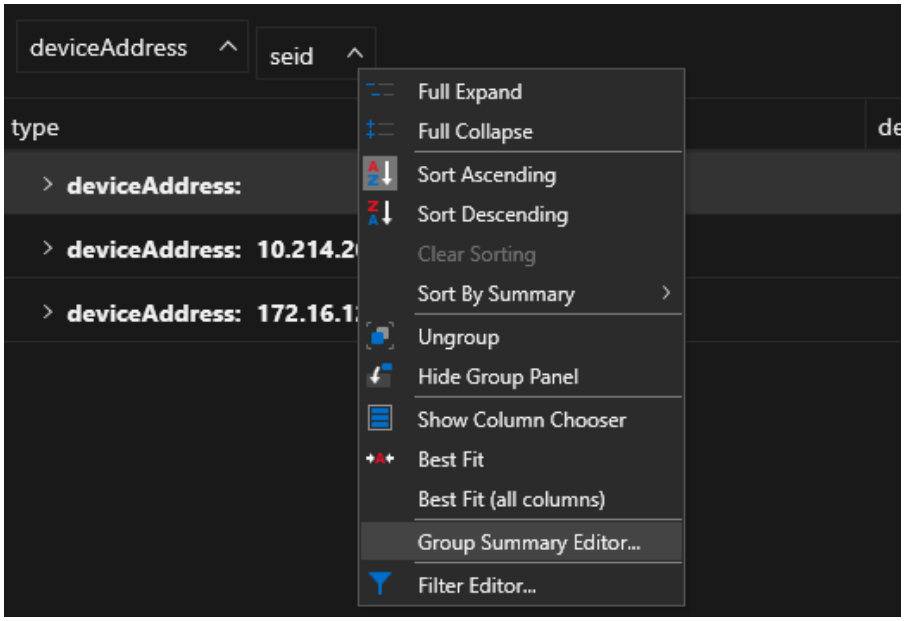


Рисунок 27. Контекстное меню элемента панели группировки

После чего откроется окно «Group Summaries», в котором необходимо поставить галочку у поля «Show row count» и нажать кнопку «OK» (см. Рисунок 28).

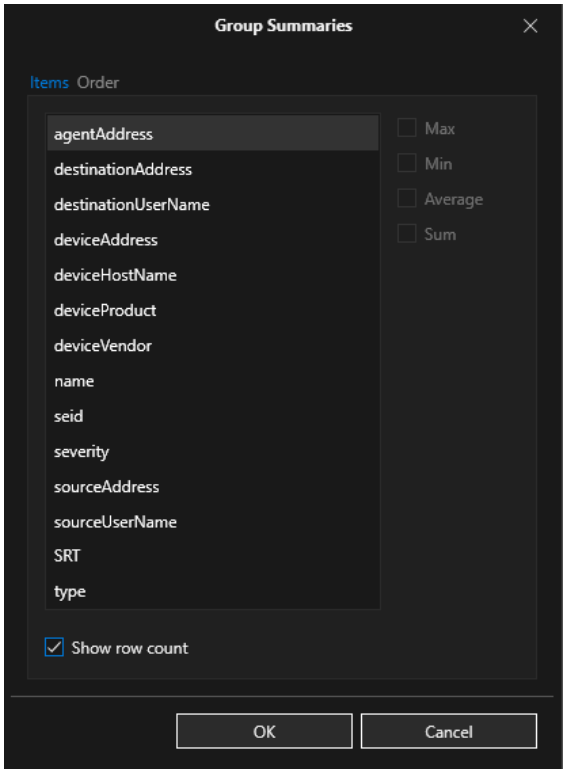


Рисунок 28. Окно редактора группировки

Пример группировки с подсчётом количества событий представлен на Рисунок 29.

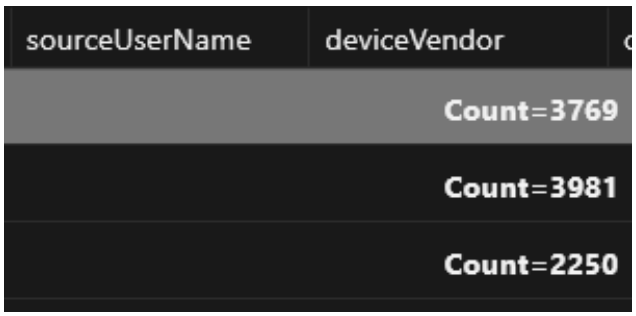


Рисунок 29. Вид группировки с подсчётом количества событий

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 30).

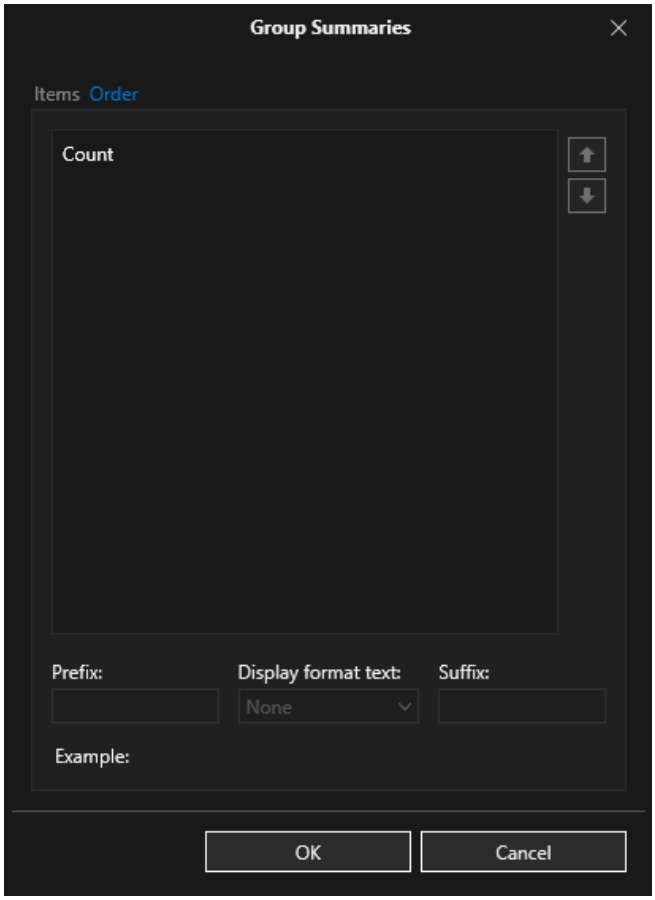


Рисунок 30. Редактор группировки

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.*

СОЗДАНИЕ ОБЪЕКТОВ ВИЗУАЛИЗАЦИИ ДАННЫХ

Для создания элемента визуализации данных, необходимо в разделе меню ресурсов перейти на вкладку «Визуализация» и нажатием ПКМ на любой строке выбрать ПМ «Создать» (см. Рисунок 31). После чего откроется окно создания элементов визуализации (см. Рисунок 32).

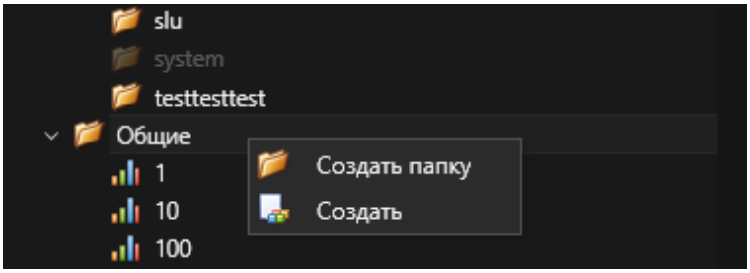


Рисунок 31. Вкладка визуализация

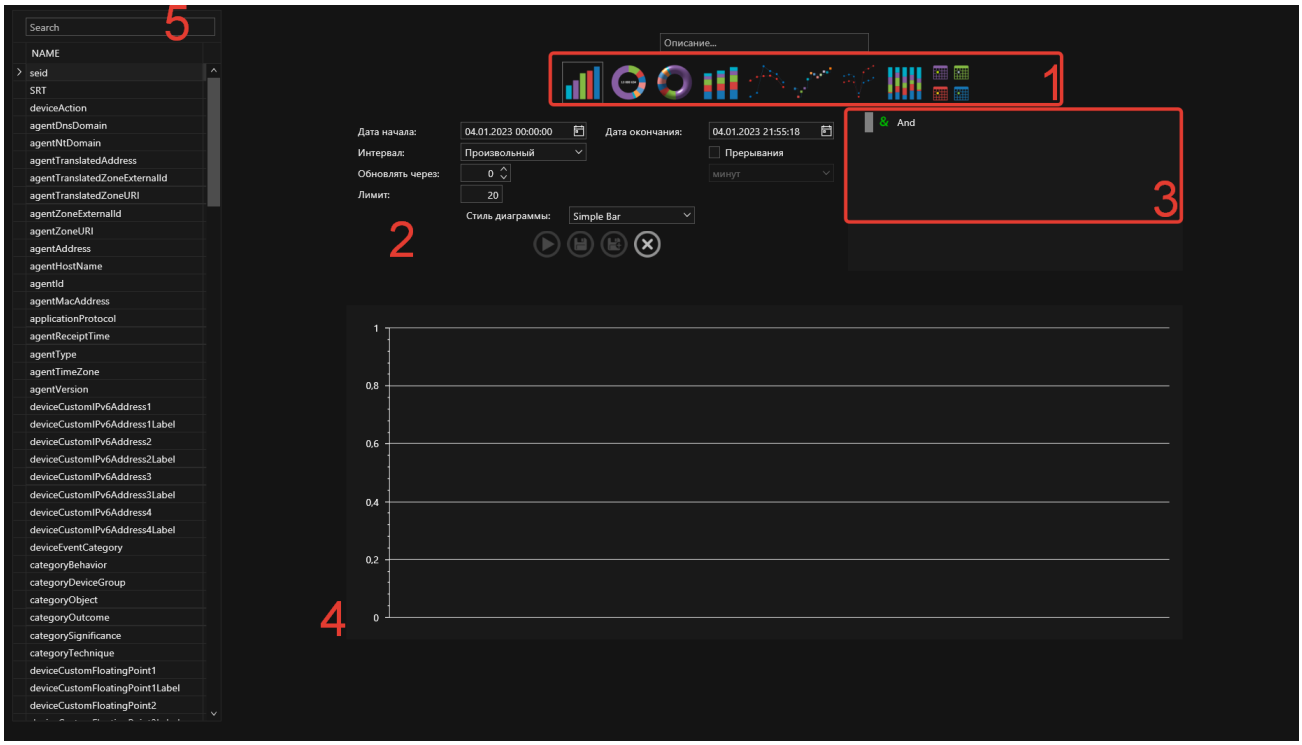


Рисунок 32. Конструктор объектов визуализации

Для создания объекта визуализации данных необходимо, выбрать тип представления данных, расположенный в области под цифрой 1 Рисунок 32.

Перечень типов представления данных:

- столбчатая диаграмма;

- круговая диаграмма;
- 3-D круговая диаграмма;
- сложенная диаграмма;
- линейная диаграмма;
- пошаговая диаграмма;
- сплайн диаграмма;
- полная сложенная диаграмма;
- таблица.

После выбора типа представления данных необходимо выбрать поля данных, по которым будет построиться визуализацию, они расположены в левой части конструктора визуализации.

Далее необходимо выбрать параметры визуализации, расположенные в области под цифрой 2 Рисунок 32. Выбрать временной диапазон данных, указать промежуток обновления данных, стиль диаграммы и при необходимости поставить галочку напротив «Прерывания», для корректного вывода диаграммы, в которой могут быть большие разлёты в данных.

При необходимости можно добавить условие на данные, для этого используется конструктор условий в области под цифрой 3 Рисунок 32 (см. «Написание условий»). Область под цифрой 4 Рисунок 32 предназначена для предварительного просмотра элемента визуализации.

Для просмотра объекта визуализации необходимо нажать на кнопку запуска . Чтобы сохранить объект визуализации данных, необходимо нажать на кнопку , затем задать имя, при необходимости описание и нажать на кнопку «OK».

Таблица 2. Описание полей при создании элементов визуализации

Название поля	Описание	Примечание
Описание	Описание объекта визуализации	Не обязательное поле
Дата начала	Дата, с которой начинается выборка событий	Временной диапазон можно регулировать при редактировании элемента визуализации
Дата окончания	Дата, на которой заканчивается выборка событий	
Стиль диаграммы	Для каждого элемента визуализации предусмотрены свои стили отображения данных	
Интервал	Временной диапазон, используемый для выборки событий	Может быть 2-х видов: • произвольный – в нем указывается дата начала и конца; • фиксированный 30 минут/1час/4часа/12 часов/1 день /2 дня/1 неделя – события за последний указанный временной диапазон.

Обновлять через	Устанавливает временной интервал, через который будет происходить обновление элемента визуализации	Не обязательное поле
Прерывание	Корректная отрисовка диаграммы при наличии большого разрыва в значениях данных	
Конструктор написания условий	Позволяет ускорить процесс написания запроса	Подробно описан в пункте «Написание условий»

Рисунок 33. Корректно заполненное окно создания объекта визуализации

При необходимости, все ранее созданные элементы визуализации можно изменить. Для этого на вкладке «Визуализация» необходимо открыть ранее созданный объект визуализации данных. Откроется окно конструктора визуализации. В нем следует внести необходимые изменения и нажать кнопку запуска. Убедившись, что отобразившийся объект отвечает внесённым изменениям, его следует сохранить.

РАБОТА С ДАШБОРДАМИ

1. Создание дашбордов

Для создания дашборда необходимо иметь созданные ранее объекты визуализации данных: диаграммы и отчетные таблицы. Далее в меню ресурсов перейти на вкладку «Дашборды», откроются все созданные ранее дашборды, щёлкнув ПКМ в любой строчке, выбрать ПМ «Создать» (см. Рисунок 34).

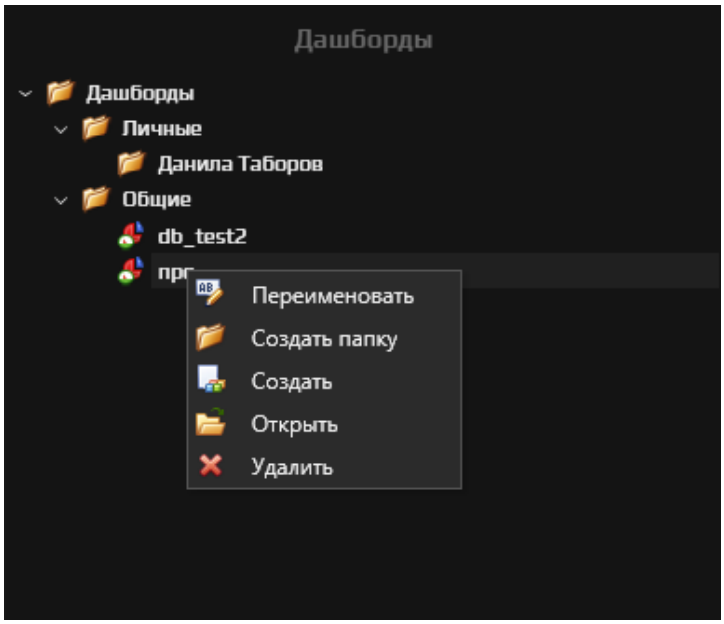


Рисунок 34. Дерево дашбордов

Откроется страница «Конструктор создания дашбордов» (Рисунок 35), в которой необходимо дать название, перетащить ранее созданный элемент визуализации из области под цифрой 1 (см. Рисунок 35) в область под цифрой 2 (см. Рисунок 35). После чего необходимо сохранить созданный дашборд, нажав на кнопку «Сохранить», для закрытия окна конструктора следует нажать на кнопку «Закрыть».

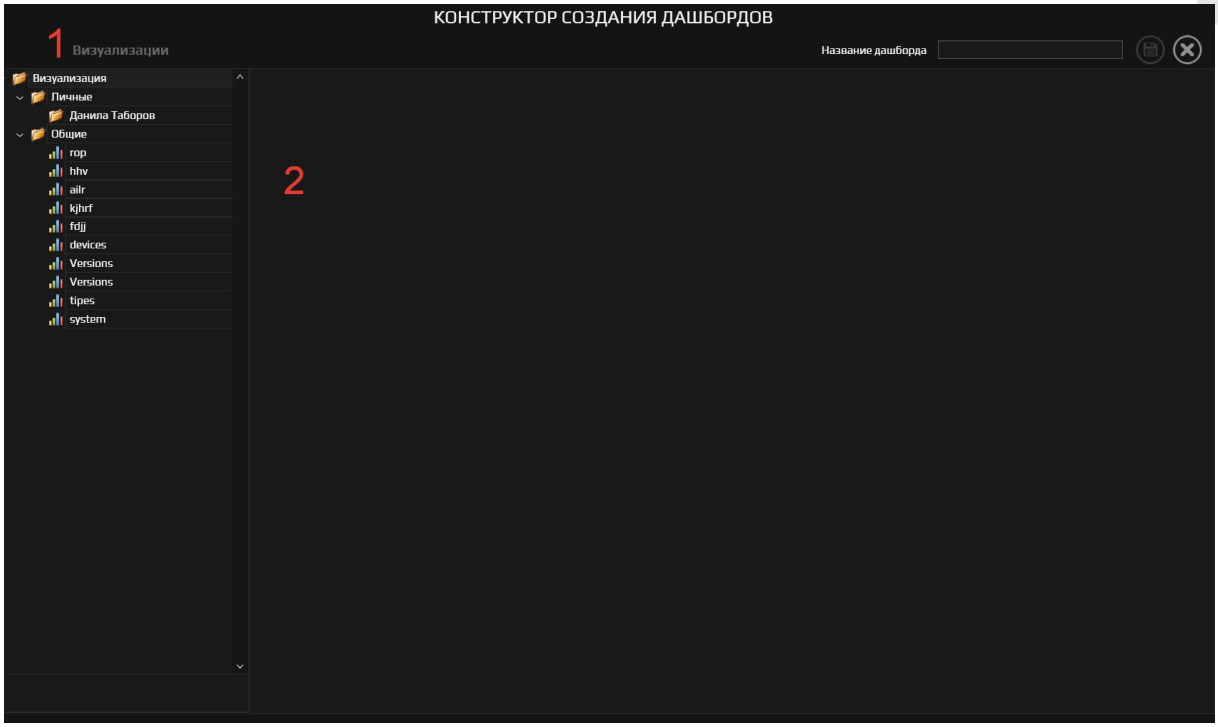


Рисунок 35. Конструктор создания дашбордов

Элементы визуализации данных можно располагать в любом порядке, для этого необходимо перетащить элемент в область, которая вам кажется наиболее подходящей из тех, что предлагает система (см. Рисунок 36), количество элементов также не ограничено.

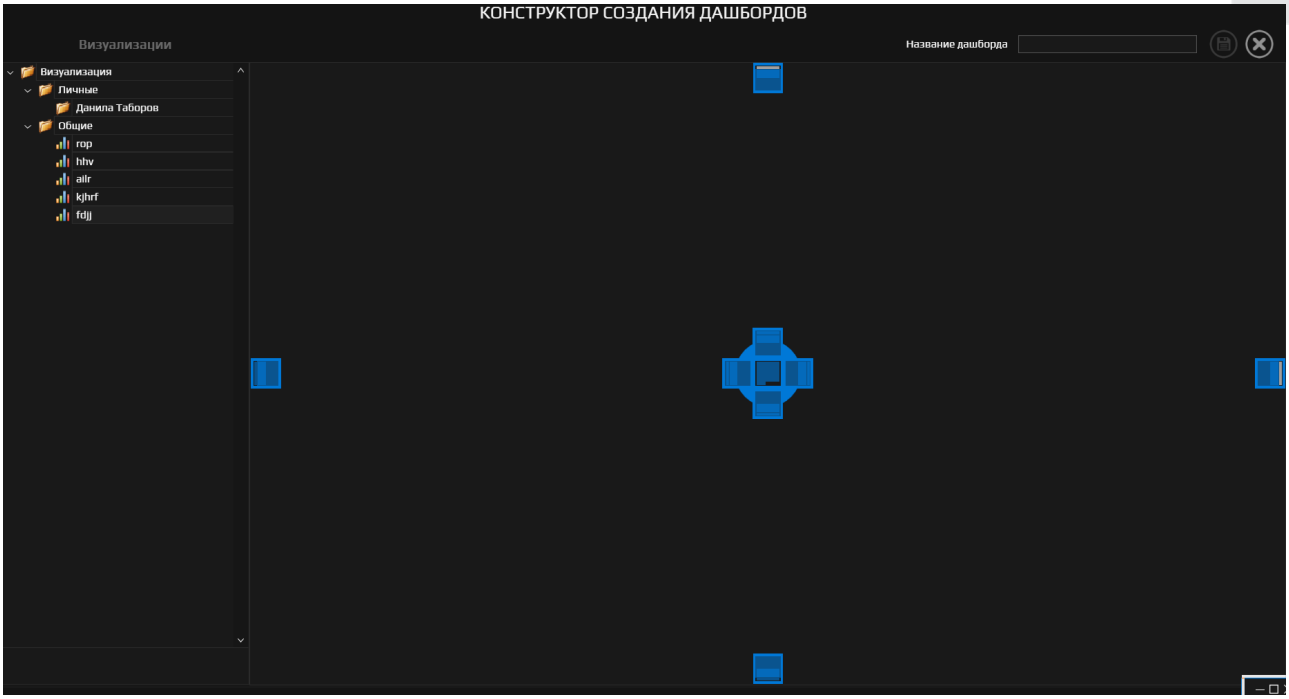


Рисунок 36. Расположение элементов на дашборде

На Рисунок 37 представлен пример дашборда с 4-мя элементами визуализации данных.

Рисунок 37. Пример создания дашбордов

2. Просмотр дашборда

Для просмотра дашборда, в меню ресурсов необходимо перейти на вкладку «Дашборды», после чего откроется перечень всех созданных в системе дашбордов. Для открытия необходимого, найдите его в списке и дважды щёлкните по нему ЛКМ, или же щёлкните ПКМ и в выпадающем меню выберете «Открыть». А для удаления дашборда необходимо выбрать пункт «Удалить». В области, выделенной красным прямоугольником (см. Рисунок 38), представлены открытые в данный момент дашборды и/или АК, для быстрого переключения между ними.

Рисунок 38. Окно дашборда

РАБОТА С АКТИВНЫМИ ЛИСТАМИ

1. Создание активного листа

Для создания АЛ в меню ресурсов необходимо перейти на вкладку «Активные листы» и выбрать необходимую папку, в которой будет располагаться новый АЛ, или создать новую, после чего выбрать ПМ «Создать» (см. Рисунок 39).

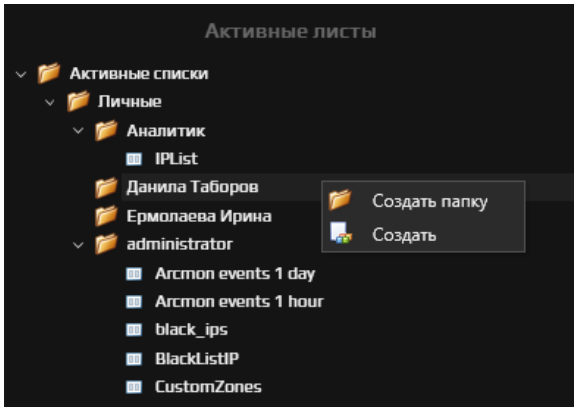


Рисунок 39. Дерево Активных листов

После чего откроется окно создания Активного листа (см. Рисунок 40).

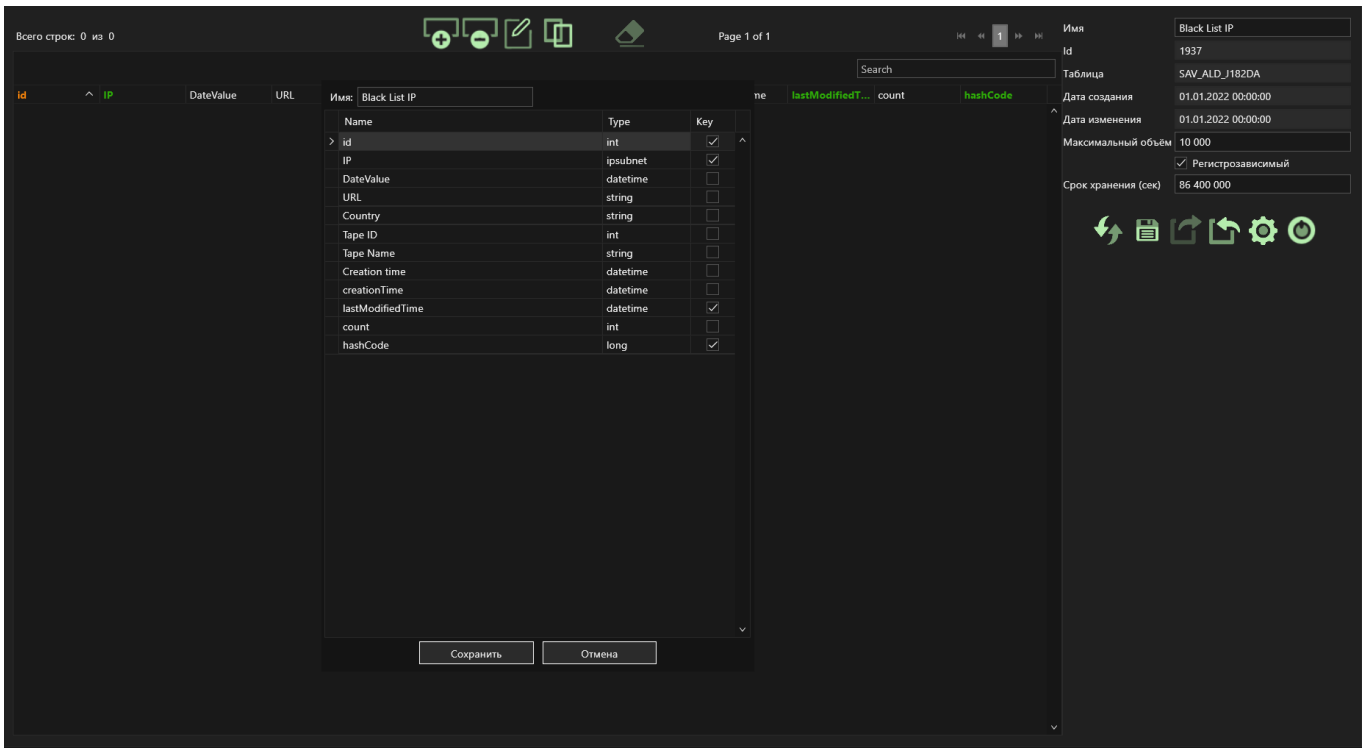


Рисунок 40. Конструктор создания Активного листа

При создании АЛ необходимо задать его название в поле «Имя» и добавить необходимые поля АЛ. Для добавления полей АЛ необходимо щёлкнуть ПКМ и выбрать ПМ «Добавить строку» (См. Рисунок 41).

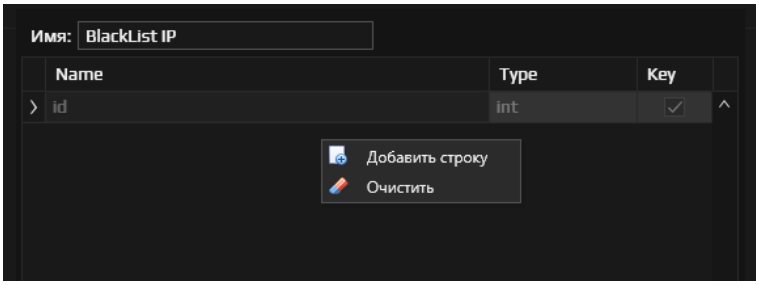


Рисунок 41. Добавление поля Активного листа

В добавившейся строке необходимо указать Наименование поля АЛ (Name), тип поля (Type) и при необходимости указать ключевое поле (Key).

Типы полей АЛ, поддерживаемые системой указаны в таблице ниже.

Таблица 3. Типы полей АЛ

№	Наименование	Описание
1.	int	32-разрядный целочисленный тип данных
2.	long	64-разрядный целочисленный тип данных
3.	string	Строковый тип данных
4.	datetime	Тип данных, содержащий в себе значение даты и времени
5.	ipsubnet	Тип данных, используемых для хранения IP

После добавления всех необходимых полей в АЛ следует нажать кнопку «Сохранить», для отмены сохранения – копку «Отменить».

Далее необходимо задать параметры АЛ (см. Рисунок 42), для этого в полях «Максимальный объём» и «Срок хранения (сек)» следует указать соответствующие значения. При необходимости учитывать регистр в таблице АЛ следует поставить галочку у параметра «Регистрозависимый». После внесения всех изменений в АЛ следует нажать на кнопку  для сохранения АЛ.

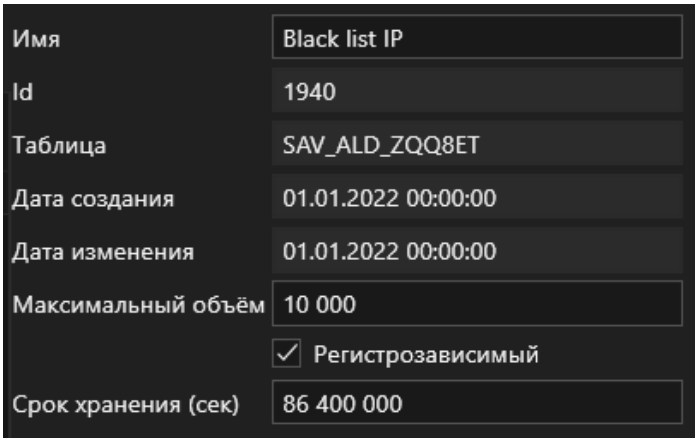


Рисунок 42. Параметры Активного листа

2. Наполнение активного листа

Наполнение АЛ может производиться как в ручном режиме, так и на основе правил корреляции событий. Для наполнения АЛ с помощью правил корреляции необходимо создать соответствующее правило и выбрать в нем действие по добавлению данных в АЛ (подробнее см. раздел «**РАБОТА С ПРАВИЛАМИ**»).

Для наполнения АЛ в ручном режиме необходимо открыть ранее созданный АЛ и нажать на кнопку . В отрывшемся диалоговом окне «Добавить строку» заполнить данными соответствующие поля (см. Рисунок 43). После чего нажать на кнопку «OK», для отмены сохранения данных следует нажать на кнопку «Cancel».

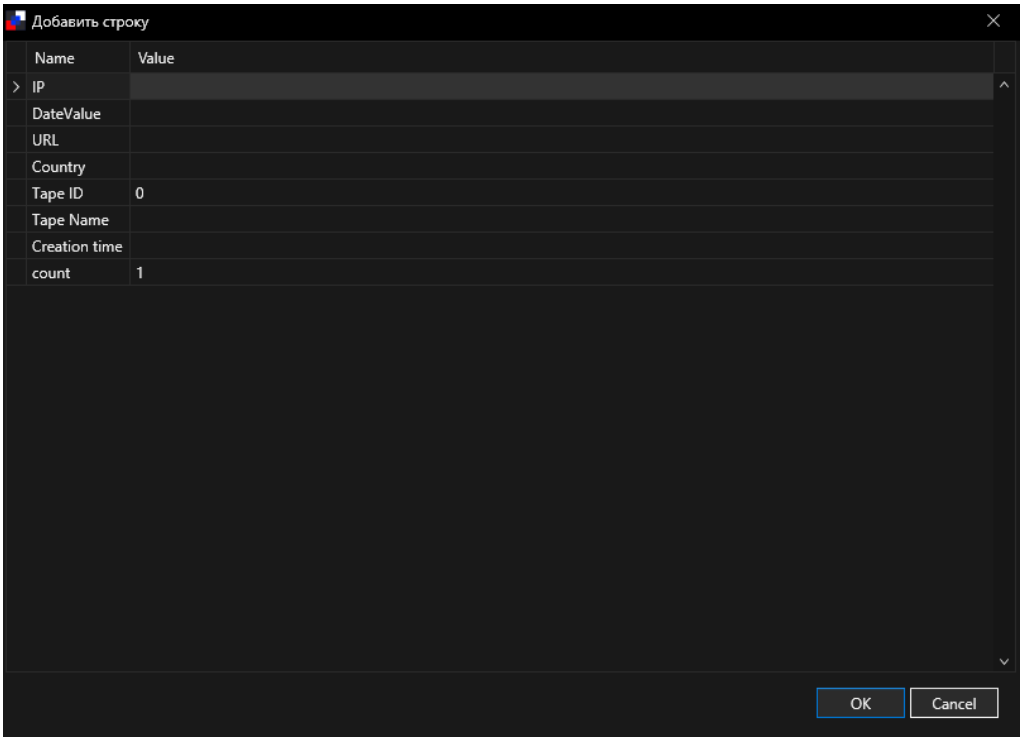


Рисунок 43. Добавление строки в АЛ

Редактирование строки АЛ можно производить с помощью кнопки редактирования, для этого выделите строку, которую необходимо отредактировать и нажмите на кнопку. После чего откроется диалоговое окно редактирования строки АЛ. Также можно щёлкнуть ПКМ по необходимой строке и в контекстном меню выбрать «Редактировать».

Удаление строки АЛ можно производить с помощью кнопки удаления, для этого выделите строку, которую необходимо удалить и нажмите на кнопку .Подтвердите удаление строки. Также можно щёлкнуть ПКМ по необходимой строке и в контекстном меню выбрать «Удалить».

Ниже представлен пример заполненного АЛ.

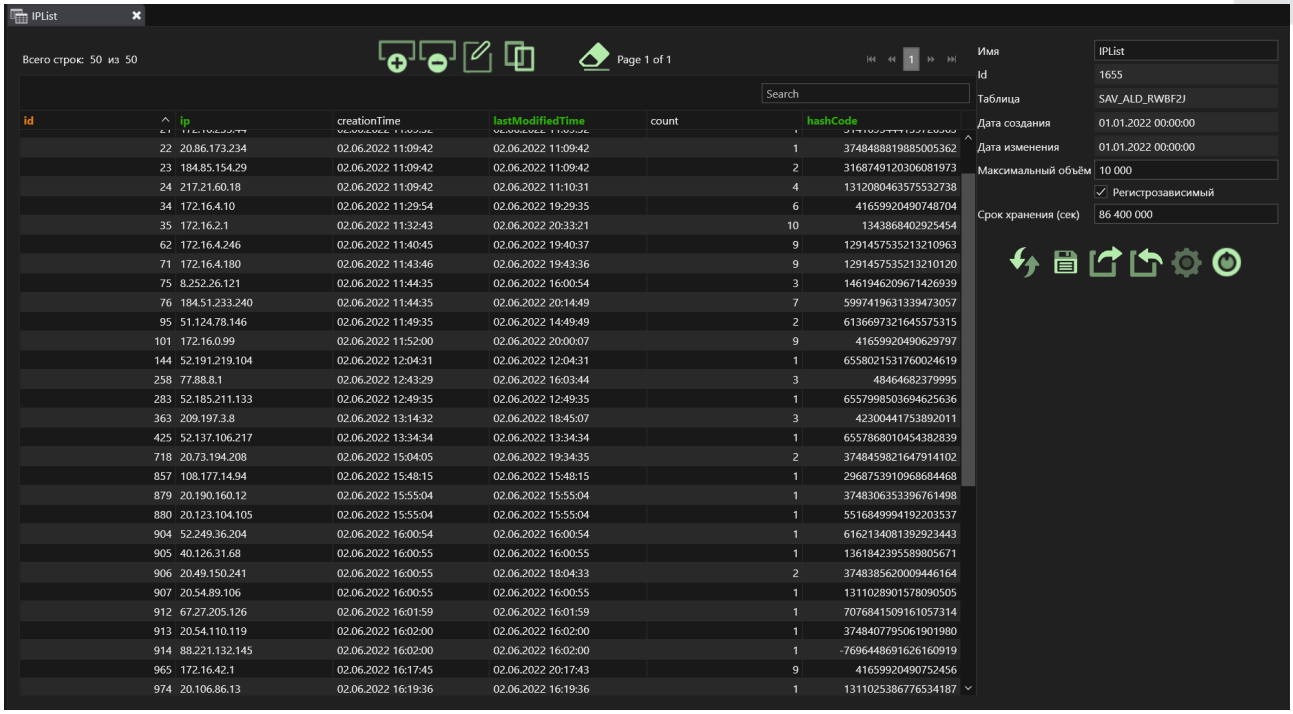


Рисунок 44. Пример заполненного АЛ

Для наполнения АЛ с помощью файла Excel, необходимо нажать на кнопку  и в появившемся диалоговом окне выбрать файл для загрузки. *Убедитесь, что в загружаемом файле количество столбцов соответствует полям АЛ.*

3. Управление активным листом

Для управления АЛ следует использовать кнопки, описанные в Таблица 4.

Таблица 4. Элементы управления АЛ

Иконка	Наименование	Назначение
	Обновить активный лист	Используется для обновления данных в АЛ
	Сохранить активный лист	Используется для сохранения изменений в АЛ
	Выгрузить в Excel	Используется для выгрузки данных из АЛ в файл Excel
	Загрузить из Excel	Используется для загрузки данных из файла Excel в АЛ
	Редактировать активный лист	Используется для редактирования полей АЛ (добавления/удаления/ переименования/изменения типа/выбора ключевого поля)

	Очистить активный лист	Используется для удаления всех данных из АЛ
	Активировать	Используется для активации АЛ

4. Удаление активного листа

Для удаления АЛ в меню ресурсов необходимо перейти на вкладку «Активные листы» и выбрать необходимый АЛ, после чего выбрать ПМ «Удалить» (см. Рисунок 45).

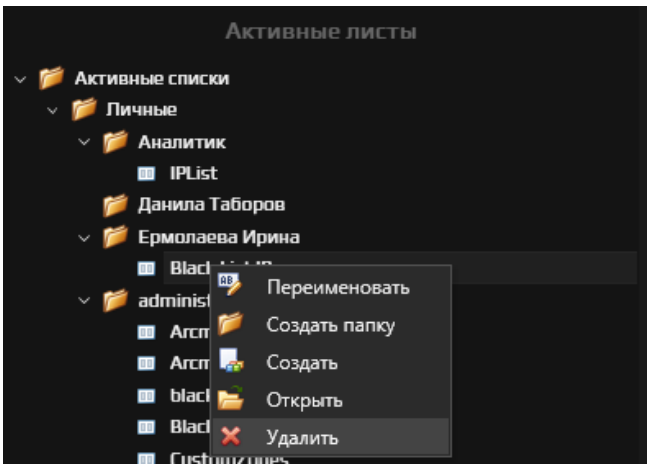


Рисунок 45. Удаление Активного листа

РАБОТА С УВЕДОМЛЕНИЯМИ

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 46).

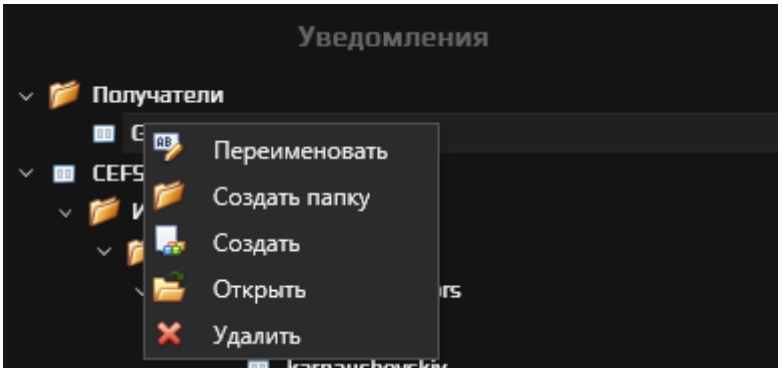


Рисунок 46. Дерево правил

После чего откроется окно создания Получателя (см. Рисунок 47), в котором необходимо указать Имя получателя, способ получения (по почте или cefsyslog), адрес почты или данные для отправки cefsyslog (хост, порт и протокол). После чего необходимо сохранить внесённые изменения.

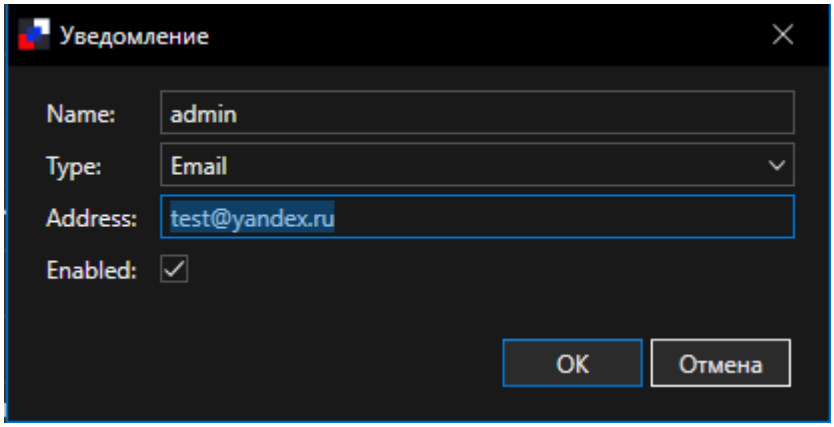


Рисунок 47. Окно создания получателя

РАБОТА С ШАБЛОНАМИ 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 48).

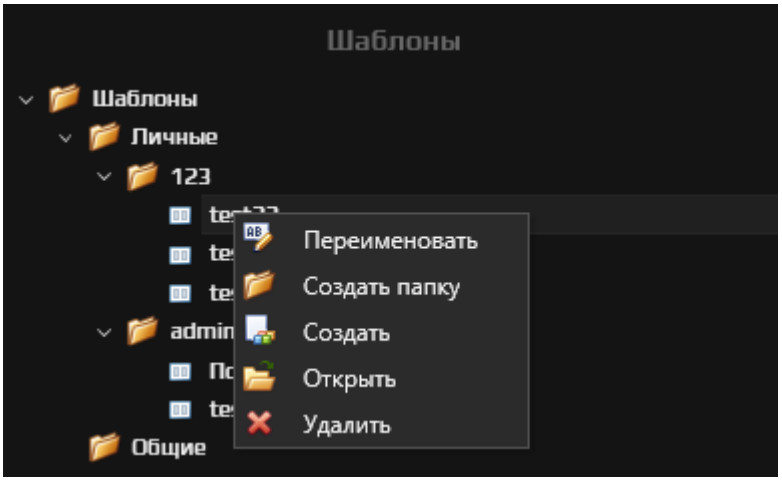


Рисунок 48. Дерево Шаблонов

После чего откроется окно создания Шаблона (см. Рисунок 49). В данном окне в поле «Имя» необходимо задать название Шаблона, в поле «Текст» добавить необходимое описание уведомление. После чего сохранить Шаблон, нажатием на кнопку «Сохранить».

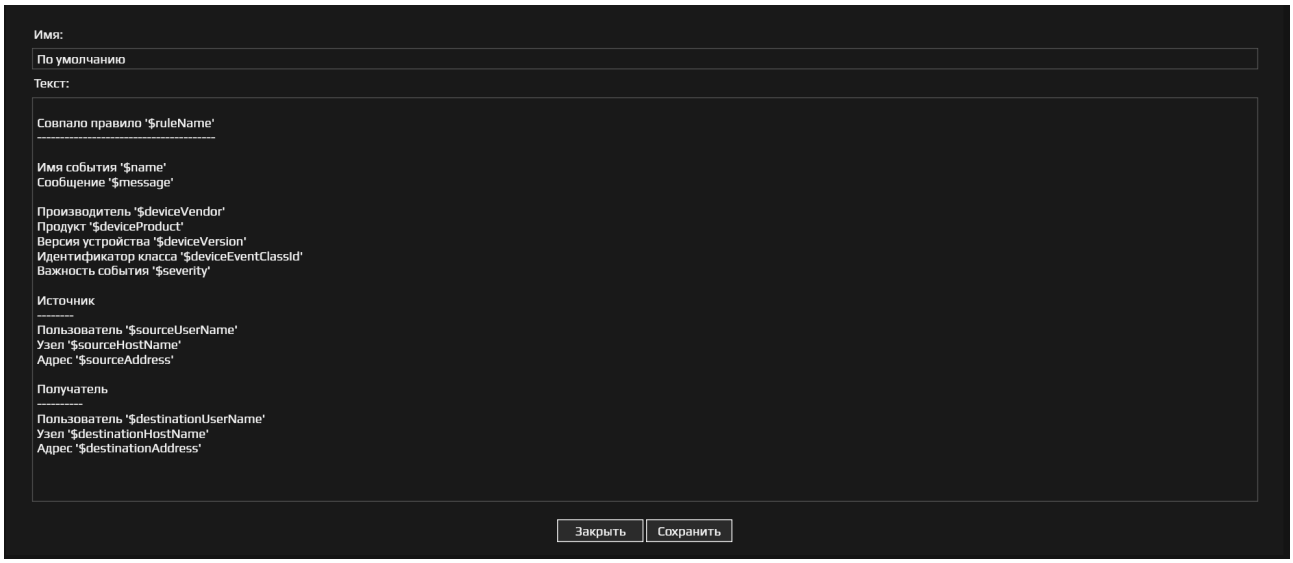


Рисунок 49. Пример Шаблона

РАБОТА С ПРАВИЛАМИ

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 ПМ «Создать» (см. Рисунок 50).

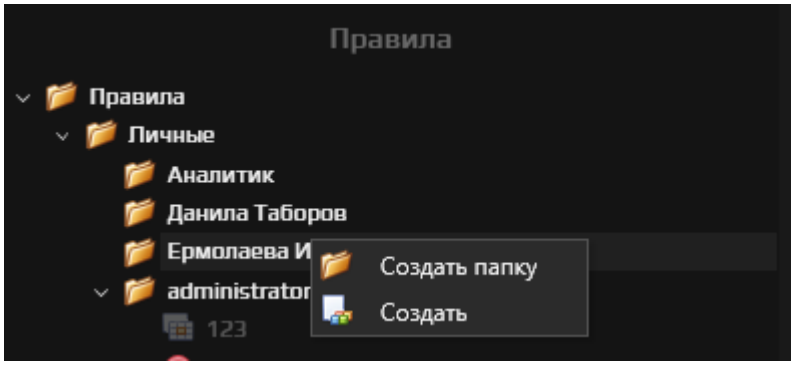


Рисунок 50. Дерево правил

После чего откроется окно создания Правил (см. Рисунок 51).

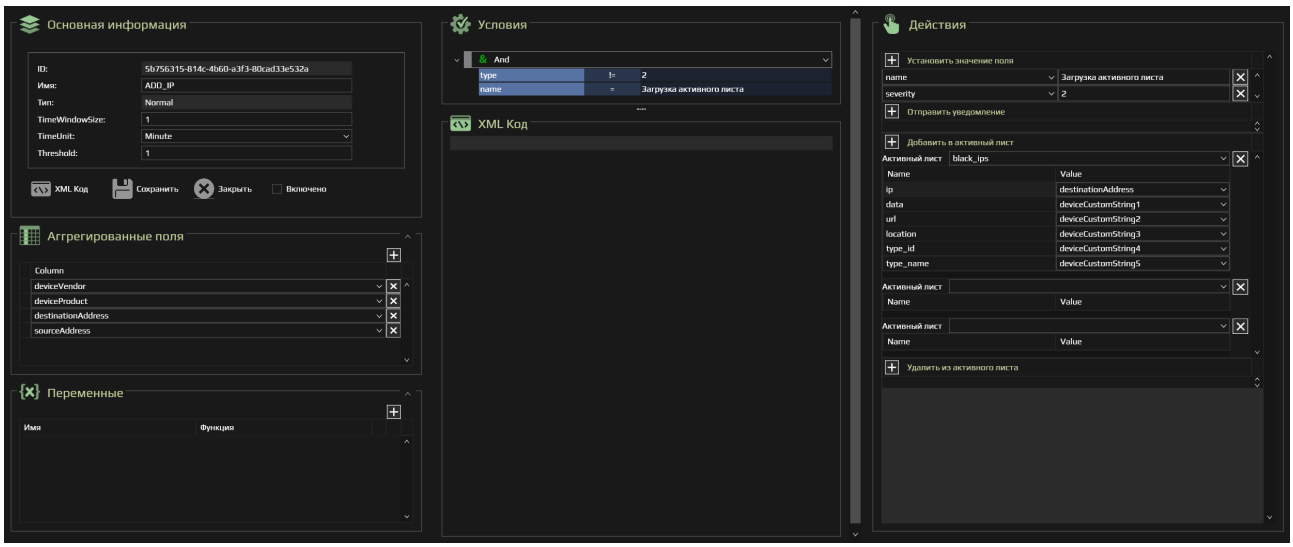


Рисунок 51. Конструктор создания Правил

Для создания правил в первую очередь необходимо заполнить основную информацию (см. Рисунок 52), где:

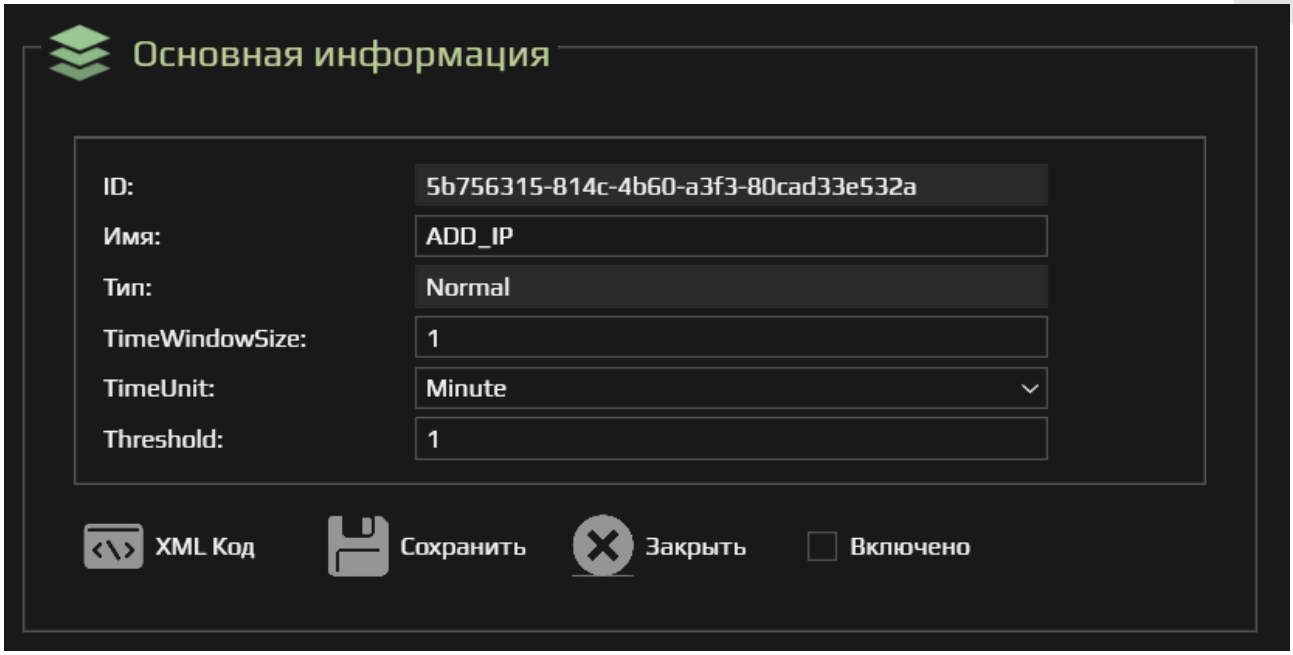


Рисунок 52. Основная информация по Правилу

- ID – уникальный идентификатор Правила присваивается автоматически;
- Имя – наименование правила;
- Включено – данный параметр необходим для активации Правила;
- XML код – кнопка предназначена для отображения правила в формате XML кода (отображается в отдельной области конструктора правил, см. Рисунок 53).

Рисунок 53. Пример отображение Правила в виде XML кода

После добавления основной информации по Правилу следует добавить условия в разделе «Условия» (см. Рисунок 54) (Подробнее как создавать условия описано в разделе «**Написание условий**»). По умолчанию Правило создаётся с условием type=2, это сделано для того, чтобы оно не уходило в рекурсию.

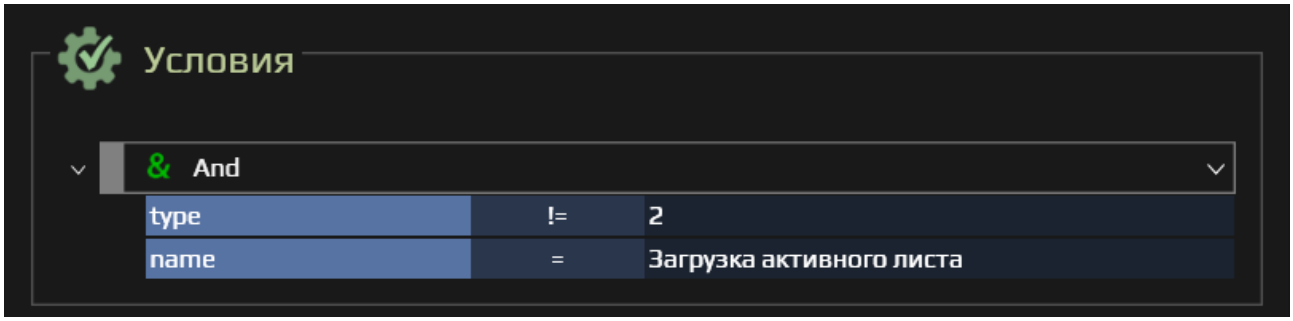


Рисунок 54. Раздел "Условия"

Далее в разделе «Действия» (см. Рисунок 55) Правилу можно назначить определённые действия, т.е. что Правило должно сделать после срабатывания.

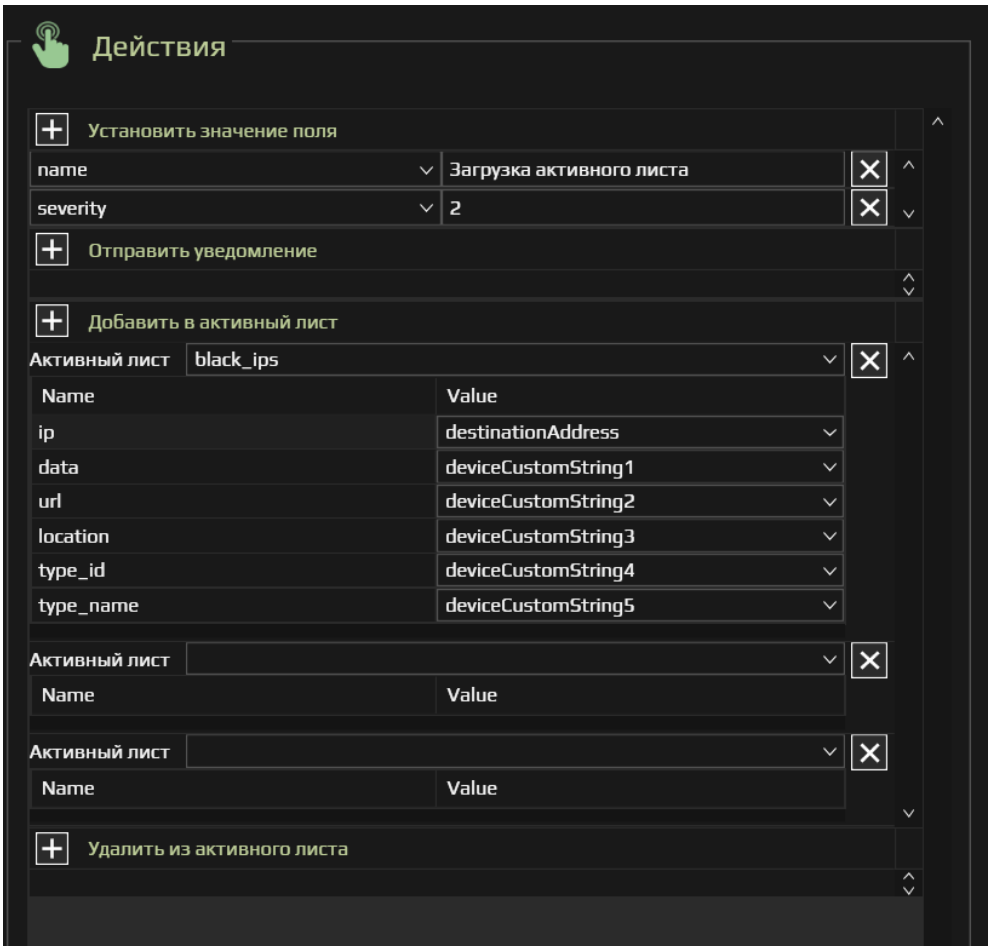


Рисунок 55. Раздел "Действия"

Правилу можно назначить следующие действия:

- **Установить значение поля** (см. Рисунок 56) – система во вновь созданном корреляционном событии присвоит выбранным полям назначенные параметры. Кнопка ⊞ предназначена для добавления нового поля, кнопка ☒ предназначена для удаление добавленного поля.

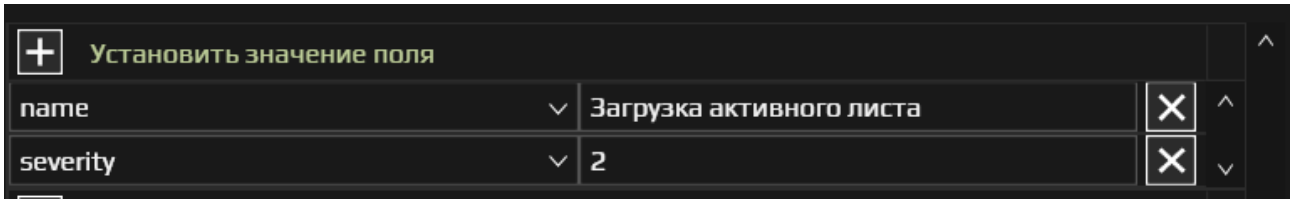


Рисунок 56. Окно установки значений полям

- **Отправить уведомление** – 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 подробнее см. «**РАБОТА С УВЕДОМЛЕНИЯМИ** и **РАБОТА С ШАБЛОНАМИ УВЕДОМЛЕНИЙ** соответственно».

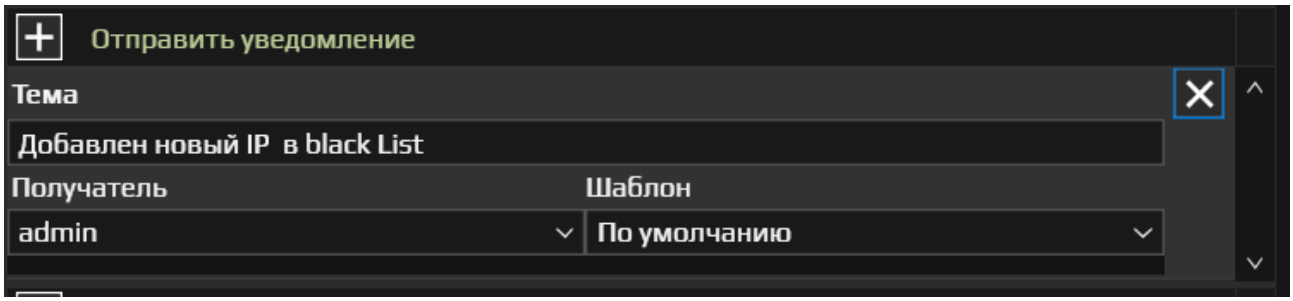


Рисунок 57. Окно настройки отправки уведомлений

- **Добавить в АЛ /Удалить из АЛ** – на основе Правил можно обновлять данные в ранее созданных АЛ. Для этого необходимо выбрать раздел «Добавление в активный лист» или «Удаление из активного листа» и в поле «Активный лист» выбрать АЛ, в который будут вноситься изменения. Далее отобразятся поля АЛ для которых необходимо выбрать значения, которые следует в них добавить после срабатывания Правила (см. Рисунок 58).

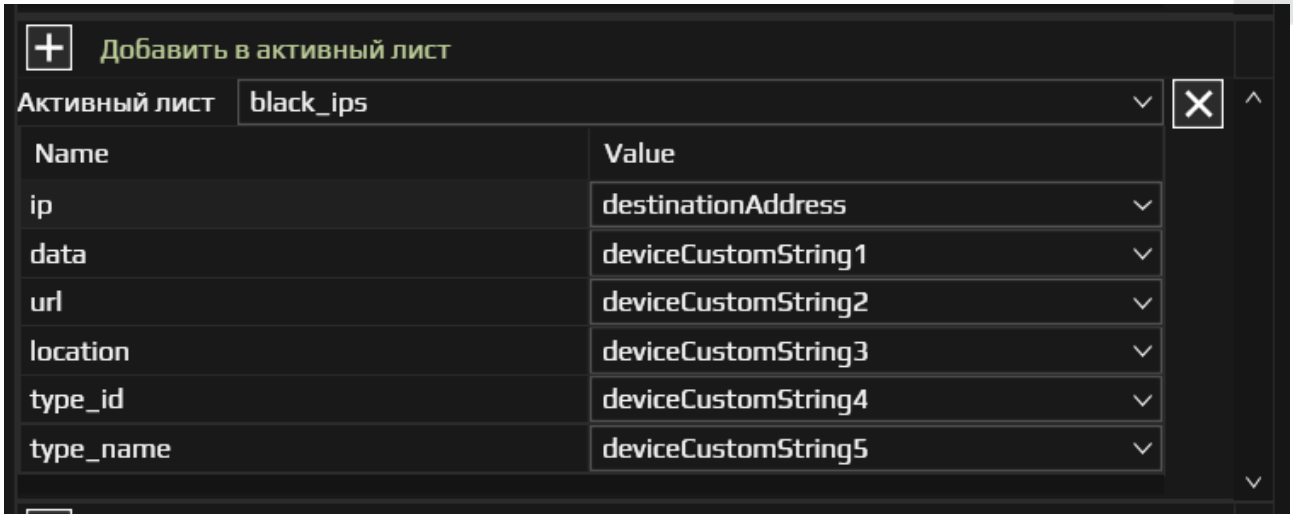


Рисунок 58. Окно обновления данных в АЛ

- **Агрегированные поля** – предназначены для обогащения корреляционных событий данными. Для обогащения необходимо в раздел «Агрегированные поля» выбрать поля, которые будут дополнительно выводиться в воссозданном корреляционном событии. (см. Рисунок 59).

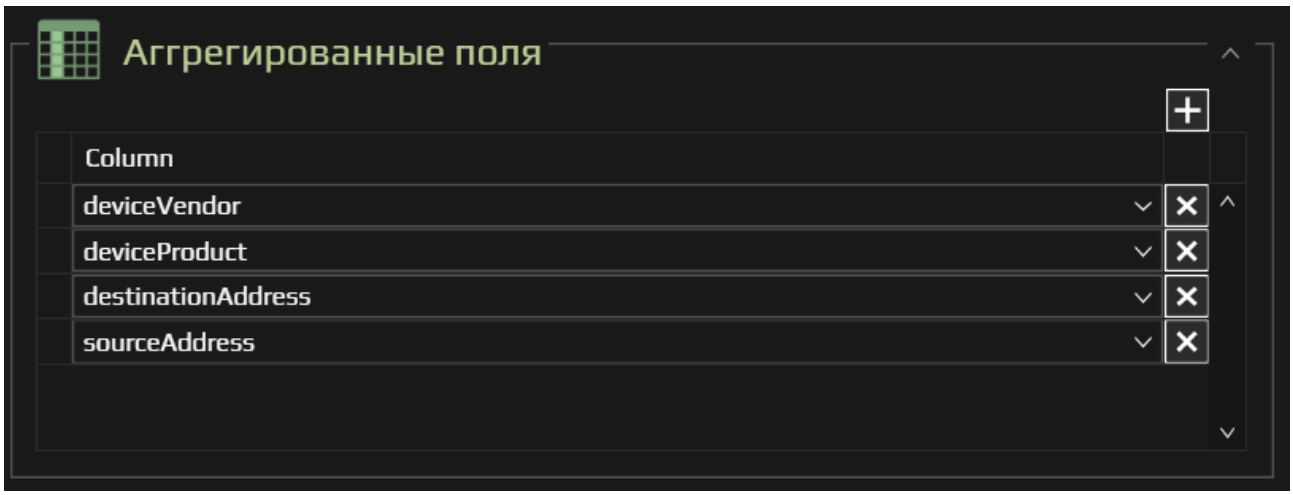


Рисунок 59. Окно агрегированных полей

- **Переменные** – при необходимости в Правила можно добавлять различные переменные (см. Рисунок 60). Подробное описание переменных представлено в разделе «**ОПИСАНИЕ ПЕРЕМЕННЫХ**».

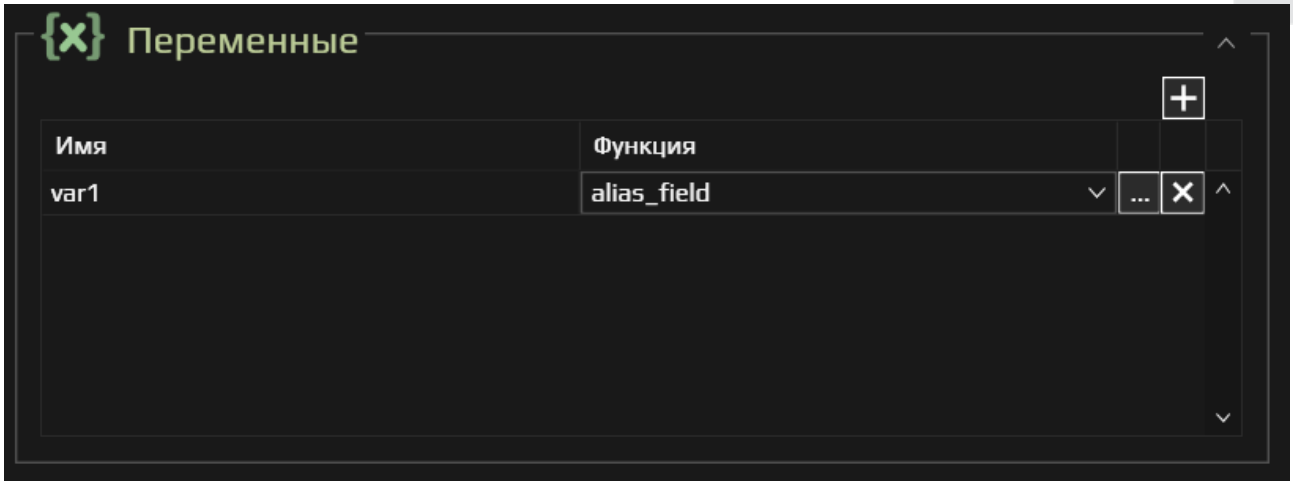


Рисунок 60. Окно добавления Переменных

2. Управление правилами

a. Включение/отключения правил

Для включения/отключения Правил в меню ресурсов необходимо перейти на вкладку «Правила» и выбрать необходимое Правило, после чего выбрать ПМ «Включить/Отключить» (см. Рисунок 61). Включённое правило помечается иконкой , а отключённое – .

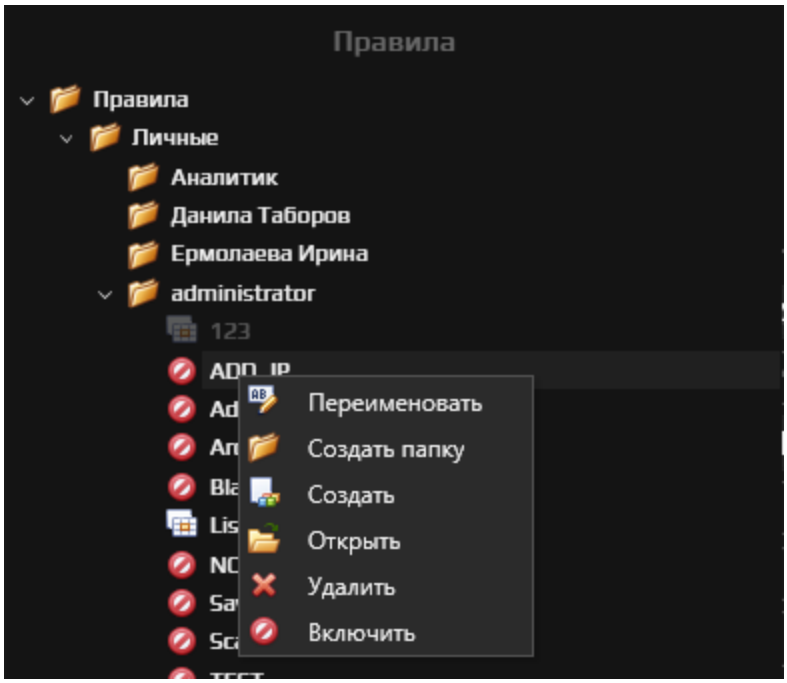


Рисунок 61. Управление Правилами

b. Редактирование Правил

Для удаления Правил в меню ресурсов необходимо перейти на вкладку «Правила» и выбрать необходимое Правило, после чего выбрать ПМ «Открыть» (см. Рисунок 61). В отрывшемся конструкторе следует внести необходимые изменения и сохранить их нажав кнопку «Сохранить».

c. Удаление Правил

Для удаления Правил в меню ресурсов необходимо перейти на вкладку «Правила» и выбрать необходимое Правило, после чего выбрать ПМ «Удалить» (см. Рисунок 61).

ОПИСАНИЕ ПЕРЕМЕННЫХ

1. Арифметические переменные

- **«absolute»**

Описание: данная переменная возвращает абсолютное значение (числовое значение без учёта знака) числового аргумента.

Алгоритм создания

Для создания переменной необходимо нажать на иконку . В открывшемся списке выбрать переменную «absolute» (см. Рисунок 62).

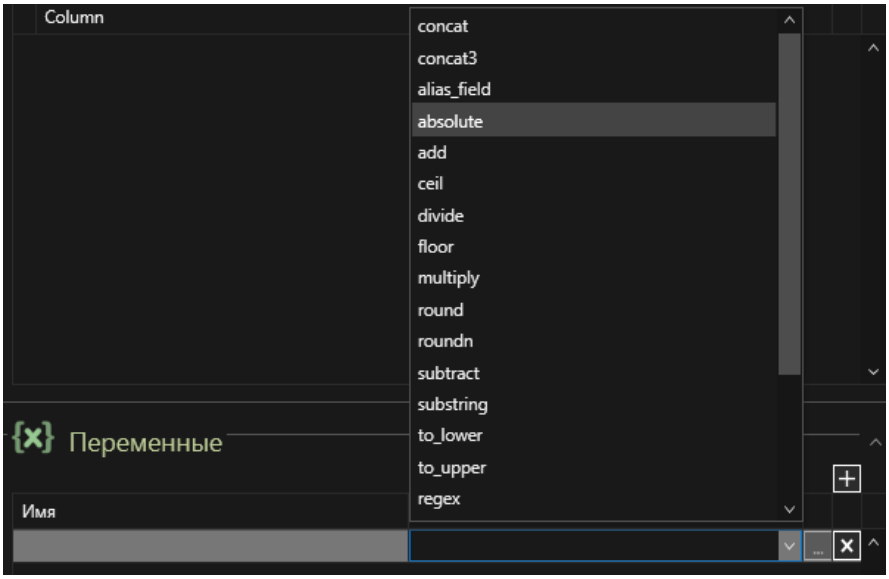


Рисунок 62. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 63) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная absolute имеет только 1 параметр – «Переменная».

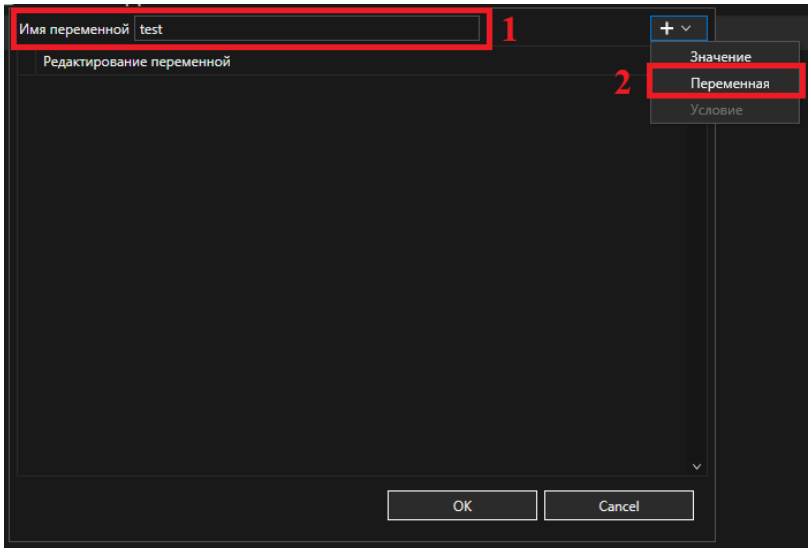


Рисунок 63. Окно параметров переменной

В параметре «Переменная» необходимо выбрать поле события, которому будет возвращаться абсолютное значение (см. Рисунок 64).

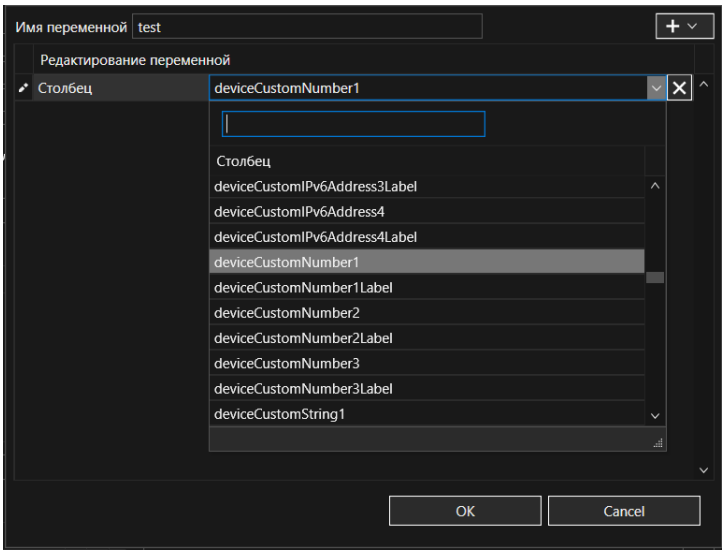


Рисунок 64. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

- **«add»**

Описание: данная переменная возвращает результат сложения двух числовых аргументов.

Алгоритм создания

Для создания переменной необходимо нажать на иконку . В открывшемся списке выбрать переменную «add» (см. Рисунок 65).

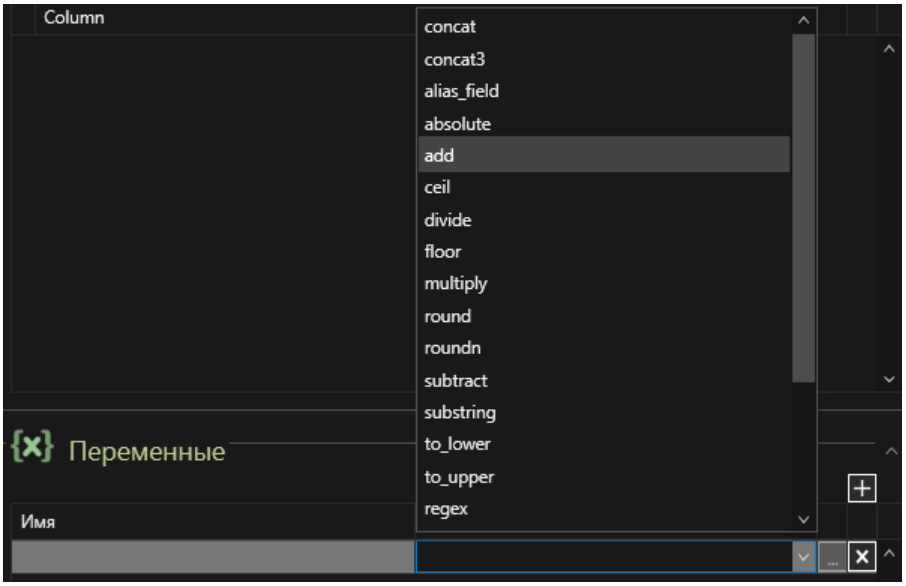


Рисунок 65. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 66) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная add имеет 2 параметра – «Значение» и «Переменная». Параметр «Значение» используется при необходимости использования константы при вычислениях.

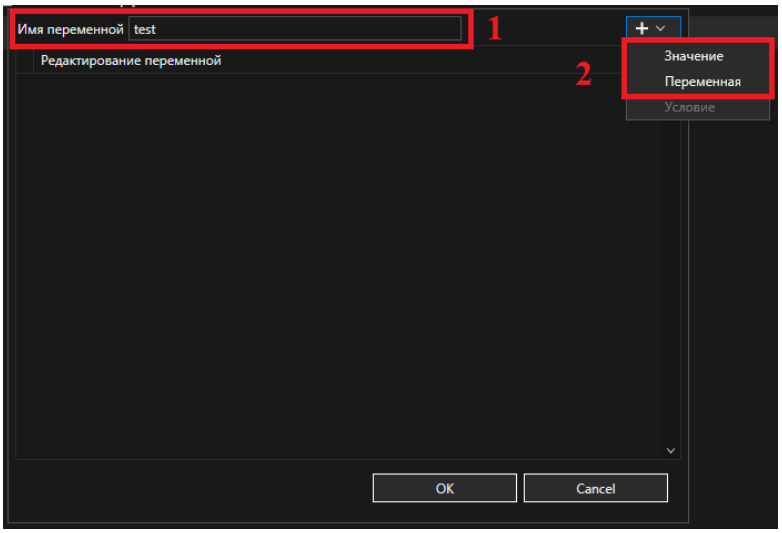


Рисунок 66. Окно создания переменной

В параметре «Значение» можно вести значение константы. Для этого необходимо выбрать тип константы (1) и ввести её значение (2) (см. Рисунок 67).

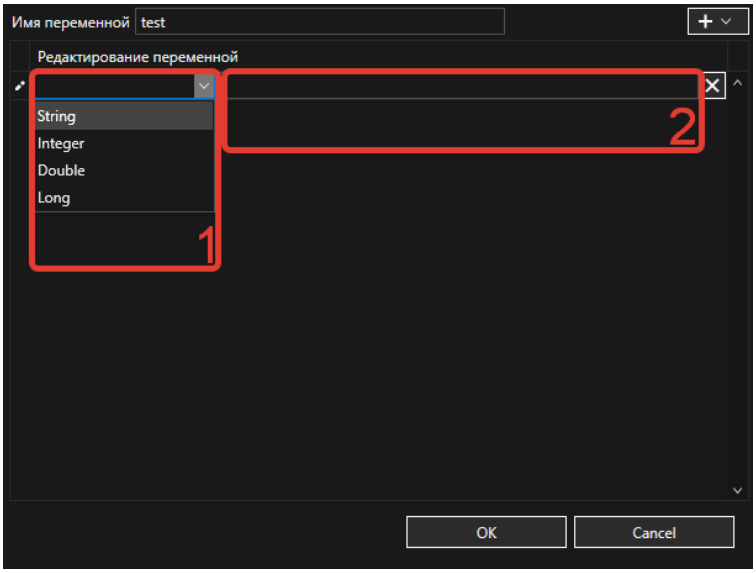


Рисунок 67. Параметр «Значение» переменной

В параметре «Переменная» необходимо выбрать поля события, с которыми необходимо произвести операцию сложения (см. Рисунок 68). Переменная «add» поддерживает сложение только 2-х слагаемых.

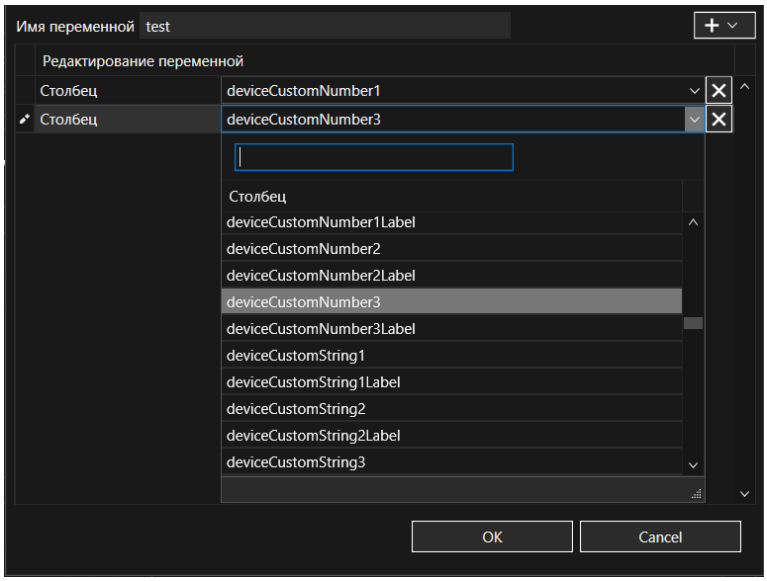


Рисунок 68. Параметр «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

- **«ceil»**

Описание: данная переменная возвращает наименьшее целочисленное значение, которое не меньше заданного аргумента.

Алгоритм создания

Для того чтобы создать данную переменную необходимо нажать на иконку . В открывшемся списке выбрать переменную «ceil» (см. Рисунок 69).

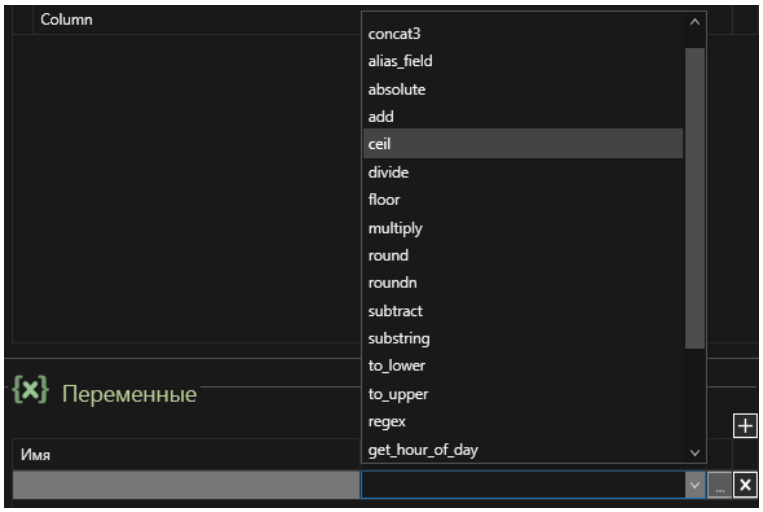


Рисунок 69. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 70) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «cell» имеет только 1 параметр – «Переменная».

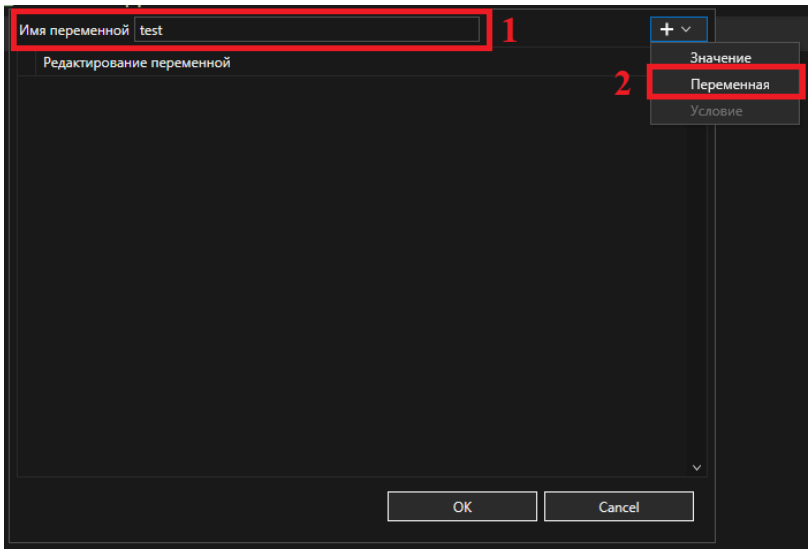


Рисунок 70. Окно создания переменной

В параметре «Переменная» необходимо выбрать поле события, которому будет возвращаться наименьшее целочисленное значение (см. Рисунок 71).

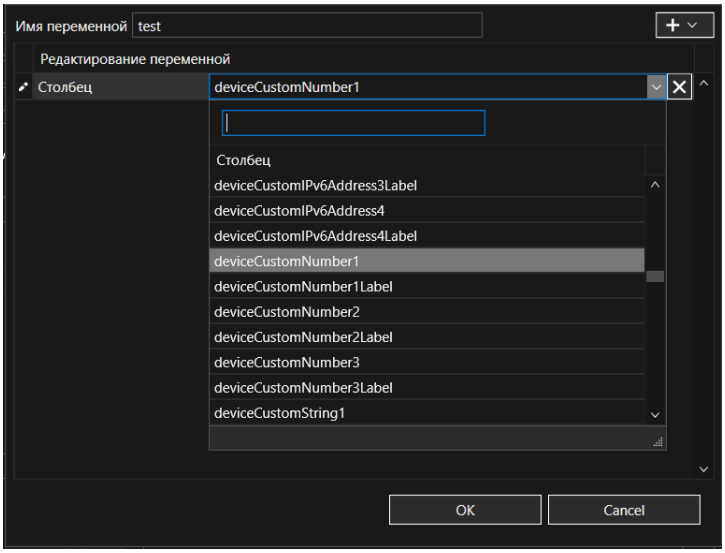


Рисунок 71. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

- **«divide»**

Описание: Данная переменная возвращает результат деления первого числового аргумента на второй числовой аргумент. Первый аргумент может принимать любые значения, а второй не может быть равен 0.

Алгоритм создания

Для того чтобы создать данную переменную необходимо нажать на иконку . В открывшемся списке выбираем переменную «divide» (см. Рисунок 72).

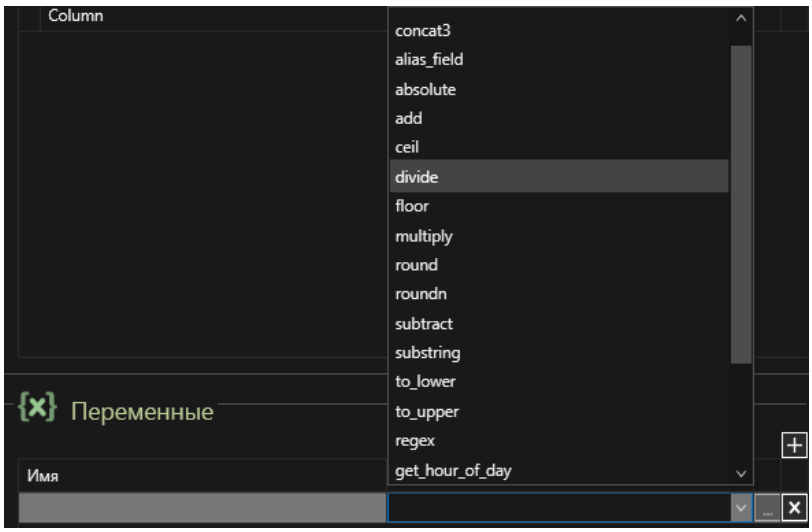


Рисунок 72. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 73) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «divide» имеет 2 параметра – «Значение» и «Переменная». Параметр «Значение» используется при необходимости использования константы при вычислениях.

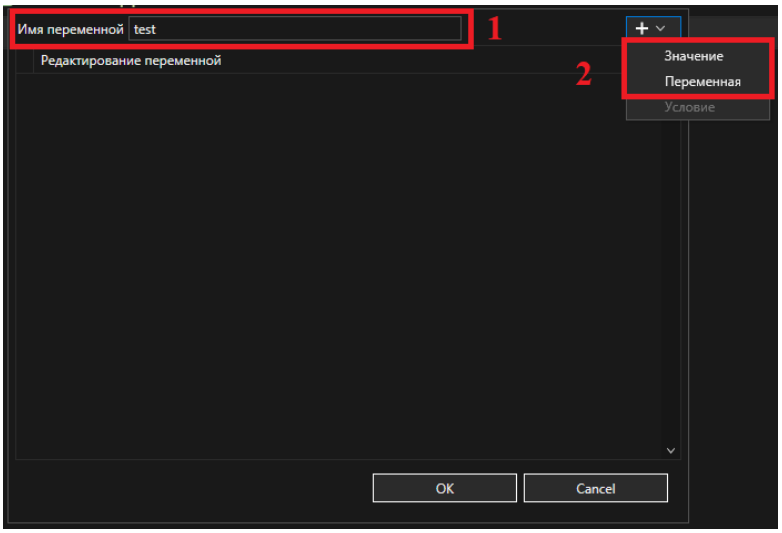


Рисунок 73. Окно создания переменной

В параметре «Значение» можно вести значение константы. Для этого необходимо выбрать тип константы (1) и ввести её значение (2) (см. Рисунок 74).

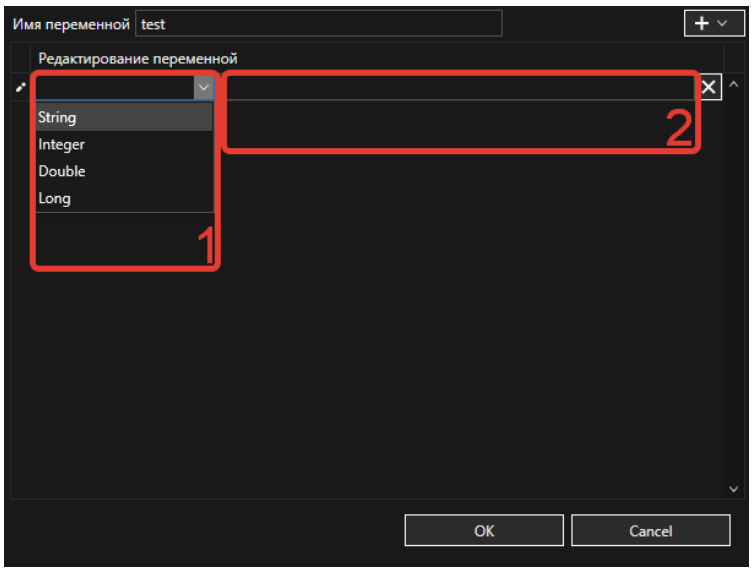


Рисунок 74. «Значение» переменной

В параметре «Переменная» необходимо выбрать поля события, с которыми необходимо произвести операцию сложения (см. Рисунок 75). Переменная «divide» поддерживает деление только 2-х аргументов.

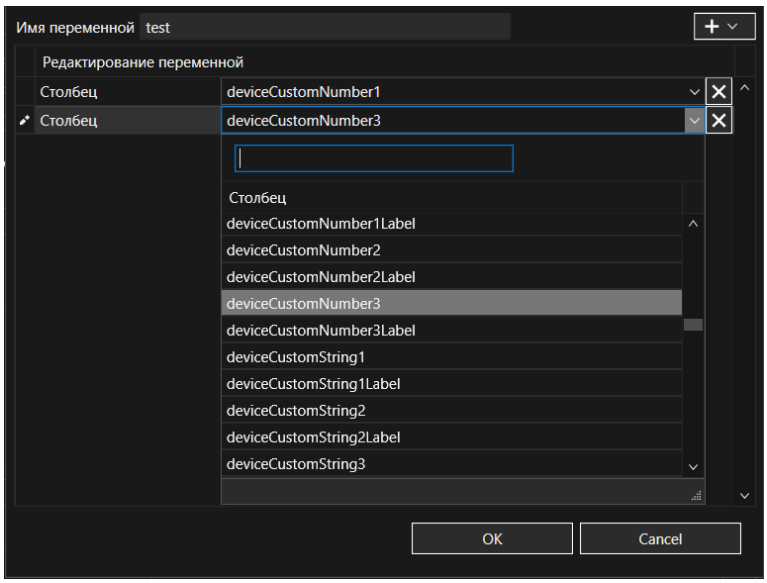


Рисунок 75. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

- **«floor»**

Описание: данная переменная возвращает наибольшее целочисленное значение, не превышающее числовой аргумент.

Алгоритм создания

Для того чтобы создать данную переменную необходимо нажать на иконку . В открывшемся списке выбирать переменную «floor» (см. Рисунок 76).

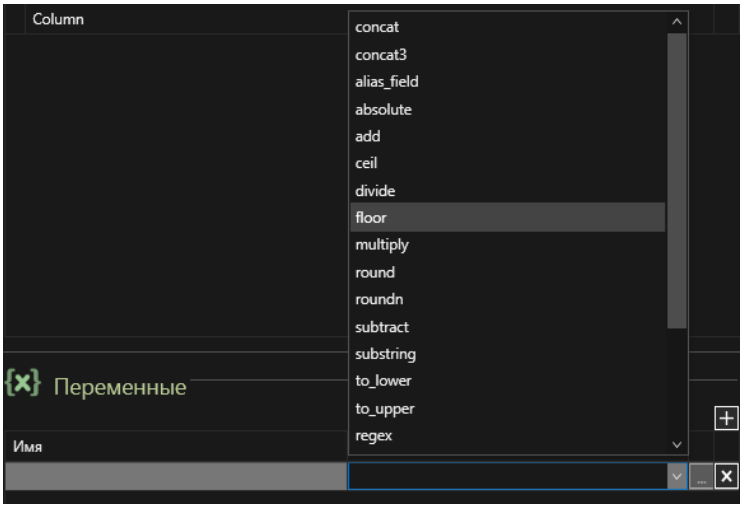


Рисунок 76. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 77) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «floor» имеет только 1 параметр – «Переменная».

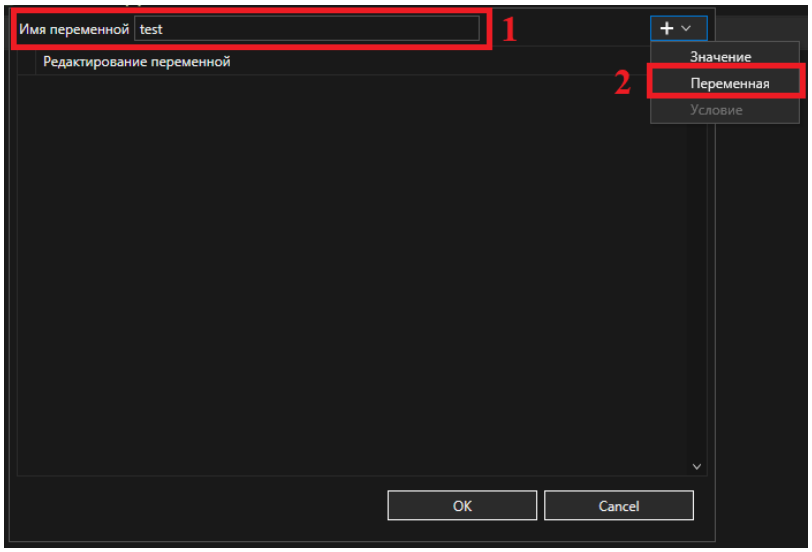


Рисунок 77. Окно создания переменной

В параметре «Переменная» необходимо выбрать поле события, которому будет возвращаться наибольшее целочисленное значение (см. Рисунок 78).

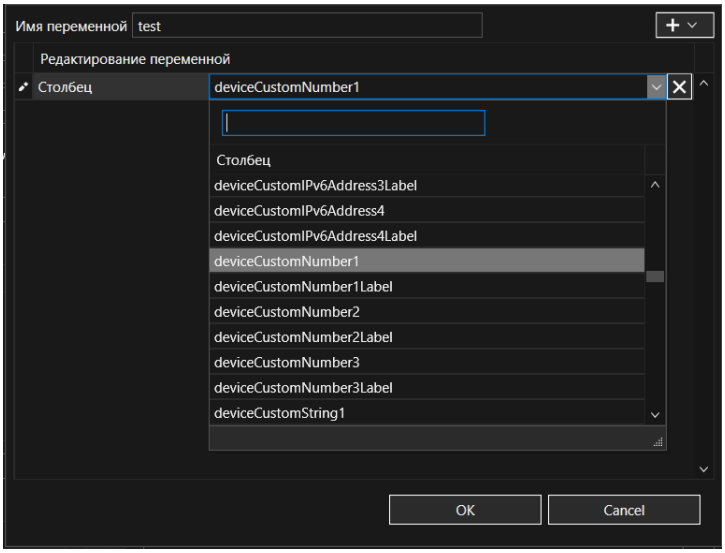


Рисунок 78. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

- **«multiply»**

Описание: данная переменная возвращает произведение двух числовых аргументов.

Алгоритм создания

Для того чтобы создать данную переменную необходимо нажать на иконку . В открывшемся списке выбираем переменную «multiply» (см. Рисунок 79).

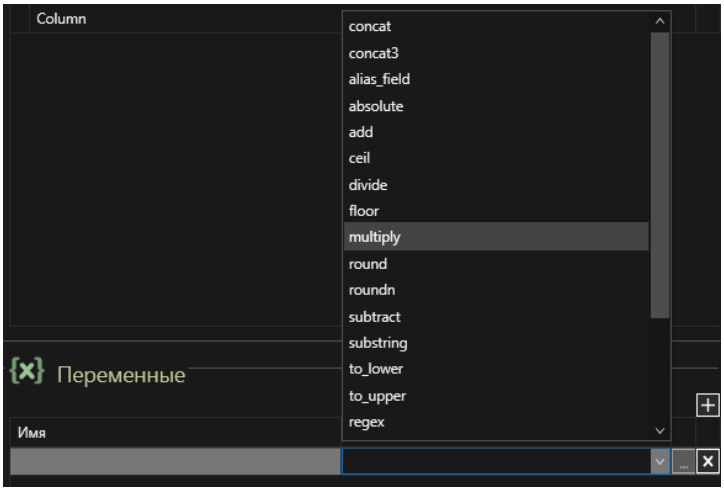


Рисунок 79. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 80) необходимо задать имя переменной (1) и её параметры (2)

(кнопка). Переменная «multiply» имеет 2 параметра – «Значение» и «Переменная». Параметр «Значение» используется при необходимости использования константы при вычислениях.

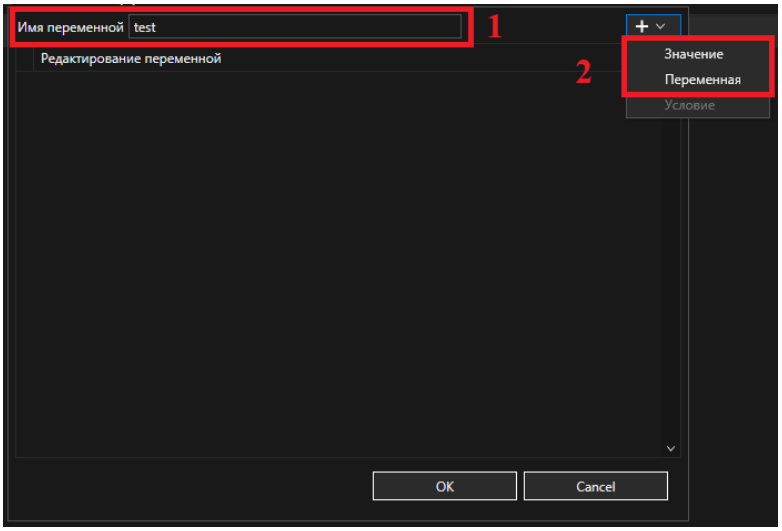


Рисунок 80. Окно создания переменной

В параметре «Значение» можно вести значение константы. Для этого необходимо выбрать тип константы (1) и ввести её значение (2) (см. Рисунок 81).

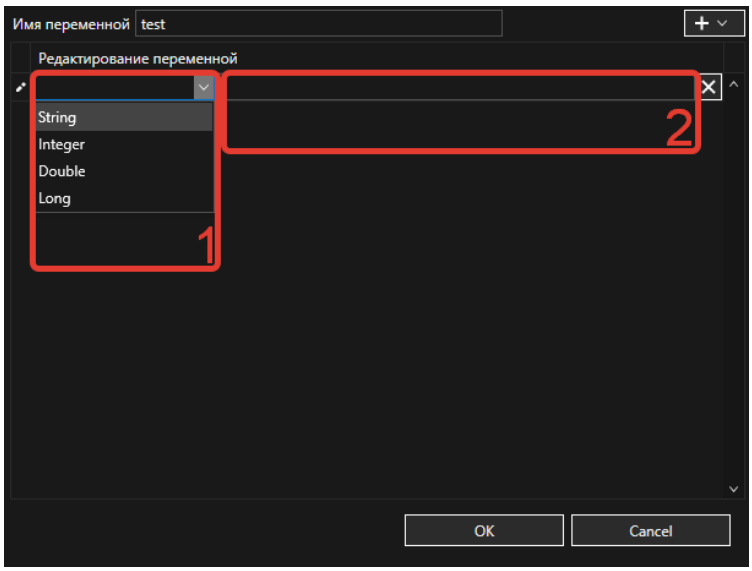


Рисунок 81. «Значение» переменной

В параметре «Переменная» необходимо выбрать поля события, с которыми необходимо произвести операцию сложения (см. Рисунок 82). Переменная «multiply» поддерживает умножение только 2-х аргументов.

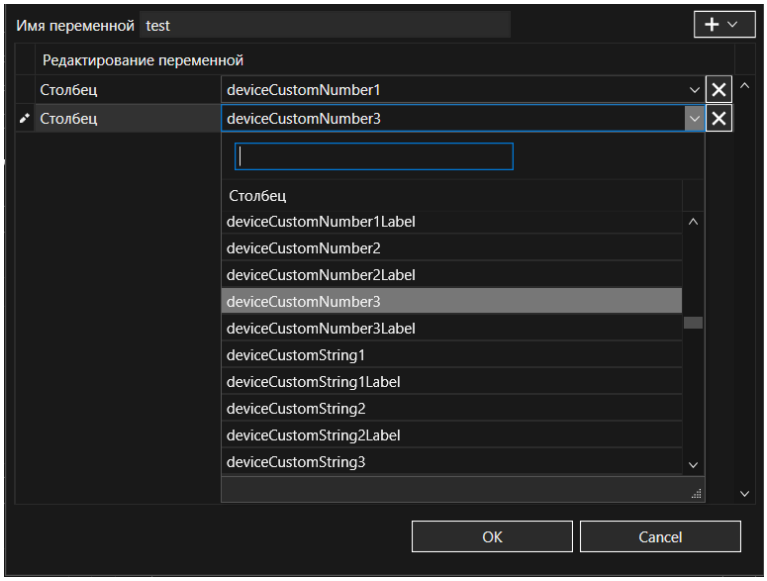


Рисунок 82. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

- **«round»**

Описание: данная переменная возвращает ближайшее целое число к числовому аргументу.

Алгоритм создания

Для того чтобы создать данную переменную необходимо нажать на иконку . В открывшемся списке выбираем переменную «round» (см. Рисунок 83).

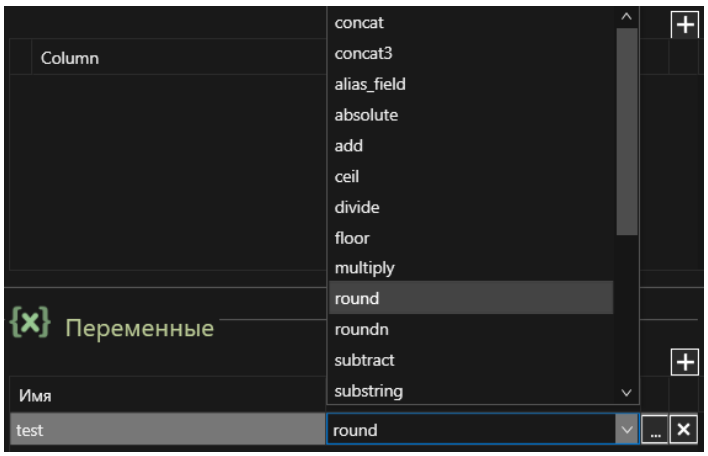


Рисунок 83. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 84) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «round» имеет только 1 параметр – «Переменная».

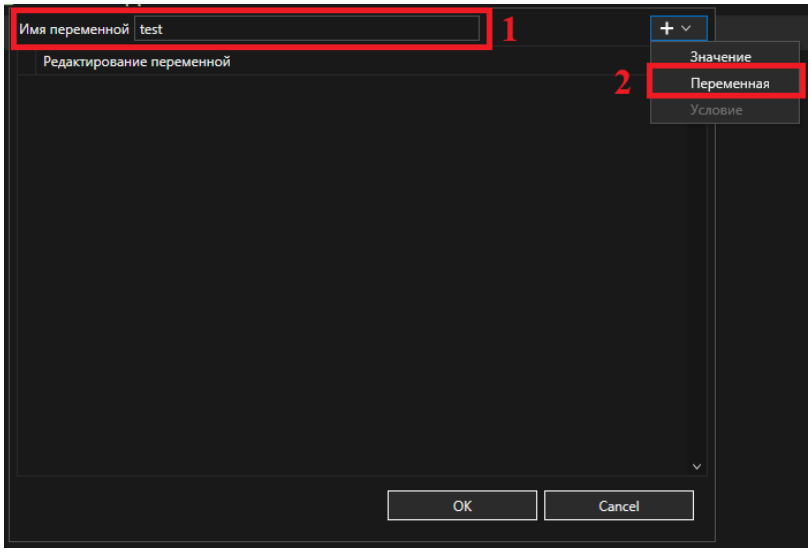


Рисунок 84. Окно создания переменной

В параметре «Переменная» необходимо выбрать поле события, которому будет возвращаться ближайшее целое число (см. Рисунок 85).

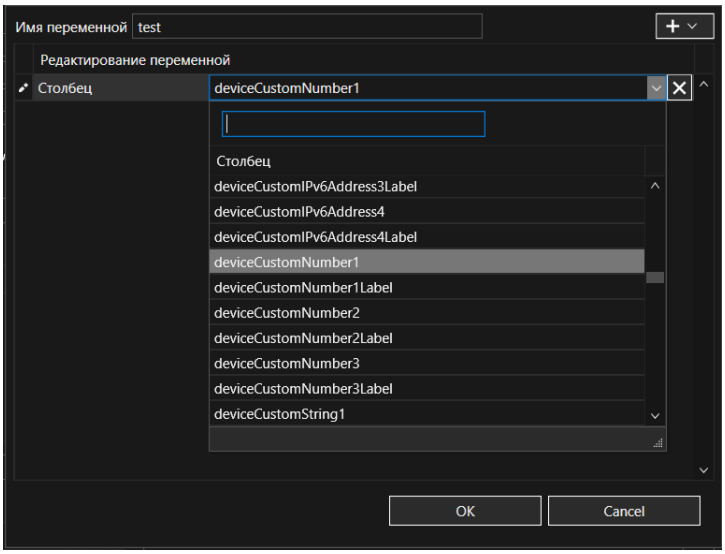


Рисунок 85. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

- **«roundn»**

Описание: данная переменная возвращает результат округления с точностью до указанного знака после запятой.

Алгоритм создания

Для того чтобы создать данную переменную необходимо нажать на иконку . В открывшемся списке выбираем переменную «roundn» (см. Рисунок 86).

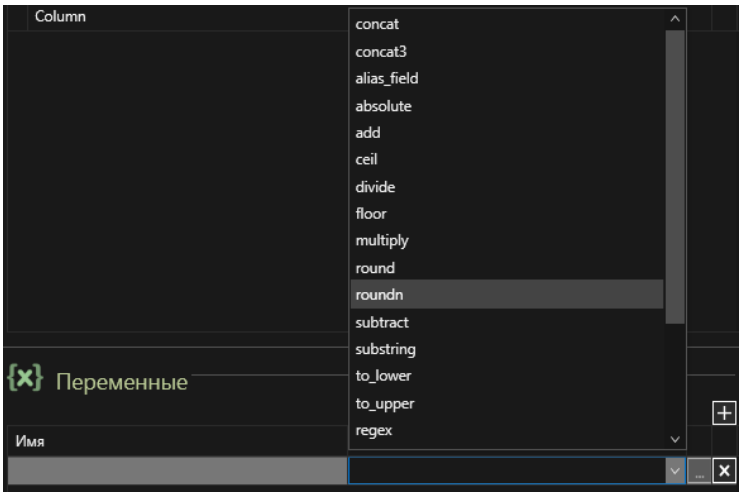


Рисунок 86. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 87) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «roundn» имеет 2 параметра – «Значение» и «Переменная». Параметр «Значение» используется для указания желаемой точности округления.

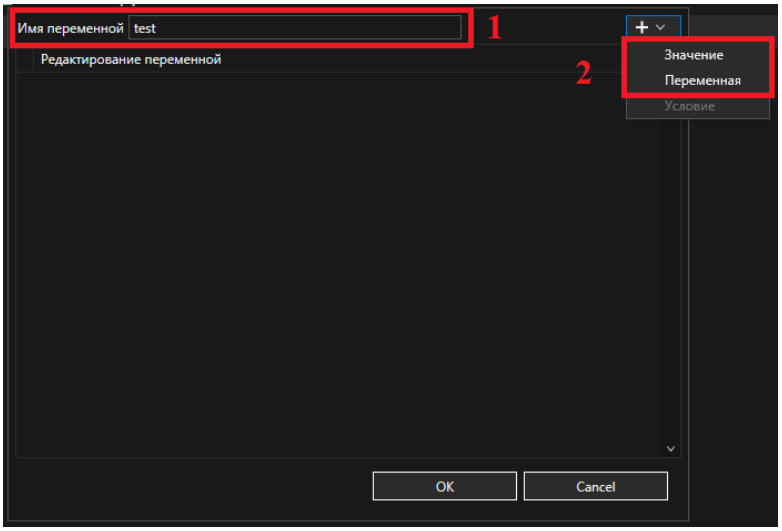


Рисунок 87. Окно создания переменной

В параметре «Значение» следует ввести значение константы. Для этого необходимо выбрать тип константы (1) и ввести её значение (2) (см. Рисунок 81). (см. Рисунок 88).

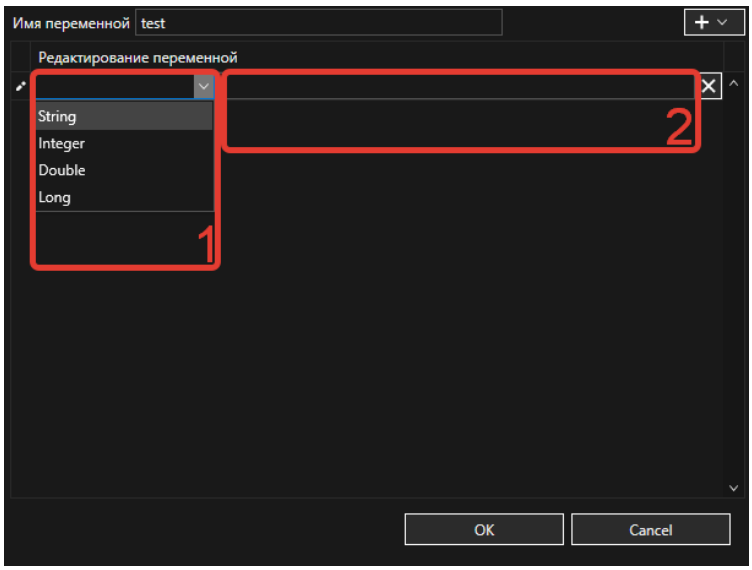


Рисунок 88. «Значение» переменной

В параметре «Переменная» необходимо выбрать поле события, с которым необходимо произвести округление (см. Рисунок 89).

ОТСУТСТВУЕТ (В консоле не верно реализовано)

Рисунок 89. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

- **«subtract»**

Описание: данная переменная возвращает результат вычитания второго числового аргумента из первого числового аргумента.

Алгоритм создания

Для того чтобы создать данную переменную необходимо нажать на иконку . В открывшемся списке выбираем переменную «subtract» (см. Рисунок 90).

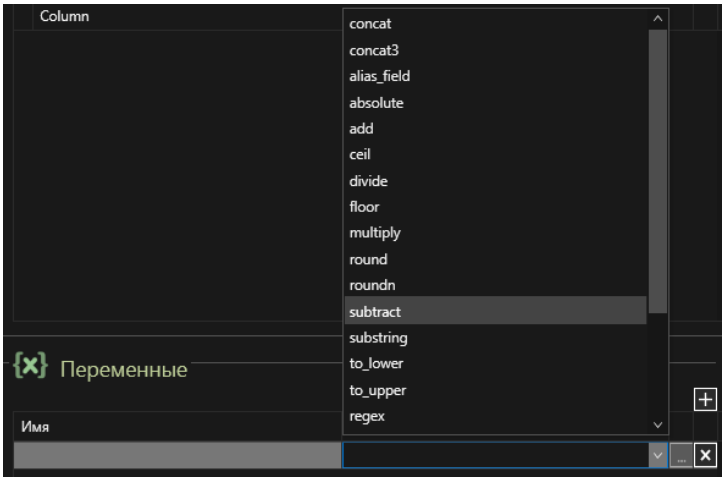


Рисунок 90. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 91) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «subtract» имеет 2 параметра – «Значение» и «Переменная». Параметр «Значение» используется при необходимости использования константы при вычислениях.

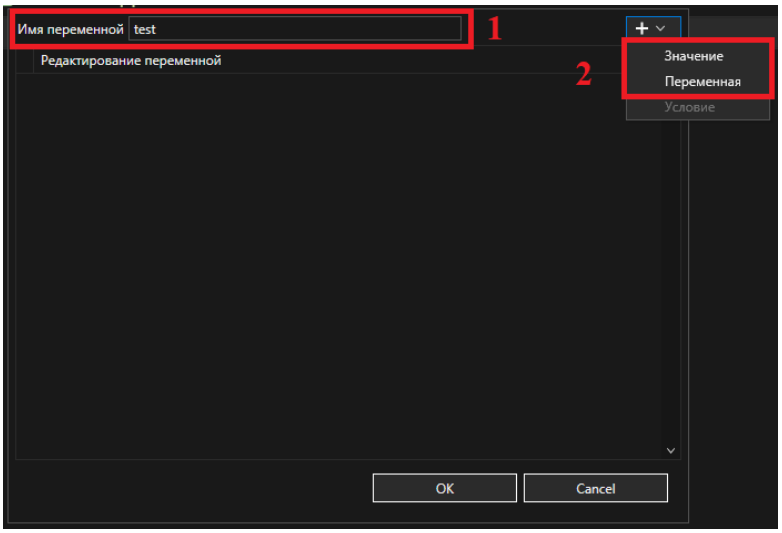


Рисунок 91. Окно создания переменной

В параметре «Значение» можно вести значение константы. Для этого необходимо выбрать тип константы (1) и ввести её значение (2) (см. Рисунок 92).

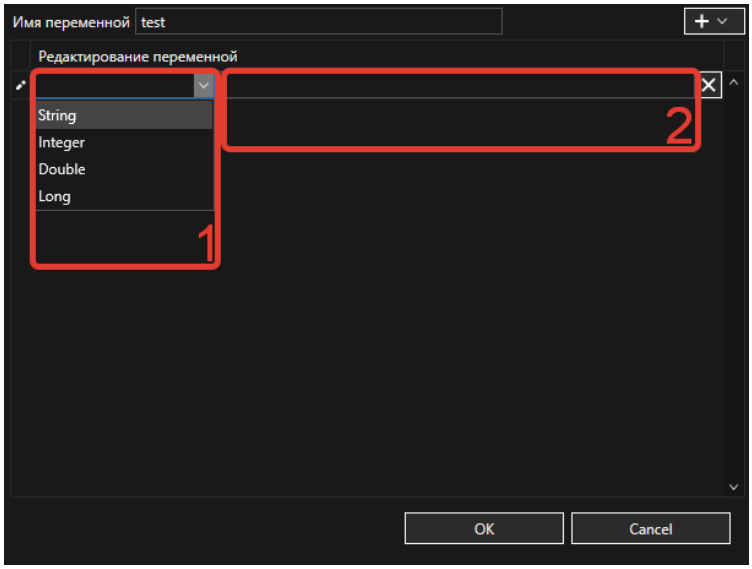


Рисунок 92. «Значение» переменной

В параметре «Переменная» необходимо выбрать поля события, с которыми необходимо произвести операцию сложения (см. Рисунок 93). Переменная «subtract» поддерживает вычитание только 2-х аргументов.

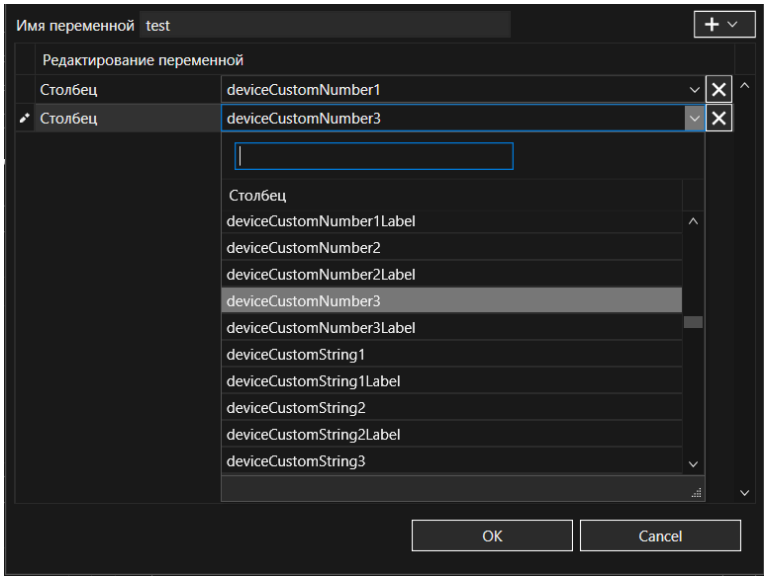


Рисунок 93. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

2. Переменные для работы с активными листами

- **«get_activelist_value»**

Описание: данная переменная возвращает значение, связанное с определённым полем указанного активного списка.

Алгоритм создания

Для создания переменной необходимо нажать на иконку . В открывшемся списке выбрать переменную «get_activelist_value» (см. Рисунок 94).

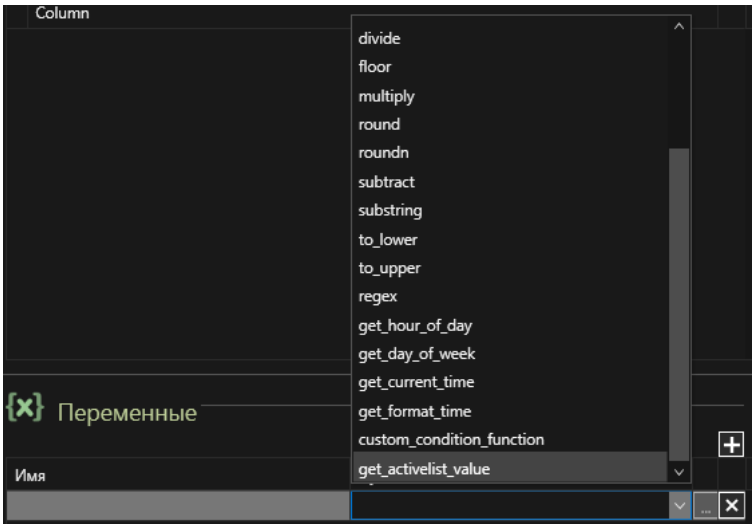


Рисунок 94. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 95) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «get_activelist_value» имеет только один параметр «Активный лист».

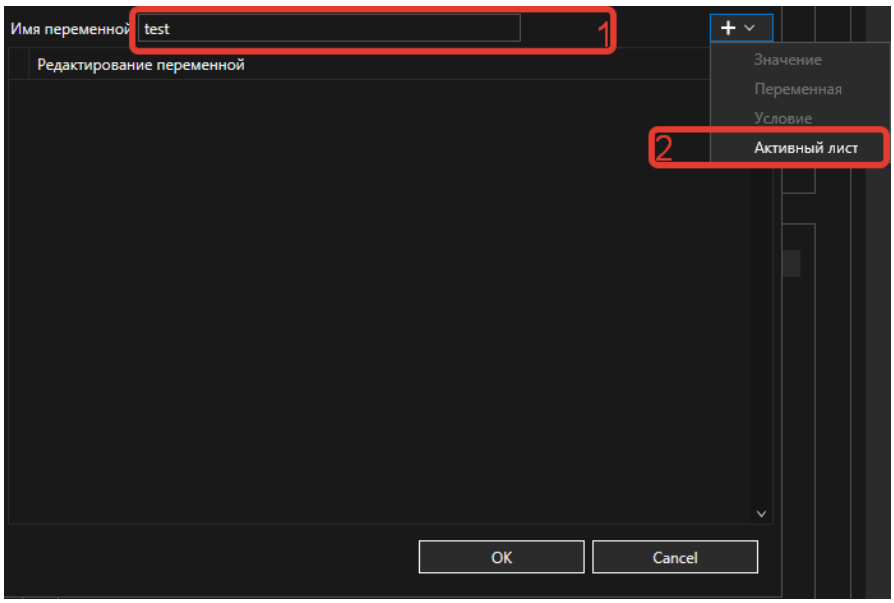


Рисунок 95. Окно создания переменной

В параметре «Активный лист» в выпадающем списке следует выбрать Активный лист, поля которого необходимо использовать в переменной (см. Рисунок 96). Активный лист должен быть заранее создан в системе.

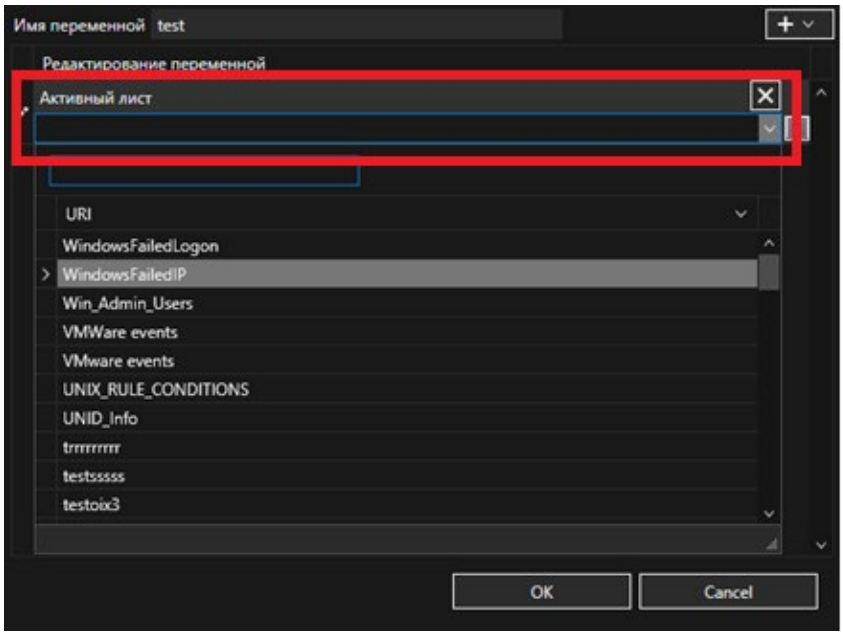


Рисунок 96. Окно «Активный лист»

В выбранном активном листе необходимо обеспечить привязку события. Следует определить поля привязки активного листа с полями базового события (см. Рисунок 97).

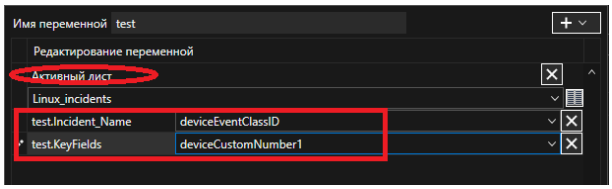


Рисунок 97. Поля активного листа

Поля, предлагаемые по умолчанию необходимо заменить на те, с которыми будет реализовываться сравнение (см. Рисунок 98).

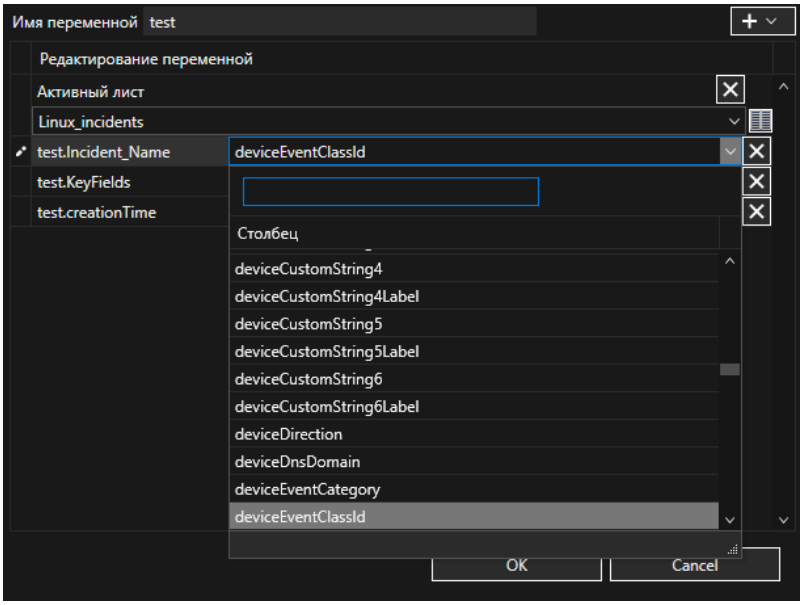


Рисунок 98. Сопоставление полей события и активного листа

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

После сохранения переменной «get_activelist_value», каждое из полей будет доступно при написании условий (см. Рисунок 99).

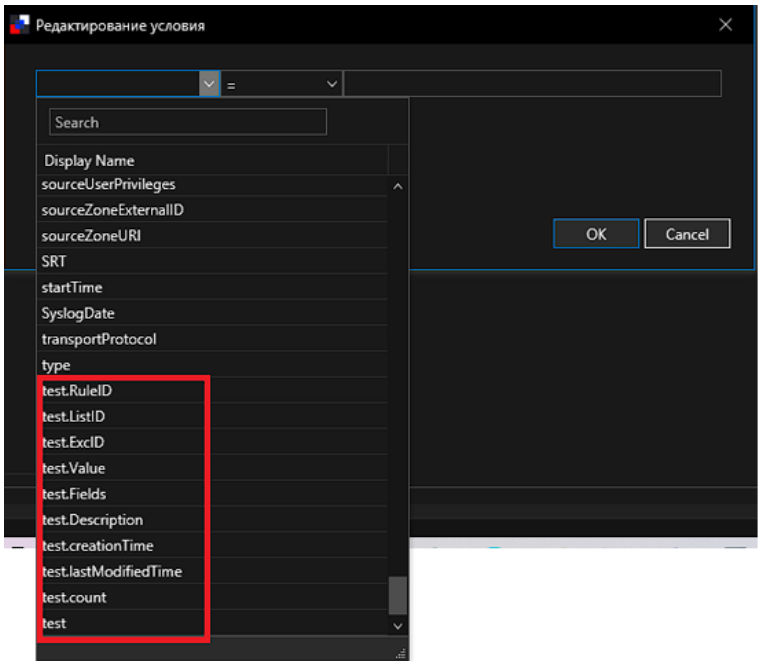


Рисунок 99. Доступные поля активного листа

3. Строковые переменные

- **«concat»**

Описание: данная переменная возвращает результат объединения двух строковых аргументов.

Алгоритм создания

Для создания переменной необходимо нажать на иконку . В открывшемся списке выбрать переменную «concat» (см. Рисунок 100).

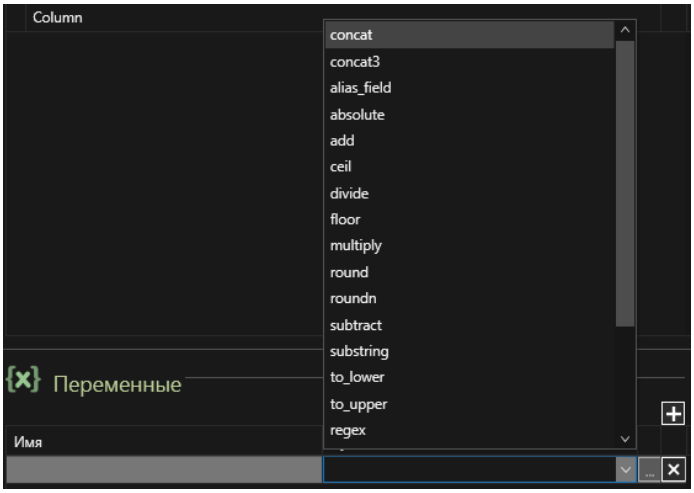


Рисунок 100. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 101) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «concat» имеет 1 параметр – «Переменная».

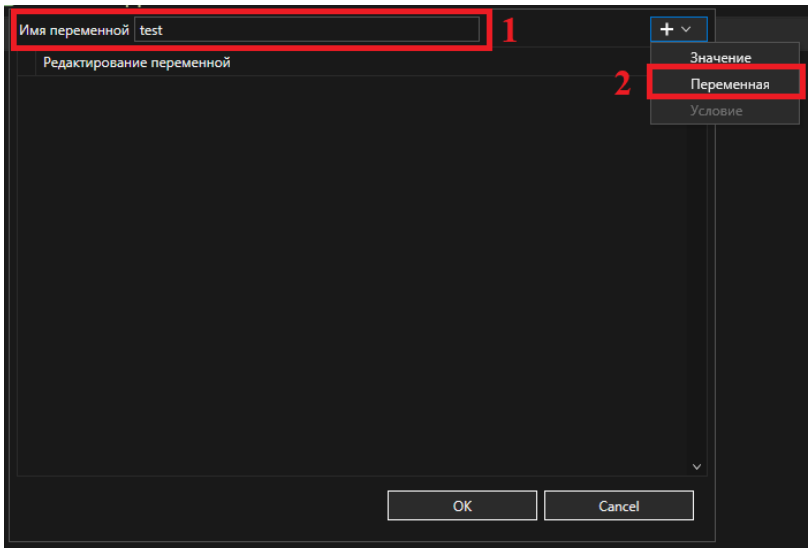


Рисунок 101. Окно создания переменной

В параметре «Переменная» необходимо выбрать поля события, с которыми необходимо произвести операцию объединения строковых выражений (см. Рисунок 102). Переменная «concat» поддерживает объединение только 2-х строковых выражений.

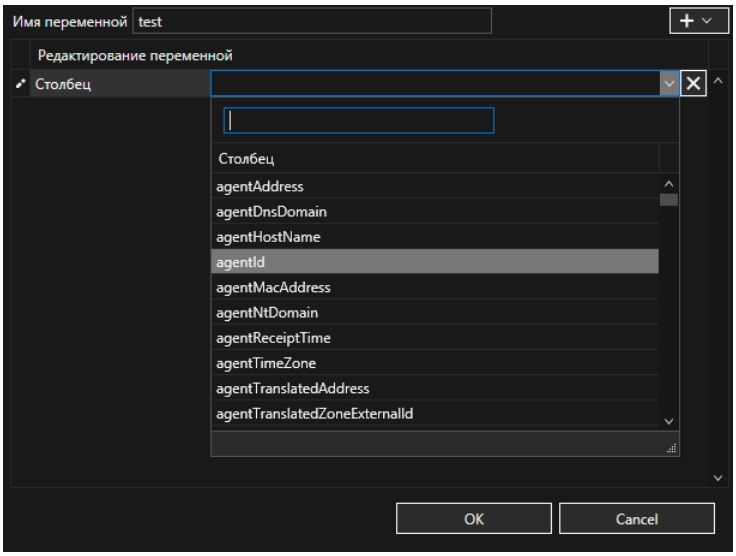


Рисунок 102. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

Если строковые выражения имеют начальные или конечные пробелы, при их объединении пробелы удаляются, даже если предварительный просмотр во время определения функции или экспорта в XML отображает пробел. Если необходимо использовать пробел, то следует воспользоваться переменной concat3.

- **«concat3»**

Описание: данная переменная возвращает результат объединения трех строковых аргументов.

Алгоритм создания

Для создания переменной необходимо нажать на иконку ⊞. В открывшемся списке выбрать переменную «concat3» (см. Рисунок 103).

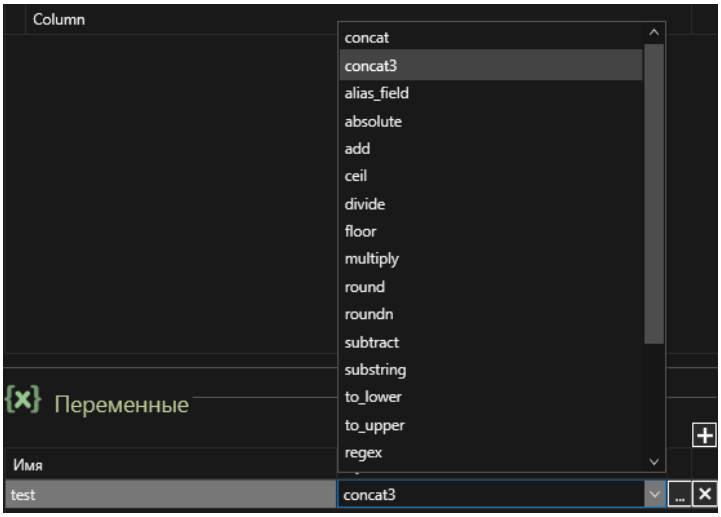


Рисунок 103. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 104) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «concat3» имеет 1 параметр – «Переменная».

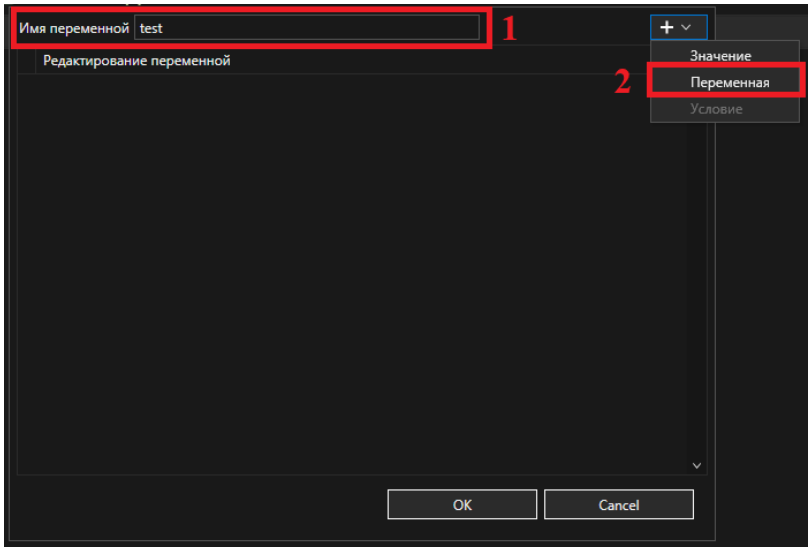


Рисунок 104. Окно создания переменной

В параметре «Переменная» необходимо выбрать поля события, с которыми необходимо произвести операцию объединения строковых выражений (см. Рисунок 105). Переменная «concat3» поддерживает объединение только 3-х строковых выражений.

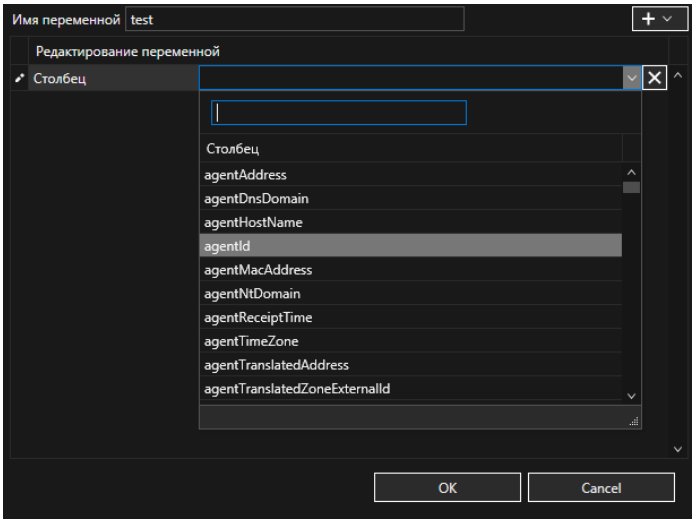


Рисунок 105. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

- **«substring»**

Описание: данная переменная 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.

Алгоритм создания

Для создания переменной необходимо нажать на иконку ⊞. В открывшемся списке выбрать переменную «substring» (см. Рисунок 106).

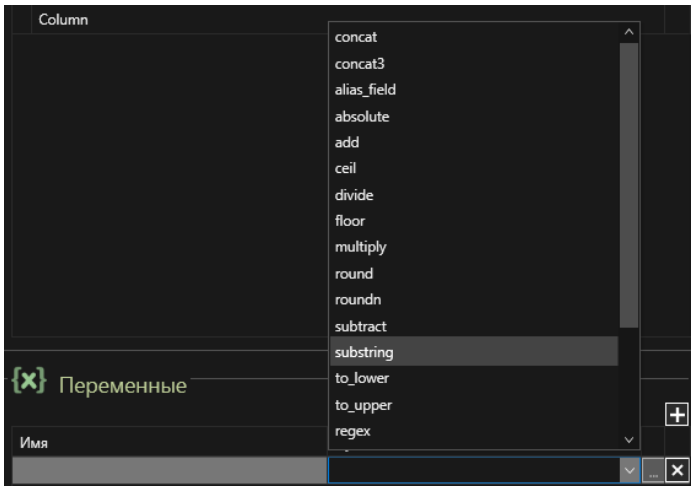


Рисунок 106. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 107) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «substring» имеет 2 параметра – «Значение» и «Переменная». Параметр «Значение» используется для указания числовых аргументов (индекс начала и количество символов).

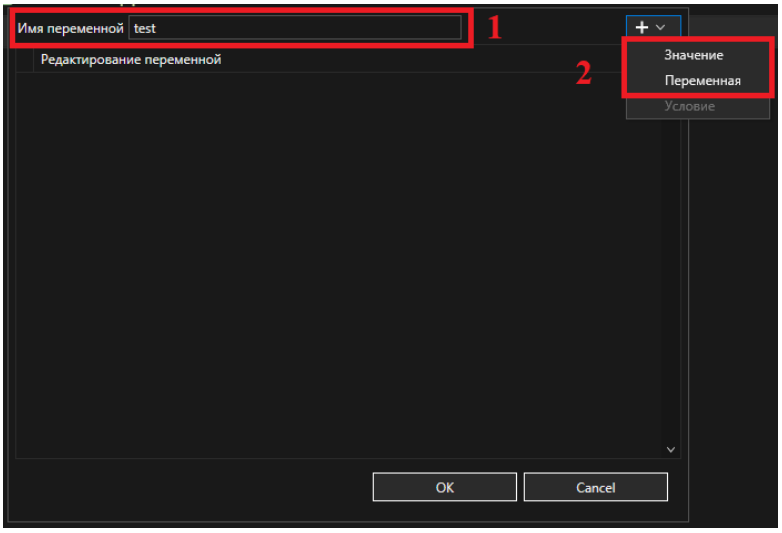


Рисунок 107. Окно создания переменной

В параметре «Переменная» в поле «Столбец» необходимо выбрать поле события, из которого необходимо «вырезать» часть строкового аргумента.

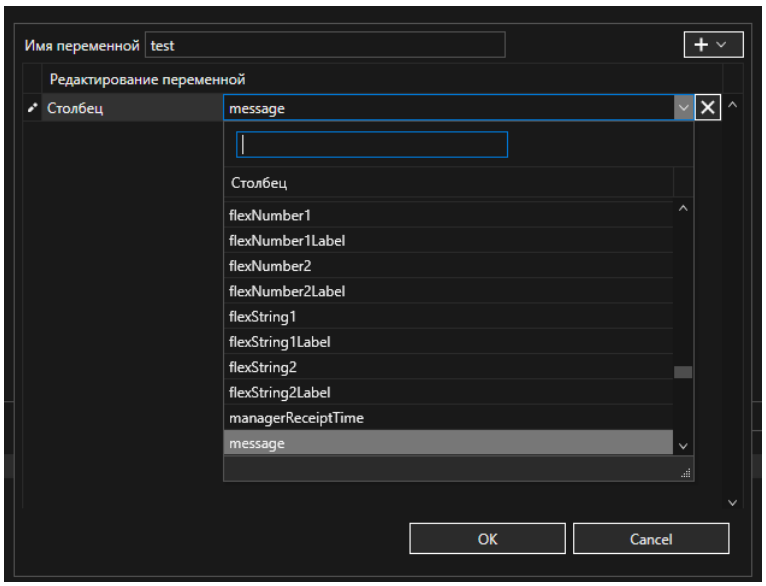


Рисунок 108. Окно добавления параметра "Переменная"

В параметре «Значение» следует вести значение числовых аргументов (индекс начала и количество символов). Для этого необходимо выбрать тип константы (1) «Integer» и ввести её значение (2) (см. Рисунок 109).

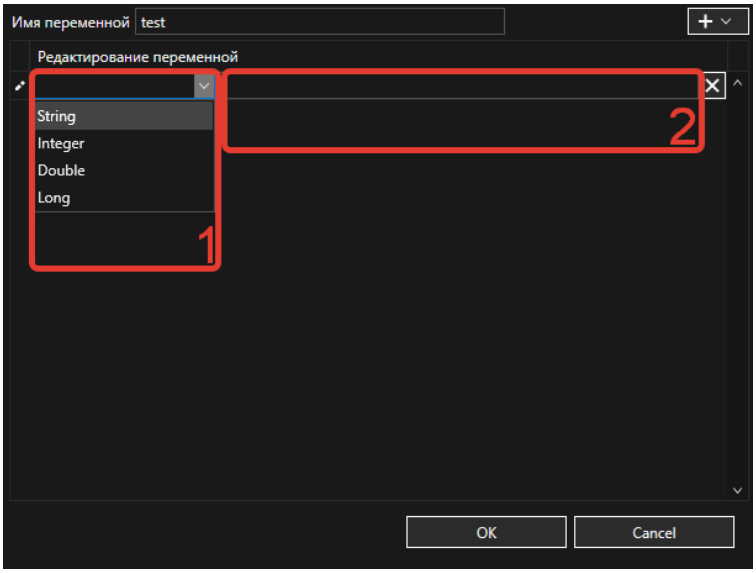


Рисунок 109. Параметр «Значение» переменной

Пример корректно заполненной переменной (см. Рисунок 110).

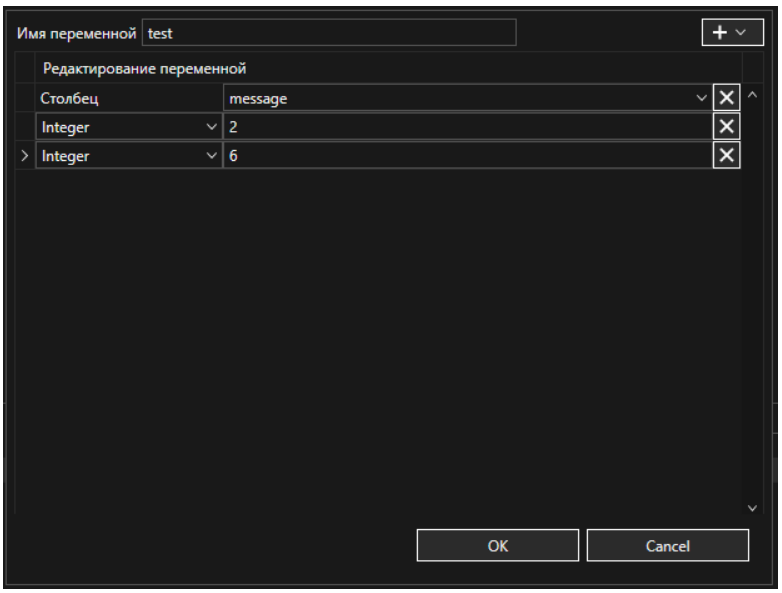


Рисунок 110. Аргументы переменной «substring»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

- **«to lower»**

Описание: данная переменная возвращает строковый аргумент, преобразованный в нижний регистр.

Алгоритм создания

Для создания переменной необходимо нажать на иконку . В открывшемся списке выбрать переменную «to lower» (см.Рисунок 111).

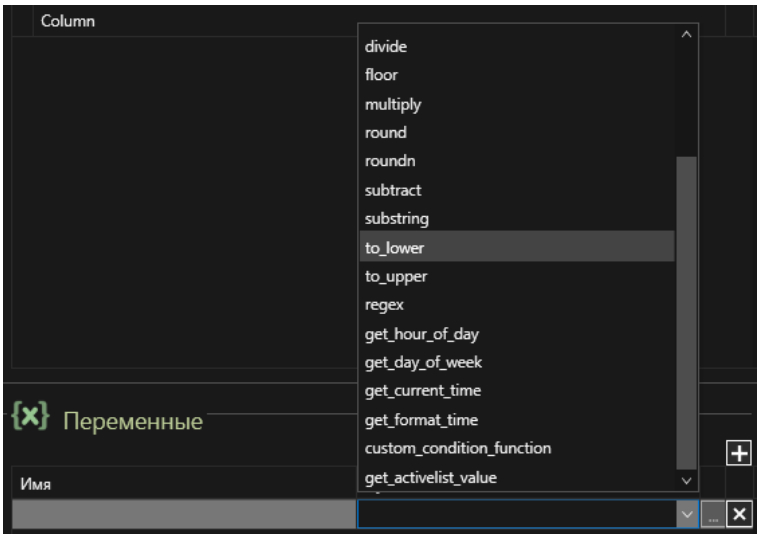


Рисунок 111. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 63) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «to lower» имеет только 1 параметр – «Переменная».

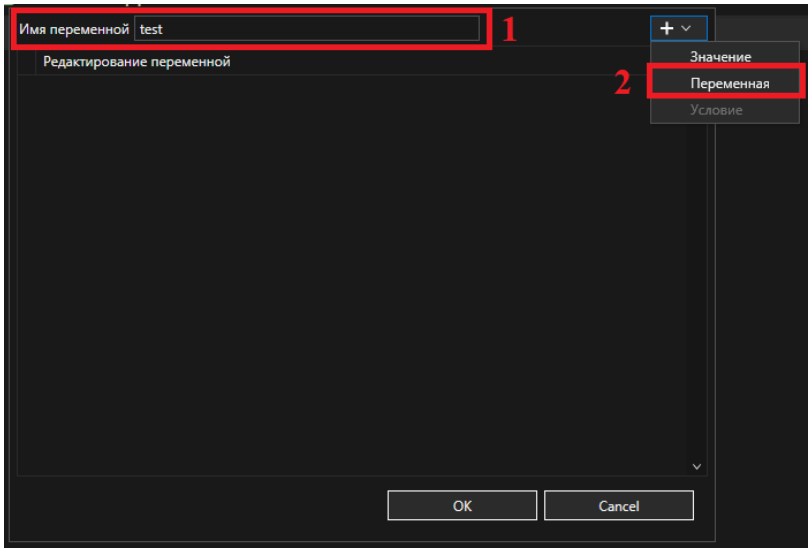


Рисунок 112. Окно создания переменной

В параметре «Переменная» необходимо выбрать поле события, которое будет преобразовано в нижний регистр (см. Рисунок 113).

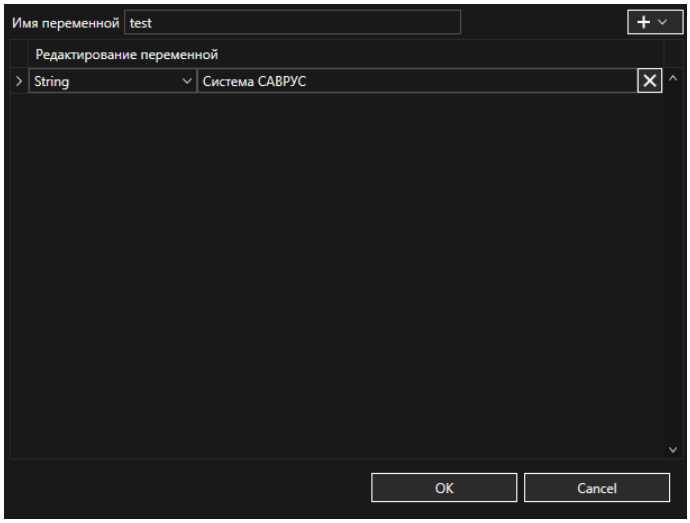


Рисунок 113. Окно «Переменная»

Например, возьмём to_lower («Система САВРУС»). Результатом будет («система саврус»). Цифры и другие неалфавитные символы не затрагиваются.

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

- **«to_upper»**

Описание: данная переменная возвращает строковый аргумент, преобразованный в верхний регистр.

Алгоритм создания

Для создания переменной необходимо нажать на иконку ⊞. В открывшемся списке выбрать переменную «to upper» (см. Рисунок 114).

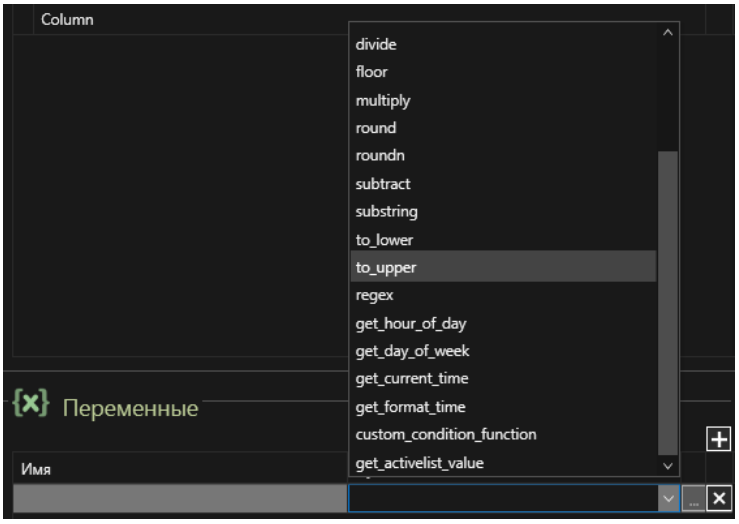


Рисунок 114. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 115) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «to upper» имеет только 1 параметр – «Переменная».

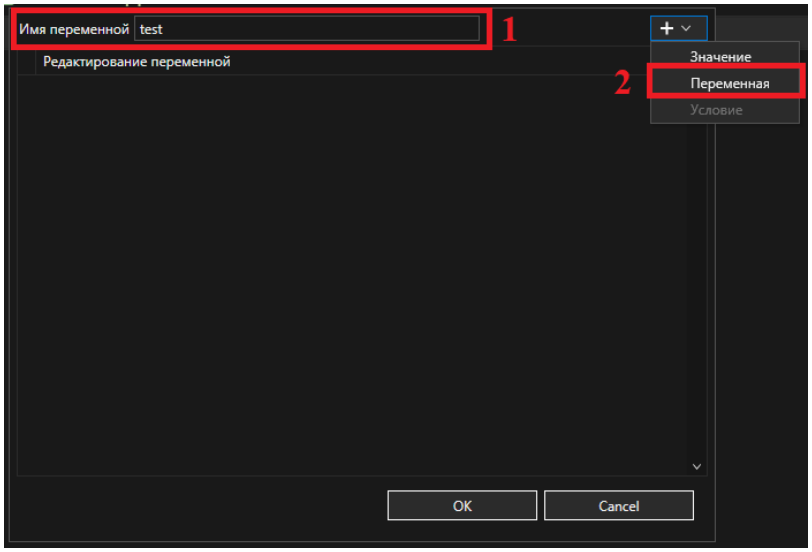


Рисунок 115. Окно создания переменной

В параметре «Переменная» необходимо выбрать поле события, которое будет преобразовано в верхний регистр (см. Рисунок 116).

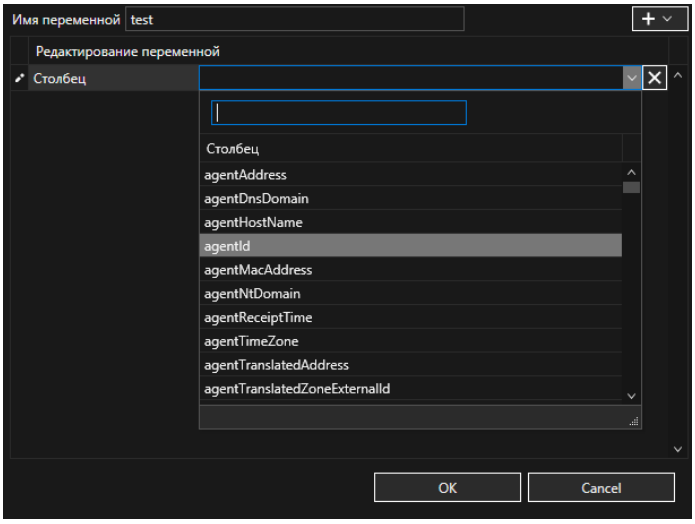


Рисунок 116. Окно «Переменная»

Например, to_upper ("Система САВРУС ") возвращает "СИСТЕМА САВРУС". Цифры и другие неалфавитные символы не затрагиваются.

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

4. Переменная alias

- **«alias_field»**

Описание: данная переменная создаёт альтернативное имя для указанного поля.

Алгоритм создания

Для создания переменной необходимо нажать на иконку ⊞. В открывшемся списке выбрать переменную «alias_field» (см. Рисунок 117).

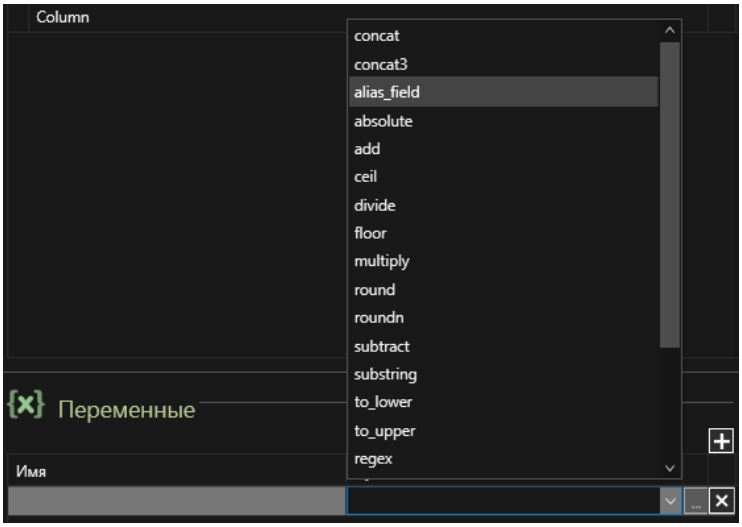


Рисунок 117. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 118) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «alias_field» имеет только 1 параметр – «Переменная».

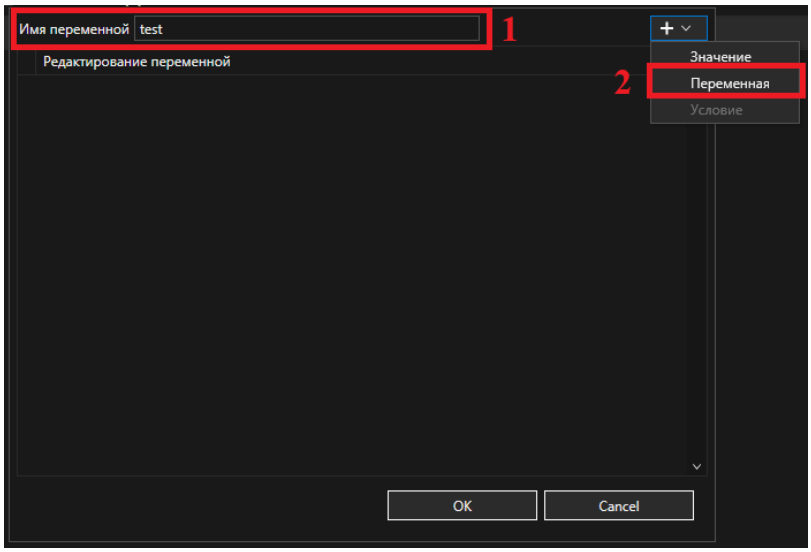


Рисунок 118. Окно создания переменной

В параметре «Переменная» необходимо выбрать поле события, которому будет назначено альтернативное наименование (см. Рисунок 119).

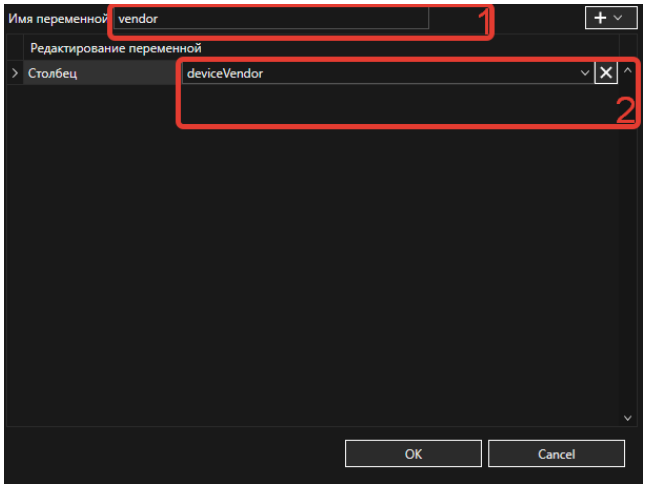


Рисунок 119. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

5. Переменные для работы с датой и временем

- **«get_hour_of_day»**

Описание: данная переменная возвращает целое число от 0 до 23 для представления часа дня на основе выбранной метки времени.

Алгоритм создания

Для создания переменной необходимо нажать на иконку ⊞. В открывшемся списке выбрать переменную «get_hour_of_day» (см. Рисунок 120).

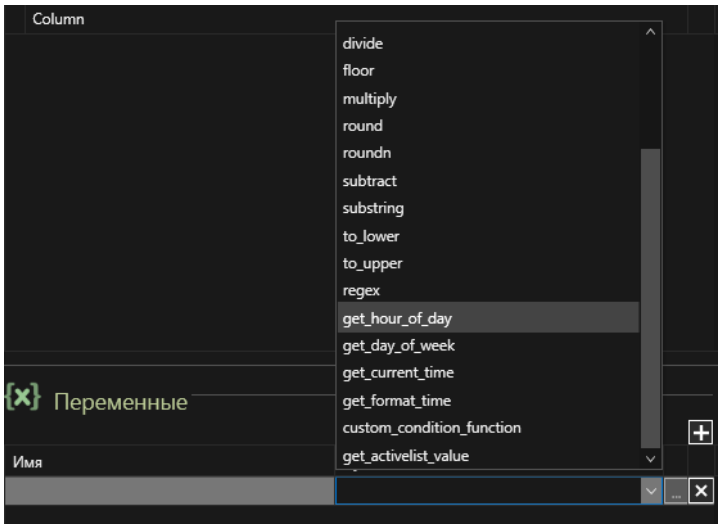


Рисунок 120. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 121) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «get_hour_of_day» имеет только 1 параметр – «Переменная».

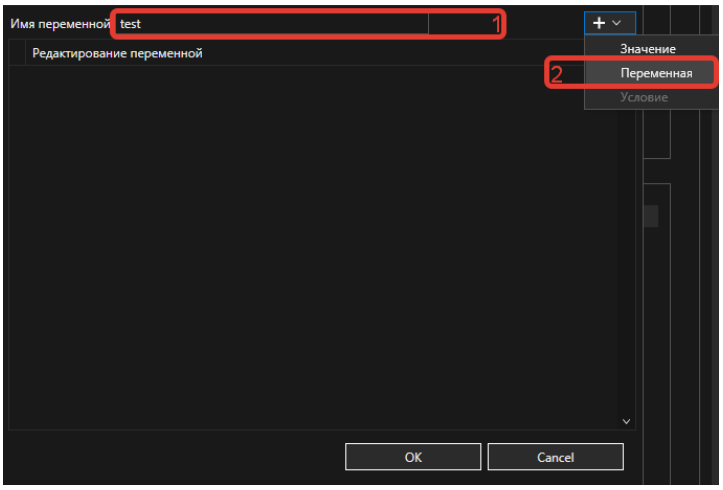


Рисунок 121.Окно создания переменной

В параметре «Переменная» необходимо выбрать поле события, по которому будет вычисляться конкретный час дня от 0 до 23 (см. Рисунок 119).

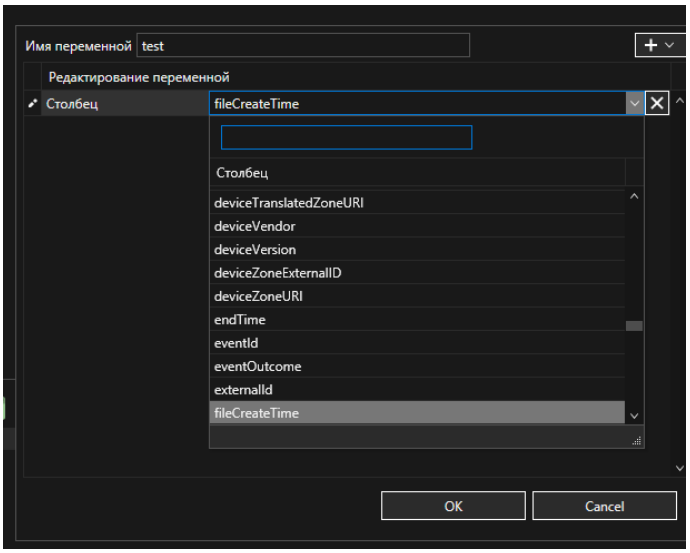


Рисунок 122. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

- **«get_day_of_week»**

Описание: данная переменная возвращает целое число от 0 до 6 (0 — воскресенье) для представления дня недели, на основе выбранной метки времени.

Алгоритм создания

Для создания переменной необходимо нажать на иконку . В открывшемся списке выбрать переменную «get_day_of_week» (см. Рисунок 123).

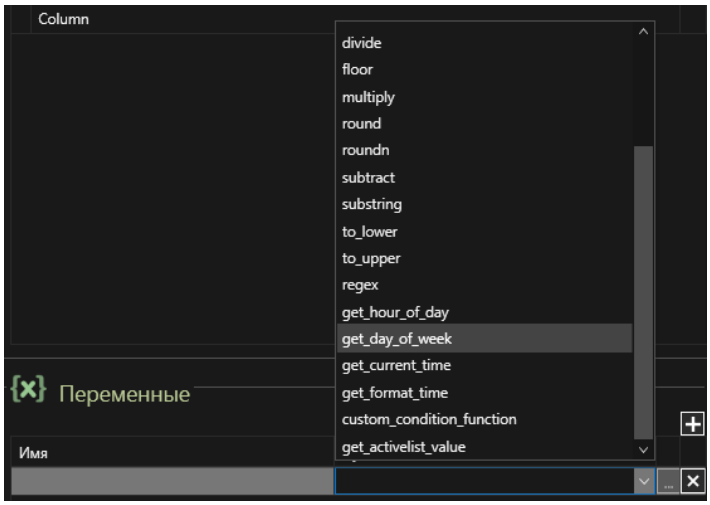


Рисунок 123. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 124) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «get_day_of_week» имеет только 1 параметр – «Переменная».

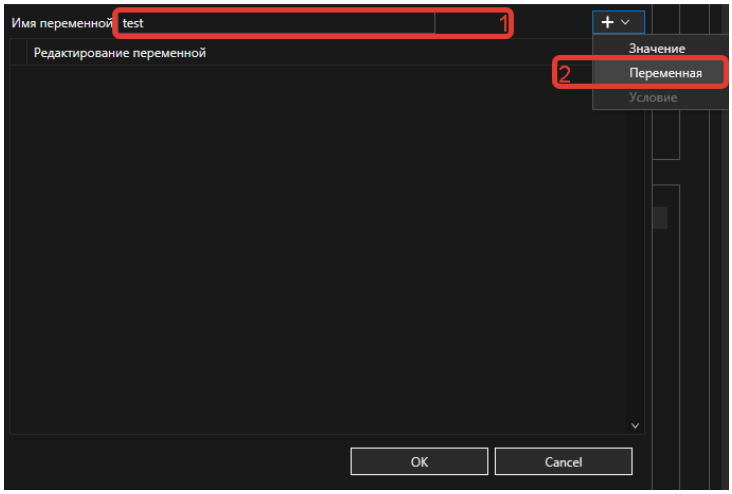


Рисунок 124. Окно создания переменной

В параметре «Переменная» необходимо выбрать поле события, по которому будет вычисляться конкретный день недели от 0 до 6 (см. Рисунок 125).

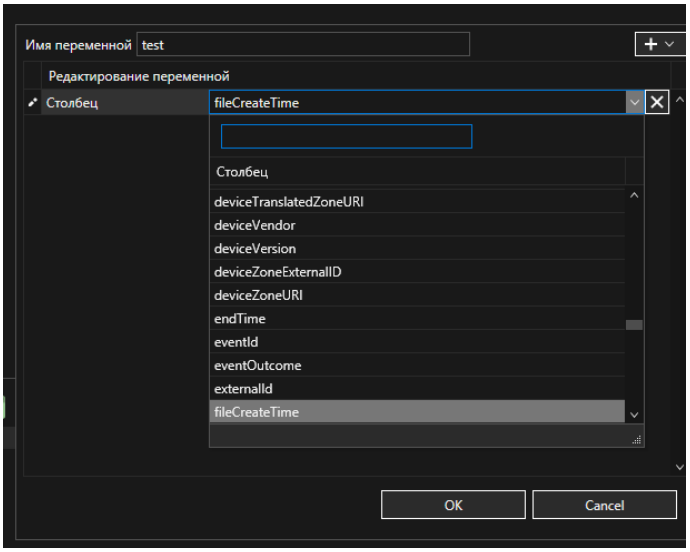


Рисунок 125. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

Вы можете проверить значение, возвращаемое этой функцией, с помощью числовых операций, таких как «>», «<», «>=», «<=», «=». Например, для переменной с именем «день», которая содержит значение, возвращаемое функцией get_day_of_week, вы можете создать логический оператор «И», который проверяет день недели со следующими условиями:

«день >= понедельник», «день <= пятница».

- **«get_current_time»**

Описание: данная переменная возвращает текущее время в формате «ДД ММ ГГГГ», «чч:мм:сс», «TIMEZONE».

Алгоритм создания

Для создания переменной необходимо нажать на иконку  . В открывшемся списке выбрать переменную «get_current_time» (см. Рисунок 126).

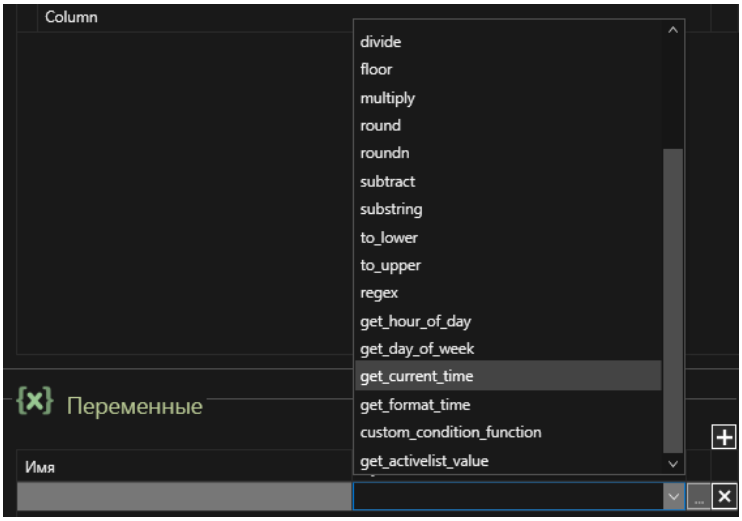


Рисунок 126. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 127) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «get_current_time» имеет только 1 параметр – «Переменная».

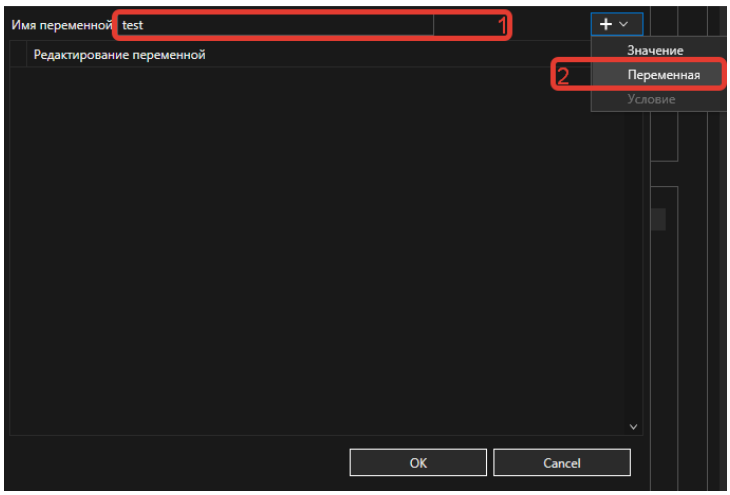


Рисунок 127. Окно создания переменной

В параметре «Переменная» необходимо выбрать поле события, по которому будет возвращено текущее время (см. Рисунок 125). Возвращаемое время основано на времени клиента.

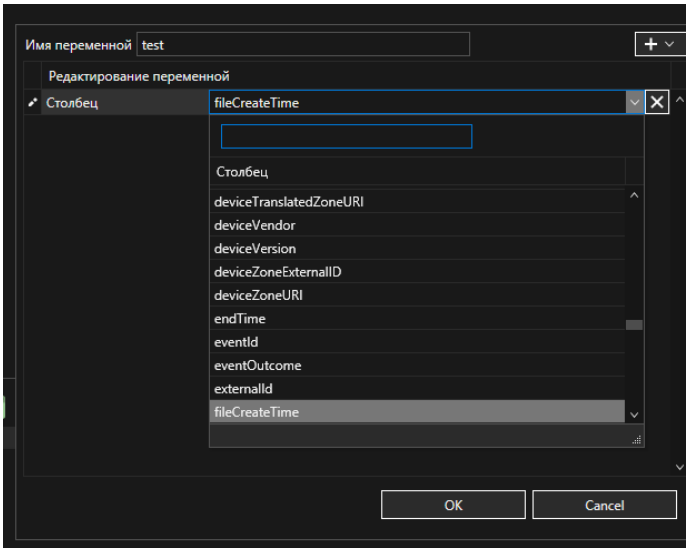


Рисунок 139. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

- **«get_format_time»**

Описание: данная переменная возвращает текущее время в заданном вами формате.

Алгоритм создания

Для того чтобы создать данную переменную необходимо нажать на иконку . В открывшемся списке выбираем переменную «get_format_time» (см. Рисунок 128).

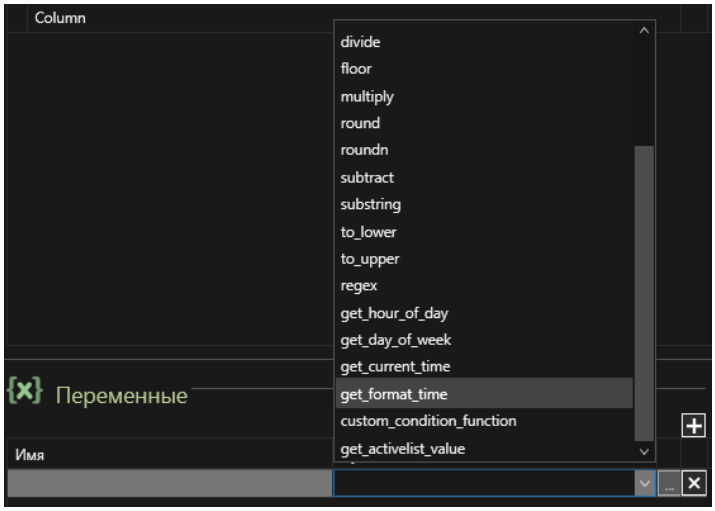


Рисунок 128. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 129) необходимо задать имя переменной (1) и её параметры (2)

(кнопка). Переменная «get_format_time» имеет 2 параметра – «Значение» и «Переменная». Параметр «Значение» используется для описания необходимого формата даты (например, '%H часов %M минут %m.%d.%Y года').

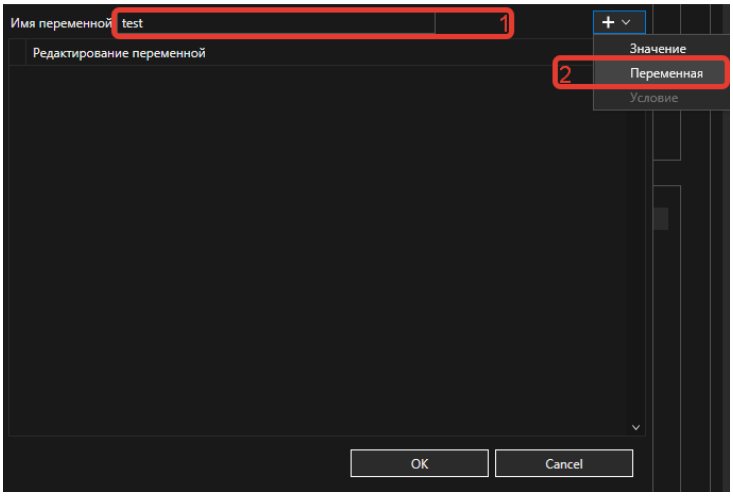


Рисунок 129. Окно создания переменной

В параметре «Переменная» необходимо выбрать поле события, которому необходимо вывести время в определённом формате (см. Рисунок 130).

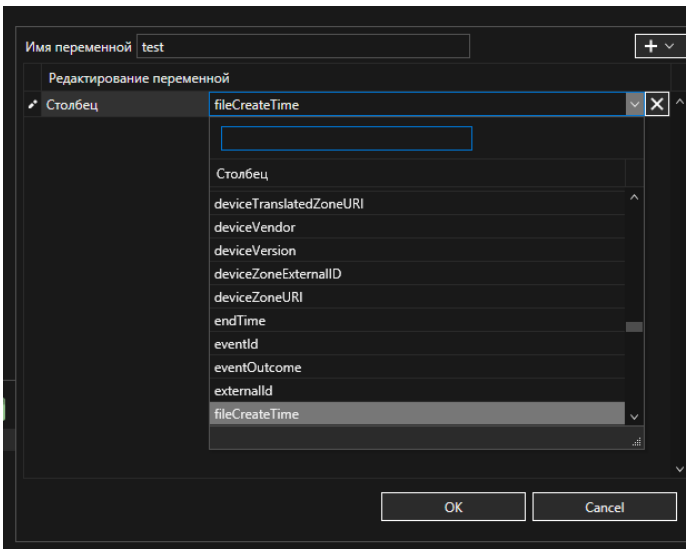


Рисунок 130. Окно «Переменная»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

6. Пользовательские переменные

- **«custom_condition _function»**

Описание: данная функция используется для написания пользовательских функций на основе фильтров.

Алгоритм создания

Для создания переменной необходимо нажать на иконку . В открывшемся списке выбрать переменную «custom_condition _function» (см. Рисунок 131).

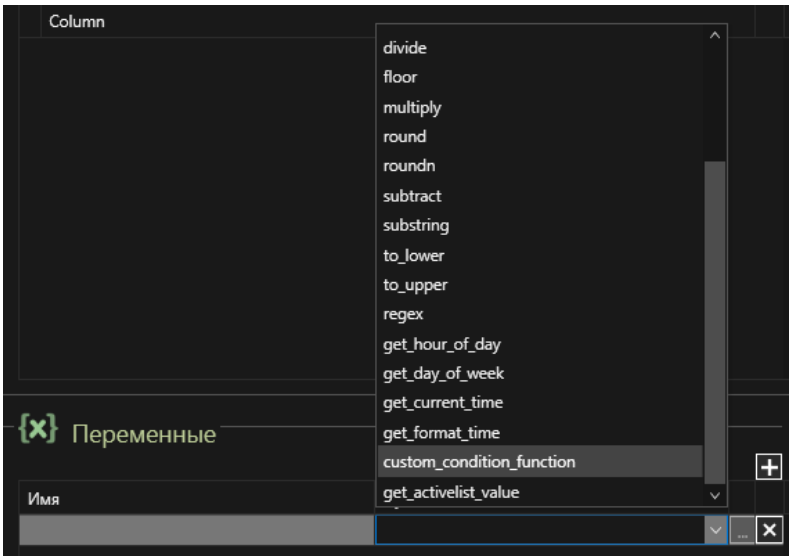


Рисунок 131. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 132) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «custom_condition _function» имеет 3 параметра – «Условие», «Переменная» и «Значение».

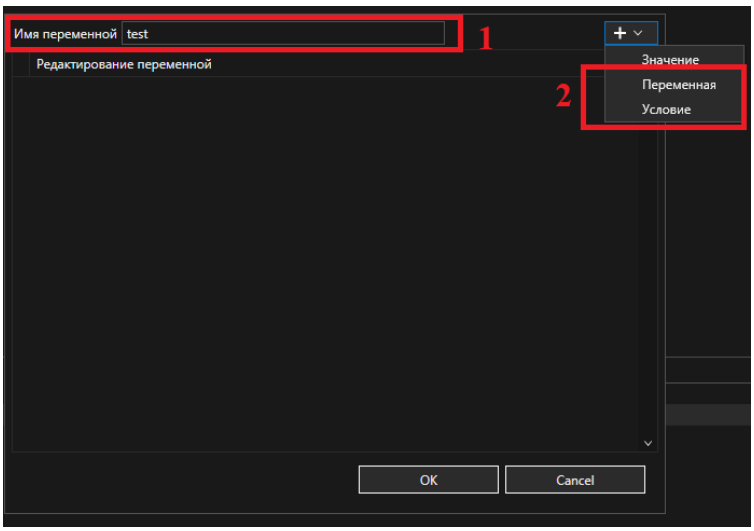


Рисунок 132. Окно создания переменной

В параметре «Условие» необходимо добавить условие или группу условий, по которым будет производиться отбор событий (см. Рисунок 133). Подробное описание создания условий описано в разделе «Написание условий» настоящего руководства.

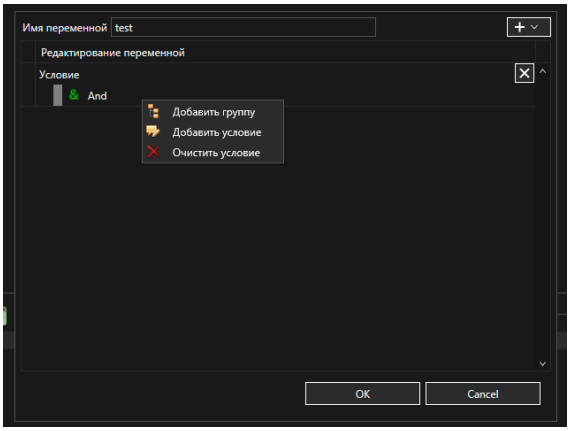


Рисунок 133. Настройка условий переменной

После добавления условия или группы условий, переменной необходимо задать параметры истинности или ложности выражения. Т. е. необходимо расписать, что переменная должна сделать в случае, если условие было верным и в случае, если оно оказалось неверным. Для этого можно использовать параметры «Значение» и «Переменная». (см. **Ошибка! Источник ссылки не найден.**).

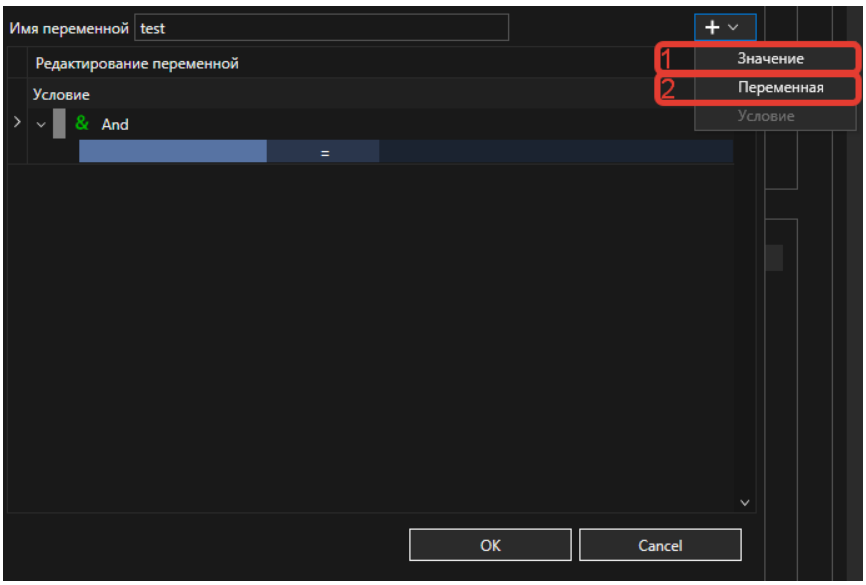


Рисунок 134. Окно создания параметров переменной

Пример переменной «custom_condition_function» (см. **Ошибка! Источник ссылки не найден.**).

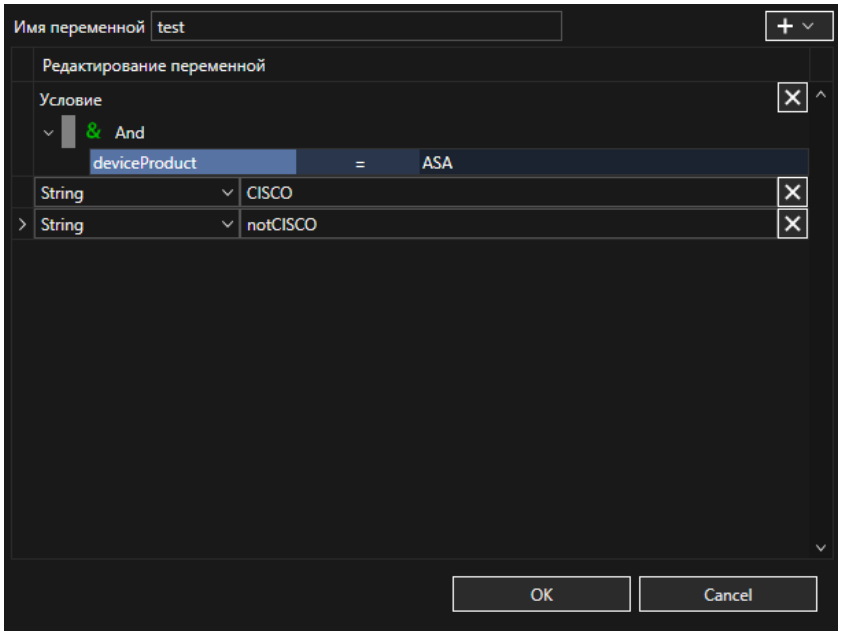


Рисунок 135. Пример заполненной переменной

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

- **«Regex»**

Описание: данная переменная возвращает значение на основе заданного регулярного выражения.

Алгоритм создания

Для создания переменной необходимо нажать на иконку ➕. В открывшемся списке выбрать переменную «regex» (см. Рисунок 136).

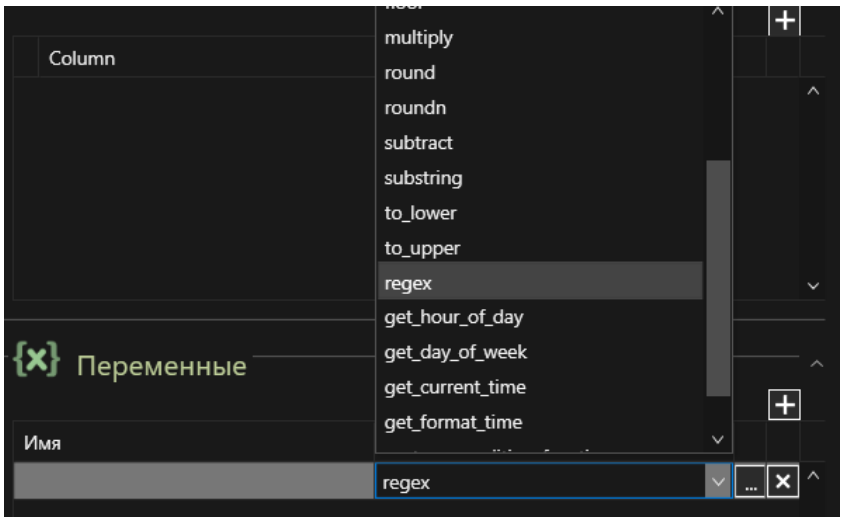


Рисунок 136. Выбор переменной

Далее, необходимо задать параметры переменной (кнопка). В открывшемся диалоговом окне (см. Рисунок 137) необходимо задать имя переменной (1) и её параметры (2) (кнопка). Переменная «rexeg» имеет 2 параметра – «Значение» и «Переменная». Параметр «Значение» используется для написания регулярного выражения.

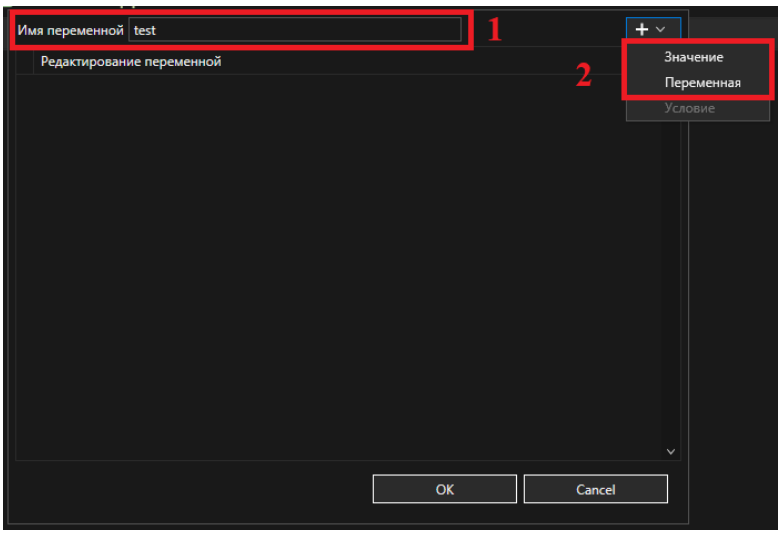


Рисунок 137. Окно переменной

В параметре «Переменная» необходимо выбрать поле события, по которому будет производиться поиск событий, подпадающих под регулярного выражения. (см. Рисунок 138).

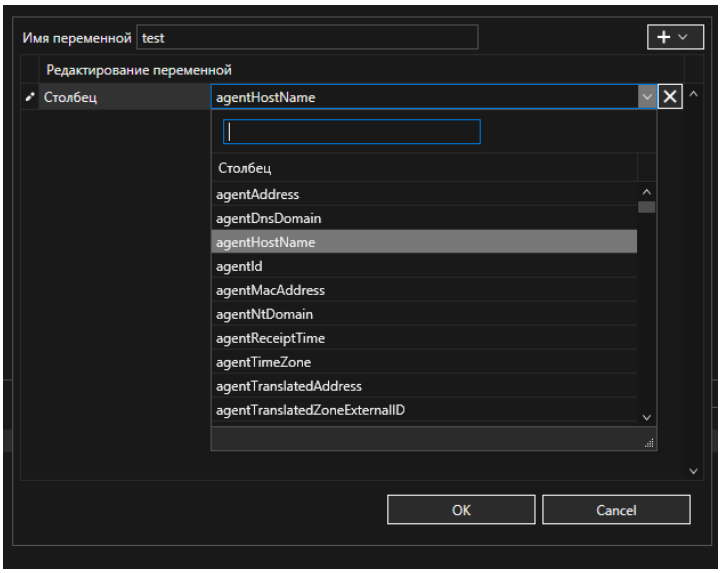


Рисунок 138. Окно параметра "Переменная"

Скобками необходимо выделить ту часть регулярного выражения, которую переменная должна вывести в ходе своей работы.

В параметре «Значение» следует вести значение регулярного выражения. Для этого необходимо выбрать тип константы «String» (1) и ввести регулярное выражение (2) (см. Рисунок 139).

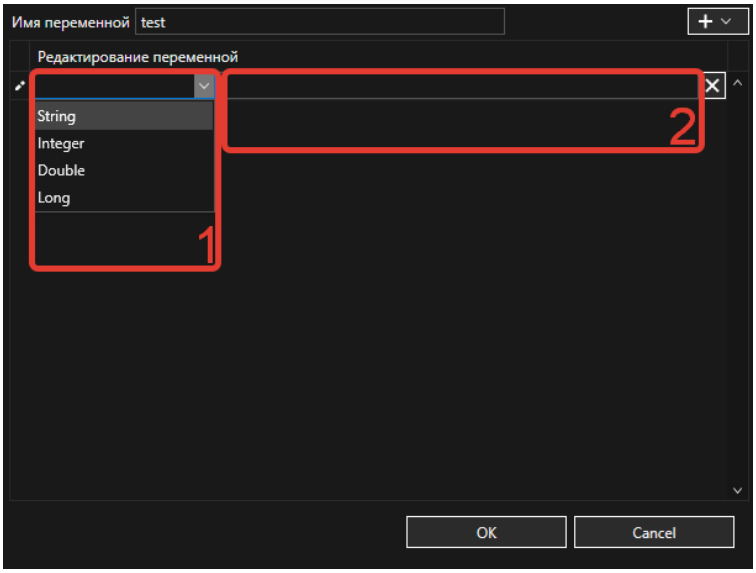


Рисунок 139. Параметр «Значение» переменной

Пример корректно заполненной переменной (см. Рисунок 140).

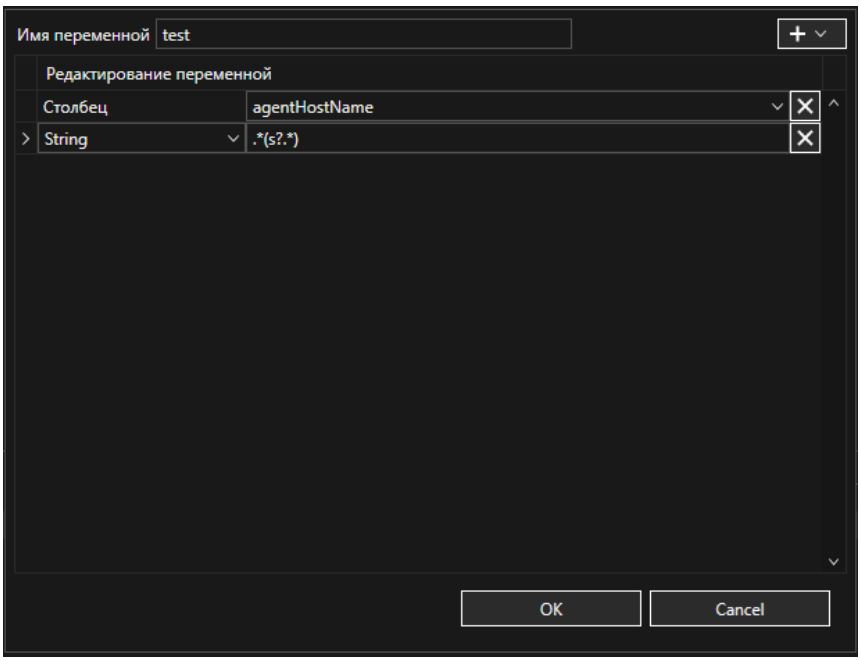


Рисунок 140. Аргументы переменной «regex»

Для сохранения изменений следует нажать на кнопку «OK», для отмены - «Cancel».

КОНТЕКСТНЫЙ ПОИСК

1. Написание запроса

Для создания документа контекстного поиска, в меню ресурсов необходимо прейти на вкладку «Контекстный поиск».

Откроется окно контекстного поиска (см. Рисунок 141). Он применяется для быстрого поиска значений в тех полях, которые отвечают за пользователя, в тех полях, которые отвечают за IP-адрес и в тех полях, которые отвечают за имя компьютера.

Далее необходимо заполнить поле «Временной диапазон». «Дата начала» и «Дата окончания» выставляются, когда нужно искать событие в определенные даты, «Интервал» при этом необходимо указать «Произвольный». В остальных случаях есть возможность выбрать интервал: 30 минут/ 1 час/ 4 часа/ 12 часов/ 1день/ 2 дня/ 1 неделя.

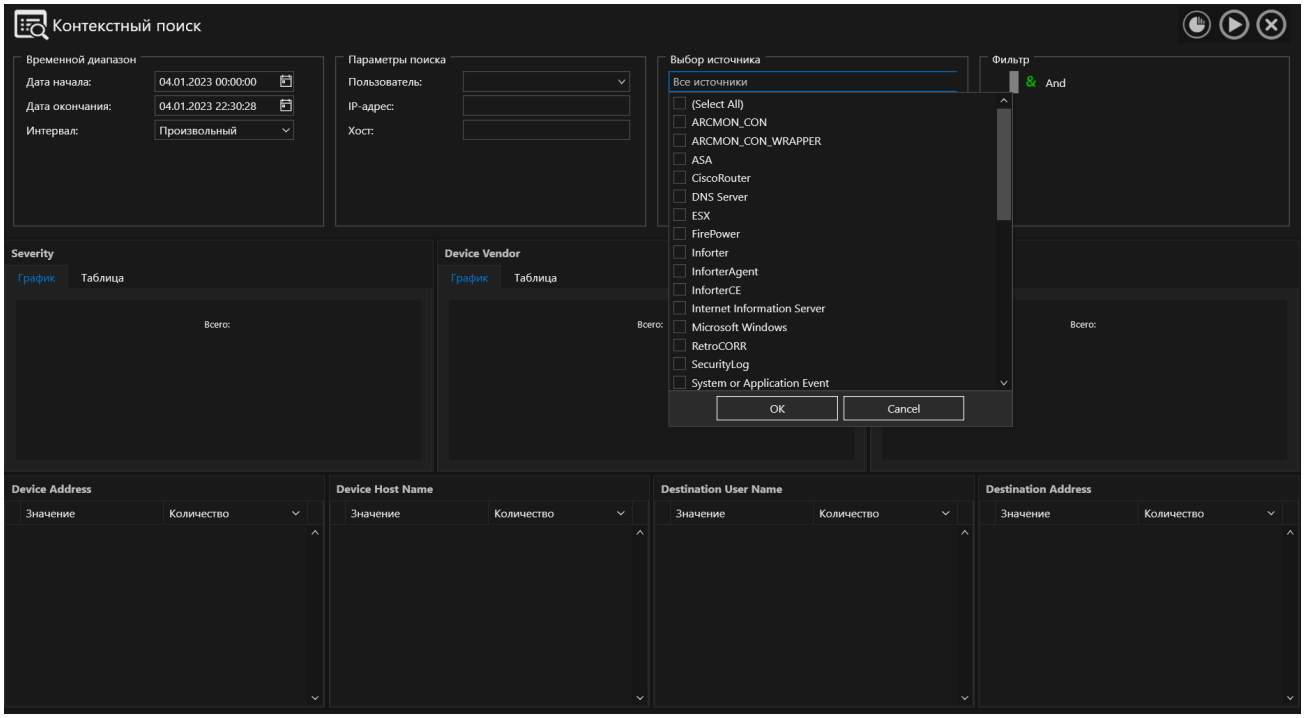


Рисунок 141. Окно контекстного поиска

Далее заполняется поле «Параметры поиска». Поиск может осуществляться по одному параметру, по двум или по трём: «Пользователь», «IP-адрес» и «Хост». При необходимости можно добавить дополнительные условия к поиску (см. «Написание условий»).

Поле «Выбор источника» заполняется в случае, если необходимо сделать выборку по определенному источнику. По умолчанию «Выбор источника» не участвует в поиске.

После заполнения всех необходимых полей следует запустить поиск кнопкой . Откроется окно с временным АК с событиями, которые удовлетворяют условиям поиска.

МОНИТОРИНГ

Для отображения компонентов подсистемы сбора, корреляции и анализа событий ИБ на географической карте РФ в меню ресурсов необходимо перейти на вкладку «Мониторинг», откроется интерактивная карта РФ (см. Рисунок 142).

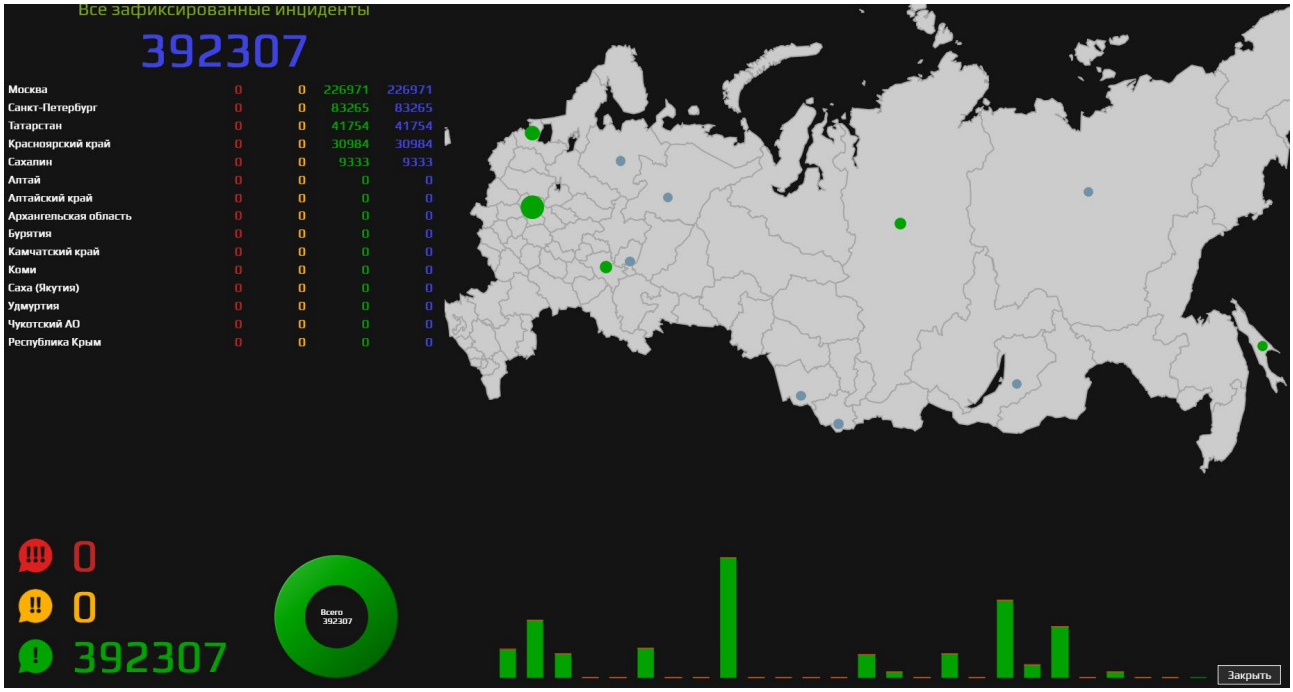


Рисунок 142. Окно мониторинга компонентов на географической карте

На этой карте вы можете увидеть города, в которых были зафиксированы инциденты, также вы увидите количество всех инцидентов вообще и по каждому региону в частности.

Для мониторинга состояния подсистемы сбора, корреляции и анализа событий ИБ в конкретном филиале необходимо дважды щёлкнуть по нему на интерактивной карте (см.Рисунок 143) Для подробного просмотра событий, возникших в филиале следует нажать

на кнопку «Открыть в АК», после чего откроется АК, в котором отображаются все события по данному филиалу.

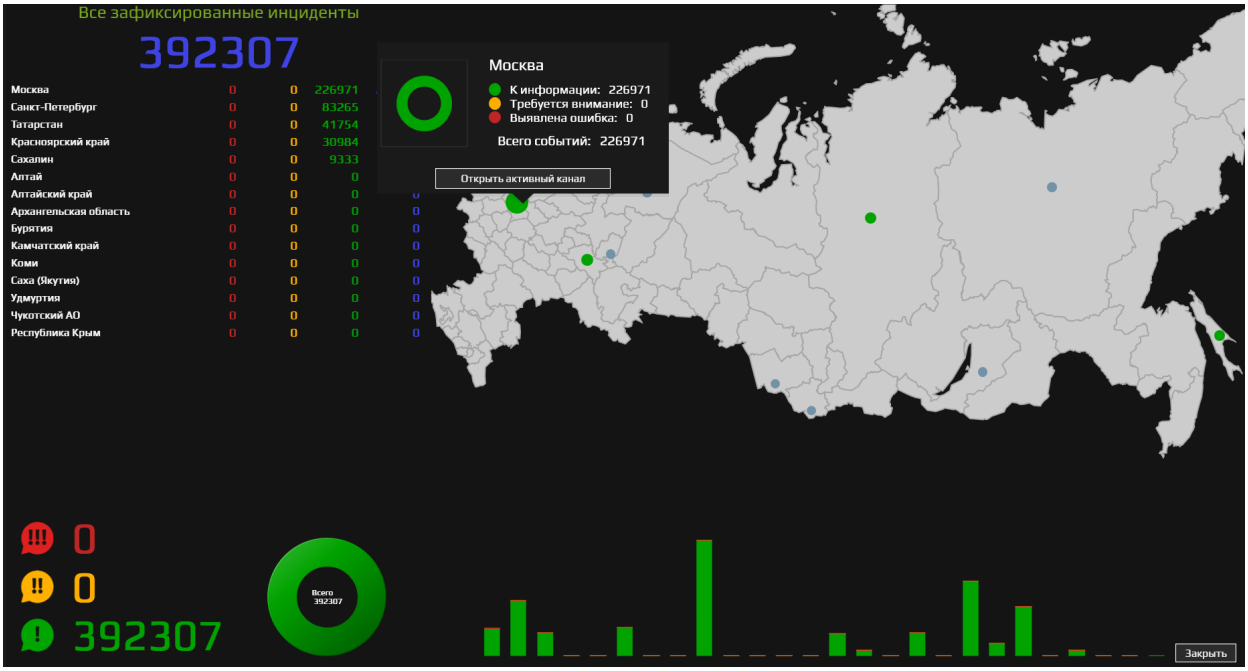


Рисунок 143. Пример мониторинга инцидентов в Москве

АДМИНИСТРИРОВАНИЕ

Для осуществления настройки системы, в меню ресурсов следует перейти на вкладку «Администрирование» (см. Рисунок 144). Данный раздел позволяет производить настройку системы, включая выбор темы и стартовый дашборд.

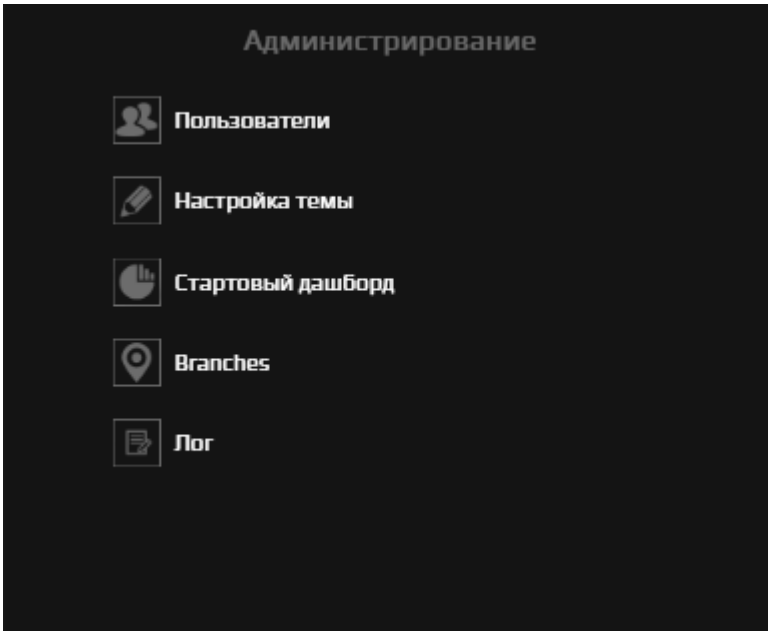


Рисунок 144. Вкладка "Администрирование"

1. Параметры программы

Для настройки параметров программы, в меню ресурсов следует перейти на вкладку «Администрирование», раздел «Параметры программы». После чего откроется окно с параметрами программы, в котором можно настроить интервалы обновления записей в АК, и проверить состояние лицензии, и входящие в неё модули системы (см. Рисунок 145).

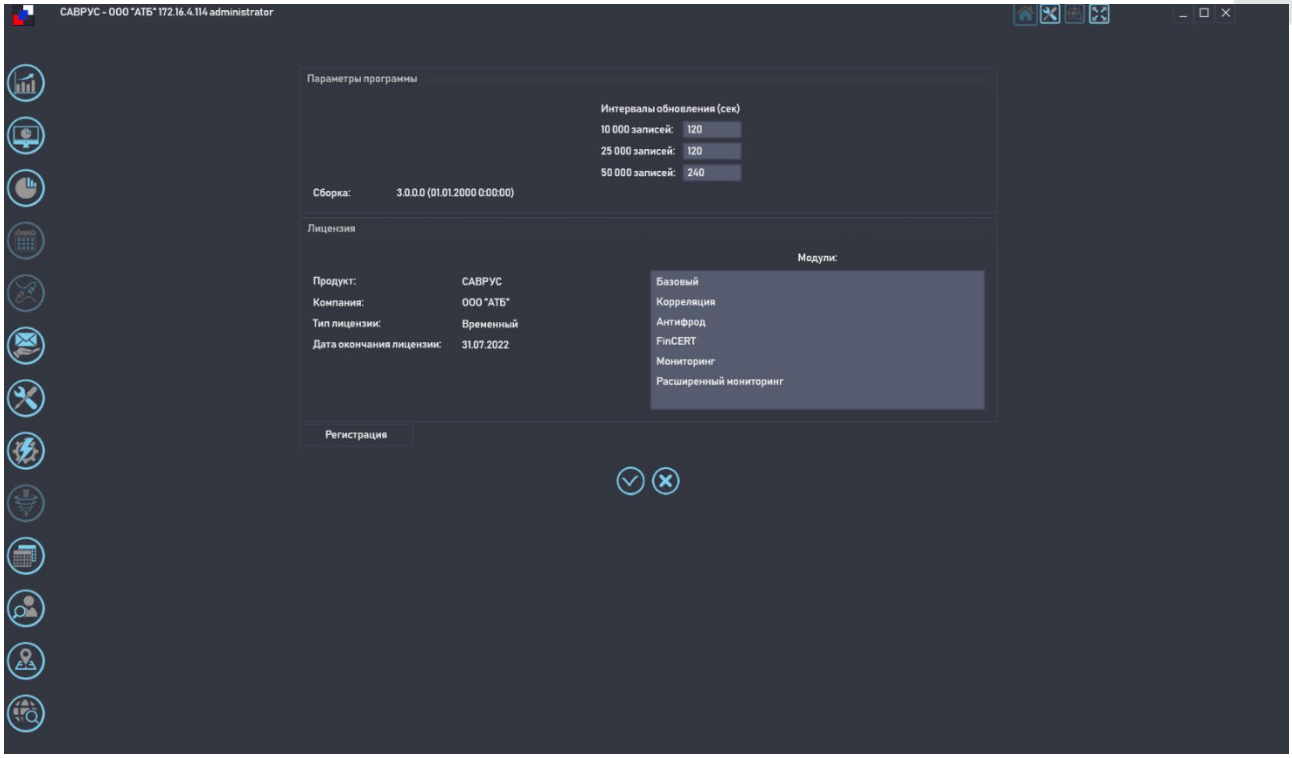


Рисунок 145. Окно "Параметры программы"

При внесении изменений в параметры программы необходимо их сохранить, для этого нажмите на кнопку , а для отмены изменений и выхода из раздела «параметры программы» нажмите кнопку .

Если у вас не отображается или закончилась лицензия, то следует обратиться к администратору САВРУС.

2. Настройка темы

Система позволяет гибко настраивать цветовое решения для каждого пользователя. Для настройки цветовой темы в меню ресурсов необходимо перейти на вкладку «Администрирование», раздел «Настройка темы» (см. Рисунок 146).

Рисунок 146. Окно настройки темы САВРУС

В системе САВРУС предусмотрено 3 цветовых темы, их можно выбрать в выпадающем списке «Тема *». Также система позволяет настроить цветовое решения для уровней критичности событий.

В разделе настройка темы можно выбрать вид отображения радара и столбчатой диаграммы в окне АК. Настроить тип отображения графических элементов, расположение легенды и размер элементов.

3. Стартовый дашборд

Стартовый дашборд – это дашборд расположенный на главном экране системы САВРУС. Его также можно изменить и кастомизировать под каждого сотрудника. Для этого в меню ресурсов необходимо перейти на вкладку «Администрирование» раздел «Стартовый дашборд» (см. Рисунок 147). Стартовый дашборд создается по аналогии с обычным дашбордом. На вкладке «Дашборды» отображаются существующие объекты визуализации данных, их можно изменить, щёлкнув ПКМ и в контекстном меню выбрав пункт «Изменить». Для создания новых объектов необходимо щёлкнуть ПКМ по пустому месту в списке дашбордов и в контекстном меню выбрать пункт «Добавить визуализацию», откроется вкладка «Визуализация», представляющая собой, конструктор объектов визуализации. После создания всех необходимых объектов визуализации следует перейти на вкладку «Дашборд» и перетащить объекты в область дашборда (см. Создание дашбордов). Также необходимо вписать название дашборда в соответствующем окне. Для сохранения стартового дашборда следует нажать на кнопку , а для отмены кнопку .

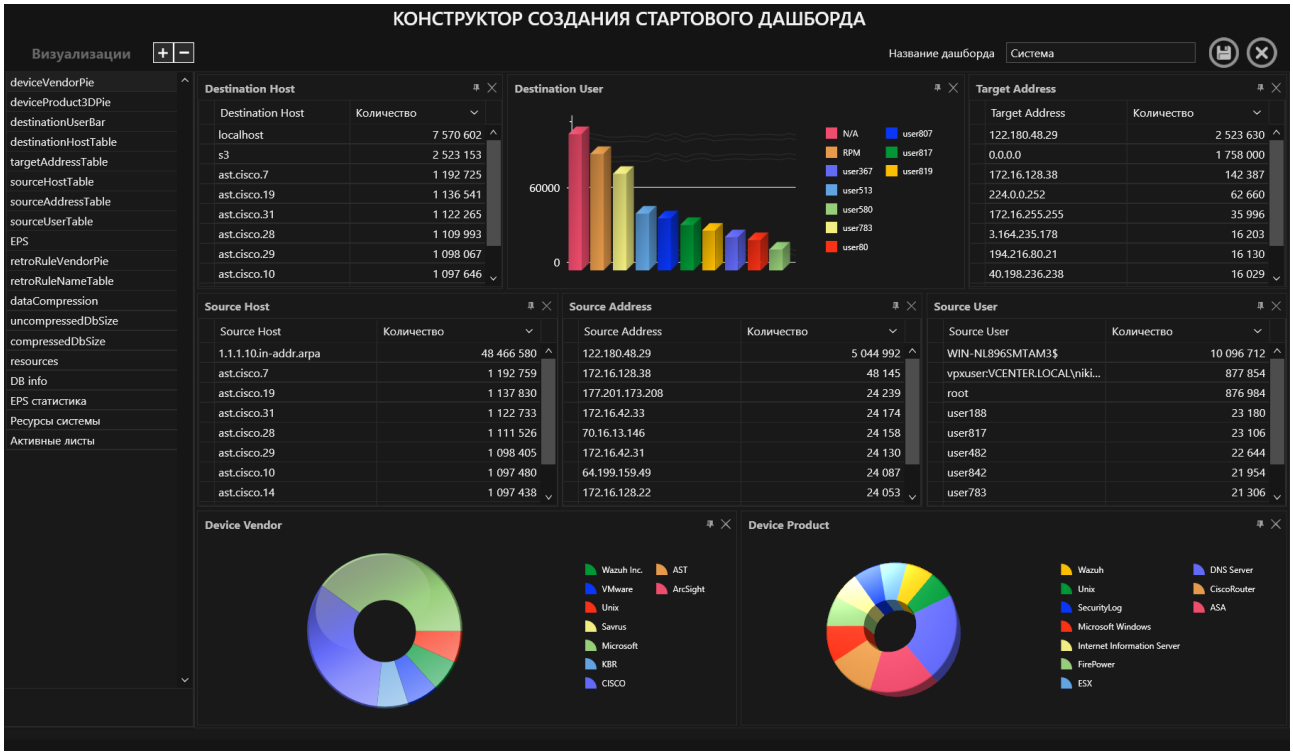


Рисунок 147. Настройка стартового дашборда

У стартового дашборда можно обновлять данные, для этого в области, отмеченной красным прямоугольником (см. Рисунок 148) следует выбрать временной диапазон событий из предложенных день/неделя/месяц.

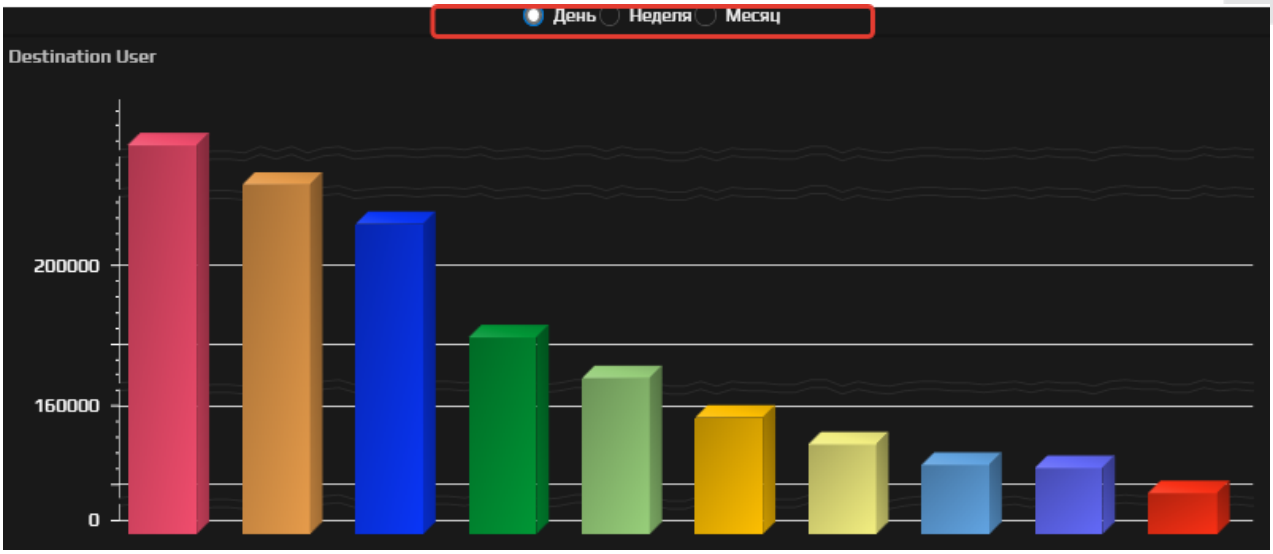


Рисунок 148. Стартовый дашборд

4. Масштабирование интерфейса

Система САВРУС поддерживает настройку масштабирования экрана, для этого в любом окне системы в верхнем правом углу располагается кнопка , при нажатии на неё открывается диалоговое окно масштабирования, в котором можно настроить отображение системы для любого экрана. Для этого необходимо настроить значение ширины и высоты экрана и нажать на кнопку «OK», для возврата на исходные значения необходимо нажать на кнопку «Исходные значения» (см. Рисунок 149).

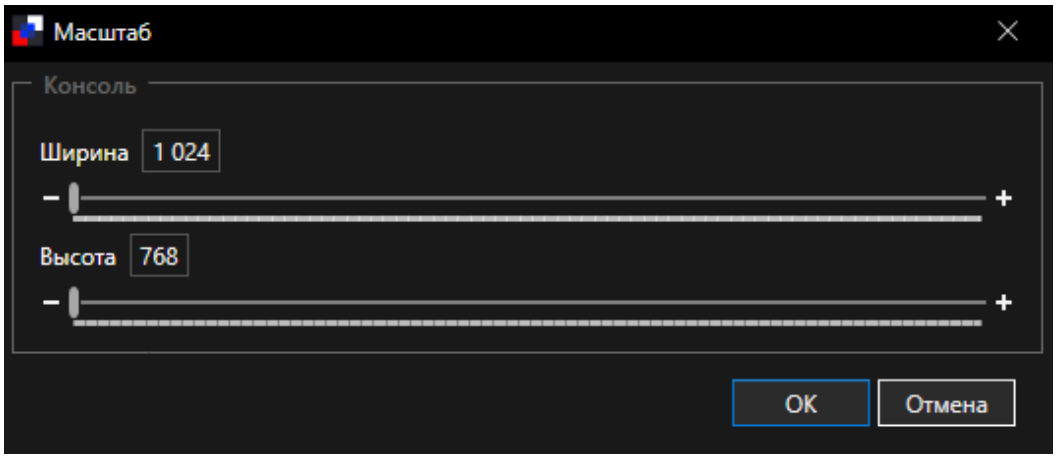


Рисунок 149. Масштабирование интерфейса