Программный комплекс автоматизации ситуационного центра информационной безопасности «Эгида»

Документация, содержащая информацию, необходимую для эксплуатации экземпляра программного обеспечения (для проведения экспертной оценки в Экспертном совете при Минцифры России)

ООО «Гефест Технолоджиз»

Содержание

1. Введение

Система «Эгида» - автоматизированный программный комплекс обеспечения работы ситуационного центра информационной безопасности (ИБ), объединяющий в себе функции систем кибербезопасности разных типов и назначений, позволяющий:

- выполнять сбор, хранение и обработку, в том числе автоматическую, событий ИБ;
- упрощать, ускорять и автоматизировать процессы обработки и расследования событий и инцидентов ИБ;
- осуществлять мониторинг, оперативно и проактивно выявлять инциденты ИБ;
- поддерживать процессы управления инцидентами ИБ, в том числе посредством постоянного расширения контекстов оценки событий с использованием инструментов автоматизации и машинного обучения;
- производить автоматическое реагирование и непрерывную корректировку эффективности функционирования, формировать отчетность;
- проводить поиск и сбор сведений об информационных активах, анализ уязвимостей, оценку допустимости деструктивных сценариев;
- поддерживать процессы повышения зрелости ситуационного центра и проведения киберучений персонала.

Детальная информация по этим задачам и инструментам, предоставляемым Системой для их решения, приведена в следующих разделах:

- Сбор событий;
- Мониторинг и контроль;
- Расследование.

2. Сбор событий

События - это информация об активности, связанной с ИБ, на защищаемых информационных ресурсах: АРМ, серверах, сетевом оборудовании, базах данных, информационных и автоматизированных системах, СЗИ, источниках сторонних систем. Отдельные события и их последовательности позволяют идентифицировать аномальную активность и выявлять угрозы ИБ. Таким образом, защищаемые ресурсы служат источниками событий, и сбор событий из них является ключевой предпосылкой для проведения мониторинга, исследований и расследований.

Сбор событий включает в себя следующие этапы:

- настройка целевых источников, из которых будет осуществляться сбор событий;
- актуализация модели события, используемой для хранения данных событий;
- подключение целевых источников событий к Системе и прием событий из них;
- подготовка принятых событий (называемых «исходными событиями»), используя нормализацию и обогащение;
- передача исходных и подготовленных событий в хранилище Системы.

Разделы ниже содержат детальную информацию о перечисленных этапах.

2.1 Настройка целевых источников событий для процесса сбора

Система поддерживает сбор событий из следующих типов источников:

- системные журналы (Linux Syslog, Windows Event Log);
- базы данных (PostgreSQL, Oracle, MySQL, Microsoft SQL Server);
- файлы журналов серверов (Microsoft DHCP Server, Microsoft Windows DNS Server, Microsoft IIS Server);
- файлы журнала брандмауэра Windows (Windows Defender Firewall);
- журналы в формате CEF, отправляемые по протоколу syslog.

Определите целевые ресурсы-источники и настройте их до состояния готовности к сбору событий из них. Настройка осуществляется в соответствии с инструкцией, поставляемой отдельным PDF-файлом.

Последующие этапы относятся к настроенным для сбора событий источникам.

2.2 Актуализация модели события

Включает в себя создание и настройку полей модели, необходимых для обеспечения процесса подготовки исходных событий к использованию в Системе:

- Поля для хранения элементов исходного события.

  Данные элементов можно преобразовать в значения полей, настроив сопоставления в целевых источниках событий. Сопоставления будут служить правилами нормализации событий.

- Поля для хранения дополнительных данных.

  Эти данные можно получить, используя обогащение нормализованных событий.

Актуализацию модели можно производить итерационно, расширяя ее новыми полями и корректируя в соответствии с изменениями, вносимыми в настройки целевых источников событий, правил обогащения и корреляции. Вы можете управлять полями модели, как описано ниже.

2.2.1 Системные поля модели события

По умолчанию модель содержит только системные поля. Эти поля хранят ключевые характеристики события и заполняются значениями автоматически. К системным полям относятся:

- **Aegis Source**.

  Хранит имя источника, создавшего событие.

- **Event Created Date**.

  Хранит дату и время возникновения события.

Вы можете добавлять к этим полям свои собственные и модифицировать поля, как описано ниже.

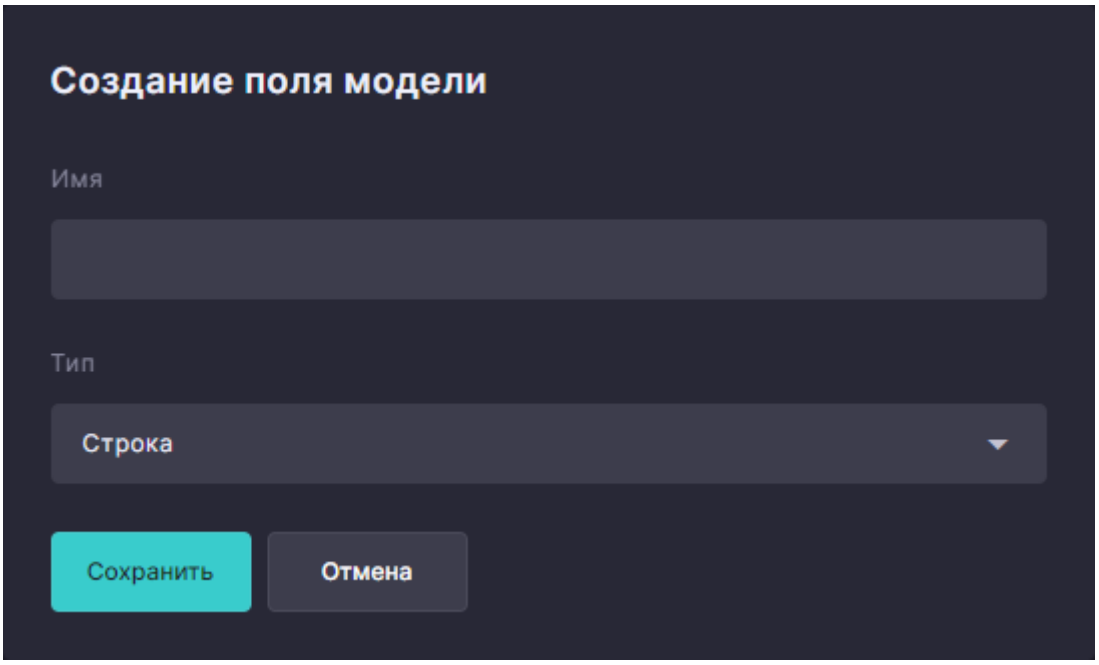
Системные поля поддерживают только переименование без изменения их типов данных.

2.2.2 Управление полями модели события

Для управления полями модели перейдите в модуль «Поля модели события» и воспользуйтесь его функциями, как описано ниже. Все созданные поля модели события отображаются в модуле в виде списка.

Создание поля модели

1. Нажмите значок + («Создать поле модели»), чтобы открыть окно «Создание поля модели».

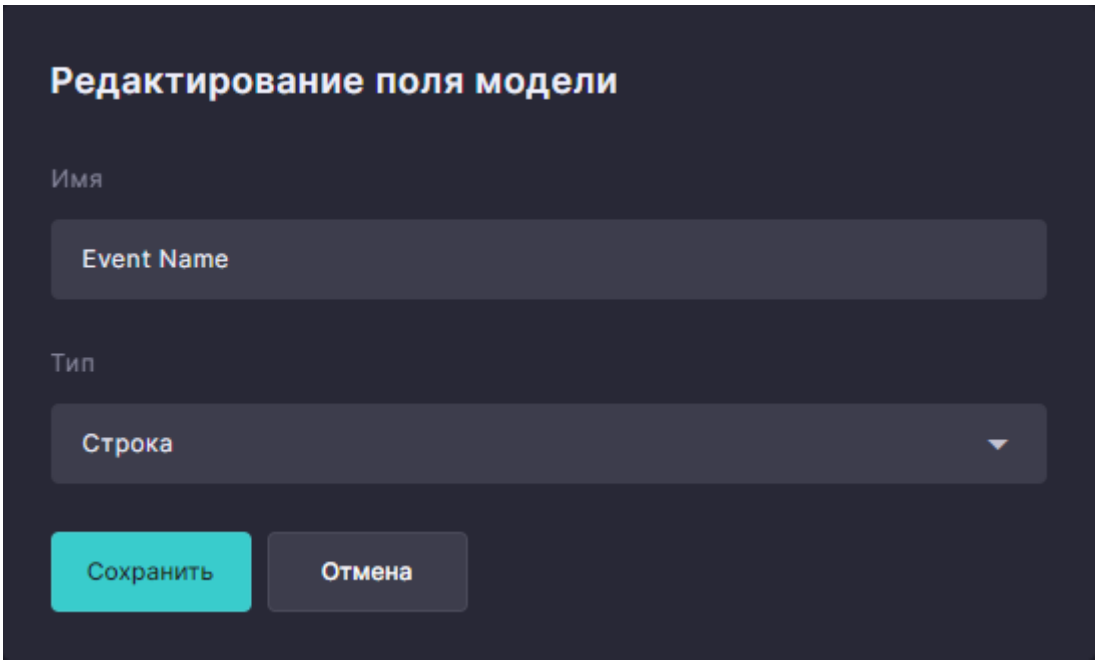


2. Введите уникальное имя поля.
3. Выберите тип данных поля из выпадающего списка.
4. Нажмите кнопку «Сохранить».

Окно «Создание поля модели» закроется, и созданное поле отобразится в списке полей модели.

Редактирование поля модели

1. Найдите в списке требуемое поле и откройте для него окно «Редактирование поля модели» одним из следующих способов:
    - Дважды щелкните мышью по полю.
    - Наведите указатель мыши на поле и нажмите контекстный значок ✎ («Редактировать поле модели»).



2. При необходимости введите новое уникальное имя поля.
3. При необходимости измените тип данных, выбрав элемент из выпадающего списка.
4. Нажмите кнопку «Сохранить».

Окно «Редактирование поля модели» закроется, и внесенные изменения применятся к полю.

2.3 Подключение источников событий к Системе и прием событий из них

Для начала приема событий из определенного источника его необходимо подключить к Системе, создав в ней новый источник и задав его характеристики:

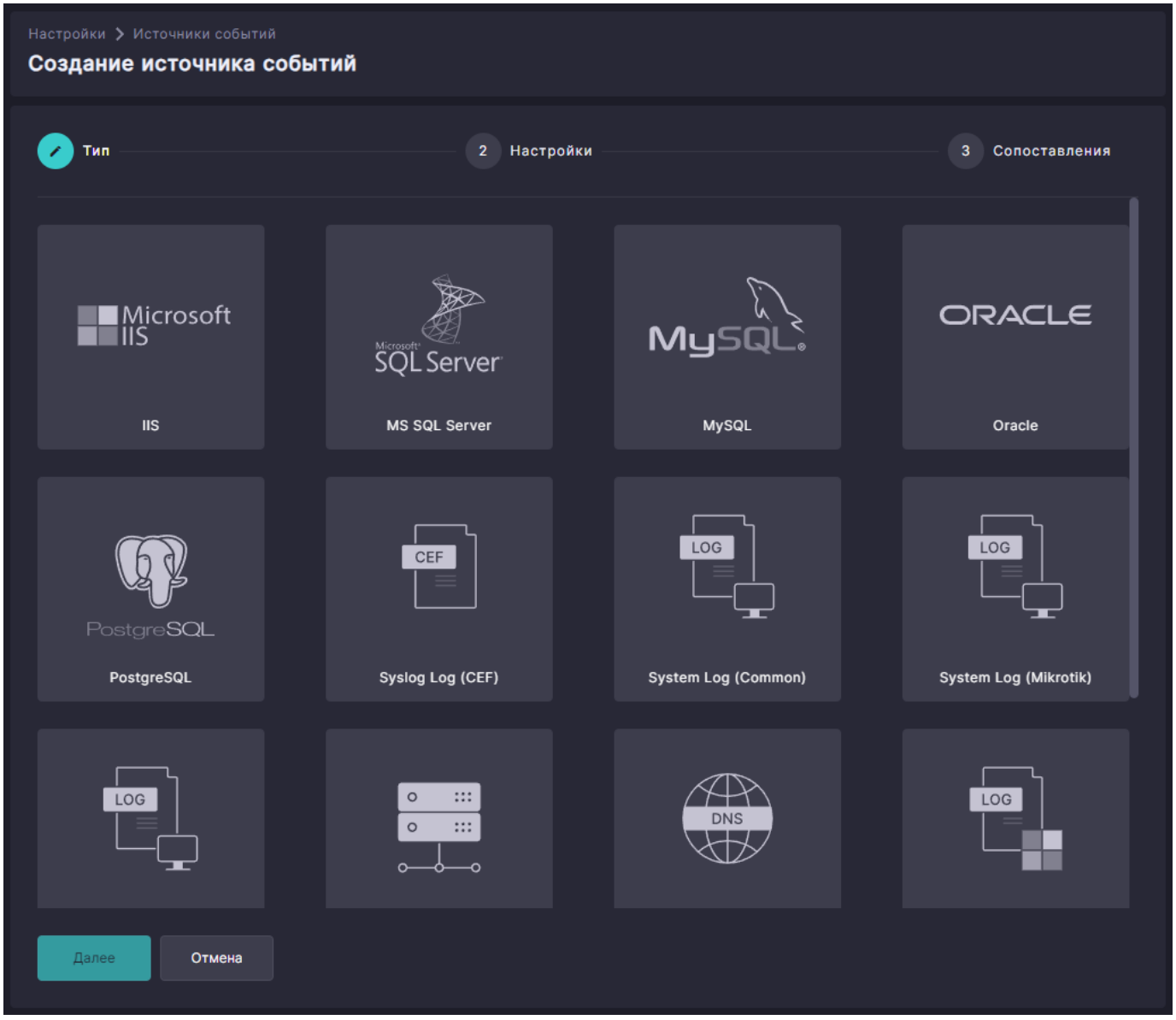
- имя (сохраняется в системном поле **Aegis Source** нормализованных событий этого источника);
- тип и специфичные для него параметры извлечения событий;
- идентификаторы ресурсов, генерирующих события;
- состояние «Включен».

Для управления источниками событий перейдите в модуль «Источники событий» и воспользуйтесь его функциями, как описано ниже. Все созданные источники событий отображаются в модуле в виде таблицы.

Чтобы иметь возможность задать сопоставления непосредственно при создании или редактировании источника, предварительно актуализируйте модель события.

2.3.1 Создание источника событий

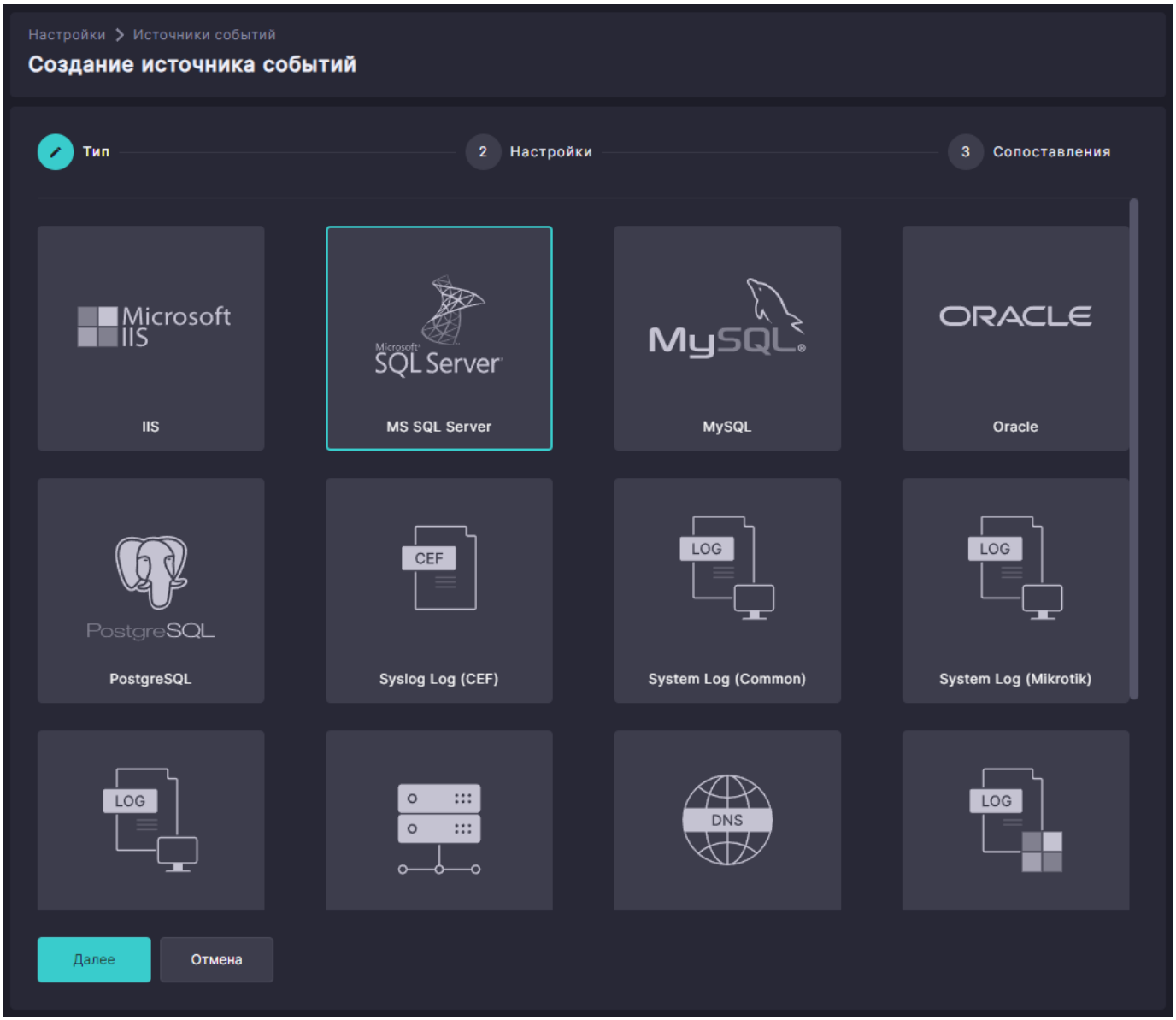
Перейдите в модуль «Источники событий» и нажмите значок + («Создать источник»). В открывшемся окне «Создание источника событий» отобразится мастер конфигурации источника событий, облегчающий процедуру задания характеристик источника.



Мастер конфигурации позволяет задать характеристики источника по шагам, используя индивидуальные страницы. Перемещаться между шагами можно с помощью кнопок «Далее» и «Назад». Чтобы закрыть мастер и отказаться от создания источника, нажмите кнопку «Отмена».

Страница «Тип»

Выберите создаваемый тип источника нажатием на соответствующий элемент-шаблон в представленном на странице списке.



В таблице ниже шаблоны сгруппированы по типу источника.

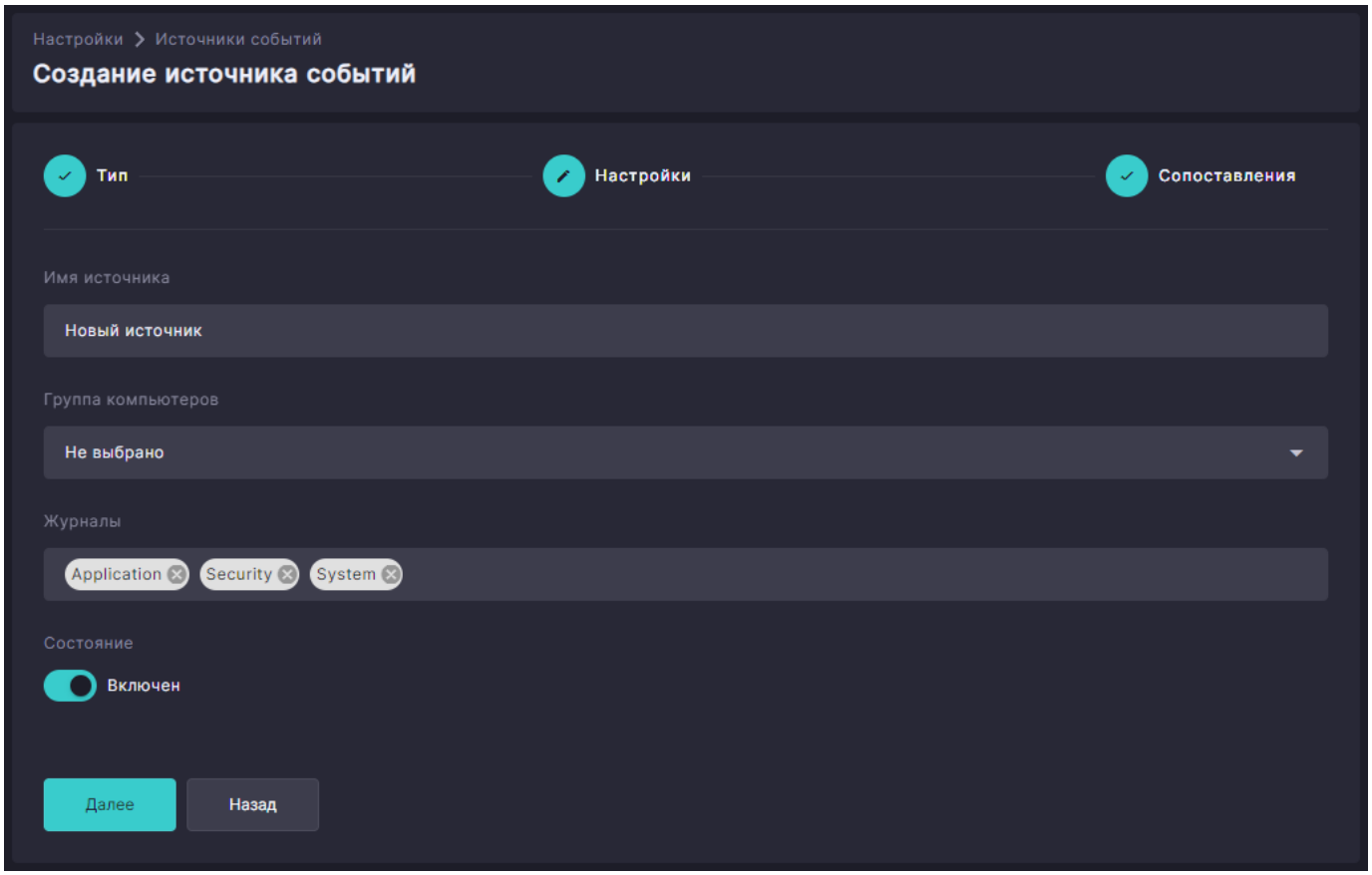
Тип источника	Шаблон
Система журналирования Windows	Windows Event Log
Журнал, отправляемый по протоколу syslog	System Log, Syslog Log (CEF)
Файл	Windows DHCP, Windows DNS, Windows Firewall, IIS
База данных	PostgreSQL, Oracle, MySQL, MS SQL Server

Нажмите кнопку «Далее» для перехода на следующую страницу мастера конфигурации.

Страница «Настройки»

Система предоставляет настройку специфичных для типа источника параметров извлечения событий. Содержимое данной страницы варьируется в зависимости от типа источника. После введения параметров нажмите кнопку «Далее» для перехода на следующую страницу мастера конфигурации.

ТИП «СИСТЕМА ЖУРНАЛИРОВАНИЯ WINDOWS»



Задайте параметры:

- Имя источника.

  Введите уникальное имя для идентификации источника в интерфейсе Системы.

- Группа компьютеров.

  Выберите из выпадающего списка группу компьютеров, с которых будет производиться сбор событий. Если группа компьютеров не выбрана, целевыми компьютерами считаются те, где установлено специализированное ПО (агент), и которые не входят ни в одну из существующих групп.

- Список источников.

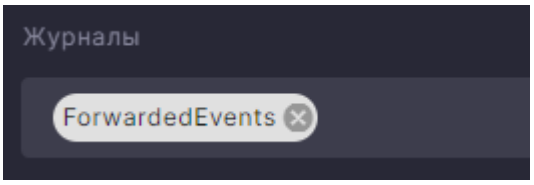
  Введите полные наименования (Full Name) журналов, из которых будут собираться события, завершая ввод каждого наименования нажатием клавиши Enter ⏎ .

  Пример ввода наименований трех журналов:

  Application Enter ⏎ Security Enter ⏎ System Enter ⏎

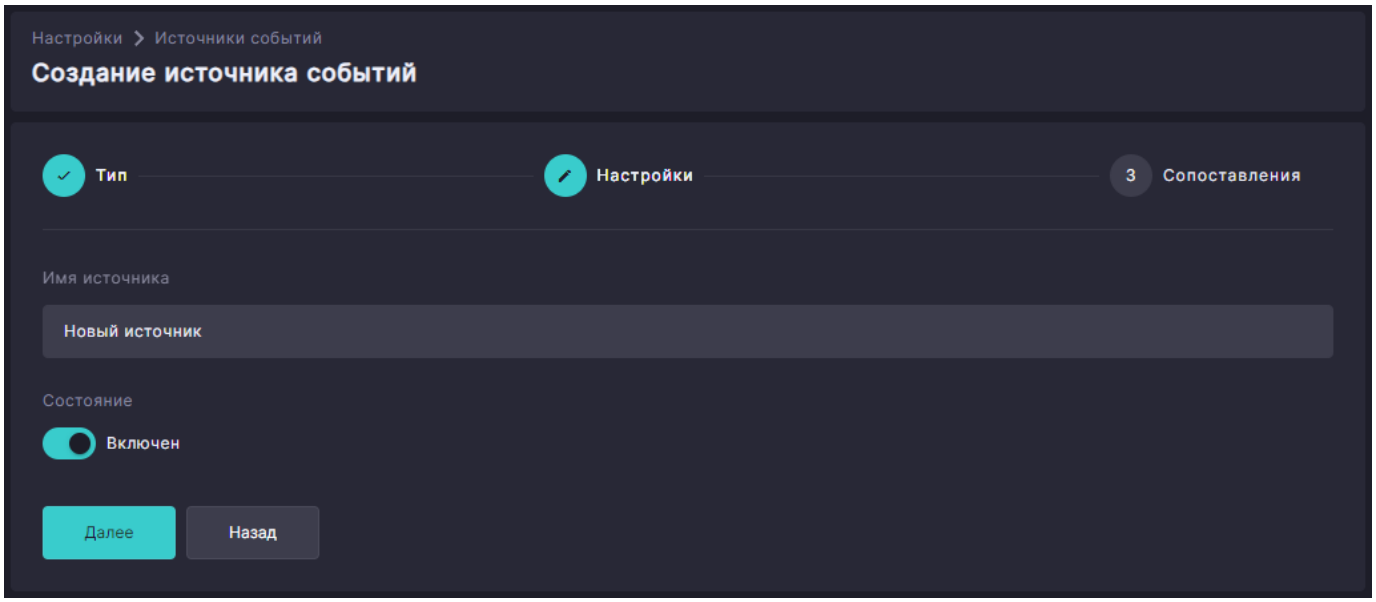
  Журнал переадресованных событий («Forwarded Events») имеет полное наименование «ForwardedEvents».

- Состояние.

  Переведите переключатель в правое положение («Включен») для включения источника в сбор событий.

ТИП «ЖУРНАЛ, ОТПРАВЛЯЕМЫЙ ПО ПРОТОКОЛУ SYSLOG»



Задайте параметры:

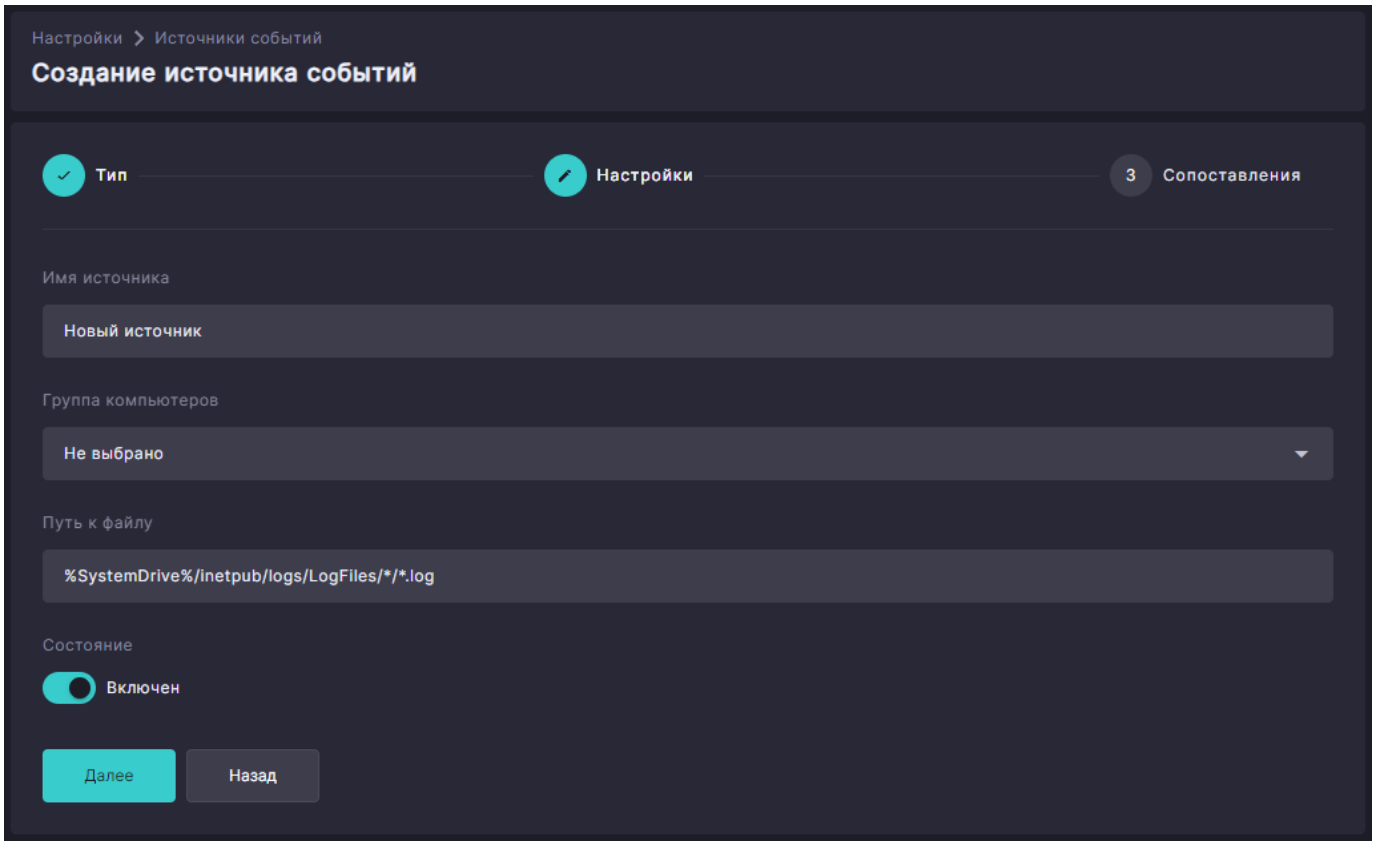
- Имя источника.

  Введите уникальное имя для идентификации источника в интерфейсе Системы.

- Состояние.

  Переведите переключатель в правое положение («Включен») для включения источника в сбор событий.

ТИП «ФАЙЛ»



Задайте параметры:

- Имя источника.

  Введите уникальное имя для идентификации источника в интерфейсе Системы.

- Группа компьютеров. Выберите из выпадающего списка группу компьютеров, с которых будет производиться сбор событий этого источника. Если группа компьютеров не выбрана, целевыми компьютерами считаются те, где установлено специализированное ПО (агент), и которые не входят ни в одну из существующих групп.

- Путь к файлу.

  Введите локальный путь к файлу, содержимое которого будет извлекаться. Путь может содержать символы шаблонов поиска: ? и *.

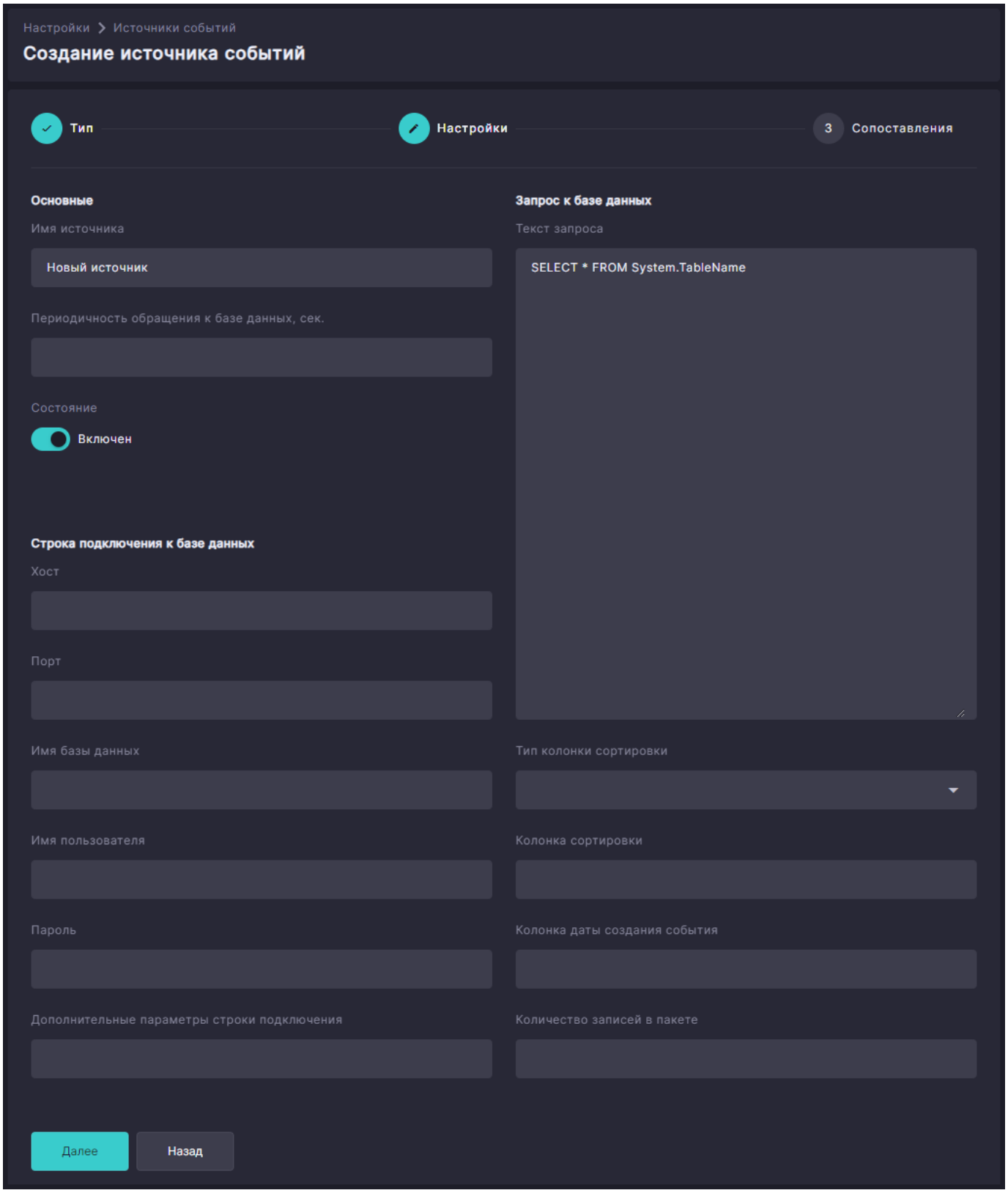
  Пример ввода:

  ```
  %SystemDrive%/inetpub/logs/LogFiles/*/*.log
  ```

- Состояние.

  Переведите переключатель в правое положение («Включен») для включения источника в сбор событий.

ТИП «БАЗА ДАННЫХ»



Данный тип источника периодически выполняет SQL-запросы к требуемому объекту базы данных (таблице или представлению) для выборки новых записей о событиях и формирования из них пакета

для передачи в хранилище Системы. Для обеспечения ранжирования записей в порядке новизны нужно выбрать колонку, по чьим значениям будет производиться сортировка.

Задайте параметры в разделе «Основные»:

- Имя источника.

  Введите уникальное имя для идентификации источника в интерфейсе Системы.

- Частота обращения к базе данных, сек.

  Введите период между выполнениями SQL-запросов.

- Состояние «Включен».

  Переведите переключатель в правое положение для включения источника в сбор событий.

Задайте параметры в разделе «Строка подключения к базе данных»:

- Хост и порт.

  Введите расположение подключаемой базы данных.

- Имя базы данных.

  Введите имя базы данных.

- Имя пользователя и пароль.

  Введите учетные данные, позволяющие подключиться к базе данных.

- Дополнительные параметры строки подключения.

  При необходимости введите параметры, которые будут добавлены к строке подключения.

Задайте параметры в разделе «Запрос к базе данных»:

- Текст запроса.

  Введите SQL-запрос, производящий выборку необходимых данных из требуемого объекта БД (таблицы или представления). Запрос может содержать любые операторы, включая WHERE и JOIN.

  При использовании селектора * для выборки всех колонок, убедитесь, что колонки не содержат чувствительную информацию.

- Тип колонки сортировки.

  Выберите тип данных, хранящихся в колонке, используемой при сортировке.

- Колонка сортировки.

  Введите имя колонки, по значениям которой должны сортироваться записи в выборке. Формирование пакета записей производится по возрастанию отсортированных значений.

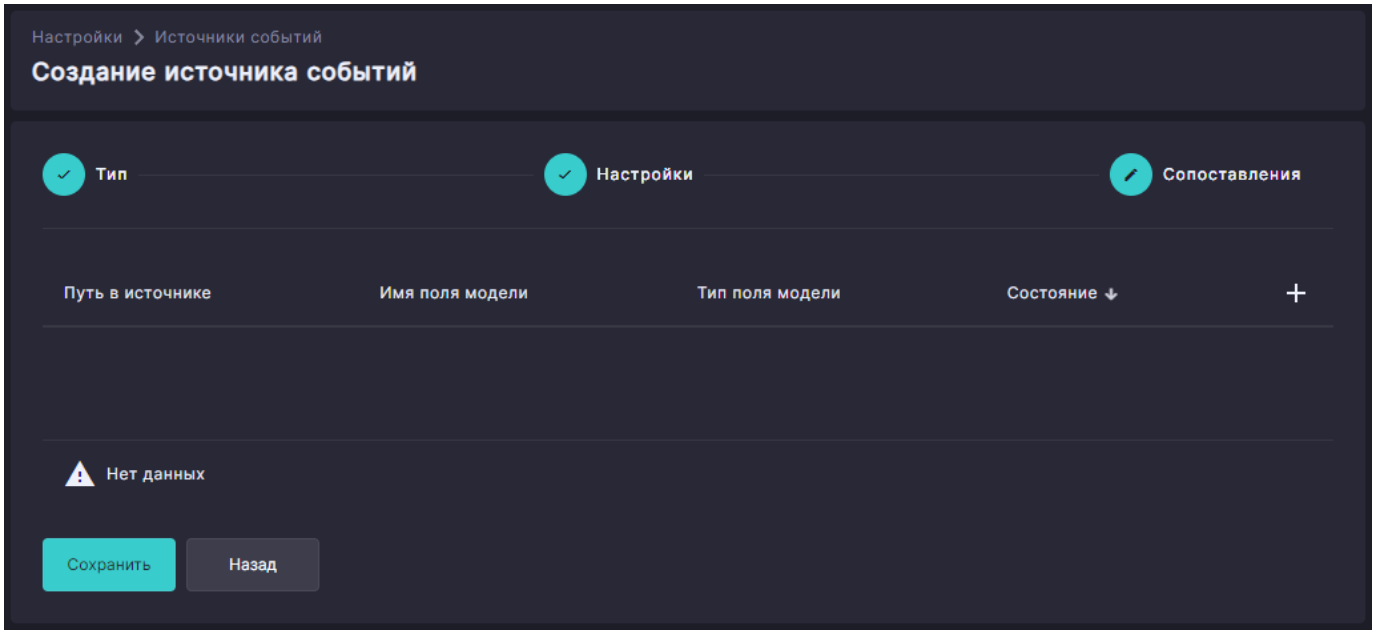
- Колонка даты создания события.

  Введите имя колонки, данные которой нужно хранить в системном поле **Event Created Date**.

- Ограничение количества записей.

  Задайте максимальное количество записей для передачи пакетом в хранилище Системы.

Страница «Сопоставления»



Создаваемый источник не содержит сопоставлений, поэтому таблица на данной странице пуста. Для задания каждого сопоставления необходимо указать:

- путь в источнике, назначаемый элементу парсером (обработчиком формата) исходного события;
- имя поля модели события.

В большинстве случаев путь в источнике не известен до получения исходных событий из этого источника. Следовательно, на этапе создания источника задание сопоставлений можно пропустить и завершить работу мастера конфигурации, нажав кнопку «Сохранить». Окно «Создание источника событий» закроется, и созданный источник добавится в таблицу модуля «Источники событий».

2.3.2 Проверка функционирования источника событий

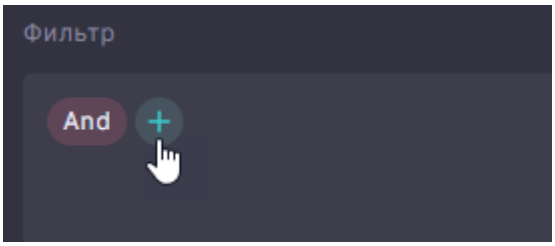
Следуйте инструкции ниже, чтобы убедиться, что настроенный для сбора событий источник функционирует корректно, и события, получаемые с использованием его характеристик, сохраняются в Системе.

1. Убедитесь, что на хостах-источниках производится активность, требуемая для генерации интересуемых событий.
2. Перейдите в модуль «Анализ данных».

   Отобразится таблица с подготовленными событиями, которые произошли за текущий день.
3. Нажмите значок  («Показать настройки фильтра») для открытия панели «Формирование данных».

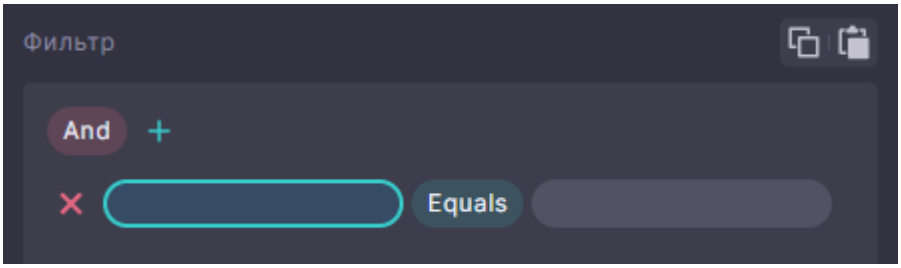
4. В секции «Фильтр» этой панели создайте фильтр по системному полю **Aegis Source**, используя графический конструктор критериев:

   - Нажмите значок + , отображаемый справа от блока **And** (логической операции группы).

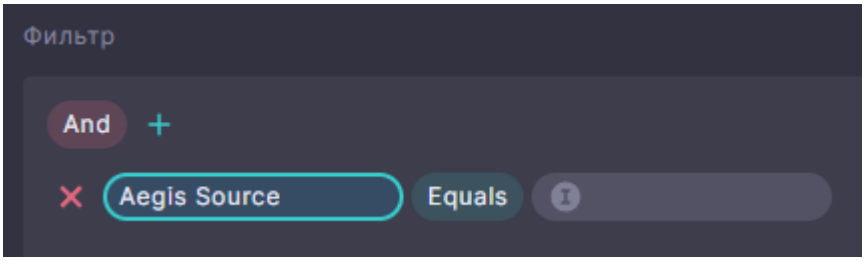
     

   - Из выпадающего меню выберите пункт «Добавить условие».

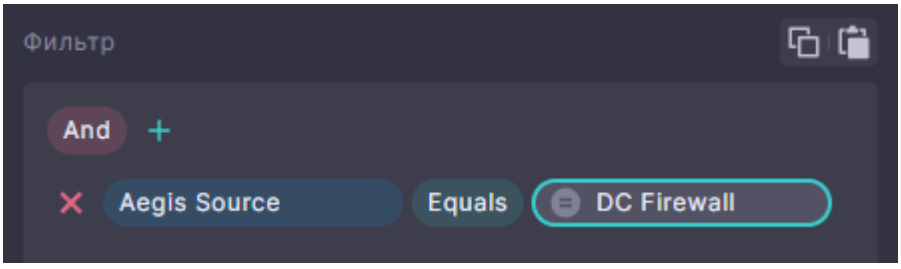
     Появится элемент условия с оператором **Equals**.

   - В элементе условия нажмите в блок левого операнда и из выпадающего списка выберите системное поле **Aegis Source**.

   - Нажмите в блок правого операнда и введите имя требуемого источника.

   - Нажмите кнопку «Применить» для применения фильтра к отображаемым событиям.

     Таблица с подготовленными событиями обновится, отображая события только этого источника.

5. Проверьте, отображаются ли в таблице события, характерные для произведенной на хостах-источниках активности. Для обновления содержимого таблицы нажмите клавишу `F5`.

   Если события отображаются, можно переходить к настройке правил нормализации и обогащения.

   Если события не отображаются, повторите этап настройки источника для сбора событий в режиме редактирования (см. ниже).

2.3.3 Редактирование источника событий

Редактирование можно производить в модуле «Источники событий» после перевода источника в режим редактирования открытием детальной информации по нему. В этом режиме можно изменить настройки источника и задать его сопоставления (правила нормализации). Инструменты редактирования аналогичны представленным в мастере конфигурации источника событий на страницах «Настройки» и «Сопоставления».

Изменение типа источника не доступно в режиме редактирования.

Для редактирования источника событий:

1. Перейдите в модуль «Источники событий».
2. Найдите в таблице запись с требуемым источником и откройте детальную информацию по нему одним из следующих способов:
   - Дважды щелкните мышью по записи.
   - Наведите указатель мыши на запись и нажмите контекстный значок () («Открыть детальную информацию»).

   Источник переведется в режим редактирования, а в открывшемся окне детальной информации по источнику отобразится таблица с его сопоставлениями. Таблица и ее функции аналогичны представленным в мастере конфигурации источника событий на странице «Сопоставления».
3. Для создания или редактирования сопоставлений используйте функции таблицы, описанные в разделах ниже.

   Предварительно выполните следующие действия:

   - Выберите поля модели события, которые будут использоваться для хранения данных элементов исходного события.

     Для просмотра существующих полей модели вы можете перейти в модуль «Поля модели события». При необходимости актуализируйте модель события и создайте в ней нужные поля.

   - Получите пути в источнике для тех элементов исходного события, данные которых будете сопоставлять выбранным полям модели события.
4. При необходимости отредактируйте настройки источника.

Создание сопоставления

В окне детальной информации по источнику нажмите значок + («Создать сопоставление») в заголовке таблицы сопоставлений, чтобы добавить в нее запись.

Далее в добавленной записи:

1. Введите путь в источнике, который будет использоваться сопоставлением.
2. Из выпадающего списка выберите имя поля модели, соответствующего введенному пути.

   Тип поля модели будет подставлен автоматически.

   В источнике не может быть создано больше одного сопоставления с одним и тем же полем модели события.
3. Задайте состояние (Включено/Выключено) сопоставления, выбрав соответствующий элемент из выпадающего списка.

   Выберите элемент «Включено» для использования сопоставления при нормализации.
4. Для завершения создания сопоставления выберите один из следующих вариантов:

   - Нажмите значок ✓ («Сохранить изменения»), чтобы создать сопоставление с введенными параметрами.

     Таблица сопоставлений обновится и отобразит созданное сопоставление с учетом примененной к таблице сортировки.

     Если созданное сопоставление включено, и источник событий тоже включен, оно начнет служить правилом нормализации событий этого источника.

   - Нажмите значок ✕ («Отменить изменения»), чтобы отказаться от создания сопоставления.

     Добавленная запись о сопоставлении будет удалена из таблицы, а все введенные в записи данные будут утеряны.

     Следующие действия приводят к аналогичному результату:

     - перевод записи, соответствующей другому сопоставлению, в режим редактирования;
     - создание новой записи нажатием значка + («Создать сопоставление») в заголовке таблицы;
     - выход из окна детальной информации по источнику нажатием значка ← («Вернуться назад»).

При необходимости созданные сопоставления можно отредактировать, как описано ниже.

Редактирование сопоставления

В окне детальной информации по источнику:

1. Найдите в таблице запись с требуемым сопоставлением.
2. Наведите указатель мыши на запись и нажмите контекстный значок (карандаш) («Редактировать сопоставление»), чтобы перевести запись в режим редактирования.

Далее в этой записи:

1. При необходимости измените путь в источнике, который будет использоваться сопоставлением.
2. При необходимости измените имя поля модели, соответствующего введенному пути, выбрав элемент из выпадающего списка.

   Тип поля модели будет изменен автоматически.

   В источнике не может быть создано больше одного сопоставления с одним и тем же полем модели события.
3. При необходимости измените состояние (Включено/Выключено) сопоставления, выбрав соответствующий элемент из выпадающего списка.

   Выберите элемент «Включено» для использования сопоставления при нормализации.
4. Для завершения редактирования сопоставления выберите один из следующих вариантов:

   - Нажмите значок (галочка) («Сохранить изменения»), чтобы применить изменения к параметрам сопоставления.

     Таблица сопоставлений обновится и отобразит измененное сопоставление с учетом примененной к таблице сортировки.

     Если созданное сопоставление включено, и источник событий тоже включен, оно будет служить правилом нормализации событий этого источника.

   - Нажмите значок (крестик) («Отменить изменения»), чтобы отказаться от применения изменений к параметрам сопоставления.

     Все изменения в записи будут утеряны.

     Следующие действия приводят к аналогичному результату:

     - перевод записи, соответствующей другому сопоставлению, в режим редактирования;
     - создание новой записи нажатием значка (плюс) («Создать сопоставление») в заголовке таблицы;
     - выход из окна детальной информации по источнику нажатием значка (стрелка влево) («Вернуться назад»).

Редактирование настроек источника

1. В окне детальной информации по источнику нажмите значок 🔧 («Редактировать настройки»).

   Откроется окно «Редактирование настроек источника событий». Состав полей этого окна аналогичен отображающемуся в мастере конфигурации источника событий на странице «Настройки» при создании источника.

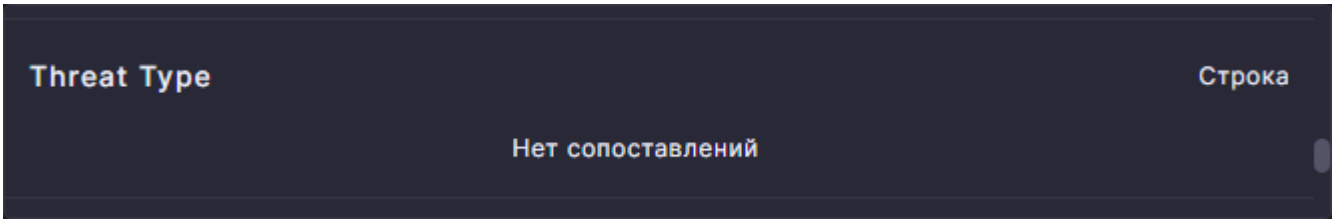
2. При необходимости внесите изменения в данные, отображенные в полях окна.
3. Нажмите кнопку «Сохранить».

Окно «Редактирование настроек источника событий» закроется, и внесенные изменения применятся к источнику.

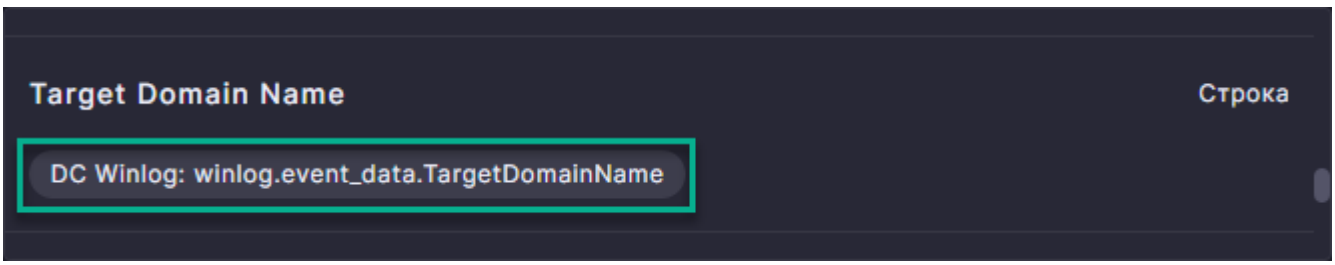
2.4 Нормализация событий

По умолчанию в процессе нормализации исходных событий функционирующего источника участвуют только управляемые Системой правила, заполняющие значениями системные поля модели. Вы можете дополнить эти правила нормализации своими, задав сопоставления в источниках событий. Для этого откройте источник в режиме редактирования и заполните его таблицу сопоставлений.

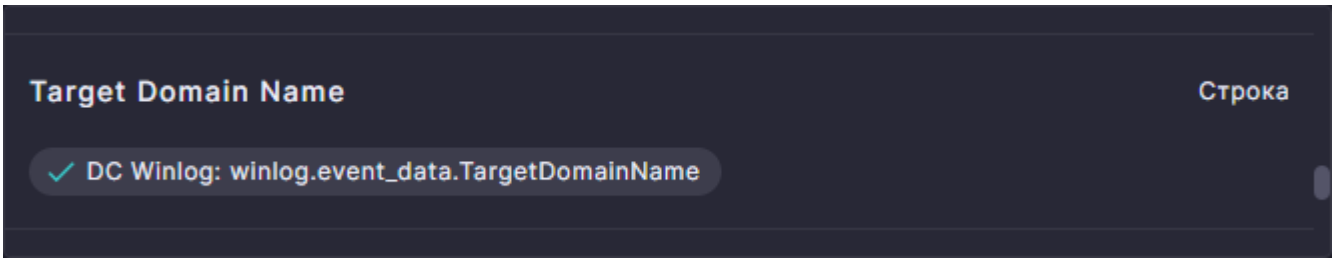
Чтобы определить, какие поля модели события используются в сопоставлениях и правилах нормализации, перейдите в модуль «Поля модели события». Не используемые в сопоставлениях поля модели отображаются с надписью «Нет сопоставлений».



У полей модели, используемых в сопоставлениях, отображаются элементы, идентифицирующие эти сопоставления. Данные элементы включают в себя имя источника и через двоеточие с пробелом путь в источнике, указанный в сопоставлении.



Сопоставления, служащие правилами нормализации, отмечаются в элементах значком ✓ слева от имени источника. Правилами нормализации служат все сопоставления включенных источников при условии, что сами сопоставления имеют состояние "Включено".



Вы можете открыть источник в режиме редактирования и перейти к таблице его сопоставлений непосредственно из элемента, нажав в нем на имени источника. Возможности режима редактирования описаны в этом разделе.

2.4.1 Получение пути в источнике

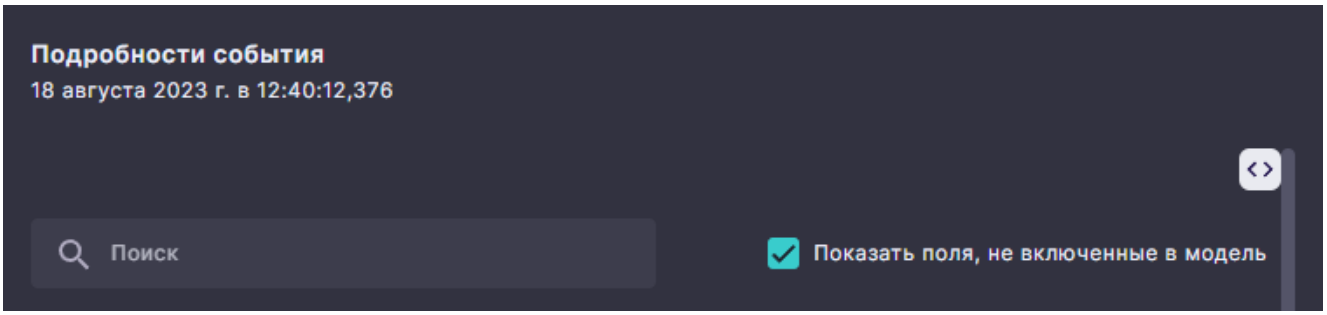
1. Перейдите в модуль «Анализ данных».

   Отобразится таблица с подготовленными событиями, которые произошли за текущий день.

2. Найдите в таблице требуемое событие и отобразите его данные, используя боковую панель с подробностями события, как описано в этом разделе.

В открывшейся панели:

1. Установите флажок «Показать поля, не включенные в модель».

   В списке под полями модели отобразятся поля, не включенные в модель события. Каждое такое поле вместо имени отображает строковый ключ, идентифицирующий относящийся к полю элемент данных исходного события. Этот ключ и является путем в источнике.

2. Найдите в списке нужный путь и выделите его мышью.

3. Нажмите комбинацию клавиш `^ Ctrl` + `C` или используйте команду контекстного меню, чтобы скопировать выделенный текст в буфер обмена.

   При редактировании источника событий и задании сопоставления в модуле «Источники событий» можно вставить путь из буфера обмена в соответствующее поле, нажав комбинацию клавиш `^ Ctrl` + `V` или использовав команду контекстного меню.

2.5 Обогащение событий

Система позволяет обогащать следующие события:

- События, прошедшие нормализацию (нормализованные события).

  Правила обогащения для этих событий задаются в модуле «Правила обогащения».

- События, прошедшие нормализацию и обогащение (подготовленные события), которые удовлетворяют условиям правил корреляции.

  Эти события обогащаются в соответствии с описаниями действий по обогащению, заданных в этих правилах с использованием модуля «Правила корреляции».

2.5.1 Управление правилами обогащения

Для управления правилами обогащения нормализованных событий перейдите в модуль «Правила обогащения» и воспользуйтесь его функциями, как описано ниже. Все созданные правила обогащения отображаются в модуле в виде таблицы.

Создание правила обогащения

1. Нажмите значок + («Создать правило»), чтобы открыть окно «Новое правило».
2. Введите уникальное имя правила.
3. При необходимости введите описание правила.
4. Задайте фильтр для выборки целевых событий, к которым будет применяться правило.
5. Задайте действия по обогащению, производимые с полями этих событий, как описано в разделе ниже.

   Данные действия будут производиться индивидуально с каждым целевым событием.
6. Переведите переключатель параметра «Состояние» в правое положение («Включено») для включения правила в процесс обогащения событий.
7. Нажмите кнопку «Применить».

Окно «Новое правило» закроется, и созданное правило отобразится в таблице правил.

Редактирование правила обогащения

1. Найдите в таблице запись с требуемым правилом и откройте детальную информацию по нему одним из следующих способов:
   - Дважды щелкните мышью по записи.
   - Наведите указатель мыши на запись и нажмите контекстный значок (карандаш) («Редактировать правило»).

Правило переведется в режим редактирования, а в открывшемся окне детальной информации по правилу отобразятся его настройки.

2. При необходимости измените настройки правила.

   Состав настроек и инструменты их редактирования аналогичны представленным в окне «Новое правило».

3. Для завершения редактирования правила выберите один из следующих вариантов:

   - Нажмите кнопку «Применить», чтобы применить изменения к правилу.

     Окно детальной информации по правилу закроется, и таблица правил будет обновлена.

     Если правило включено, оно будет использоваться для обогащения целевых событий.

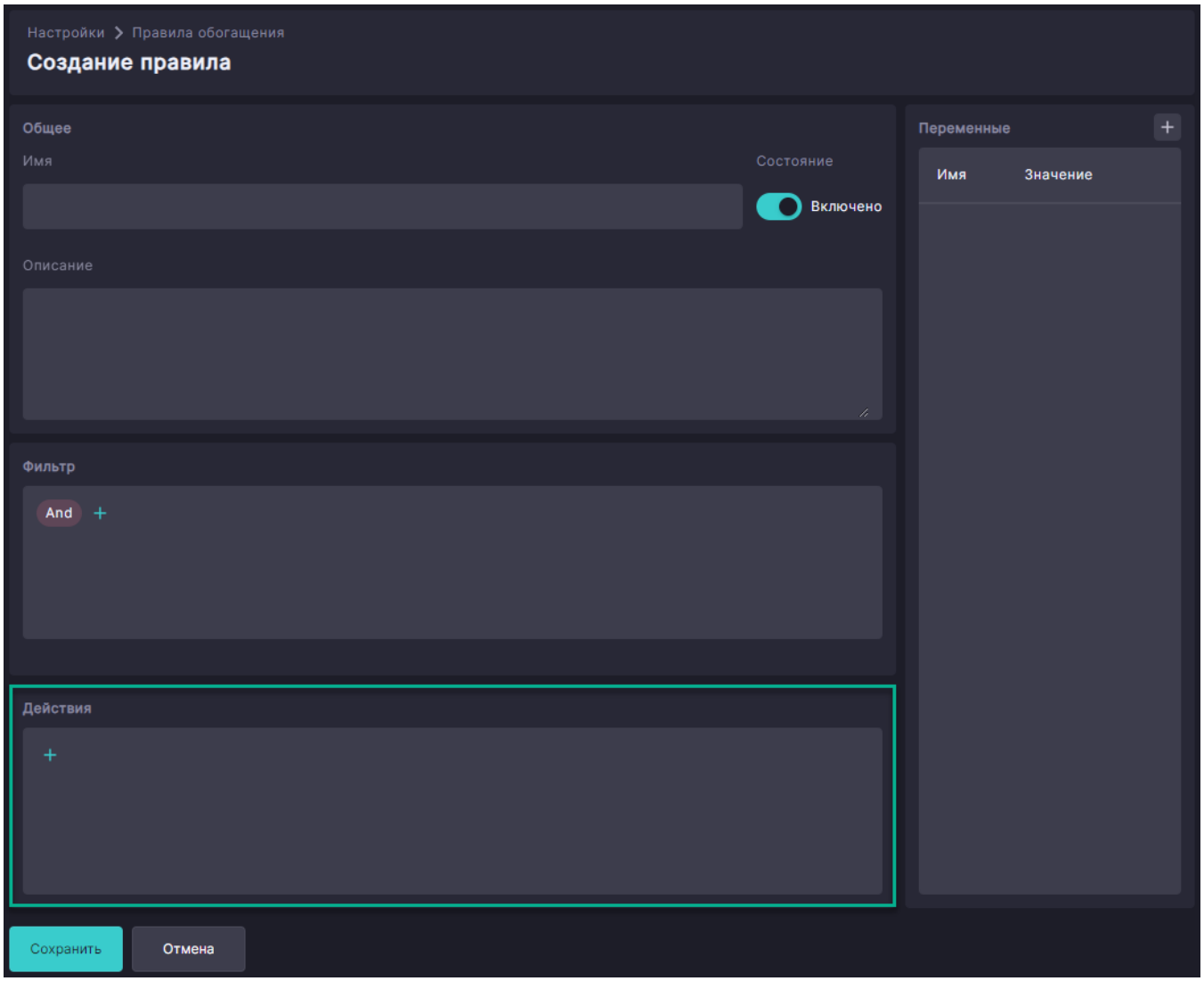
   - Нажмите кнопку «Отмена», чтобы отказаться от применения изменений к правилу.

     Все изменения настроек правила будут утеряны.

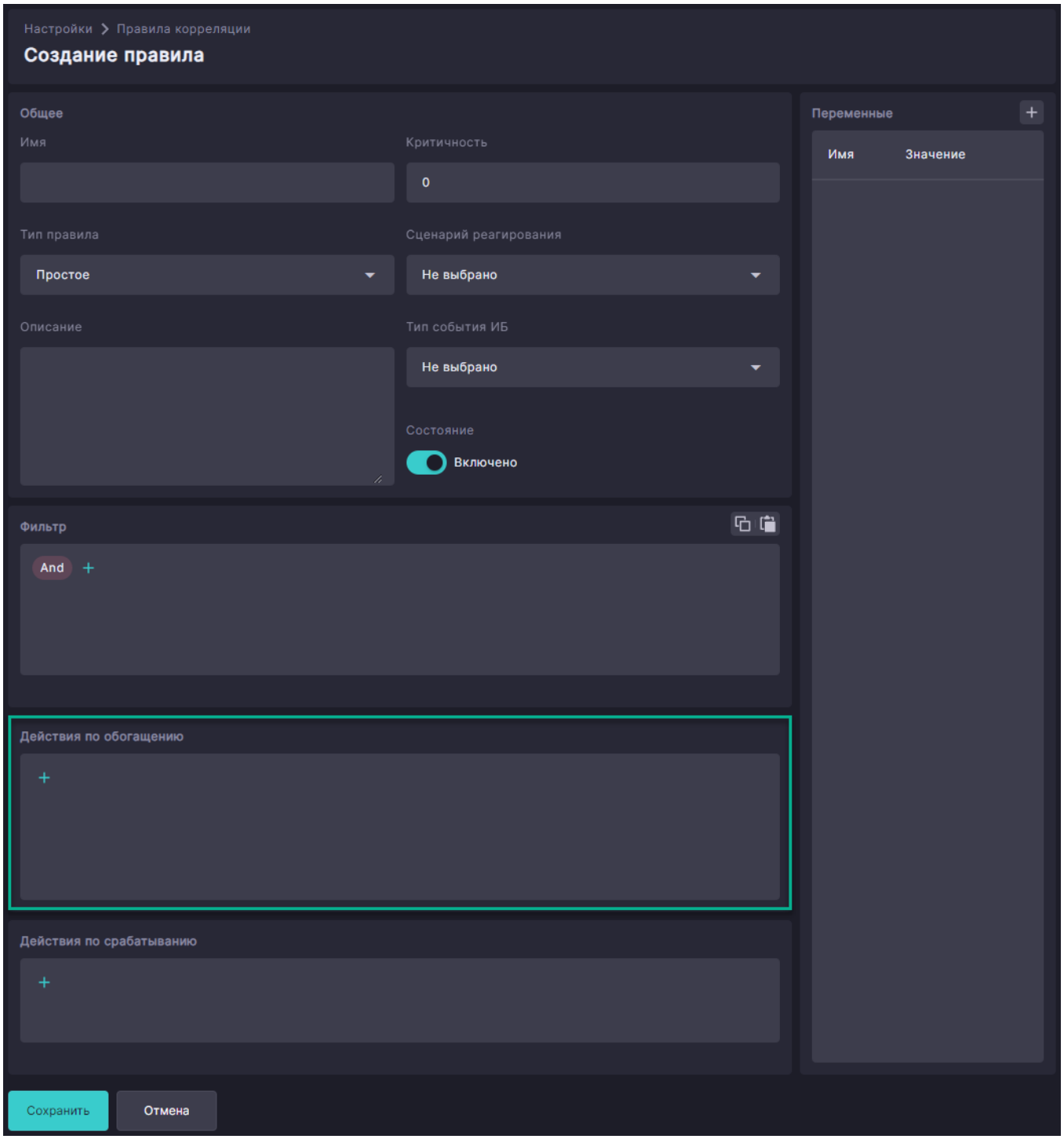
2.5.2 Настройка действий по обогащению

Система позволяет настроить действия по обогащению целевых событий с помощью специализированного инструмента, расположенного в следующих панелях:

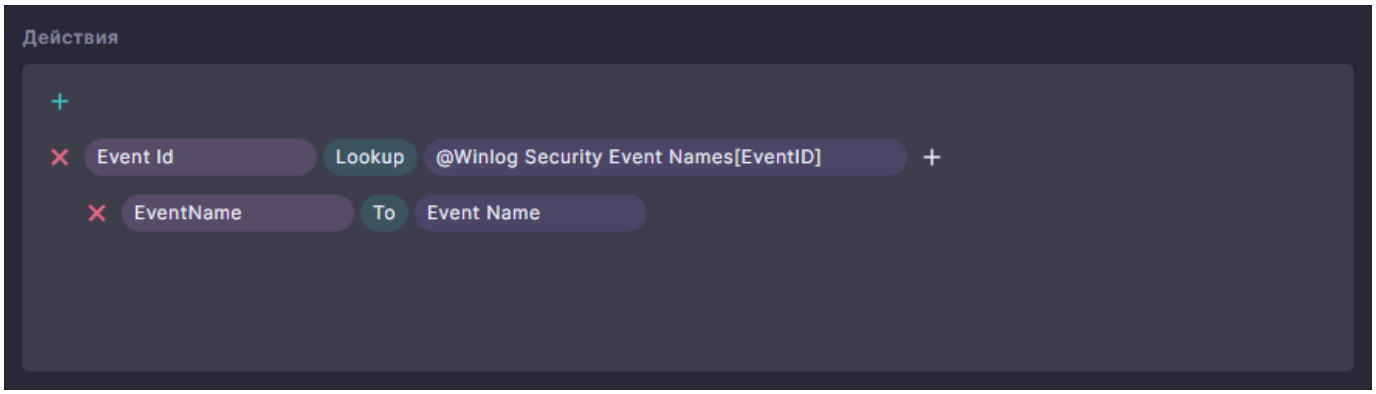
- панель «Действия» в модуле «Правила обогащения»;



- панель «Действия по обогащению» в модуле «Правила корреляции».



Инструмент отображает последовательность действий по обогащению в виде настраиваемого списка, каждый элемент которого определяет производимую операцию и ее параметры. Наименование операции и значения параметров указываются в блоках элемента. Операции будут выполняться в порядке следования элементов списка.

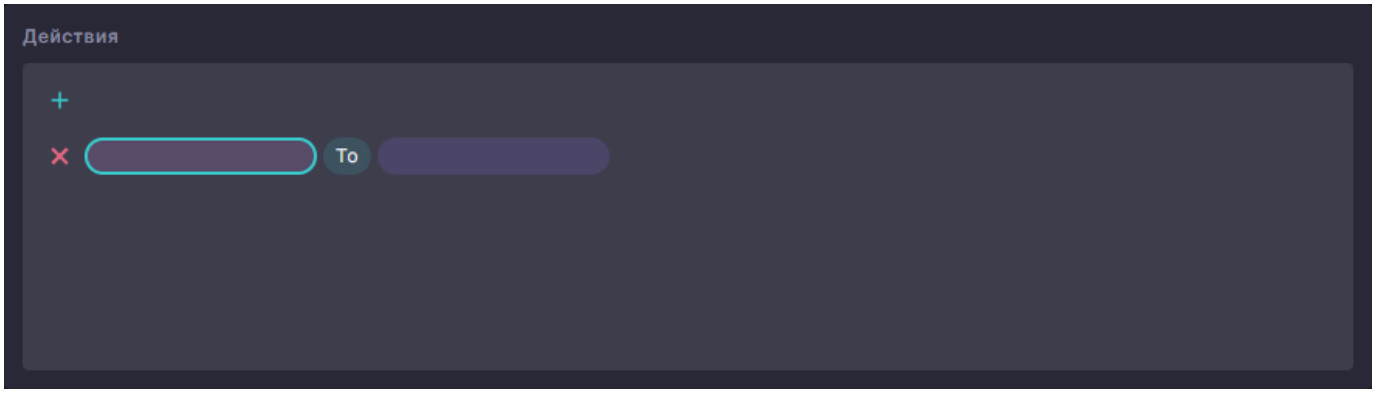


Изначально список действий пуст. Вы можете заполнить его, как описано ниже.

Создание действия

Нажмите значок + , отображаемый в начале списка, чтобы создать действие.

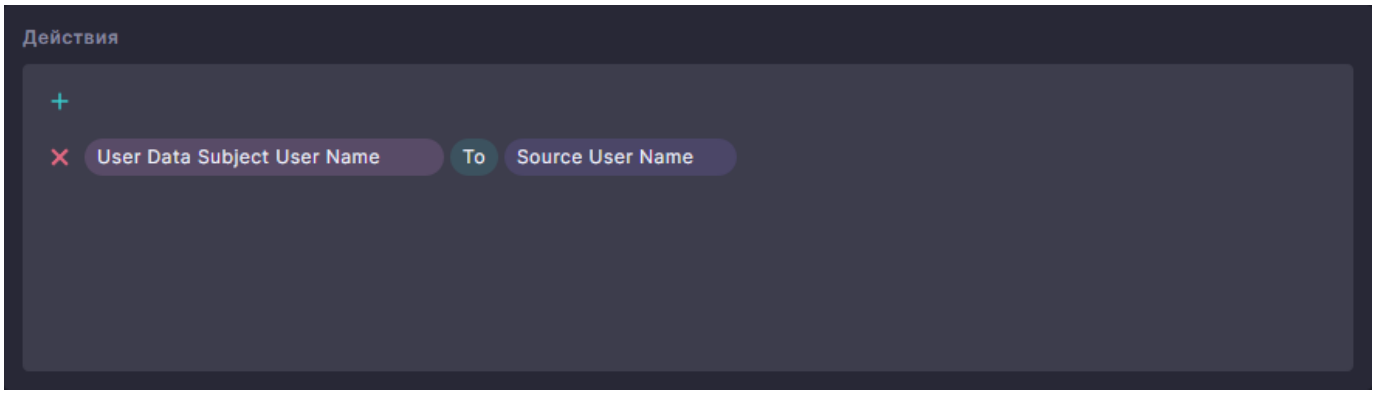
Действие будет добавлено в конец списка.



В созданном действии задана только операция присваивания значения (**To**). Параметры этой операции (левый и правый операнды) не заданы.

Вы можете настроить операцию и параметры операции, задав значения в соответствующих блоках. Для задания операции нажмите на блок операции (оператора) и выберите ее наименование из выпадающего списка.

ОПЕРАЦИЯ ПРИСВАИВАНИЯ ЗНАЧЕНИЯ (TO)



Данная операция присваивает значение (левый операнд) полю целевого события (правый операнд).

Параметры операции:

- Значение (левый операнд).

  Доступные варианты:

  - Переменная.

    Нажмите на блок левого операнда и выберите из выпадающего списка переменную, из которой берется значение.

    Имя переменной начинается с символа $.

  - Поле.

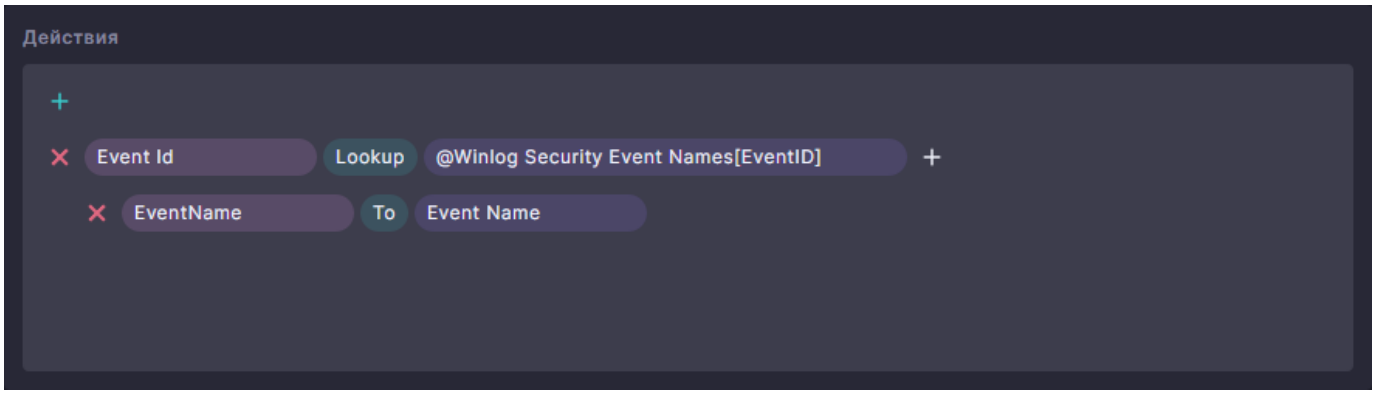
    Нажмите на блок левого операнда и выберите из выпадающего списка поле целевого события, из которого будет браться значение.

- Поле (правый операнд).

  Нажмите на блок правого операнда и выберите из выпадающего списка поле целевого события, которому будет присваиваться значение.

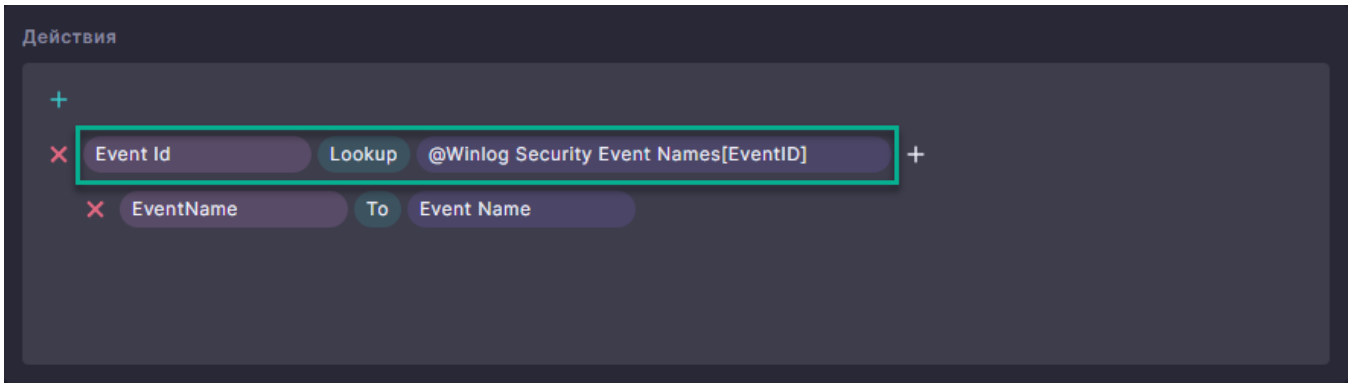
  Список содержит только поля, тип данных которых соответствует этому значению.

ОПЕРАЦИЯ ПРИСВАИВАНИЯ ЗНАЧЕНИЙ ИЗ СПРАВОЧНИКА (LOOKUP)

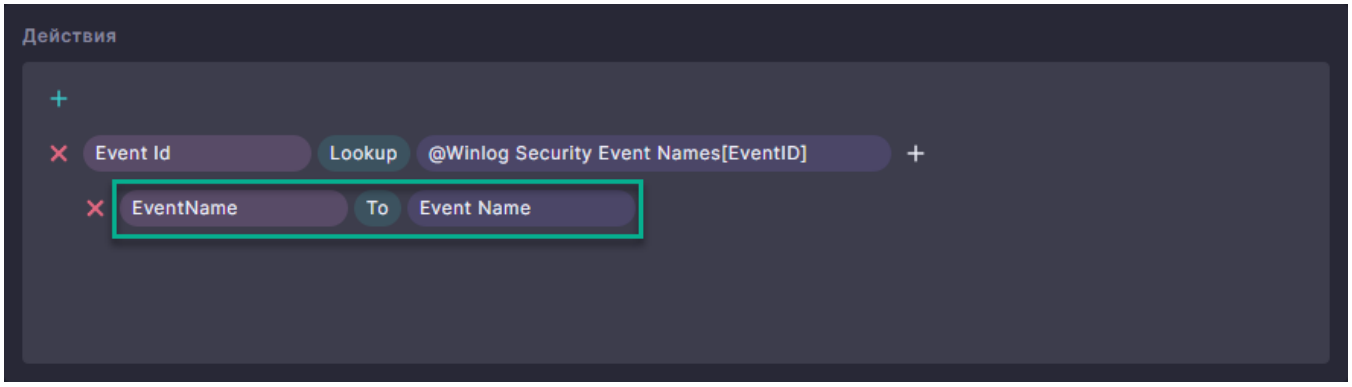


Данная операция состоит из подопераций, выполняющих:

- поиск строки справочника, содержащей заданное значение поля из целевого события;



- если строка найдена, присвоение значений полей из этой строки заданным полям целевого события.



Параметры подоперации поиска строки:

- Значение (левый операнд).

  Доступные варианты:

  - Переменная.

    Нажмите на блок левого операнда и выберите из выпадающего списка переменную, чье значение берется для поиска в справочнике.

    Имя переменной начинается с символа $.

  - Поле.

    Нажмите на блок левого операнда и выберите из выпадающего списка поле целевого события, чье значение берется для поиска в справочнике.

- Поле (правый операнд).

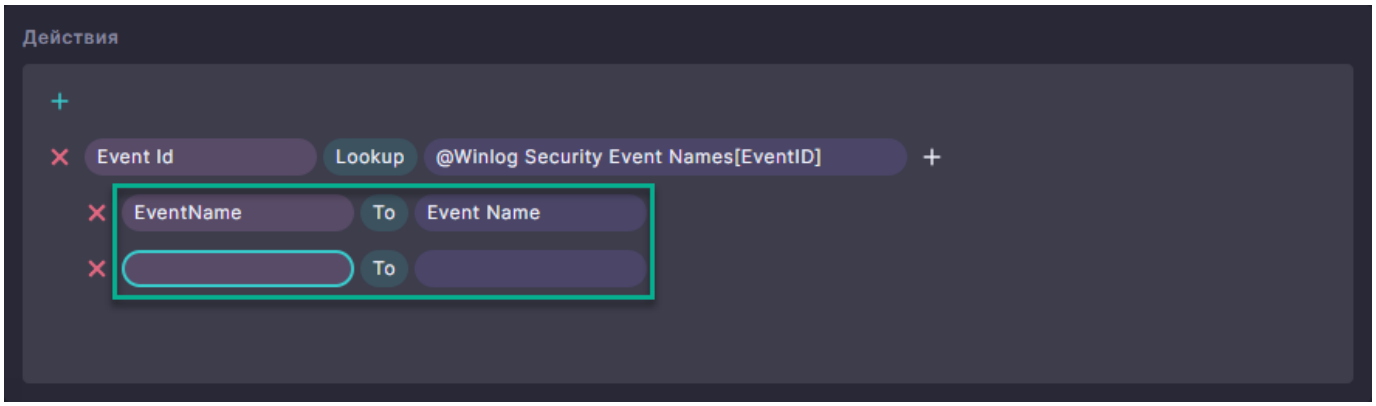
  Нажмите на блок правого операнда и выберите из выпадающего списка справочник, а затем в раскрывшемся списке поле, в значениях которого производится поиск значения левого операнда.

  Список содержит только справочники с полями, тип данных которых соответствует этому значению.

  Выбранные справочник и поле отображаются в блоке правого операнда следующим образом:

  `@имя справочника[имя поля]`

Нажмите значок + , отображаемый справа от блока правого операнда, чтобы создать одно и более подопераций присваивания значений строки. Эти подоперации будут отображены в виде дочерних элементов **Lookup** операции.



В отличие от стандартных операций присваивания описанных выше, подоперации присваивания позволяют использовать в левых операндах только поля справочника.

Параметры подопераций присваивания:

- Значение (левый операнд).

  Нажмите на блок левого операнда и выберите из выпадающего списка поле справочника, значение которого берется в найденной строке.

- Поле (правый операнд).

  Нажмите на блок правого операнда и выберите из выпадающего списка поле целевого события, которому присваивается значение.

  Выпадающий список содержит только имена полей, тип данных которых соответствует этому значению.

Удаление действия

Нажмите значок ✕, отображаемый у элемента списка слева от блока левого операнда, чтобы удалить этот элемент.

Вместе с удаляемым элементом будут удалены и его дочерние элементы.

3. Мониторинг и контроль

Данный раздел описывает задачи по оперативному выявлению (актуальных и потенциальных) угроз ИБ и аномальной активности, решаемые с помощью Системы.

- оперативно выявлять актуальные и потенциальные угрозы ИБ и аномальной активности;
- модифицировать конфигурацию Системы;
- контролировать непрерывность и надежность работы процесса мониторинга, настраивая доступ пользователей к данным и функциям Системы.

3.1 Поиск событий, соответствующих определенным критериям

Для оперативного выявления актуальных и потенциальных угроз ИБ и аномальной активности на защищаемых информационных ресурсах необходимо производить поиск событий, удовлетворяющих/соответствующих определенным критериям:

- используя правила корреляции;
- выявляя события вручную.

3.1.1 Поиск с использованием правил корреляции

Критерии поиска событий задаются в правилах корреляции. Поиск событий осуществляется автоматически запущенными правилами корреляции. Для управления правилами корреляции перейдите в модуль «Правила корреляции» и воспользуйтесь его функциями, как описано в этом разделе.

3.1.2 Поиск вручную с использованием критериев выявления

Для выполнения поиска событий перейдите в модуль «Анализ данных» и задайте критерии в параметрах поиска, используя инструменты модуля.

3.2 Регистрация событий и инцидентов ИБ на основе результатов поиска

На основе выявленных в результате поиска событий необходимо зарегистрировать событие ИБ для его дальнейшей обработки, включая связанные данные и иную вспомогательную информацию, расширяющую его контекст.

3.2.1 Регистрация с использованием правил корреляции

Регистрация событий ИБ на основе результатов поиска осуществляется автоматически для запущенных правил корреляции. Связывание новых возникающих событий, удовлетворяющих критериям этих правил, с зарегистрированными событиями ИБ также осуществляется автоматически.

3.2.2 Регистрация вручную

Регистрация события ИБ на основе событий, выявленных с использованием инструментов поиска модуля «Анализ данных», можно производить непосредственно в этом модуле, как описано в этом разделе. При возникновении новых событий, удовлетворяющих критериям выявления, их связывание с зарегистрированными событиями ИБ также необходимо производить вручную.

3.3 Обработка зарегистрированных событий и инцидентов ИБ

Данные зарегистрированного события ИБ отображаются/представлены в его карточке, которую можно открыть из таблицы модуля «События ИБ» одним из следующих способов:

- Дважды щелкните мышью по событию.
- Наведите указатель мыши на событие и нажмите контекстный значок  .

В рамках обработки производятся следующие действия:

- анализ событий, связанных с событием ИБ, с целью определения ложных срабатываний и инцидентов;
- назначение инцидентам категории;
- выполнение управляющих действий в карточке события/инцидента ИБ согласно процессной модели;
- внесение комментариев и/или файлов в карточку события/инцидента ИБ в виде записей журнала на основе обнаруженных фактов;
- инициирование процессов реагирования на события и инциденты ИБ и расследования инцидентов.

3.4 Настройка доступа к данным и функциям Системы

Система позволяет настроить многопользовательский доступ к своим данным и функциям и определить задачи, которые пользователи могут выполнять с их помощью. Совокупность таких задач определяется группой. Иными словами, группа описывает некоторую роль пользователя в Системе. Пользователь может входить в одну или несколько групп. Группа наделяет своих пользователей единым набором прав на действия с объектами/сущностями Системы. Можно создать любое количество групп и задать каждой требуемые права пользователей.

Для регистрации пользователя в Системе необходимо создать его учетную запись (УЗ). Настройка доступа пользователя как к самой Системе, так и к ее данным и функциям осуществляется через параметры УЗ пользователя. Добавление пользователя в одну или несколько групп также осуществляется/производится параметрами УЗ. Для управления УЗ пользователей перейдите в модуль «Пользователи» и воспользуйтесь его функциями.

Группы пользователей и права каждой из групп на действия с объектами/сущностями Системы задаются в конфигурации Системы.

3.4.1 Создание УЗ пользователя

Система предоставляет следующие возможности создания УЗ пользователей:

- ввод данных вручную индивидуально для каждого пользователя;
- импорт данных о пользователях из Active Directory.

Ввод данных вручную

1. Нажмите кнопку + («Создать пользователя») и выберите пункт «Вручную» из выпадающего меню.

   Откроется окно «Создание пользователя», в котором можно задать данные УЗ пользователя.
2. Введите уникальный в рамках Системы логин пользователя, который будет использоваться для входа в Систему.
3. При необходимости введите полное имя пользователя.

   Данное имя будет идентифицировать пользователя в графическом интерфейсе Системы. Если имя не задано, для идентификации будет использоваться логин пользователя.
4. Введите пароль пользователя, который будет использоваться для входа в Систему.
5. Переведите переключатель параметра «Доступ к Системе» в правое положение («Разрешен»), чтобы разрешить пользователю входить в Систему, используя данные УЗ.
6. Добавить пользователя в одну или несколько групп пользователей, установив флажок напротив нужного наименования группы.
7. Нажмите кнопку «Сохранить».

Окно «Создание пользователя» закроется, и данные созданной УЗ отобразятся в таблице пользователей. Созданная таким образом УЗ имеет тип "Локальная УЗ".

Импорт данных из Active Directory

1. Нажмите кнопку + («Создать пользователя») и выберите пункт «Импортировать из Active Directory» из выпадающего меню.

Откроется окно «Импортирование из Active Directory», в котором можно ввести данные доменной УЗ (логин и пароль). Эти данные будут использованы для подключения к Active Directory и получения данных УЗ пользователей, зарегистрированных в домене..

2. Введите доменное имя и пароль пользователя, которые будут использоваться для подключения к Active Directory.
3. Нажмите кнопку «Показать пользователей».

   Далее происходит авторизация и подключение к Active Directory с использованием введенных данных. При успешном выполнении этих операций в окне отобразится таблица с данными УЗ пользователей, которые еще не зарегистрированы в Системе.
4. Установите флажок напротив УЗ пользователей, которых необходимо зарегистрировать в Системе.
5. Для каждой отмеченной флажком УЗ выберите одну или несколько групп пользователей, в которые пользователь должен быть добавлен при импорте.
6. Нажмите кнопку «Импортировать».

Для каждого выбранного в окне пользователя в Системе будет создана УЗ, связанная с соответствующей доменной УЗ. Созданная таким образом УЗ имеет тип "Доменная УЗ". Для входа в Систему пользователь с такой УЗ должен вводить данные своей доменной УЗ.

После этого окно «Импортирование из Active Directory» закроется, и данные созданных УЗ отобразятся в таблице пользователей.

3.4.2 Редактирование УЗ пользователя

1. Найдите в таблице запись с требуемым пользователем и откройте для него окно «Редактирование пользователя» одним из следующих способов:
   - Дважды щелкните мышью по записи.
   - Наведите указатель мыши на запись и нажмите контекстный значок  («Редактировать пользователя»).

   В открывшемся окне отобразятся параметры УЗ пользователя. Тип УЗ отображается под заголовком окна.
2. При необходимости измените параметры УЗ.

   Состав параметров и инструменты их редактирования аналогичны представленным в окне «Создание пользователя».

   Для УЗ типа "Доменная УЗ" логин и пароль не доступны для редактирования.

3. Для завершения редактирования параметров УЗ выберите один из следующих вариантов:

   - Нажмите кнопку «Сохранить», чтобы применить изменения к УЗ.

     Окно «Редактирование пользователя» закроется, и таблица пользователей будет обновлена.

   - Нажмите кнопку «Отмена», чтобы отказаться от применения изменений к УЗ.

     Все изменения параметров УЗ будут утеряны.

3.5 Контроль непрерывности и надежности работы процесса мониторинга

Для осуществления контроля Система предоставляет инструменты для отображения и оценки следующей информации:

- Оперативная сводка по показателям надежности защиты от угроз ИБ.

  Позволяют своевременно реагировать на превышение пороговых значений показателя SLA и эскалировать инциденты ИБ.

- Метрики состояния процесса мониторинга.

  Включают статистические данные, информацию по критическим функциям ситуационного центра по ИБ и индикаторы нахождения метрик в заданных пользователем рамках.

К инструментам для осуществления контроля относятся:

- операционные и статистические дашборды (настраиваемые панели индикаторов), представленные в модулях «Работа смены» и «Статистический дашборд»;
- панель с показателем SLA (соглашения об уровне обслуживания), отображаемая в карточках событий/инцидентов ИБ модуля «События ИБ».

4. Расследование

Расследование позволяет определить характеристики угрозы (критичность, взаимосвязи, масштабы, источник кибератаки, ее вектор проникновения и инструментарий), представляемой инцидентом ИБ, с целью последующего инициирования процесса реагирования на угрозу. В ходе расследования изучаются детали инцидента ИБ по расширенному контексту, используя связанные данные и иную вспомогательную информацию, в том числе результаты ретроспективного анализа.

Данный раздел описывает инструменты, предоставляемые Системой для выполнения/решения этих задач.

4.1 Изучение деталей расследуемого инцидента ИБ

1. Перейдите в модуль «События ИБ».

   Все зарегистрированные события и инциденты ИБ отображаются в модуле в виде таблицы. Если в процессной модели организации используются линии обработки событий и инцидентов ИБ, можно перейти при необходимости на соответствующую линию, нажав на ее имени в списке модулей Системы. Таблица отобразит события/инциденты ИБ на выбранной линии.

2. Найдите в таблице требуемый инцидент.

   Для быстрого поиска можно воспользоваться фильтрацией и/или сортировкой, предоставляемыми таблицей.

3. Изучите детали инцидента, отображаемые в колонках таблицы.

   Для удобства можно отобразить детали в виде списка полей и их данных, используя боковую панель. Для этого выберите инцидент в таблице и нажмите значок  («Открыть детальную информацию»), чтобы открыть панель.

4.2 Изучение данных расширенного контекста расследуемого инцидента ИБ

Расширенный контекст позволяет определить взаимосвязи, масштабы и критичность угрозы, представляемой расследуемым инцидентом ИБ. Данные расширенного контекста отображаются/представлены в карточке инцидента, которую можно открыть из таблицы модуля «События ИБ» одним из следующих способов:

- Дважды щелкните мышью по инциденту.
- Наведите указатель мыши на инцидент и нажмите контекстный значок  («Открыть детальную информацию»).

4.2.1 Получение дополнительной информации из собранных событий

Данный этап необходим для уточнения характеристик угрозы, представляемой расследуемым инцидентом. Для получения дополнительной информации перейдите в модуль «Анализ данных», чтобы произвести поиск событий, удовлетворяющих критериям обнаружения. При обнаружении аномальной активности, индикаторов компрометации, вы можете произвести обработку инцидента с выполнением управляющих действий в карточке инцидента согласно процессной модели.

На основе обнаруженных фактов можно добавлять комментарии и/или файлы в карточку инцидента в виде записей журнала.

4.3 Проведение ретроспективного анализа

Данный этап завершает расследование инцидента.

На данном этапе производится:

- сбор артефактов кибератаки и восстановление ее хронологии;
- определение вектора проникновения, источник и инструментарий кибератаки;
- составление сценария кибератаки, на основе которого дополняются данные по масштабу и критичности *расследуемого* инцидента.

  На основе составленного сценария вы можете дополнить данные по масштабу и критичности *расследуемого* инцидента,

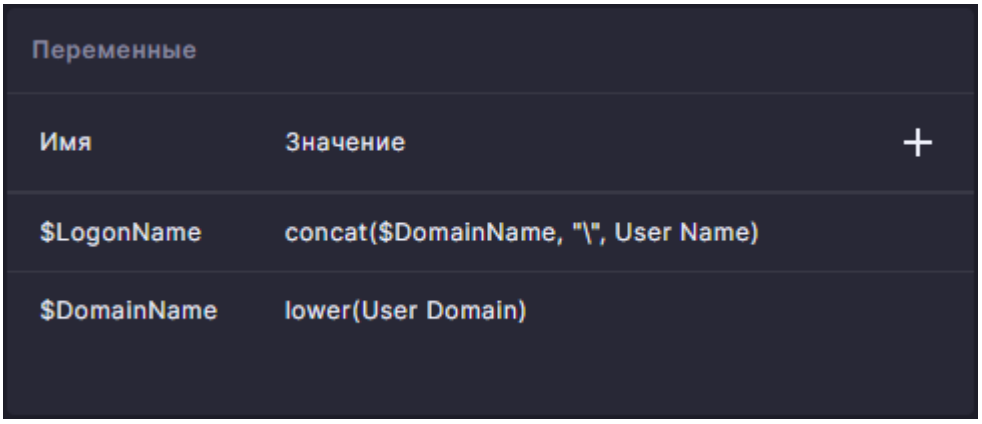
5. Работа с переменными

Переменная позволяет хранить значение поддерживаемого типа данных и многократно использовать это значение в той сущности Системы, где переменная была объявлена:

- правило корреляции;
- правило обогащения;
- фильтр панели «Формирование данных».

Вы можете создавать, редактировать и удалять переменные, используя функции таблицы «Переменные», отображаемой в модулях:

- «Анализ данных»;
- «Правила корреляции»;
- «Правила обогащения».



Объявление переменной содержит:

- Имя.

  Должно начинаться с символа $ и не содержать пробелы. Имена должны быть уникальными в рамках таблицы.

- Значение.

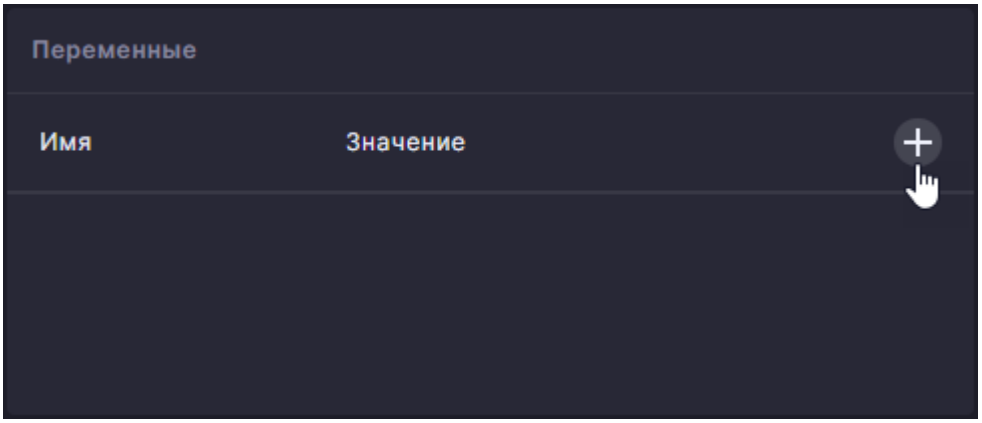
  Константа или результат преобразования одного или более значений полей события или других переменных, используя функции преобразования. Значения переменных вычисляются на момент:

  - выборки целевых событий, удовлетворяющих критериям фильтров;
  - применения действий по обогащению к этим событиям.

  Порядок следования переменных в таблице не влияет на вычисления.

5.1 Создание переменной

Нажмите значок + («Создать переменную») над таблицей «Переменные», чтобы добавить в нее запись.



Далее в добавленной записи:

1. Введите символ $ и уникальное в рамках таблицы имя переменной без пробелов.
2. Введите значение переменной, которым может служить:

   - Константа.

     Введите значение в формате одного из поддерживаемых типов данных. Для введения строки заключите ее в кавычки (").

   - Выражение преобразования.

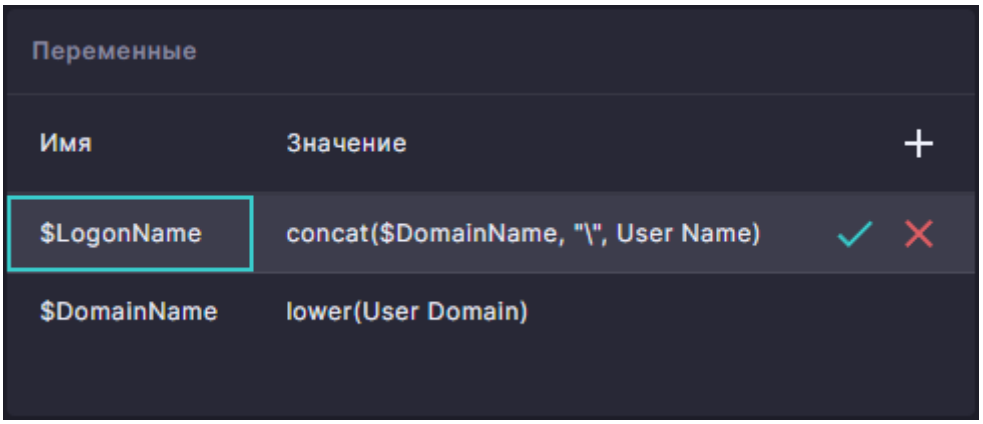
     Введите текстовое выражение, определяющее преобразование значений одного или нескольких полей события или другой переменной, используя функции преобразования.

     Пример применения функции **lower** к значению поля **User Domain**:

     ```
     lower(User Domain)
     ```

     Пример применения функции **concat** для конкатенации значения переменной **$DomainName**, строковой константы (символ обратной косой черты) и значения поля **User Name**:

     ```
     concat($DomainName, "\", User Name)
     ```



3. Для завершения создания переменной выберите один из следующих вариантов:

   - Нажмите значок ✓ («Сохранить изменения»), чтобы создать переменную с введенными параметрами.

     Созданная переменная добавится в таблицу.

   - Нажмите значок ✕ («Отменить изменения»), чтобы отказаться от создания переменной.

     Добавленная запись о переменной будет удалена из таблицы, а все введенные в записи данные будут утеряны.

     Следующие действия приводят к аналогичному результату:

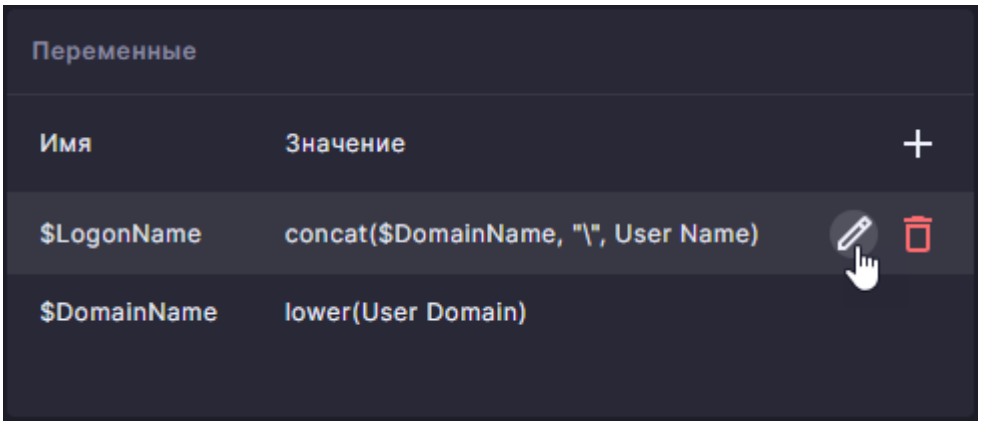
     - перевод записи, соответствующей другой переменной, в режим редактирования;
     - создание новой переменной, нажав значок + («Создать переменную») над таблицей.

При необходимости созданные переменные можно отредактировать или удалить, как описано ниже.

5.2 Редактирование переменной

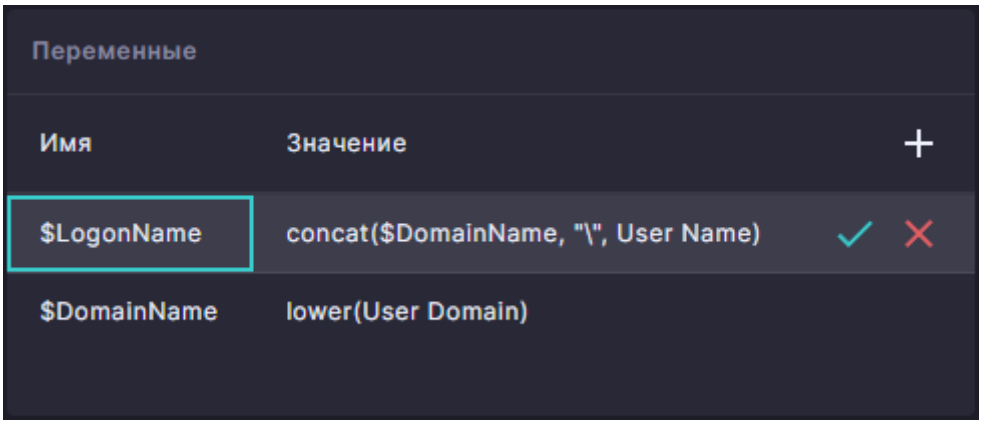
В таблице «Переменные»:

1. Найдите запись с требуемой переменной.
2. Наведите указатель мыши на запись и нажмите контекстный значок ✎ («Редактировать переменную»), чтобы перевести запись в режим редактирования.



Далее в этой записи:

1. При необходимости введите новое, уникальное в рамках таблицы имя переменной.
2. При необходимости измените значение переменной, отредактировав константу или выражение преобразования.



3. Для завершения редактирования переменной выберите один из следующих вариантов:

   - Нажмите значок ✓ («Сохранить изменения»), чтобы применить изменения к параметрам переменной.

     Таблица переменных обновится и отобразит изменения.

   - Нажмите значок ✕ («Отменить изменения»), чтобы отказаться от применения изменений к параметрам переменной.

     Все изменения в записи будут утеряны.

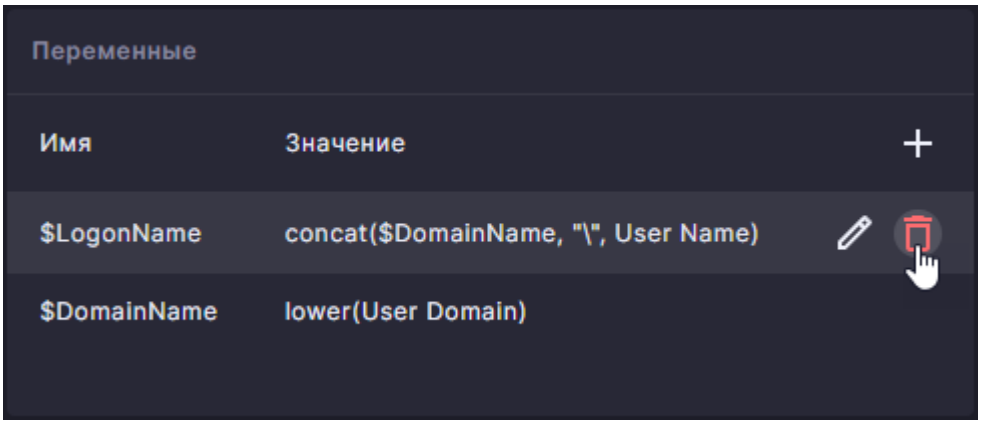
     Следующие действия приводят к аналогичному результату:

     - перевод записи, соответствующей другой переменной, в режим редактирования;
     - создание новой переменной, нажав значок + («Создать переменную») над таблицей.

5.3 Удаление переменной

В таблице «Переменные»:

1. Найдите запись с требуемой переменной.
2. Наведите указатель мыши на запись и нажмите контекстный значок 🗑 («Удалить переменную»).



Переменная будет удалена из таблицы.

5.4 Преобразование значений

Вы можете использовать переменную для хранения результата преобразования значений полей события или других переменных. Переменную и хранимый в ней результат преобразования можно затем использовать при задании:

- критериев фильтра выборки целевых событий;
- действий по обогащению этих событий.

Для задания преобразования введите в значение переменной текстовое выражение, состоящее из имени функции преобразования и одного или более аргументов, которые указываются в скобках после имени и разделяются запятыми. Аргументы определяют источники преобразуемых значений.

В качестве аргумента может использоваться:

- имя поля события;
- имя другой переменной.

5.4.1 Функции преобразования

Поддерживаются следующие функции:

- **concat** – объединяет строковые значения, заданные аргументами, в одну строку путем их конкатенации.
- **lower** – преобразует все символы строки значения в нижний регистр.
- **trim** – удаляет начальные и конечные символы пробела из строки значения.
- **upper** – преобразует все символы строки значения в верхний регистр.

5.5 Использование в фильтрах

Переменные можно использовать в критериях следующих фильтров:

- фильтр правила корреляции;
- фильтр правила обогащения;
- фильтр панели «Формирование данных».

6. Работа с правилами корреляции

Работа с правилами корреляции осуществляется в рамках процесса мониторинга и контроля. Для работы с правилами перейдите в модуль «Правила корреляции» и воспользуйтесь его функциями, описанными ниже.

6.1 Создание правила корреляции

1. Нажмите значок + («Создать правило»), чтобы открыть окно «Создание правила».
2. Введите уникальное имя правила.
3. При необходимости введите описание правила.
4. При необходимости измените тип правила, выбрав элемент из выпадающего списка.

   Содержимое окна варьируется в зависимости от выбранного типа правила. Для оконного правила будут отображены параметры, описанные в этом разделе.
5. Задайте фильтр для выборки корреляционных событий, к которым будет применяться правило.
6. При необходимости задайте действия по обогащению, производимые с полями этих событий, как описано в этом разделе.

   Данные действия будут производиться индивидуально с каждым корреляционным событием.
7. Задайте действия, которые должны выполняться по срабатыванию правила, как описано в этом разделе.

   Если действия включают создание события ИБ, можно задать его критичность.
8. Переведите переключатель параметра «Состояние» в правое положение («Включено»), если правило нужно запустить, то есть включить его в процесс корреляции.
9. Нажмите кнопку «Сохранить».

Окно «Создание правила» закроется, и созданное правило отобразится в таблице правил.

6.2 Редактирование правила корреляции

1. Найдите в таблице запись с требуемым правилом и откройте детальную информацию по нему одним из следующих способов:
   - Дважды щелкните мышью по записи.
   - Наведите указатель мыши на запись и нажмите контекстный значок (карандаш) («Редактировать правило»).

   Правило переведется в режим редактирования, а в открывшемся окне детальной информации по правилу отобразятся его настройки.

2. При необходимости измените настройки правила.

   Состав настроек и инструменты их редактирования аналогичны представленным в окне «Создание правила».

3. Для завершения редактирования правила выберите один из следующих вариантов:

   - Нажмите кнопку «Сохранить», чтобы применить изменения к правилу.

     Окно детальной информации по правилу закроется, и таблица правил будет обновлена.

     Если правило включено, оно будет использоваться в корреляции при анализе подготовленных событий.

   - Нажмите кнопку «Отмена», чтобы отказаться от применения изменений к правилу.

     Все изменения настроек правила будут утеряны.

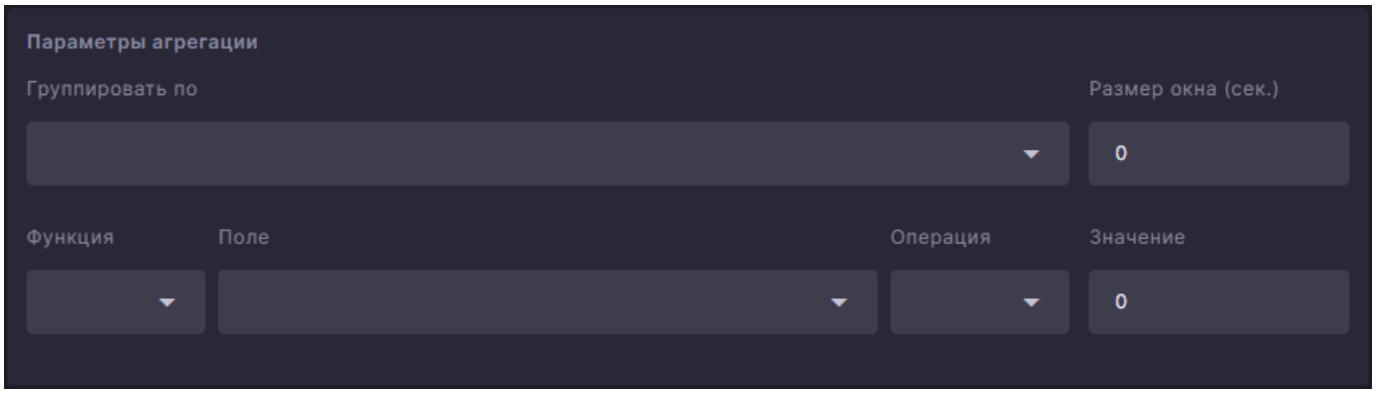
6.3 Запуск и останов правила корреляции

Запуск и останов правила осуществляется с использованием переключателя параметра «Состояние». Для изменения параметра:

1. Откройте требуемое правило корреляции в режиме редактирования.
2. Измените положение переключателя:
   - Переведите переключатель в правое положение («Включено») для запуска правила и его включения в процесс анализа событий коррелятором.
   - Переведите переключатель в левое положение («Выключено») для останова правила и его исключения из процесса анализа событий коррелятором/из перечня активных правил коррелятора.
3. Нажмите кнопку «Сохранить», чтобы применить изменения к правилу.

6.4 Настройка параметров оконного правила

В отличие от обычного правила, оконное правило включает параметры, позволяющие выявлять последовательность корреляционных событий. Эти параметры являются обязательными для заполнения.



1. Задайте перечень полей, по которым будут группироваться данные вошедших в последовательность корреляционных событий.

   Перечень должен включать одно или несколько полей. Поля можно выбирать из выпадающего списка, в котором они располагаются в алфавитном порядке. Повторный выбор поля в списке или нажатие значка ✕, отображенного после имени поля, удалит это поле из перечня. Группировка данных производится для вычисления агрегированного значения с использованием функции, заданной в условии срабатывания правила.

2. Задайте размер временного интервала (так называемого «окна»), в течение которого будет выявляться последовательность корреляционных событий.
3. Задайте параметры, определяющие условие срабатывания правила, как описано ниже.

6.4.1 Задание условия срабатывания

Оконное правило корреляции срабатывает, как только условие, заданное параметрами панели «Параметры агрегации», выполняется для последовательности выявленных корреляционных событий.

Используйте следующие параметры для задания условия срабатывания:

- Функция.

  Выберите агрегатную функцию из выпадающего списка. Аргументами в функцию будут переданы значения поля корреляционных событий, указанного справа от функции. Поддерживаемые агрегатные функции для этих значений:

  - **count** – подсчет количества значений (результат совпадает с количеством корреляционных событий в последовательности).
  - **distinctCount** – подсчет количества уникальных значений.
  - **sum** – подсчет суммы значений.
  - **avg** – подсчет среднего значения.

- Поле.

  Выберите из выпадающего списка числовое поле корреляционного события, чьи значения будут передаваться аргументами в агрегатную функцию.

- Операция.

  Выберите операцию сравнения из выпадающего списка. Сравнение будет производиться между вычисленным агрегированным значением и числовым значением, заданным в поле справа от операции.

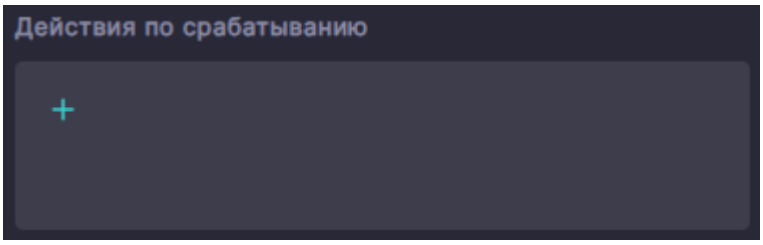
- Значение.

  Введите числовое значение, с которым будет сравниваться вычисленное агрегированное значение.

Правило сработает, когда результат операции сравнения будет Истина (True).

6.5 Настройка действий по срабатыванию

Система позволяет настроить действия, производимые по срабатыванию правила корреляции, с помощью специализированного инструмента, расположенного в панели «Действия по срабатыванию». Инструмент отображает последовательность действий в виде настраиваемого списка, каждый элемент которого определяет выполняемую функцию и ее параметры. Имя функции и значения параметров указываются в блоках элемента. Функции будут выполняться в порядке следования элементов списка.

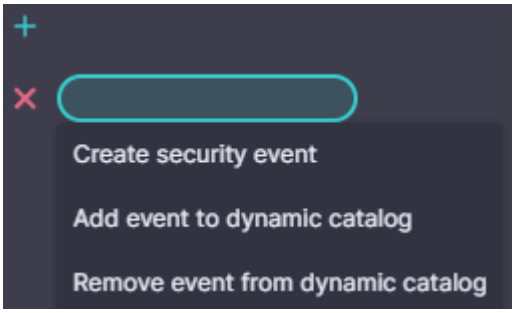


Изначально список действий пуст. Вы можете заполнить его, как описано ниже.

6.5.1 Создание действия

Нажмите значок + , отображаемый в начале списка, чтобы создать действие. Действие будет добавлено в конец списка.

В созданном действии не задана его функция. Для задания функции нажмите на блок функции и выберите ее имя из выпадающего списка.



Поддерживаемые функции:

- Create security event.

  Создать событие ИБ. Корреляционные события, вызвавшие срабатывание правила, будут автоматически связаны с созданным событием ИБ. Для задания его критичности используйте соответствующий параметр правила.

- Add event to dynamic catalog.

  Добавить корреляционное событие в динамический справочник.

- Remove event from dynamic catalog.

  Удалить корреляционное событие из динамического справочника.

6.5.2 Удаление действия

Нажмите значок ✕, отображаемый слева от элемента списка, чтобы удалить этот элемент.

7. Работа со справочниками

Справочник позволяет хранить данные для совместного использования пользователями и модулями Системы. В графическом интерфейсе данные справочника отображаются в виде таблицы, где каждое поле данных справочника представлено колонкой, а связанные значения нескольких полей объединены в строку (запись). Справочник может содержать неограниченное количество полей и записей.

Как и поля модели события, поля справочников имеют следующие характеристики:

- Имя.

  Идентифицирует данные поля справочника в графическом интерфейсе Системы. Является уникальным в справочнике. Допускает использование пробелов.

- Тип данных.

  Определяет формат представления и диапазон значений данных поля.

Для управления справочниками перейдите в модуль «Справочники» и воспользуйтесь его функциями, описанными ниже.

7.1 Создание справочника

Система предоставляет следующие возможности создания справочника:

- вручную определяя структуру (поля и их типы) и заполняя содержимое (значения полей);
- используя импорт данных из CSV-файла.

7.1.1 Ввод данных вручную

1. Нажмите значок + («Создать справочник») и выберите пункт «Вручную» из выпадающего меню.

   Откроется окно «Создание справочника», в котором можно задать настройки справочника.
2. Введите уникальное имя справочника.
3. При необходимости введите описание справочника.
4. Выберите тип справочника из выпадающего списка.

   Тип справочника после его создания изменить нельзя.
5. В таблице «Поля» создайте одно или более полей, как описано в этом разделе.
6. Нажмите кнопку «Сохранить».

Окно «Создание справочника» закроется, и справочник будет создан. Он не содержит записей, поэтому будет автоматически переведен в режим редактирования для их ввода. Вы можете продолжить работу со справочником в этом режиме либо вернуться к таблице справочников модуля «Справочники», нажав значок ← («Вернуться назад»).

7.1.2 Импорт данных из CSV-файла

1. Нажмите значок + («Создать справочник») и выберите пункт «Импортировать из CSV» из выпадающего меню.

   Откроется окно «Создание справочника», в котором можно задать настройки справочника.
2. Введите уникальное имя справочника.
3. При необходимости введите описание справочника.
4. Нажмите кнопку «Импортировать из CSV» и в открывшемся окне выберите CSV-файл, содержащий данные справочника.

Окно «Создание справочника» закроется, и справочник (включая поля, их типы и значения) будет создан на основе данных CSV-файла. Тип каждого поля определяется по первому значению, считанному для этого поля из строк CSV-файла, следующих за строкой заголовка. Справочник автоматически будет переведен в режим редактирования для корректировки характеристик полей и ввода записей. Вы можете продолжить работу со справочником в этом режиме либо вернуться к таблице справочников модуля «Справочники», нажав значок ← («Вернуться назад»).

7.2 Редактирование справочника

Редактирование можно производить в модуле «Справочники» после перевода справочника в режим редактирования открытием детальной информации по нему. В этом режиме можно изменить настройки справочника и отредактировать его записи. Инструменты редактирования настроек аналогичны представленным в окне «Создание справочника».

Для редактирования справочника:

1. Перейдите в модуль «Справочники».
2. Найдите в таблице запись с требуемым справочником и откройте детальную информацию по нему одним из следующих способов:
   - Дважды щелкните мышью по записи.
   - Наведите указатель мыши на запись и нажмите контекстный значок () («Открыть детальную информацию»).

   Справочник переведется в режим редактирования, а в открывшемся окне детальной информации по справочнику отобразится его содержимое (поля и записи) в виде таблицы. Используйте функции таблицы для управления записями, как описано в этом разделе.
3. При необходимости отредактируйте настройки и записи справочника, как описано ниже.
4. Нажмите значок () («Вернуться назад»), чтобы выйти из режима редактирования справочника и вернуться к таблице справочников модуля «Справочники».

7.2.1 Редактирование настроек

В окне детальной информации по справочнику:

1. Нажмите значок () («Редактировать настройки»).

   Откроется окно «Редактирование настроек справочника».
2. При необходимости измените имя справочника. Имя должно быть уникальным.
3. При необходимости измените описание справочника.
4. В таблице «Поля» можно изменить состав полей справочника, как описано в разделе ниже.
5. Нажмите кнопку «Сохранить», чтобы применить изменения к справочнику.

Окно «Редактирование настроек справочника» закроется, и содержимое справочника будет изменено в соответствии с правками в составе полей.

Управление полями

Вы можете создавать, редактировать и удалять поля, используя функции таблицы «Поля», отображаемой в следующих окнах модуля «Справочники»:

- окно «Создание справочника»;
- окно «Редактирование настроек справочника».

СОЗДАНИЕ ПОЛЯ

Нажмите значок () («Создать поле») над таблицей «Поля», чтобы добавить в нее запись.

Далее в добавленной записи:

1. Введите уникальное в рамках справочника имя поля.
2. Выберите тип данных поля из выпадающего списка.
3. Для завершения создания поля выберите один из следующих вариантов:

    - Нажмите значок ✓ («Сохранить изменения»), чтобы создать поле с введенными параметрами.

      Созданное поле добавится в таблицу.

    - Нажмите значок ✕ («Отменить изменения»), чтобы отказаться от создания поля.

      Добавленная запись будет удалена из таблицы полей, а все введенные в записи данные будут утеряны.

      Следующие действия приводят к аналогичному результату:

        - перевод записи, соответствующей другому полю, в режим редактирования;
        - создание нового поля, нажав значок + («Создать поле») над таблицей.

При необходимости созданные поля можно отредактировать или удалить, как описано ниже.

РЕДАКТИРОВАНИЕ ПОЛЯ

В окне настроек справочника:

1. Найдите в таблице запись с требуемым полем.
2. Наведите указатель мыши на запись и нажмите контекстный значок ✎ («Редактировать поле»), чтобы перевести запись в режим редактирования.

Далее в этой записи:

1. При необходимости измените имя поля.
2. При необходимости измените тип данных поля, выбрав элемент из выпадающего списка.

   Изменение типа можно производить только в справочнике без записей.
3. Для завершения редактирования поля выберите один из следующих вариантов:

   - Нажмите значок ✓ («Сохранить изменения»), чтобы применить изменения к параметрам поля.

     Таблица полей обновится и отобразит измененное поле.

   - Нажмите значок ✕ («Отменить изменения»), чтобы отказаться от применения изменений к параметрам поля.

     Все изменения в записи будут утеряны.

     Следующие действия приводят к аналогичному результату:

     - перевод записи, соответствующей другому полю, в режим редактирования;
     - создание нового поля, нажав значок + («Создать поле») над таблицей.

УДАЛЕНИЕ ПОЛЯ

В окне настроек справочника:

1. Найдите в таблице запись с требуемым полем.
2. Наведите указатель мыши на запись и нажмите контекстный значок 🗑 («Удалить поле»).

   Поле будет удалено из таблицы.

7.2.2 Управление записями

В окне детальной информации по справочнику можно создавать, редактировать и удалять записи справочника, используя функции таблицы, отображающей записи справочника.

Создание записи

В окне детальной информации по справочнику нажмите значок + («Создать запись») над таблицей, чтобы добавить запись.

Далее в добавленной записи:

1. Заполните ячейки значениями полей.
2. Для завершения создания записи выберите один из следующих вариантов:
    - Нажмите значок ✓ («Сохранить изменения»), чтобы создать запись с введенными значениями.
    - Нажмите значок ✕ («Отменить изменения»), чтобы отказаться от создания записи.

      Добавленная запись будет удалена из таблицы, а все введенные в записи данные будут утеряны.

      Следующие действия приводят к аналогичному результату:

        - перевод другой записи в режим редактирования;
        - создание новой записи нажатием значка + («Создать запись») в заголовке таблицы;
        - выход из окна детальной информации по справочнику нажатием значка ← («Вернуться назад»).

При необходимости созданные поля можно отредактировать или удалить, как описано ниже.

Редактирование записи

В окне детальной информации по справочнику:

1. Найдите в таблице требуемую запись.
2. Наведите указатель мыши на запись и нажмите контекстный значок ✎ («Редактировать запись»), чтобы перевести запись в режим редактирования.

Далее в этой записи:

1. При необходимости измените значения полей в ячейках.
2. Для завершения редактирования записи выберите один из следующих вариантов:
    - Нажмите значок ✓ («Сохранить изменения»), чтобы применить изменения к записи.
    - Нажмите значок ✕ («Отменить изменения»), чтобы отказаться от применения изменений к записи.

      Все изменения в записи будут утеряны.

      Следующие действия приводят к аналогичному результату:

        - перевод другой записи в режим редактирования;
        - создание новой записи нажатием значка + («Создать запись») в заголовке таблицы;
        - выход из окна детальной информации по справочнику нажатием значка ← («Вернуться назад»).

Удаление записи

В окне детальной информации по справочнику наведите указатель мыши на нужную запись и нажмите контекстный значок  («Удалить запись»).

7.2.3 Экспорт в CSV-файл

Данные справочника (включая поля и их значения) можно экспортировать/сохранить в CSV-файл. Для этого в окне детальной информации по справочнику нажмите кнопку «Экспортировать в CSV». Выгрузка данных справочника осуществится в CSV файл системной папки «Загрузки». Имя файлу присваивается автоматически. Оно включает в себя дату и время создания файла.

7.2.4 Импорт из CSV-файла

Как и при создании справочника, его данные (включая поля и их значения) можно импортировать из CSV-файла.

Для импортирования данных в окне детальной информации по справочнику:

1. Нажмите кнопку «Импортировать из CSV» и в открывшемся окне выберите CSV-файл, содержащий данные справочника.
2. Подтвердите удаление существующих данных и их замещение данными из файла.

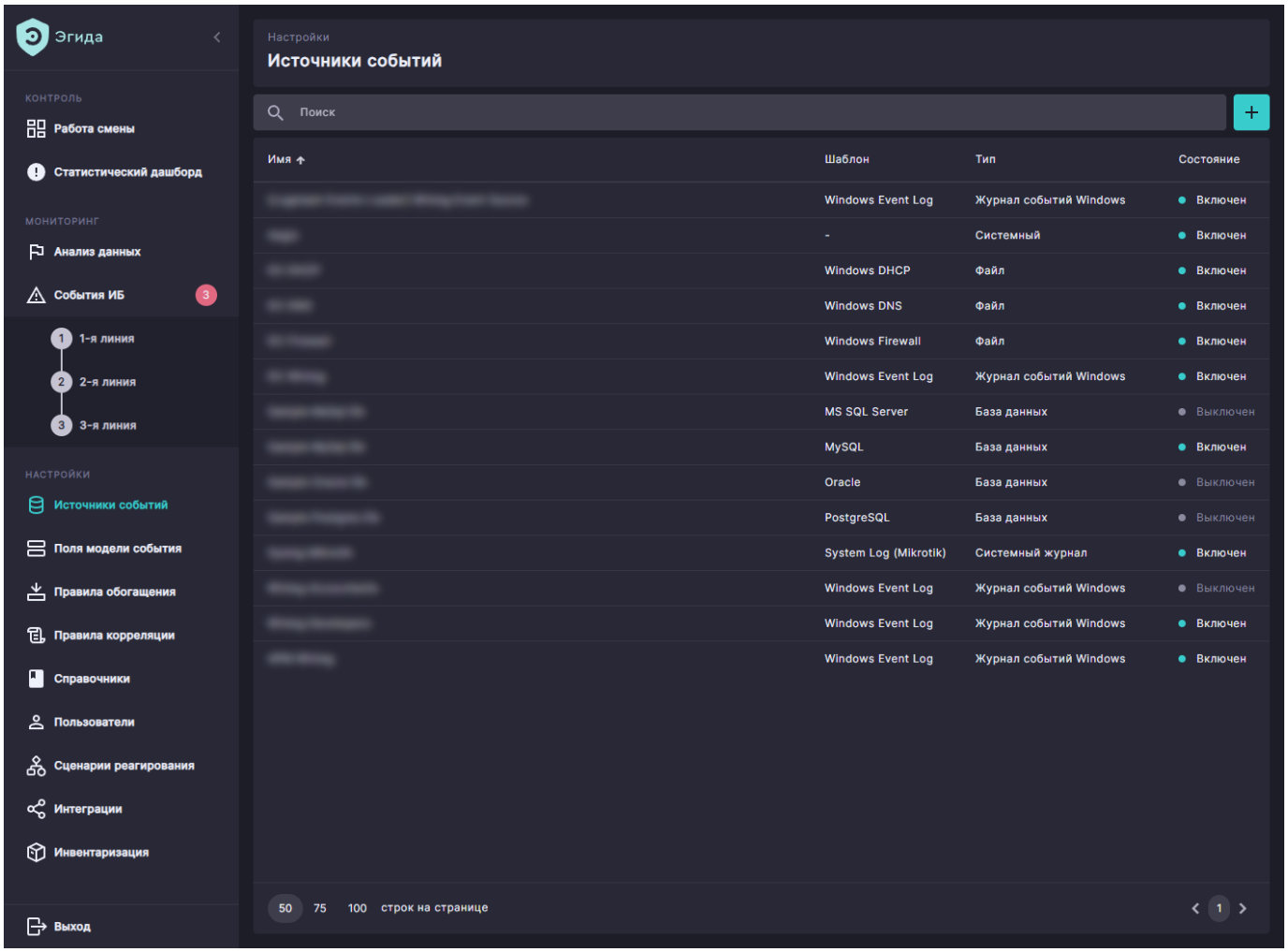
Будут замещены данными CSV-файла только поля, их типы и значения. Имя справочника, его описание и тип остаются без изменений.

8. Пользовательский интерфейс

8.1 Принципы взаимодействия с пользовательским интерфейсом

8.1.1 Основные элементы интерфейса

Интерфейс управления Системой реализован в виде веб-приложения.

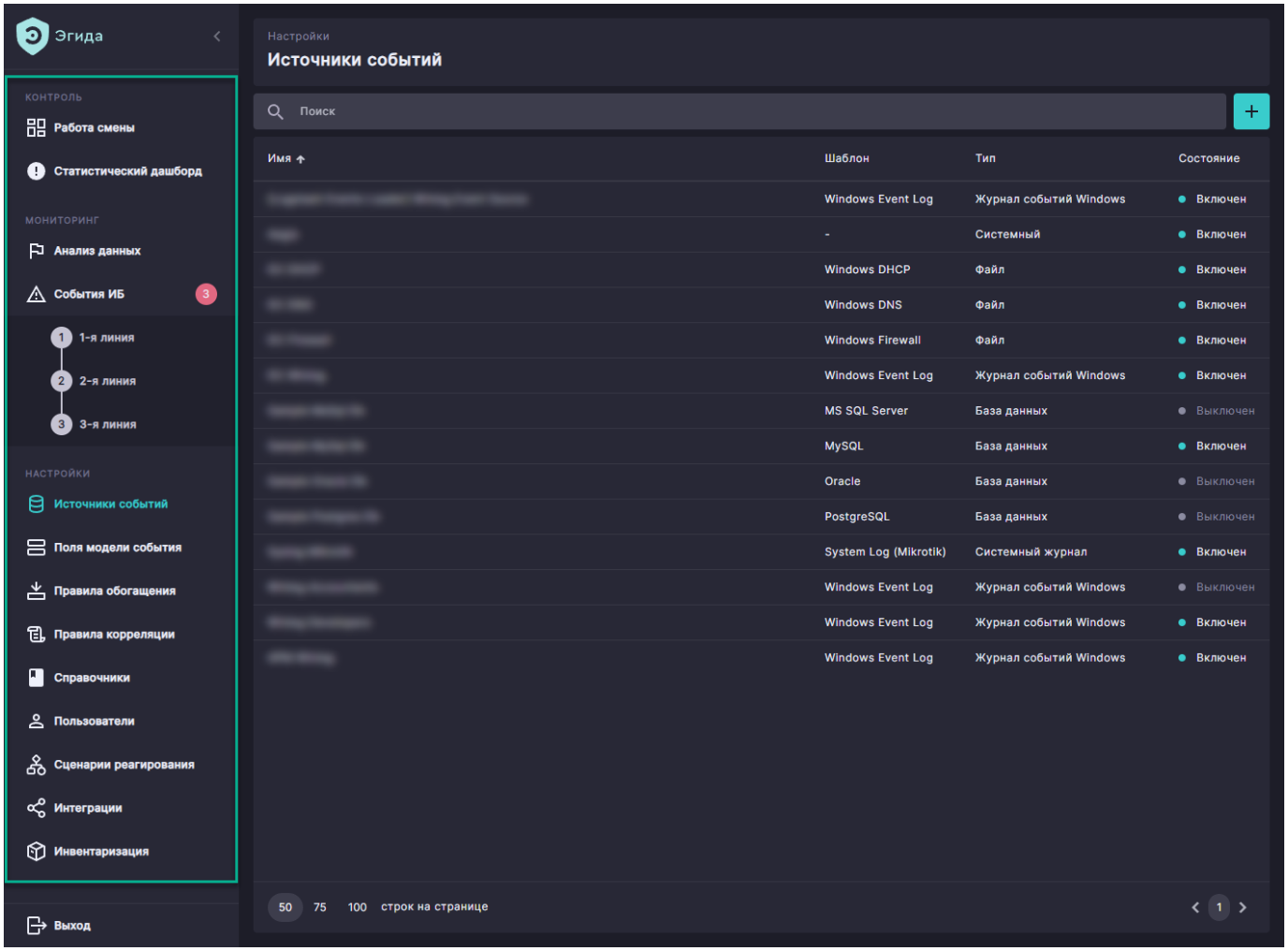


Интерфейс содержит следующие элементы:

- список модулей Системы с индикацией текущего выбранного модуля;
- область заголовка и строки навигации по разделам модуля;
- основная рабочая область, занимающая остальную часть окна.

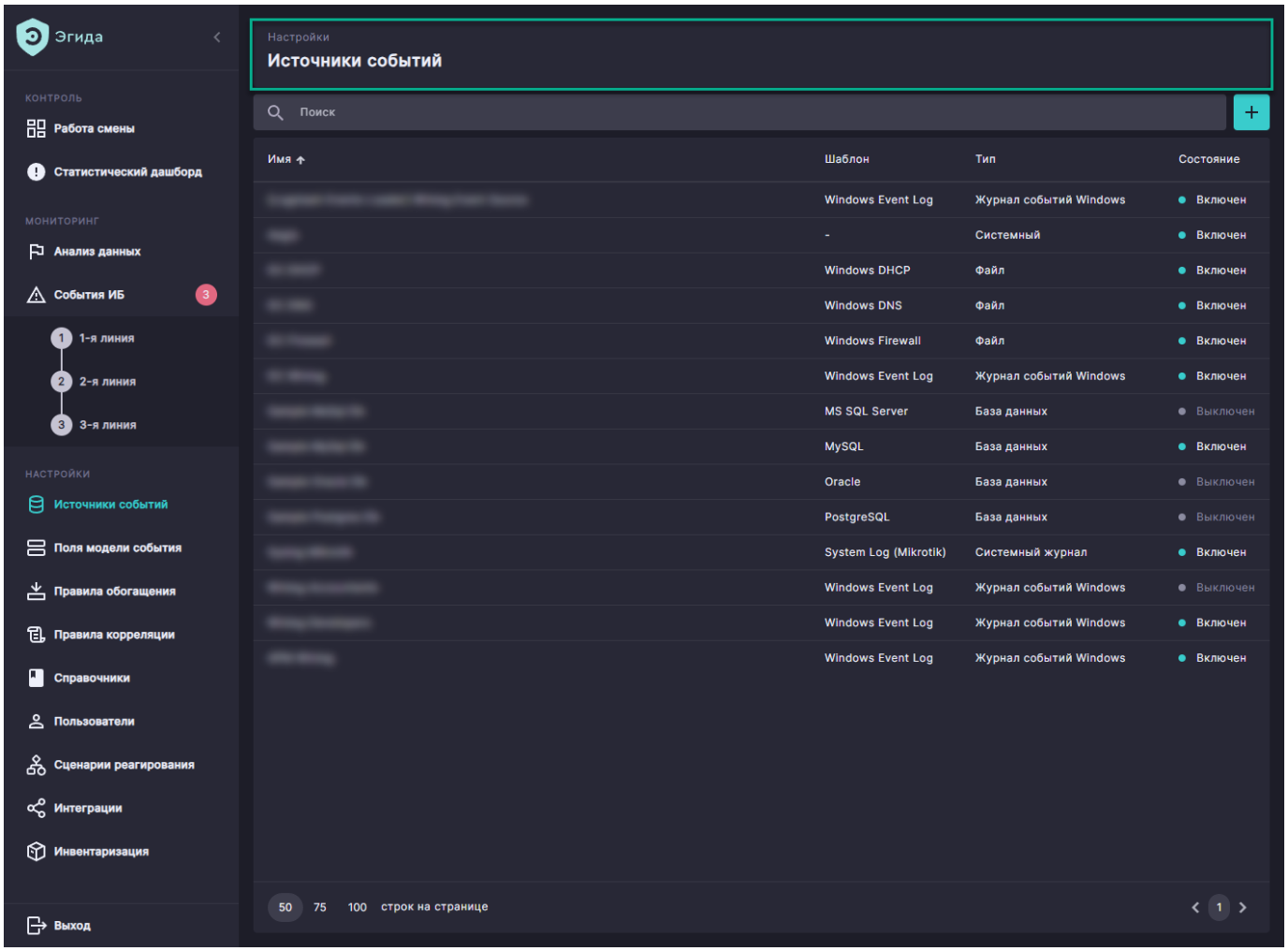
Список модулей Системы

Отображается в левой части окна веб-приложения. Выбор модуля осуществляется нажатием на его имени в списке. Текущий выбранный модуль выделяется цветом.

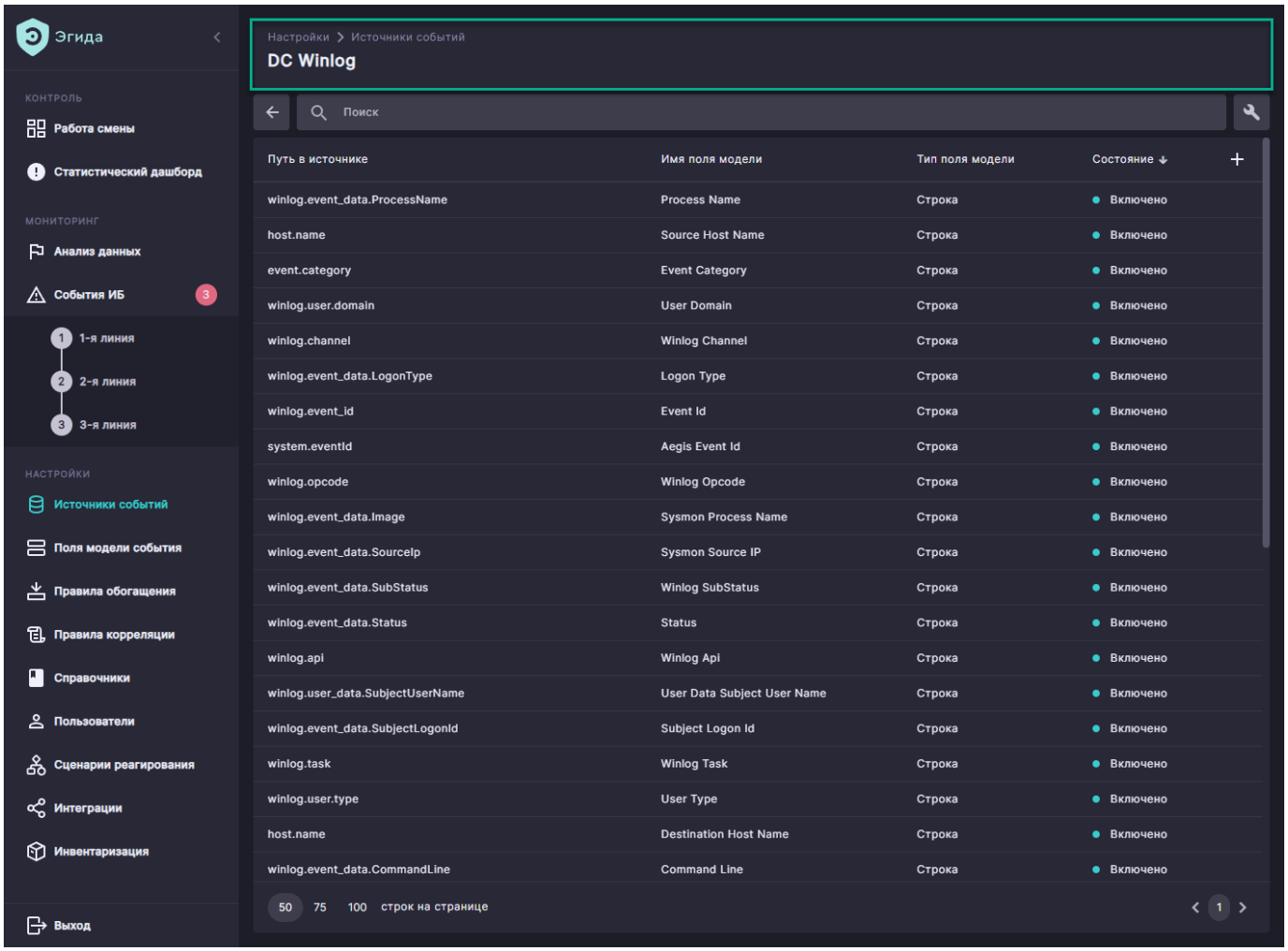


Область заголовка и строки навигации по разделам модуля

Располагается в верхней части окна веб-приложения. Заголовок отображает имя модуля или его редактируемого объекта.

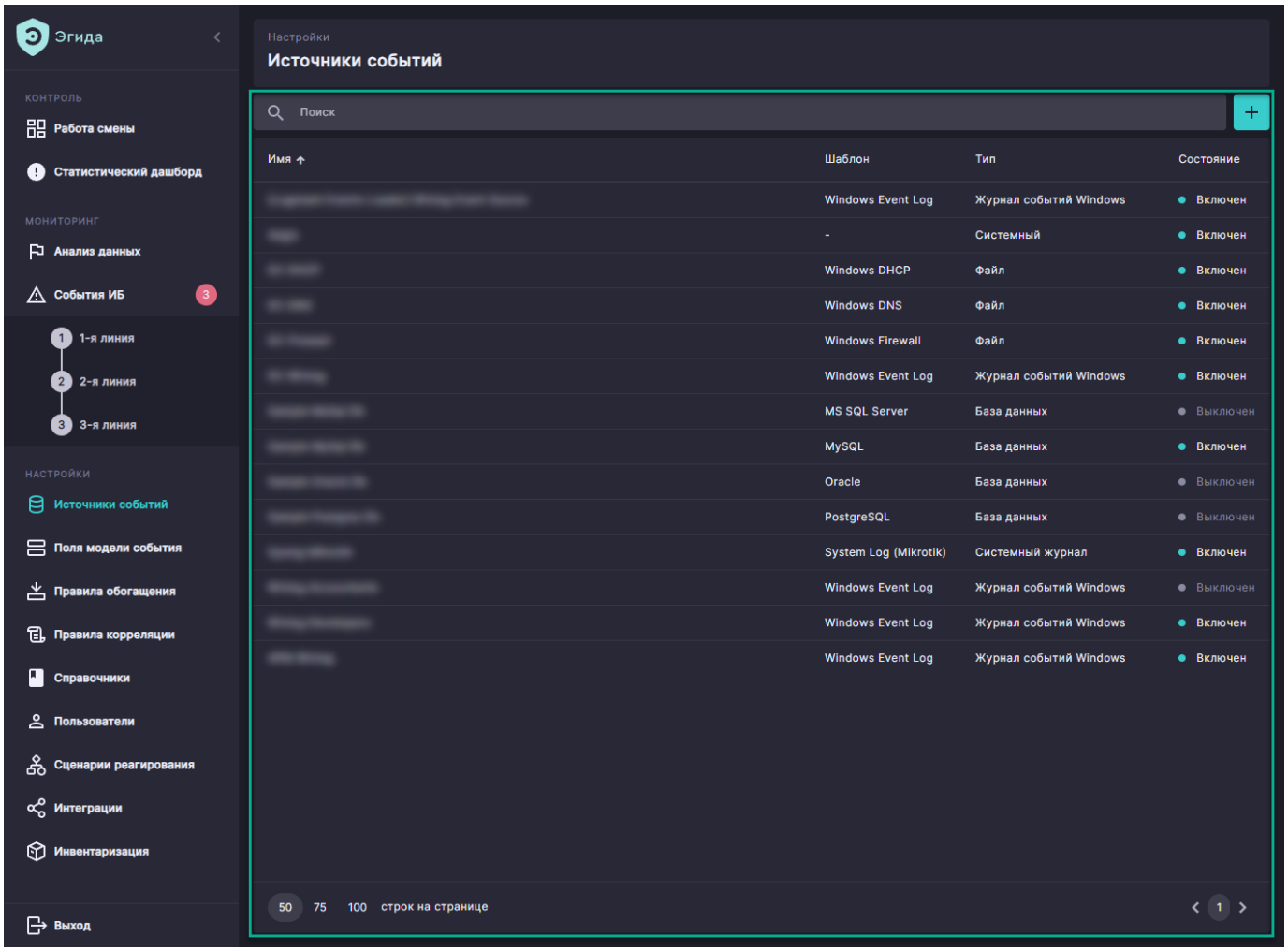


Строка навигации расположена над заголовком. Навигация по разделам осуществляется нажатием на элементы строки.



Основная рабочая область

Занимает большую часть окна веб-приложения. Здесь отображаются данные и элементы управления текущего модуля.



8.1.2 Табличное представление данных

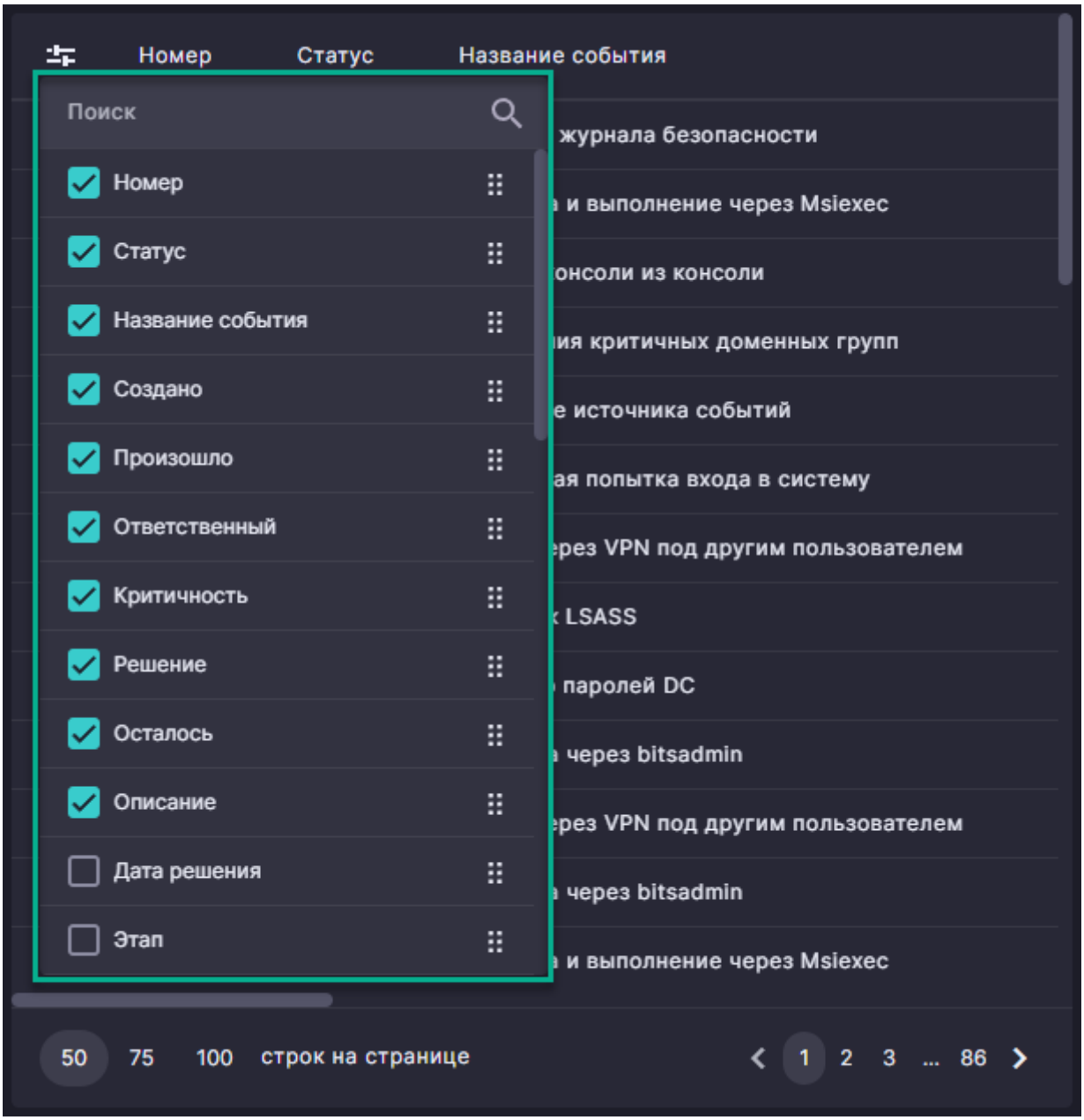
Отображает данные в виде таблицы, где каждое поле данных представлено колонкой, а связанные значения нескольких полей объединены в запись (строку). Таблица предоставляет пользователям следующие функции и возможности настройки:

- выбор отображаемых колонок;
- изменение местоположения колонок;
- фильтрация и поиск данных;
- сортировка записей;
- разбиение на страницы и межстраничная навигация;
- контекстные действия с объектом, отображаемым в записи;
- экспорт данных в формат CSV;
- выбор записей.

Выбор отображаемых колонок

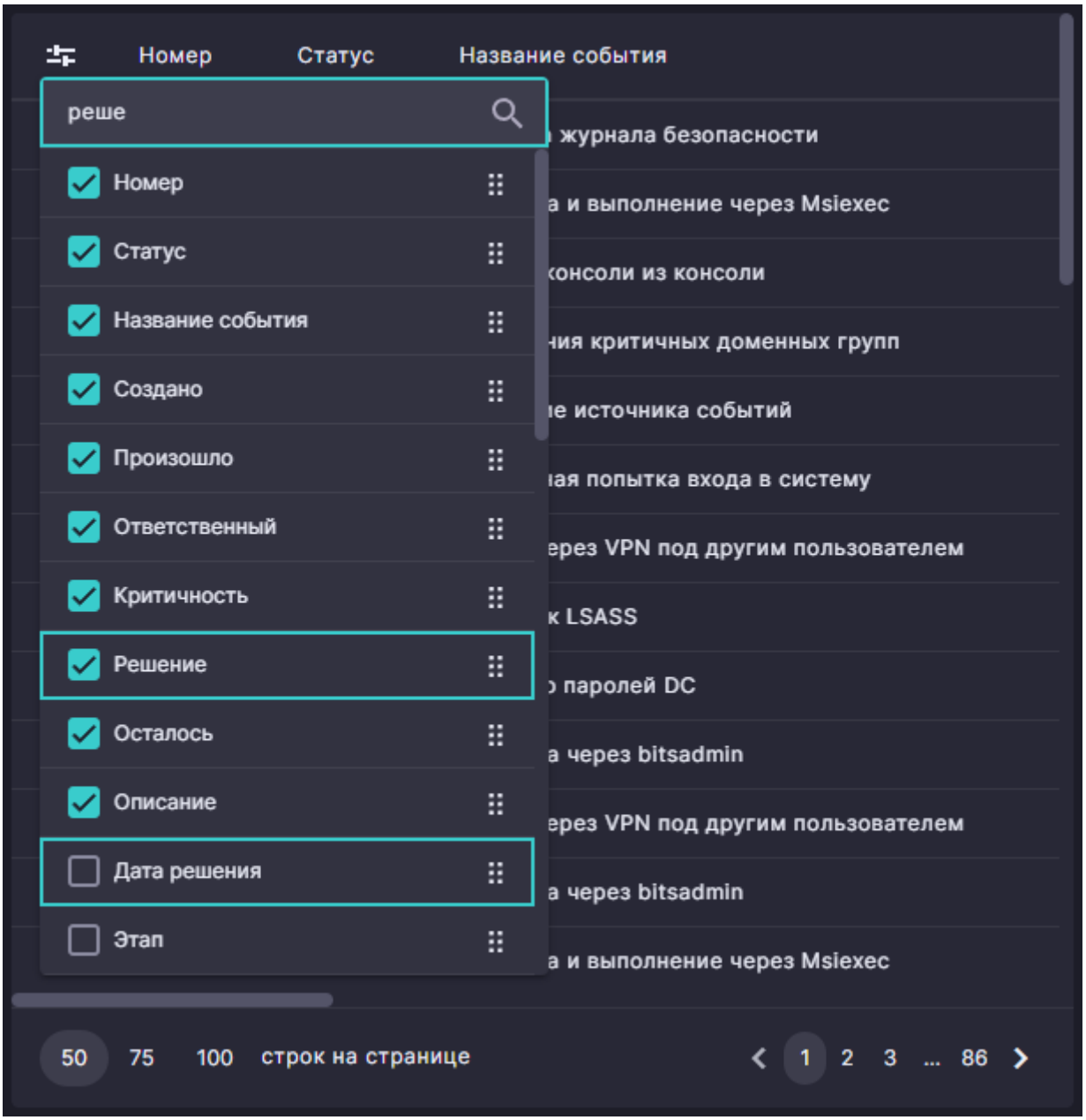
Для настройки видимости колонки выполните следующие действия:

1. Нажмите значок в заголовке таблицы, чтобы отобразить всплывающее окно со списком колонок.



2. Найдите в списке нужную колонку.

   Для удобства можно воспользоваться поиском по ее наименованию, введя его часть в поле «Поиск». Колонки, соответствующие строке поиска, будут выделены прямоугольными рамками.



3. В списке установите или снимите флажок напротив колонки для изменения ее видимости в таблице.

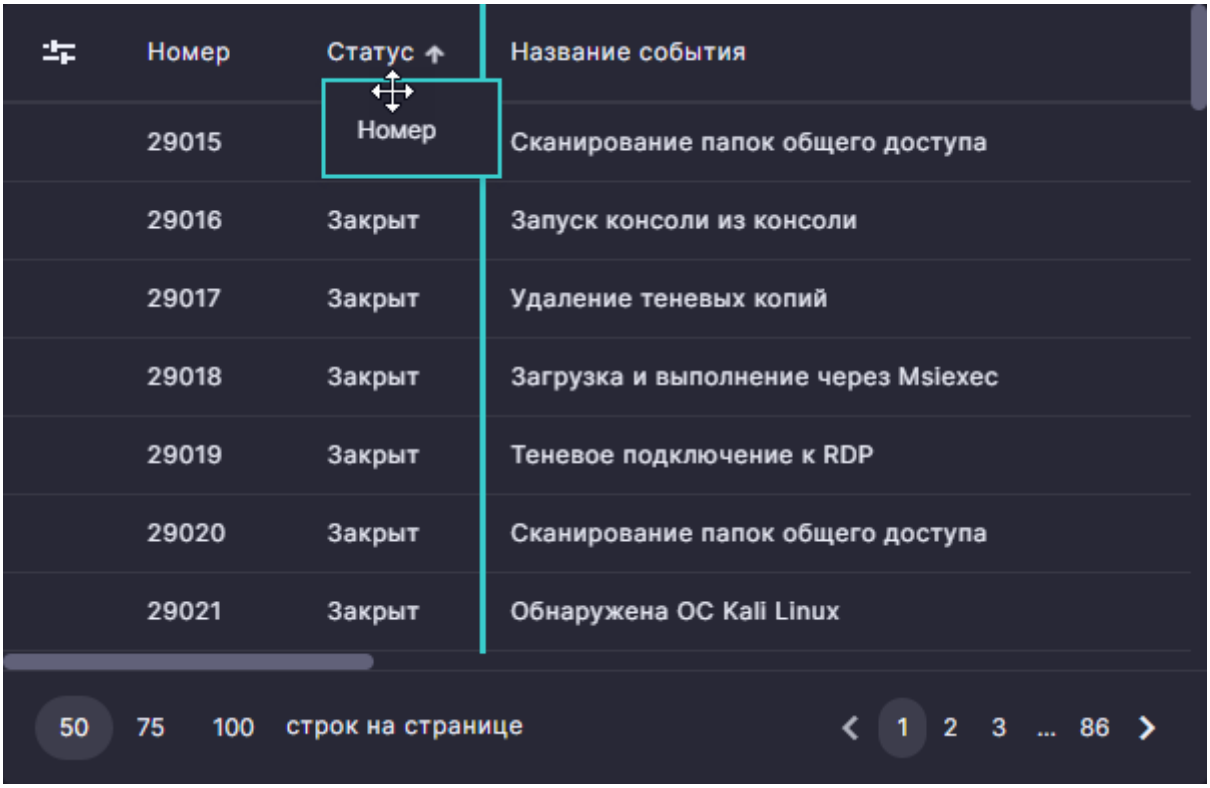
После настройки видимости колонок окно можно скрыть, нажав вне него.

Изменение порядка расположения колонок

Для перемещения колонки выполните следующие действия:

1. Наведите указатель мыши на заголовок колонки.
2. Зажмите левую кнопку мыши и перетащите заголовок в нужном направлении.

   Новое положение колонки отмечается вертикальным индикатором.



3. Отпустите левую кнопку мыши, когда индикатор занимает нужное положение.

Колонка будет перемещена.

Фильтрация и поиск данных

Вы можете задать фильтр для поиска записей, удовлетворяющих определенным критериям, используя графический конструктор.

Сортировка записей

Чтобы отсортировать записи в таблице по значениям определенной колонки, нажмите на ее заголовок. Повторное нажатие на заголовок изменит направление сортировки на противоположное. Направление сортировки отображается после имени колонки в виде стрелки, направленной вверх (по возрастанию значений) или вниз (по убыванию значений).

Контекстные действия с записью

Поддерживается выполнение следующих контекстных действий:

- Переход в режим редактирования объекта, отображенного в записи.

  Чтобы осуществить переход, выберите один из следующих вариантов:

  - Дважды щелкните мышью по записи.
  - Наведите указатель мыши на запись и нажмите появившийся контекстный значок: («Открыть детальную информацию») или («Редактировать»).

  Перейдите в одноименный раздел описания соответствующего модуля для получения дополнительной информации по функциям, предоставляемым им в режиме редактирования.

- Показ выпадающего списка доступных управляющих действий для объекта в строке.

  В модуле «События ИБ» наведите указатель мыши на запись и нажмите появившийся контекстный значок («Выполнить действие»). Чтобы выполнить действие из , нажмите на него в списке.

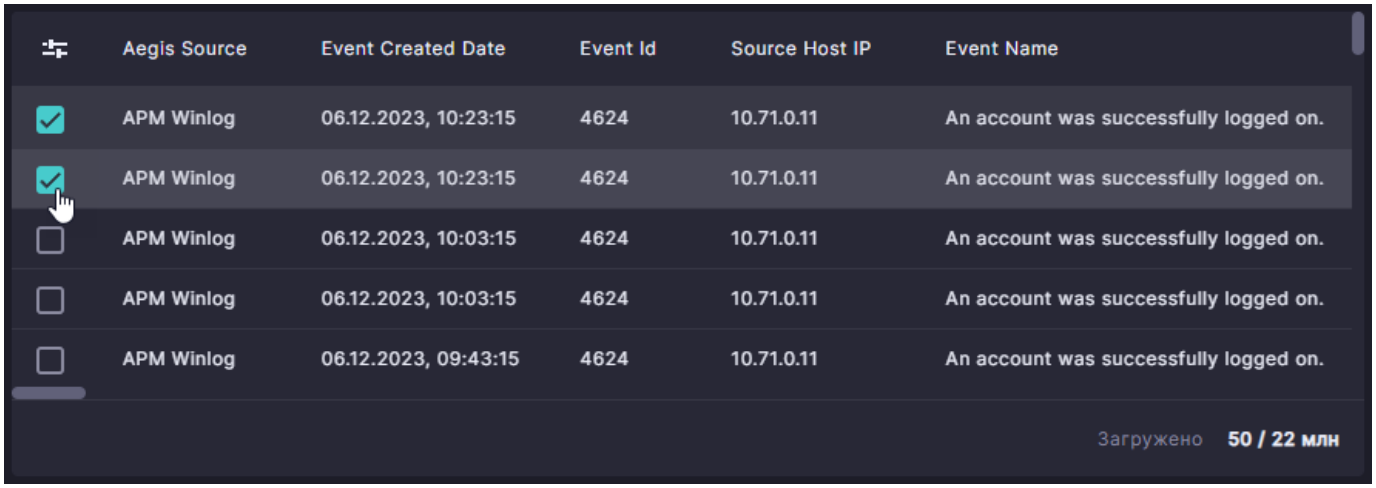
Выбор записей

Данная функция обычно используется, чтобы:

- применить к одной или нескольким записям внешнюю функцию (находящуюся вне таблицы);
- связать эти записи с внешним инструментом.

Выбор записи можно осуществить нажатием в ее пределах. Выбранная запись будет выделена цветом.

В таблице с включенной поддержкой выбора нескольких записей выбор также можно осуществить, установив флажки напротив нужных записей в служебной колонке, отображаемой слева от всех остальных колонок.

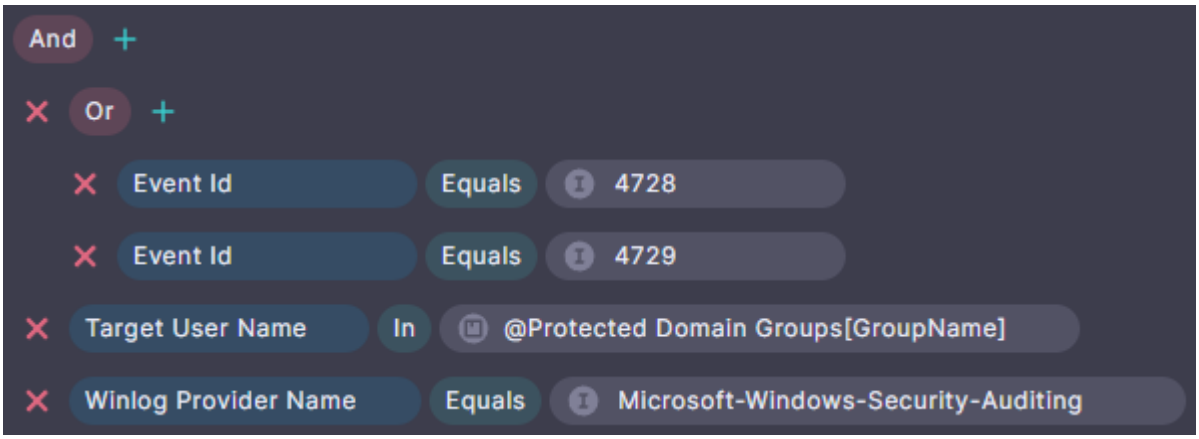


8.1.3 Графические инструменты

Конструктор критериев

Позволяет задать критерии поиска для следующих объектов:

- целевых событий при создании и настройке правил корреляции и обогащения;
- событий при анализе данных;
- событий и инцидентов ИБ при их обработке.



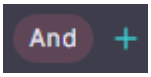
Критерии представляют собой логическое выражение, составленное из логических операций с одним и более условиями. Условие состоит из оператора (функции) и его операндов (аргументов) и возвращает результат выполнения оператора - значение Истина (True) или Ложь (False), определяющее истинность или ложность условия. Для удобства работы логическая операция представляется группой, объединяющей в виде своих дочерних элементов условия и другие (вложенные) группы. Результат операции (группы) рассчитывается на основе этих дочерних элементов.

Объект поиска (событие или событие/инцидент ИБ) считается удовлетворяющим определенным критериям, когда результатом представляющего их логического выражения будет Истина (True). Такой объект будет добавлен в результаты поиска.

Критерии отображаются в виде настраиваемого списка, каждый элемент которого представляет собой один из следующих вариантов:

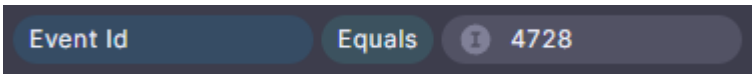
- Логическая группа.

  Отображается в виде блока с наименованием операции.

- Логическое условие в составе группы.

  Отображается в виде дочернего элемента группы и содержит три блока: левый операнд, оператор и правый операнд.

Для управления элементами критериев воспользуйтесь функциями списка, описанными ниже.

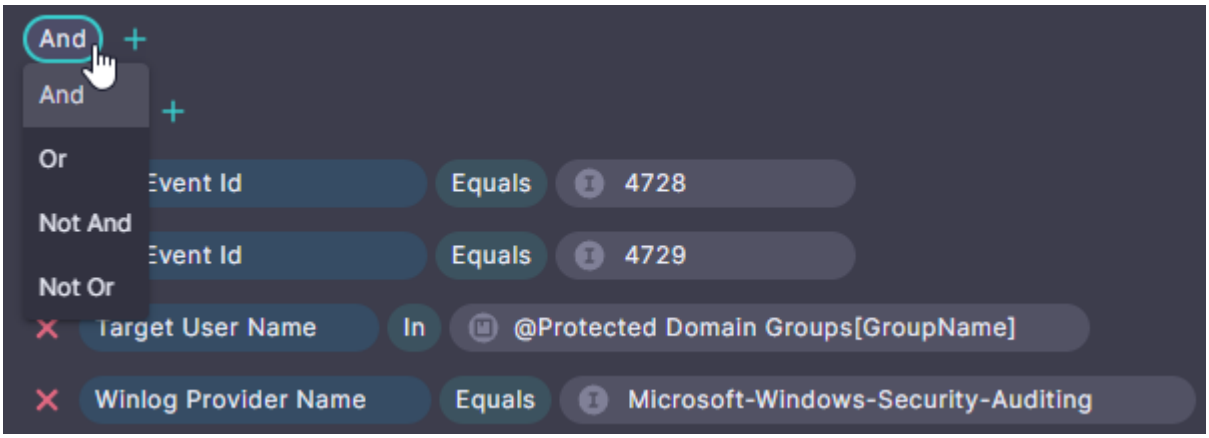
СОЗДАНИЕ ЛОГИЧЕСКОЙ ГРУППЫ

Нажмите значок + , отображаемый справа от блока логической группы, и выберите пункт «Добавить группу» из выпадающего меню, чтобы создать в ней дочернюю группу. Элемент созданной группы будет добавлен в конец списка дочерних элементов.

По умолчанию создается группа, представляющая операцию конъюнкции (**And**).

ЗАМЕНА ОПЕРАЦИИ У ЛОГИЧЕСКОЙ ГРУППЫ

Нажмите на блок операции и выберите нужный элемент из выпадающего списка.

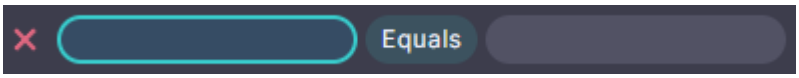


УДАЛЕНИЕ ЛОГИЧЕСКОЙ ГРУППЫ

Нажмите значок ✕, отображаемый слева от элемента группы, чтобы удалить этот элемент и все его дочерние элементы.

СОЗДАНИЕ ЛОГИЧЕСКОГО УСЛОВИЯ

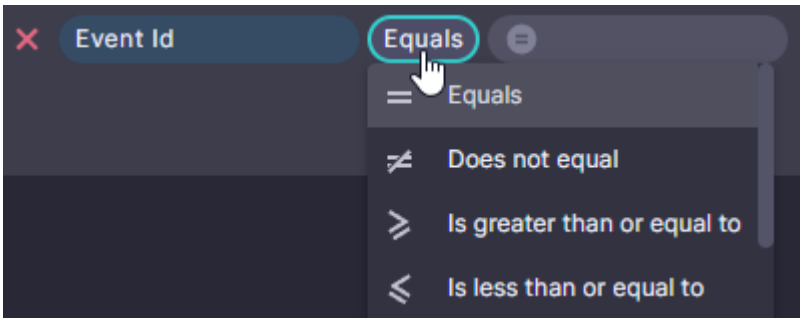
Нажмите значок +, отображаемый справа от блока логической группы, и выберите пункт «Добавить условие» из выпадающего меню, чтобы создать в ней условие в виде дочернего элемента. Элемент созданного условия будет добавлен в конец списка дочерних элементов этой группы.

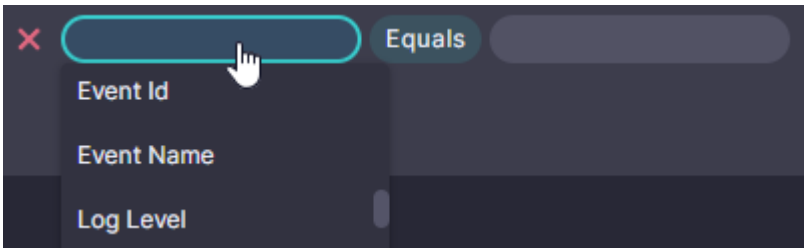


По умолчанию создается условие с оператором равенства (**Equals**).

ЗАМЕНА ОПЕРАТОРА ИЛИ ОПЕРАНДА У ЛОГИЧЕСКОГО УСЛОВИЯ

Нажмите на блок оператора или операнда и выберите нужный элемент из выпадающего списка.





Значение правого операнда сбрасывается, если оно становится несовместимым с измененным значением левого операнда.

УДАЛЕНИЕ ЛОГИЧЕСКОГО УСЛОВИЯ

Нажмите значок ✕, отображаемый слева от элемента условия, чтобы удалить этот элемент.

ЛОГИЧЕСКИЕ ОПЕРАЦИИ

- **And** – логическое И (конъюнкция).
- **Or** – логическое ИЛИ (дизъюнкция).
- **Not And** – инверсия (отрицание) конъюнкции.
- **Not Or** – инверсия (отрицание) дизъюнкции.

ОПЕРАТОРЫ

Оператор определяет соотношение между операндами (аргументами) в условии. Результат выполнения оператора - значение Истина (True) или Ложь (False), определяющее истинность или ложность условия. По умолчанию создается оператор **Equals**.

Поддерживаемые операторы сгруппированы по типам в подразделах ниже.

Отношения

- **Equals** – левый операнд равен правому операнду.
- **Does not equal** – левый операнд не равен правому операнду (инверсия **Equals**).
- **Is less than** – левый операнд меньше правого операнда.
- **Is less than or equal to** – левый операнд меньше или равен правому операнду.
- **Is greater than** – левый операнд больше правого операнда.
- **Is greater than or equal to** – левый операнд больше или равен правому операнду.

Строковые

- **Contains** – левый операнд содержит подстроку, заданную правым операндом.
- **Does not contain** – левый операнд не содержит подстроку, заданную правым операндом (инверсия **Contains**).
- **Starts with** – левый операнд начинается подстрокой, заданной правым операндом.
- **Does not start with** – левый операнд не начинается подстрокой, заданной правым операндом (инверсия **Starts with**).
- **Ends with** – левый операнд заканчивается подстрокой, заданной правым операндом.
- **Does not end with** – левый операнд не заканчивается подстрокой, заданной правым операндом (инверсия **Ends with**).
- **Matches** – левый операнд соответствует регулярному выражению, заданному правым операндом.
- **Does not match** – левый операнд не соответствует регулярному выражению, заданному правым операндом (инверсия **Matches**).

Операторы этого типа применимы только к операндам со значениями строкового типа данных.

Вхождения

- **In** – левый операнд найден в объекте, заданным правым операндом.
- **Not in** – левый операнд не найден в объекте, заданным правым операндом (инверсия **In**).

У этого типа операторов правым операндом может служить:

- список, содержащий значения констант поддерживаемого типа данных, полей, переменных;
- поле справочника.

ОПЕРАНДЫ

Каждое условие состоит из оператора (функции) и двух операндов (аргументов), отображаемых в блоках слева и справа от него. Левым операндом может служить значение поля или переменной. При этом блок операнда будет отображать имя поля/переменной.

Имя переменной начинается с символа $.

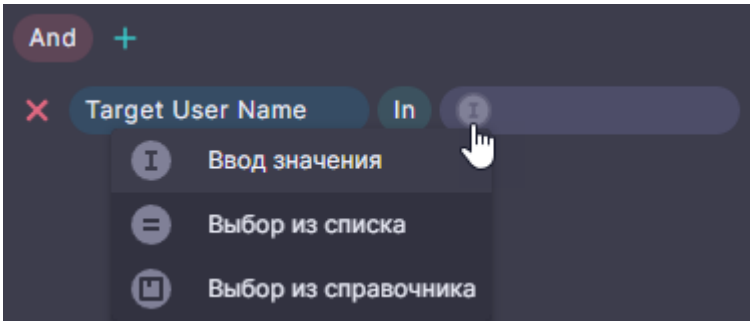
У всех типов операторов, кроме вхождений, правым операндом может служить значение константы поддерживаемого типа данных, поля или переменной. Значение поля или переменной отображается с использованием их имени, аналогично блоку левого операнда.

В зависимости от объектов поиска с использованием конструктора критериев, полем любого операнда является:

- поле нормализованного или подготовленного события;
- поле события/инцидента ИБ.

Способы задания значения правого оператора

Чтобы выбрать способ задания значения, нажмите на значок, отображаемый в блоке правого операнда, и выберите нужный элемент из выпадающего списка.



Если доступен только один способ задания значения, он применяется по умолчанию, и значок не отображается.

Поддерживаются следующие способы задания значения:

- Ввод значения.

  Нажмите на блок операнда перед началом ввода. Введенные в блоке символы будут интерпретироваться как значение того же типа данных, что и левый операнд.

- Выбор из списка.

  Нажмите на блок операнда и выберите из выпадающего списка элемент (поле, переменную или значение поля с фиксированным набором значений).

  Список содержит элементы того же типа данных, что и левый операнд.

- Выбор из справочника.

  Нажмите на блок операнда и выберите из выпадающего списка поле справочника.

  Список содержит поля того же типа данных, что и левый операнд.

  Выбранные справочник и поле отображаются в блоке следующим образом:

  `@@<имя справочника>[<имя поля>]`

  Пример отображения поля **SourceHostIP** справочника **ActiveVPN**:

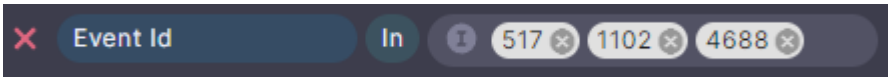
  `@@ActiveVPN[SourceHostIP]`

Задание списка значений правого оператора

У операторов вхождений, в правом операнде можно задать список значений. Для этого введите или выберите значение для каждого элемента списка, завершая определение элемента нажатием клавиши `Enter ⏎` .

Пример задания списка из трех значений:

517 `Enter ⏎` 1102 `Enter ⏎` 4688 `Enter ⏎`

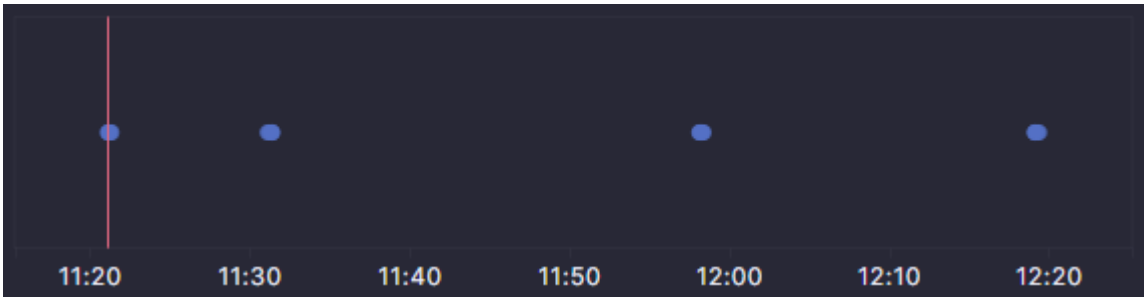


КОПИРОВАНИЕ И ВСТАВКА ФИЛЬТРА ЧЕРЕЗ БУФЕР ОБМЕНА

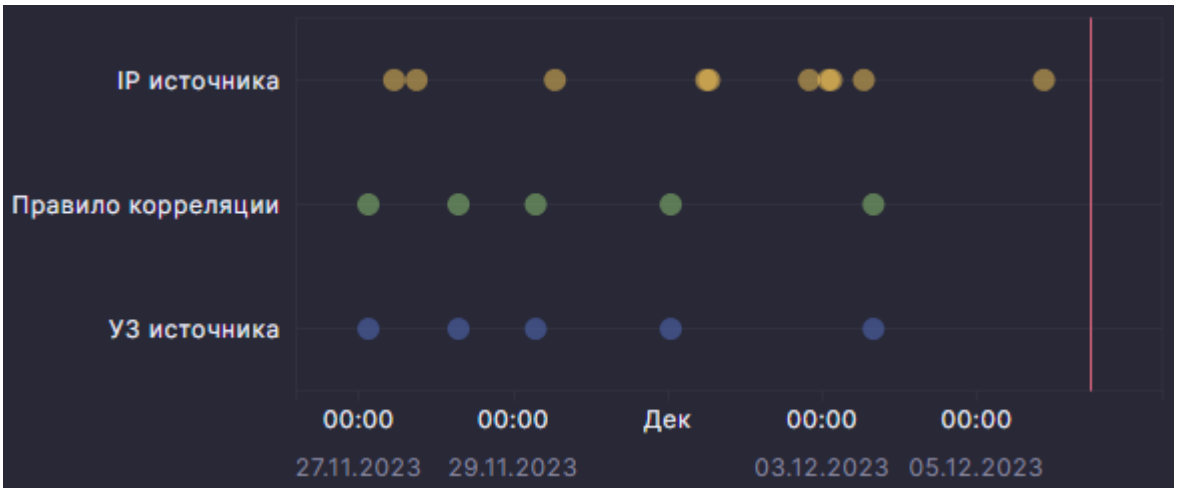
При анализе данных событий и создании правил корреляции вы можете использовать буфер обмена для переноса критериев фильтра между модулями или сохранении их в текстовом виде вне Системы. Для этого воспользуйтесь значками («Копировать») и («Вставить»), расположенными над конструктором критериев.

Хронологический график

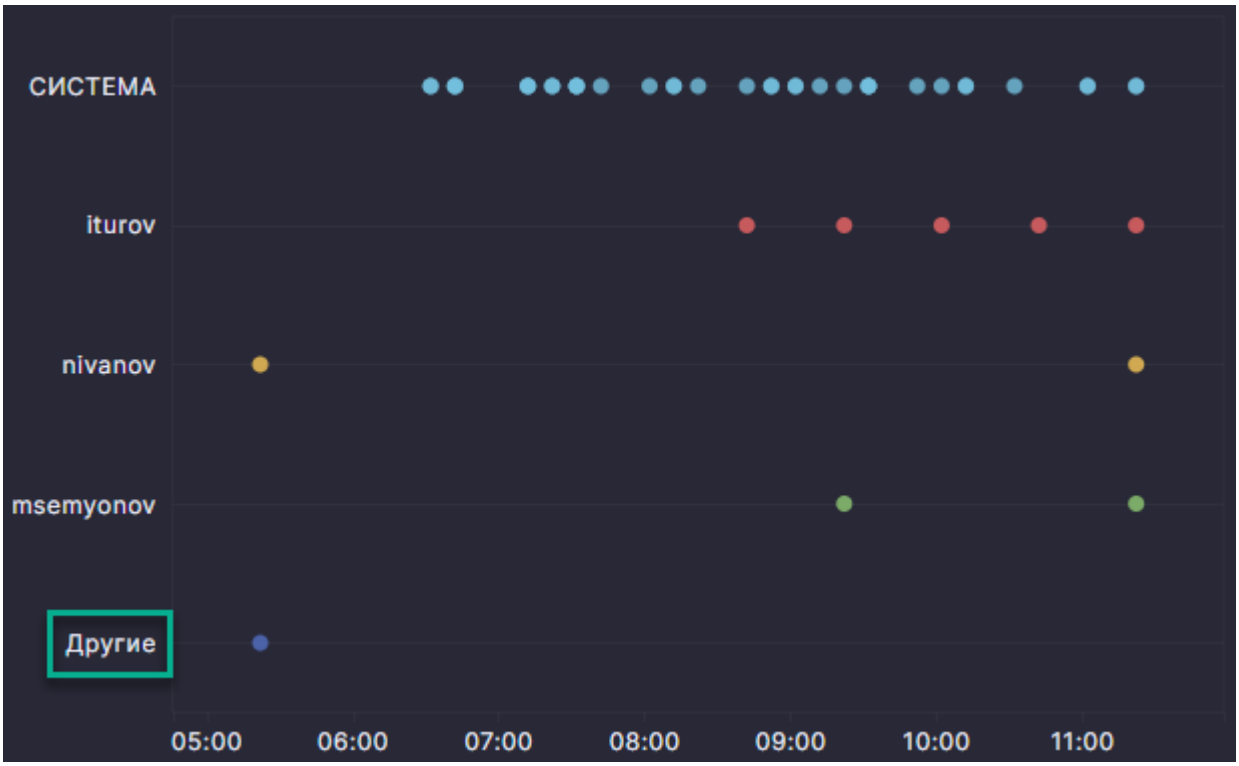
Отражает факты возникновения событий в виде точек вдоль горизонтальной оси (оси времени).



При отображении графиком двух и более параметров их наименования располагаются вдоль вертикальной оси (оси параметров). Данные откладываются по осям и изображаются рядом точек напротив соответствующего параметра, где каждая точка отмечает факт возникновения события, обладающего этим параметром. Параметры и ряды их точек следуют сверху вниз в порядке уменьшения количества точек ряда. Ряды выделяются индивидуальными цветами.

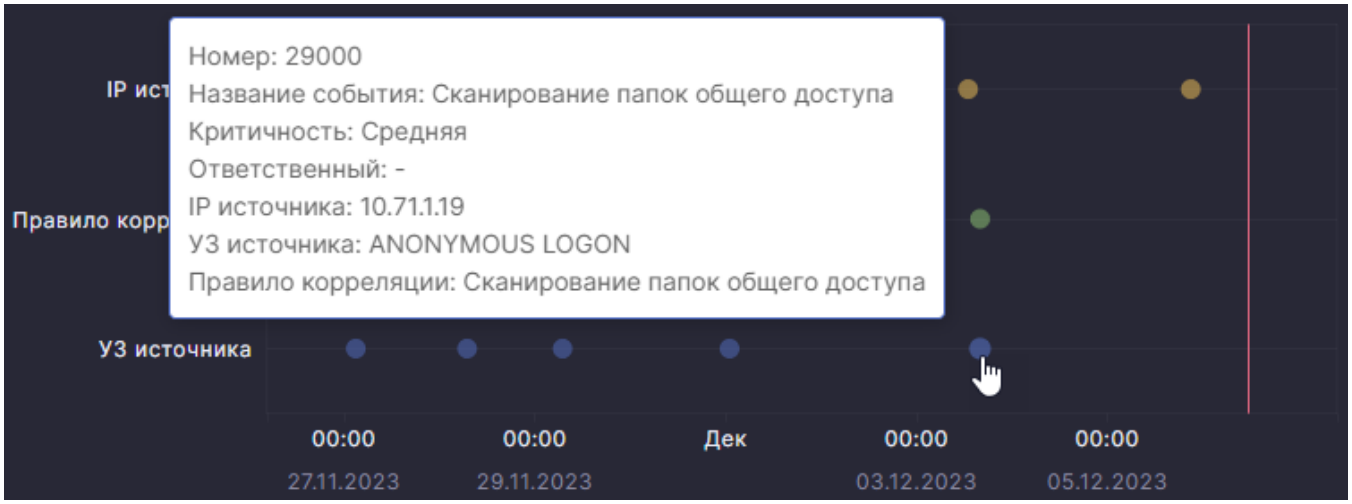


Если для графика задано ограничение одновременно изображаемых параметров, параметры вне изображаемого диапазона скрываются, а их точки объединяются в ряд автоматически создаваемого параметра «Другие». Его положение на вертикальной оси определяется количеством объединенных точек.



Вы можете выполнять следующие действия с графиком:

- Показать всплывающее окно с информацией, относящейся к точке, наведя на нее указатель мыши.



- Изменить масштаб временной оси (масштабировать на позиции курсора/указателя мыши), используя колесо мыши.

  Увеличение масштаба временной оси позволяет разделить точки, находящиеся слишком близко друг к другу.

- Сдвинуть точки вдоль временной шкалы/оси, зажав левую кнопку мыши внутри области графика и перетащив его по горизонтали в нужную сторону.

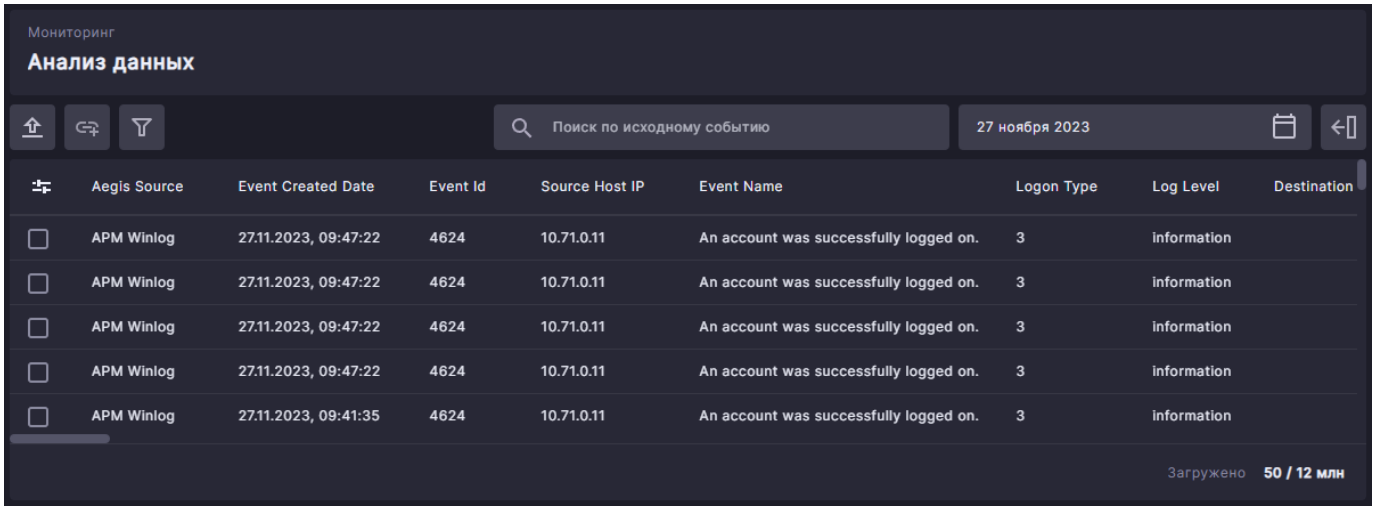
8.2 Функциональные модули

8.2.1 Модуль «Анализ данных»

Позволяет находить подготовленные и исходные события, удовлетворяющие определенным критериям, группировать и анализировать данные результатов поиска для выполнения следующих задач:

- настройка источников в рамках процесса сбора событий;
- регистрация событий ИБ в рамках процессов мониторинга и исследования событий;
- проведение расследований инцидентов ИБ.

Для отображения найденных событий и групп используется табличное представление.



Поиск событий

Вы можете использовать следующие элементы модуля, чтобы задать параметры поиска:

- Редактор дат для указания временного диапазона создания событий.

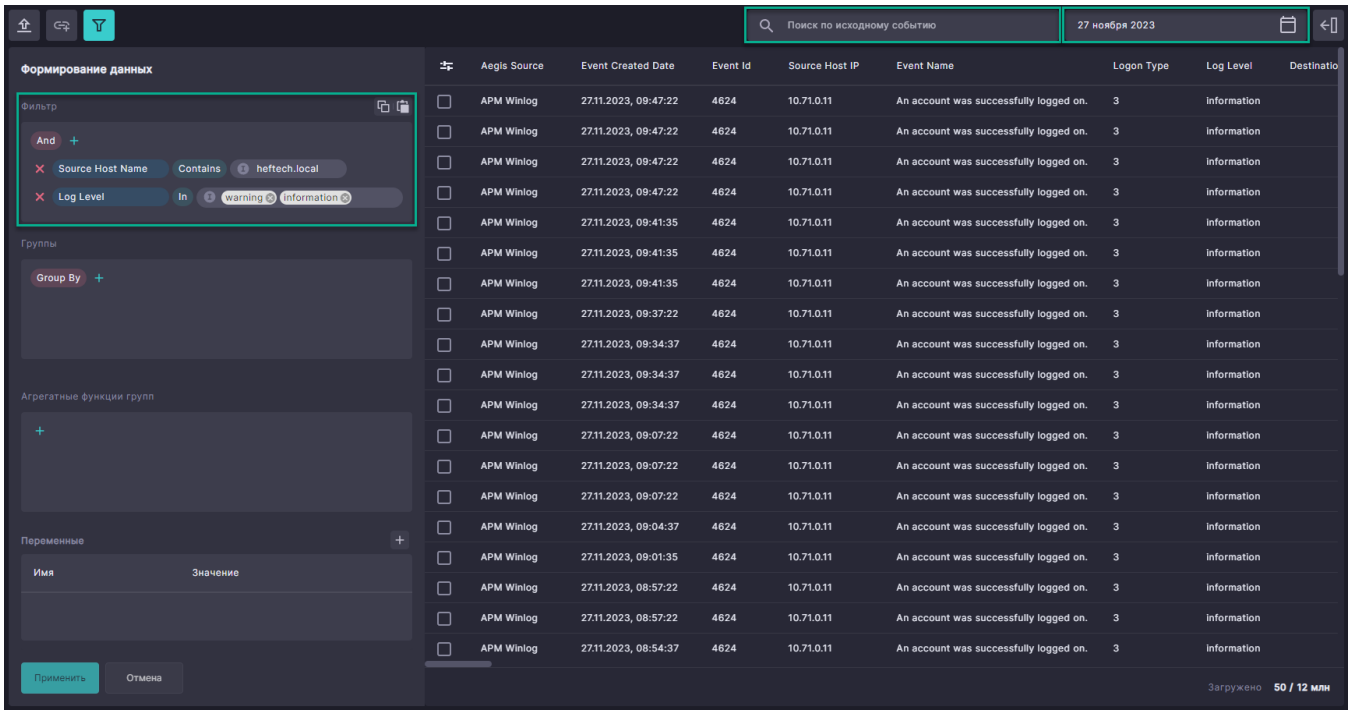
Позволяет исключить события, которые были созданы вне указанного диапазона дат (определяется по значению системного поля **Event Created Date**).

- Строка поиска по исходному событию.

  Позволяет найти события, в тексте исходного события которых содержится заданная строка.

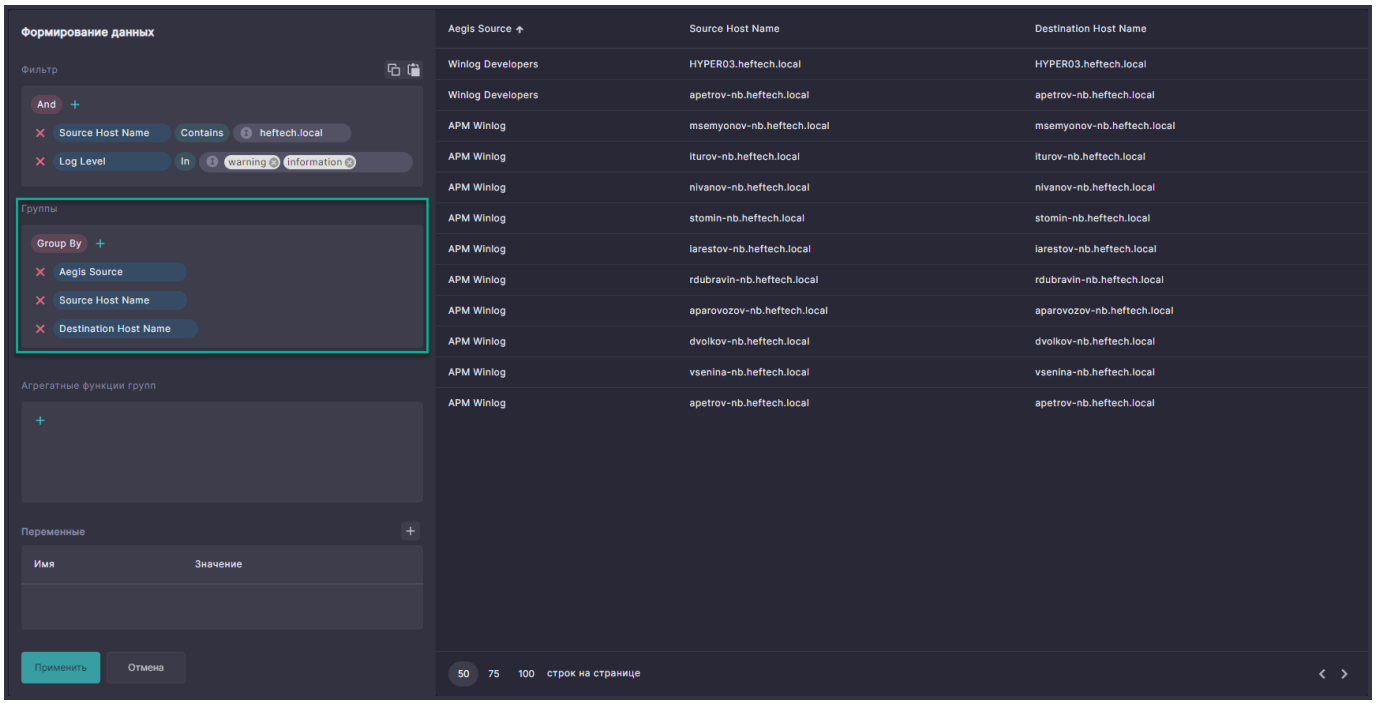
- Настройки фильтрации событий.

  Для изменения настроек воспользуйтесь функциями секции «Фильтр» в панели «Формирование данных».



Группировка событий

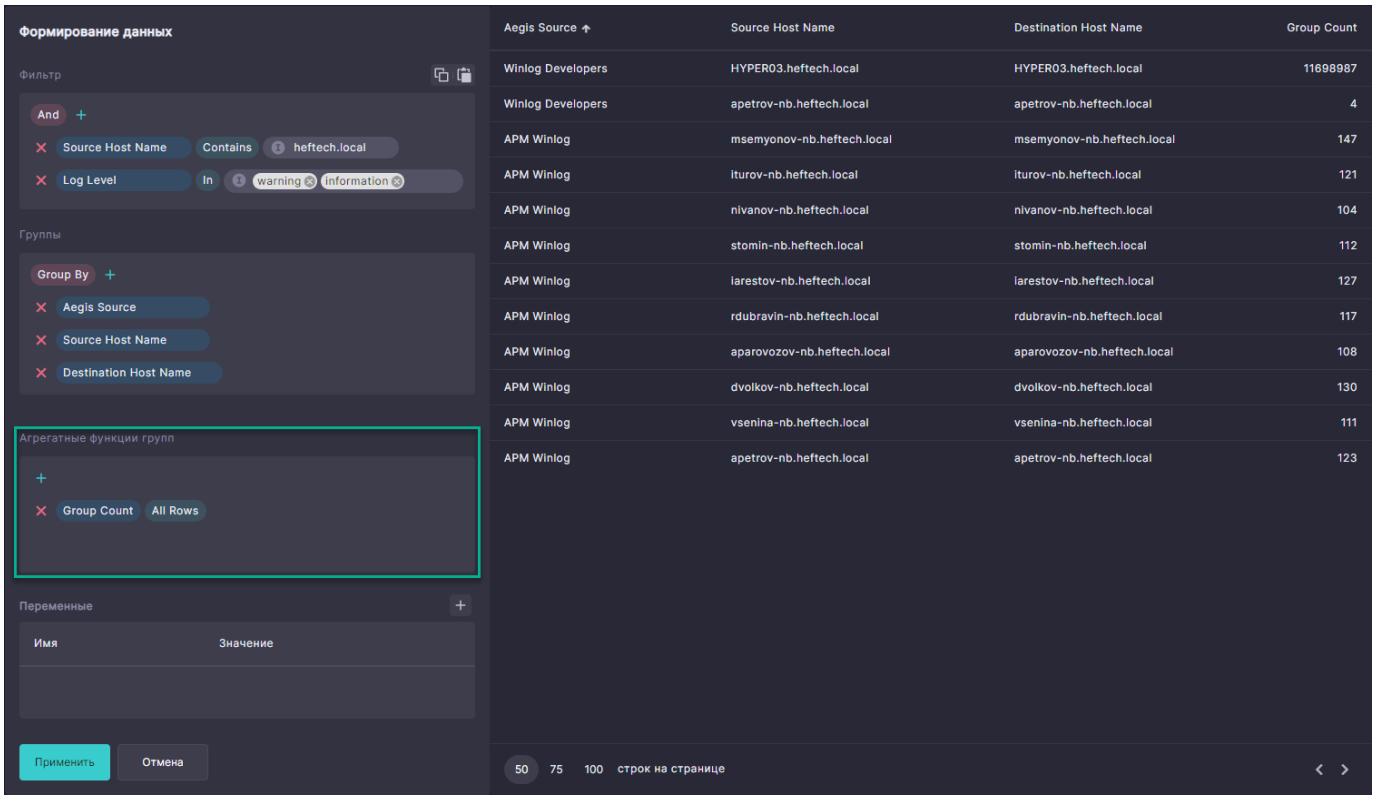
Для настройки воспользуйтесь функциями секции «Группы» в панели «Формирование данных».



При примененной группировке события в таблице замещаются группами. Группа представляет собой уникальное сочетание значений заданных полей и объединяет в себе соответствующие этому сочетанию события.

РАСЧЕТ АГРЕГИРОВАННЫХ ЗНАЧЕНИЙ ПО ГРУППАМ

При заданных полях группировки вы можете настроить расчет агрегированных значений по событиям каждой из групп. Для настройки воспользуйтесь функциями секции «Агрегатные функции групп» в панели «Формирование данных».



Значения полей группы отображаются в строках таблицы совместно с агрегированными значениями.

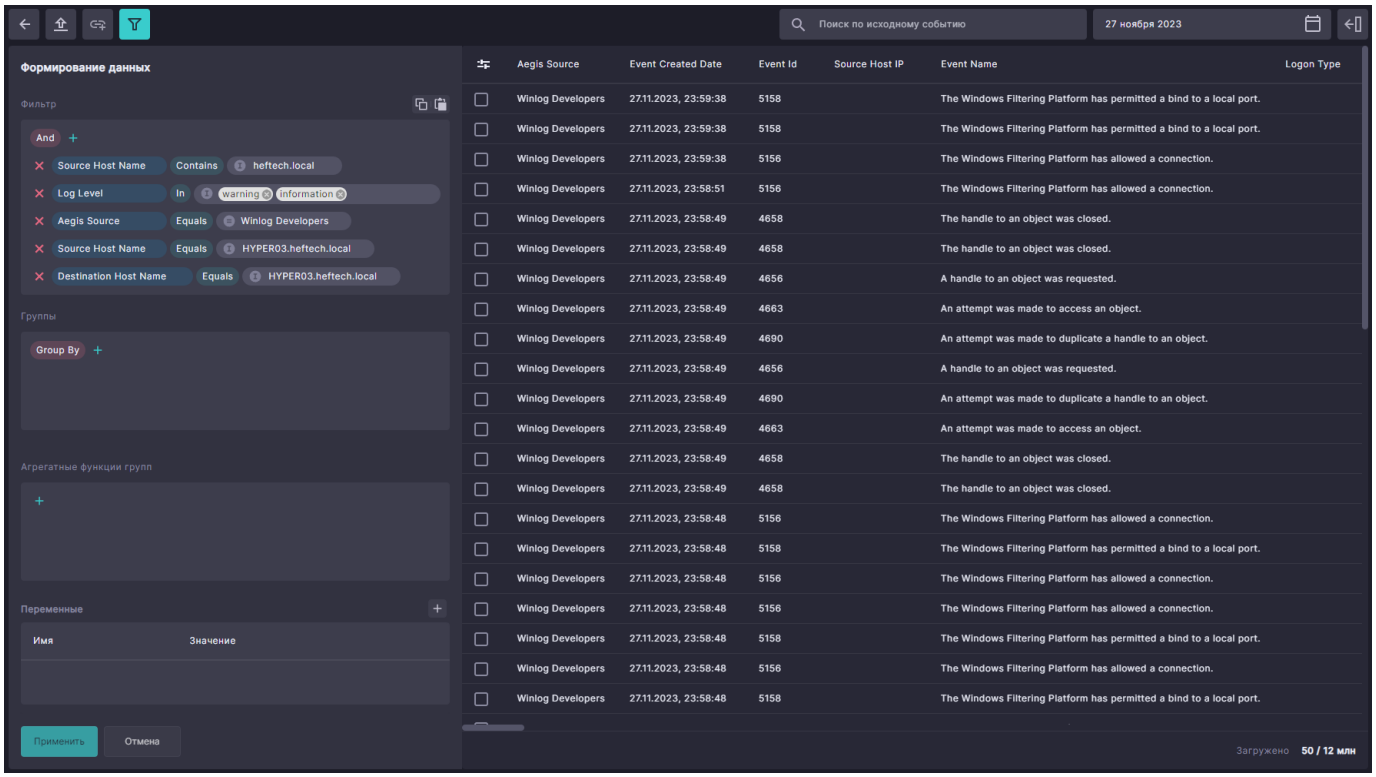
ПРОСМОТР ДЕТАЛЬНОЙ ИНФОРМАЦИИ ПО ГРУППЕ

Найдите в таблице запись с требуемой группой и откройте детальную информацию по ней одним из следующих способов:

- Дважды щелкните мышью по записи.
- Наведите указатель мыши на запись и нажмите появившийся контекстный значок .

Модуль перейдет в режим просмотра детальной информации по группе:

- В таблице будут показаны события, объединенные в эту группу.
- В фильтр будут добавлены критерии с оператором **Equals** и его операндами, заполненными соответствующими группе полями и их значениями.



Чтобы вернуться в предыдущий режим просмотра, нажмите значок ← («Вернуться назад»).

Связывание событий с событием/инцидентом ИБ

Вы можете использовать следующие элементы модуля, чтобы выполнить связывание:

1. В таблице выбрать одно или более событий, которые нужно связать с событием/инцидентом ИБ.
2. Нажать значок 🔗 («Связать с событием ИБ»).
3. В открывшемся окне «Связывание событий с событием ИБ» выберите вариант связывания:

    - Чтобы связать с существующим событием/инцидентом ИБ, нажмите опцию «Существующее» в качестве типа события ИБ и выберите нужный элемент из выпадающего списка «Событие ИБ».

    - Чтобы создать новое событие ИБ и связать с ним, нажмите опцию «Новое» в качестве типа события ИБ и заполните необходимые поля создаваемого события ИБ.

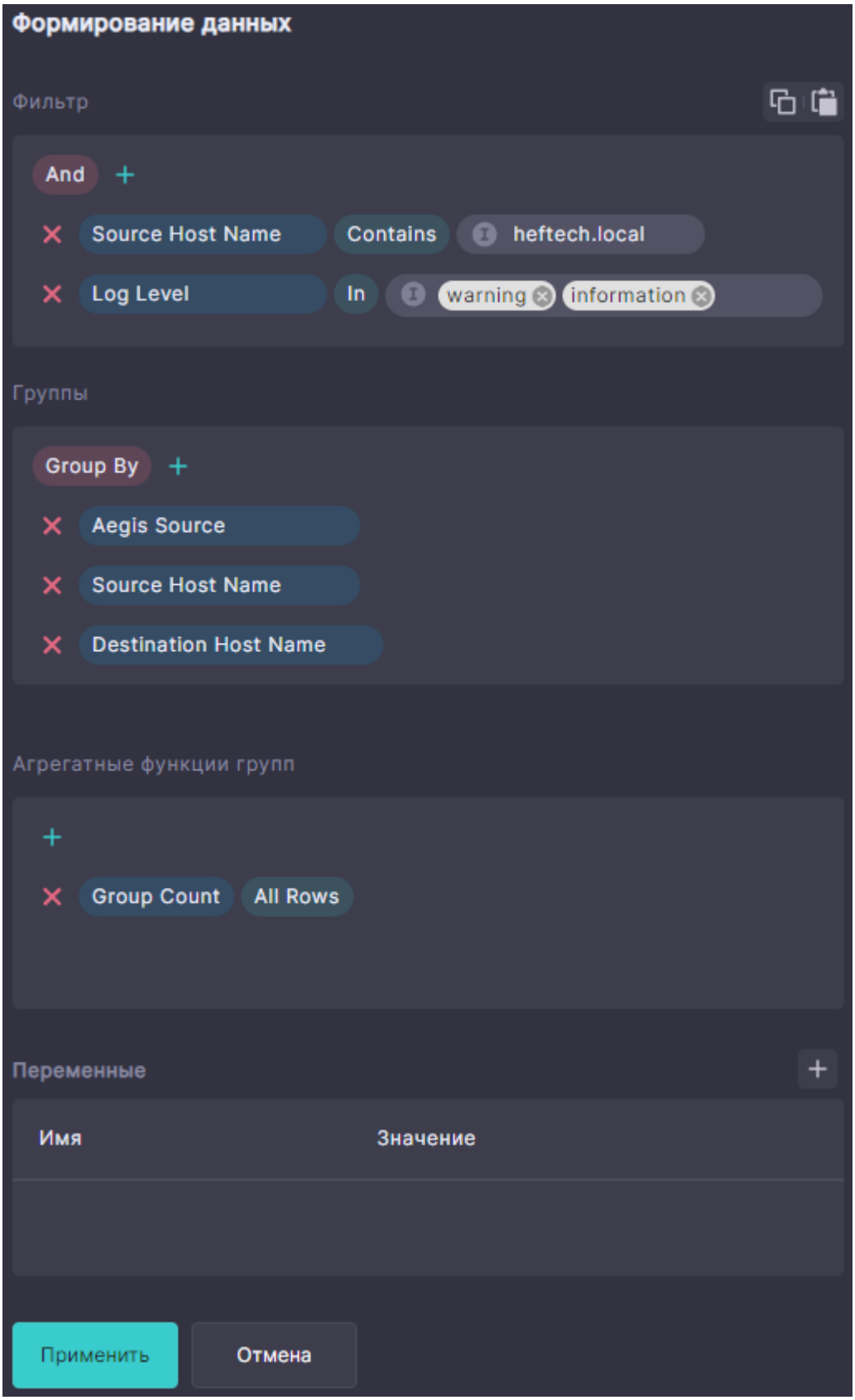
4. Нажмите кнопку «Сохранить».

    Окно «Связывание событий с событием ИБ» закроется, и откроется карточка связанного события/инцидента ИБ.

Чтобы отказаться от связывания, нажмите кнопку «Отмена». Окно «Связывание событий с событием ИБ» закроется, а все введенные в нем данные будут утеряны.

Панель «Формирование данных»

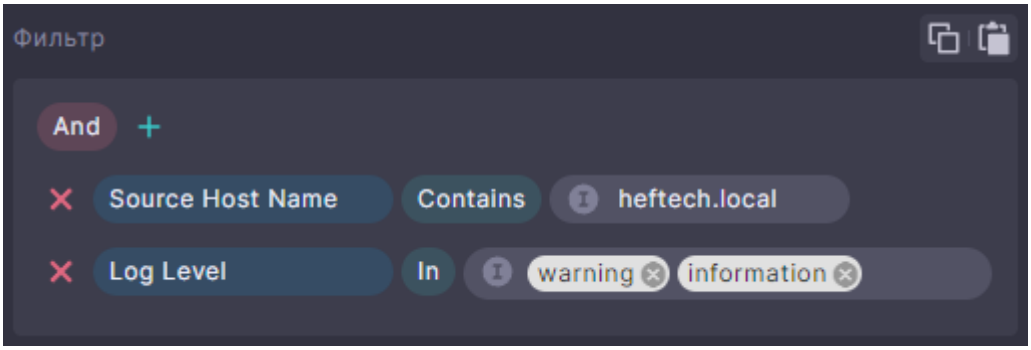
Чтобы открыть панель, нажмите значок  («Показать настройки фильтра»). Повторное нажатие значка закроет панель.



В панели параметры поиска и группировки разделены на секции, описанные ниже. Нажмите кнопку «Применить», чтобы применить введенные в панели изменения к параметрам. Для сброса последних, не примененных изменений нажмите кнопку «Отмена».

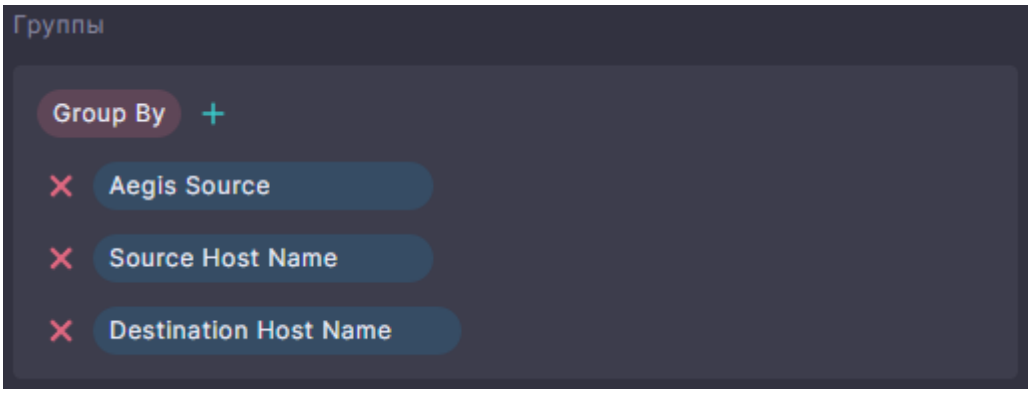
СЕКЦИЯ «ФИЛЬТР»

Позволяет задать критерии поиска подготовленных событий на основе их полей, значений полей и переменных, используя графический конструктор.



СЕКЦИЯ «ГРУППЫ»

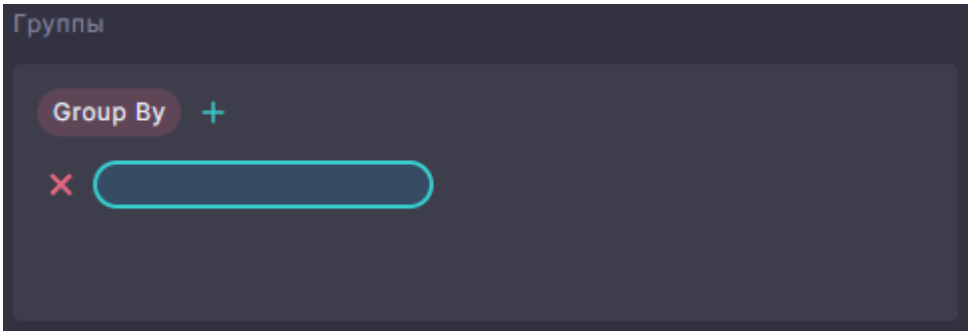
В этой секции можно задать группировку отображенных в таблице событий по определенным полям. Поля группировки отображаются в виде настраиваемого списка, каждый элемент которого содержит блок с именем поля.



Для управления полями группировки воспользуйтесь функциями списка, описанными ниже.

Создание поля группировки

Нажмите значок + , отображаемый в начале списка, чтобы создать его элемент. Элемент будет добавлен в конец списка.



В созданном элементе не задано имя поля. Нажмите на его блок и выберите нужное имя из выпадающего списка.

Замена поля группировки

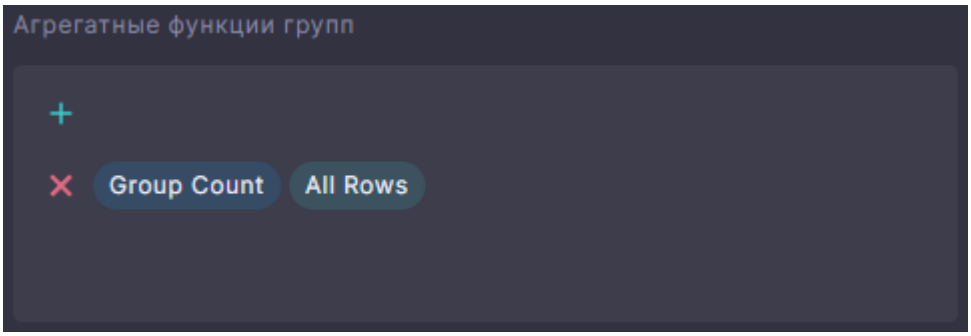
Нажмите на блок поля и выберите другое имя из выпадающего списка.

Удаление поля группировки

Нажмите значок ✕, отображаемый слева от элемента списка, чтобы удалить этот элемент.

СЕКЦИЯ «АГРЕГАТНЫЕ ФУНКЦИИ ГРУПП»

Секция позволяет задать функции для расчета агрегированных значений по событиям каждой из групп. Функции отображаются в виде настраиваемого списка, каждый элемент которого содержит блок с именем функции и блок аргумента.



Поддерживается функция **Group Count** (подсчет количества элементов группы) и ее аргумент **All Rows**, означающий подсчет по всем строкам, включая содержащих значения Null (Нет данных). Расчет производится только при заданных полях группировки. Рассчитанные значения будут отображены в таблице совместно со значениями полей соответствующей группы.

Для управления агрегатными функциями и их аргументами воспользуйтесь функциями списка, описанными ниже.

Создание агрегатной функции

Нажмите значок +, отображаемый в начале списка, чтобы создать его элемент. Элемент будет добавлен в конец списка.

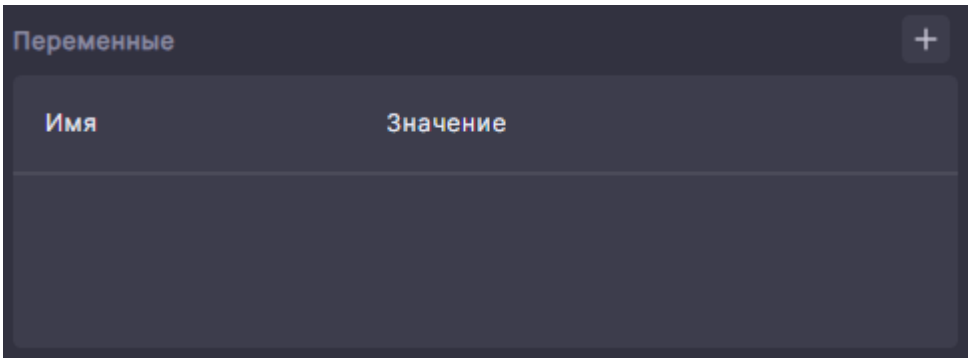
В созданном элементе по умолчанию задана функция **Group Count** и ее аргумент **All Rows**.

Удаление агрегатной функции

Нажмите значок ✕, отображаемый слева от элемента списка, чтобы удалить этот элемент.

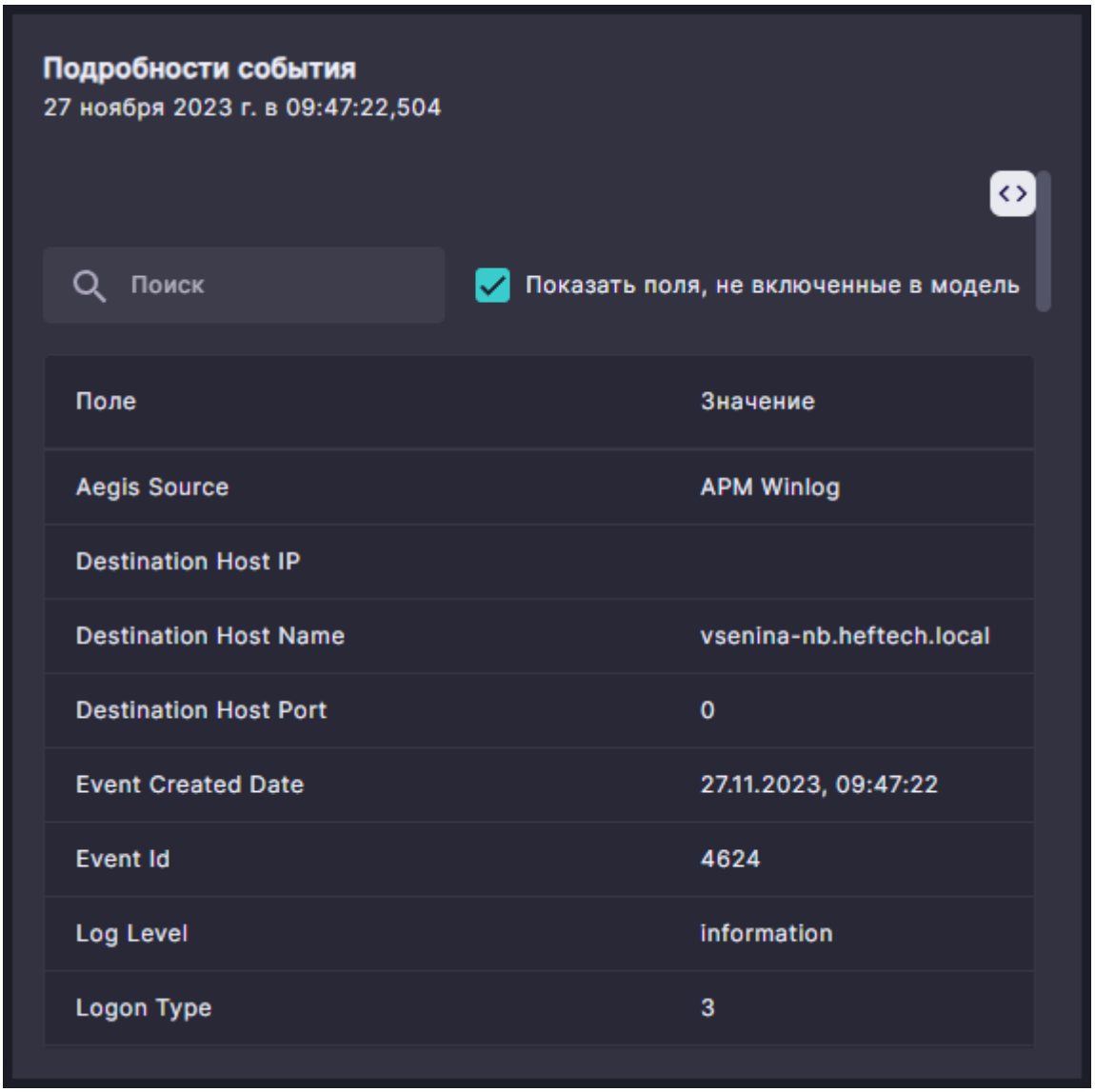
СЕКЦИЯ «ПЕРЕМЕННЫЕ»

В этой секции можно задать переменные для использования в фильтре.



Панель с подробностями события

Позволяет просмотреть поля подготовленного события, их значения, а также данные исходного события.



ПРОСМОТР ДАННЫХ ПОДГОТОВЛЕННОГО СОБЫТИЯ

1. Найдите в таблице требуемое событие и выберите его.
2. Нажмите значок () («Показать подробности события»), чтобы открыть панель для отображения информации о выбранном событии.

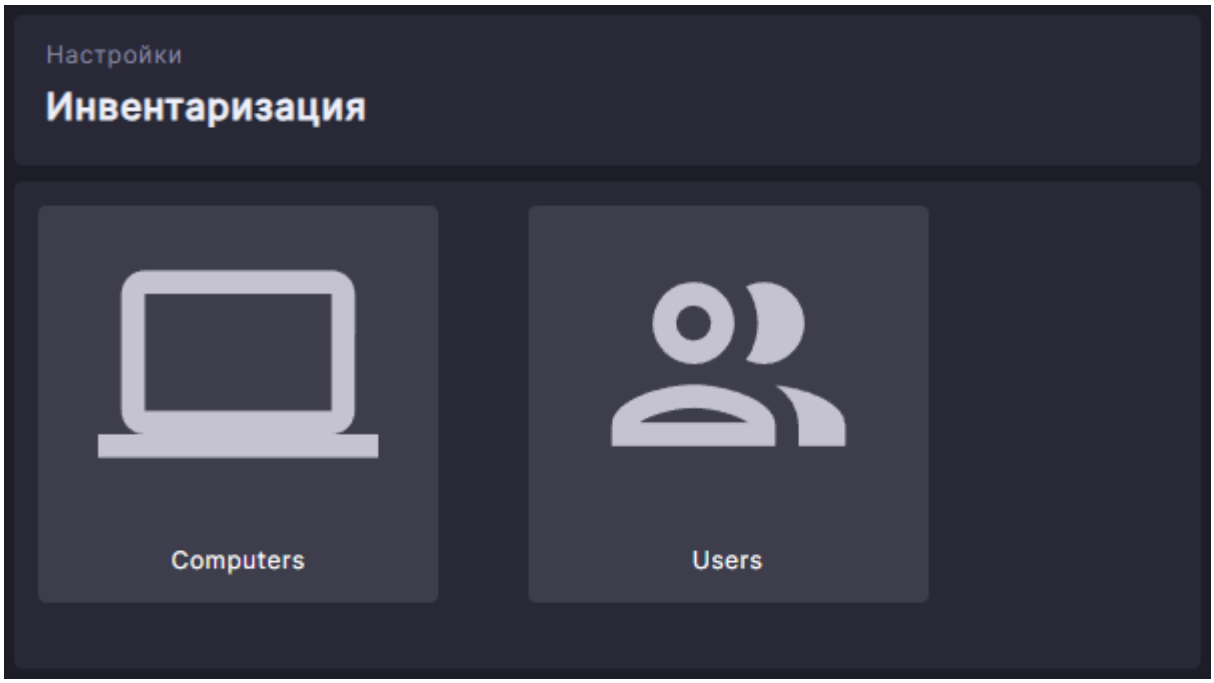
Панель отобразит список полей модели, использованных при подготовке события, и их данные, полученные из исходного события в результате нормализации. Чтобы закрыть панель, нажмите значок () («Скрыть подробности события»).

ПРОСМОТР ДАННЫХ ИСХОДНОГО СОБЫТИЯ

Доступен при показе в панели данных подготовленного события. Нажмите значок () («Показать исходное событие») над полями подготовленного события для отображения данных исходного события. Повторное нажатие значка скроет их.

8.2.2 Модуль «Инвентаризация»

Позволяет вводить данные об активах организации, используемые в рамках процессов сбора событий, мониторинга и контроля, расследования и исследования событий и инцидентов ИБ. В Системе используется два типа активов: компьютеры (Computers) и пользователи (Users).

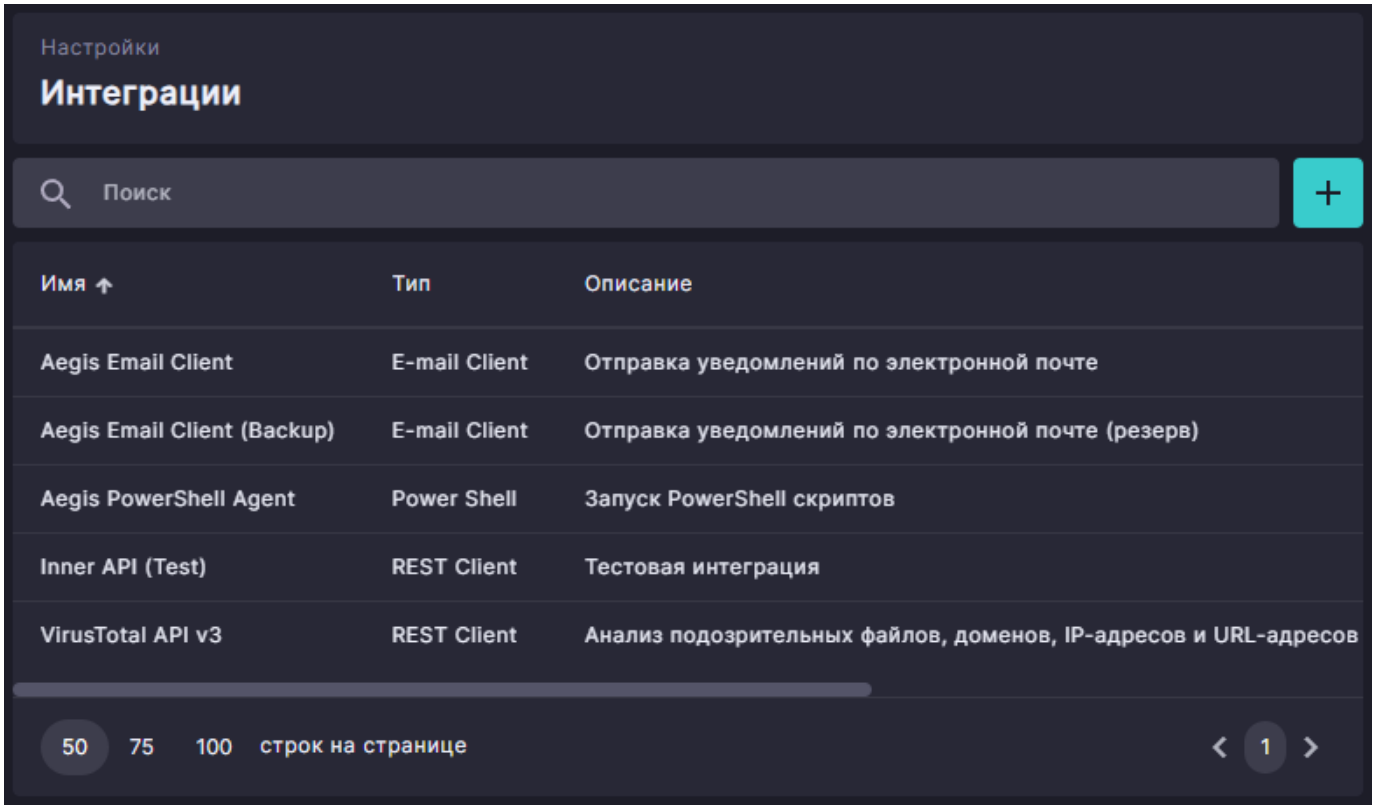


Нажмите на нужный тип актива для перехода к его данным. Для их отображения используется табличное представление.

В текущей версии Системы доступен режим просмотра данных активов. В следующих версиях будет доступен режим редактирования.

8.2.3 Модуль «Интеграции»

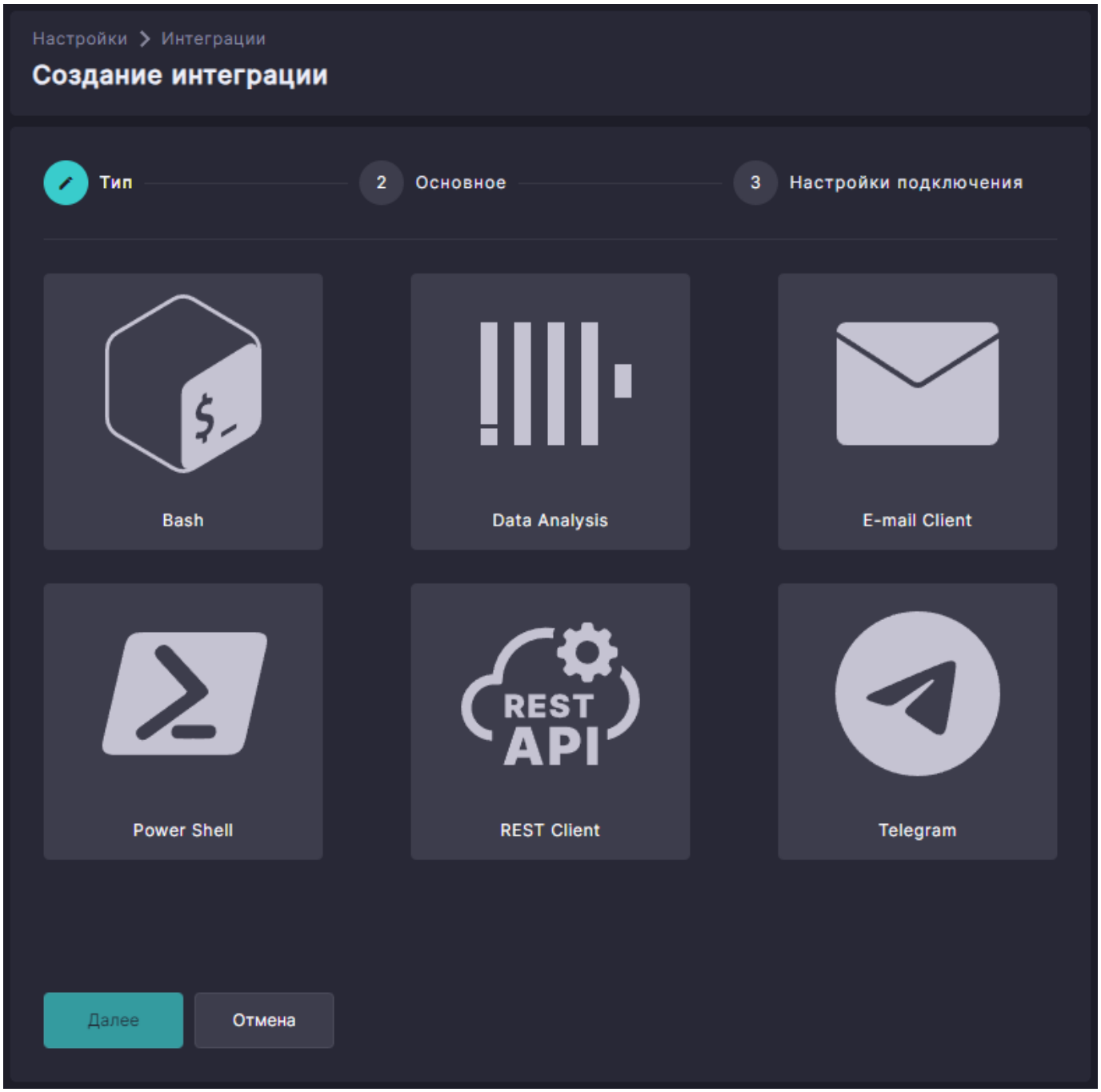
Позволяет настраивать параметры интеграции Системы с другими решениями и внешними источниками данных в целях выполнения автоматизированных действий сценариев реагирования.



Для отображения созданных интеграций используется табличное представление.

Создание интеграции

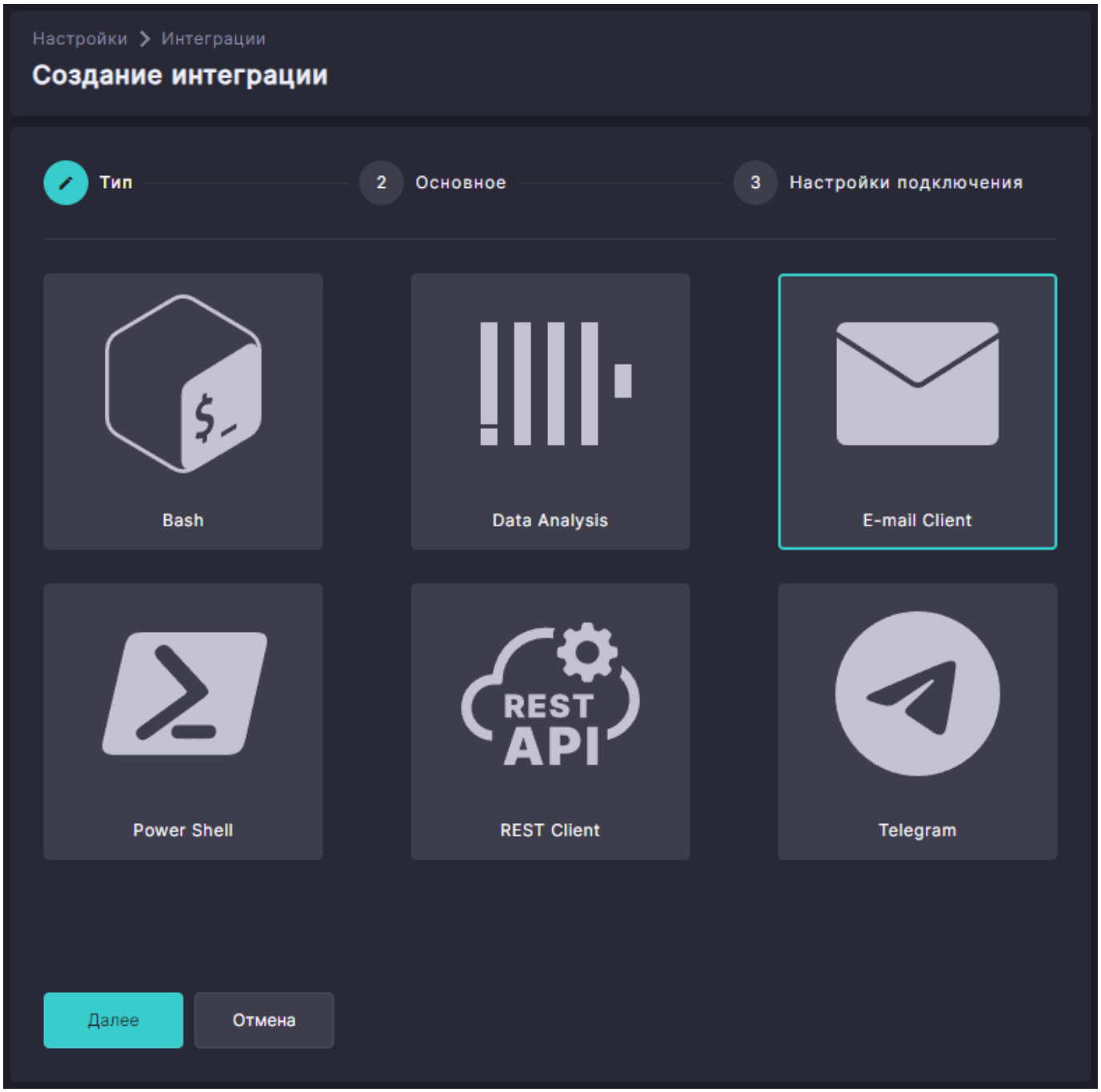
Нажмите значок + («Создать интеграцию»). В открывшемся окне «Создание интеграции» отобразится мастер конфигурации интеграции, облегчающий процедуру задания параметров интеграции.



Мастер конфигурации позволяет задать параметры интеграции по шагам, используя индивидуальные страницы. Перемещаться между шагами можно с помощью кнопок «Далее» и «Назад». Чтобы закрыть мастер и отказаться от создания интеграции, нажмите кнопку «Отмена».

СТРАНИЦА «ТИП»

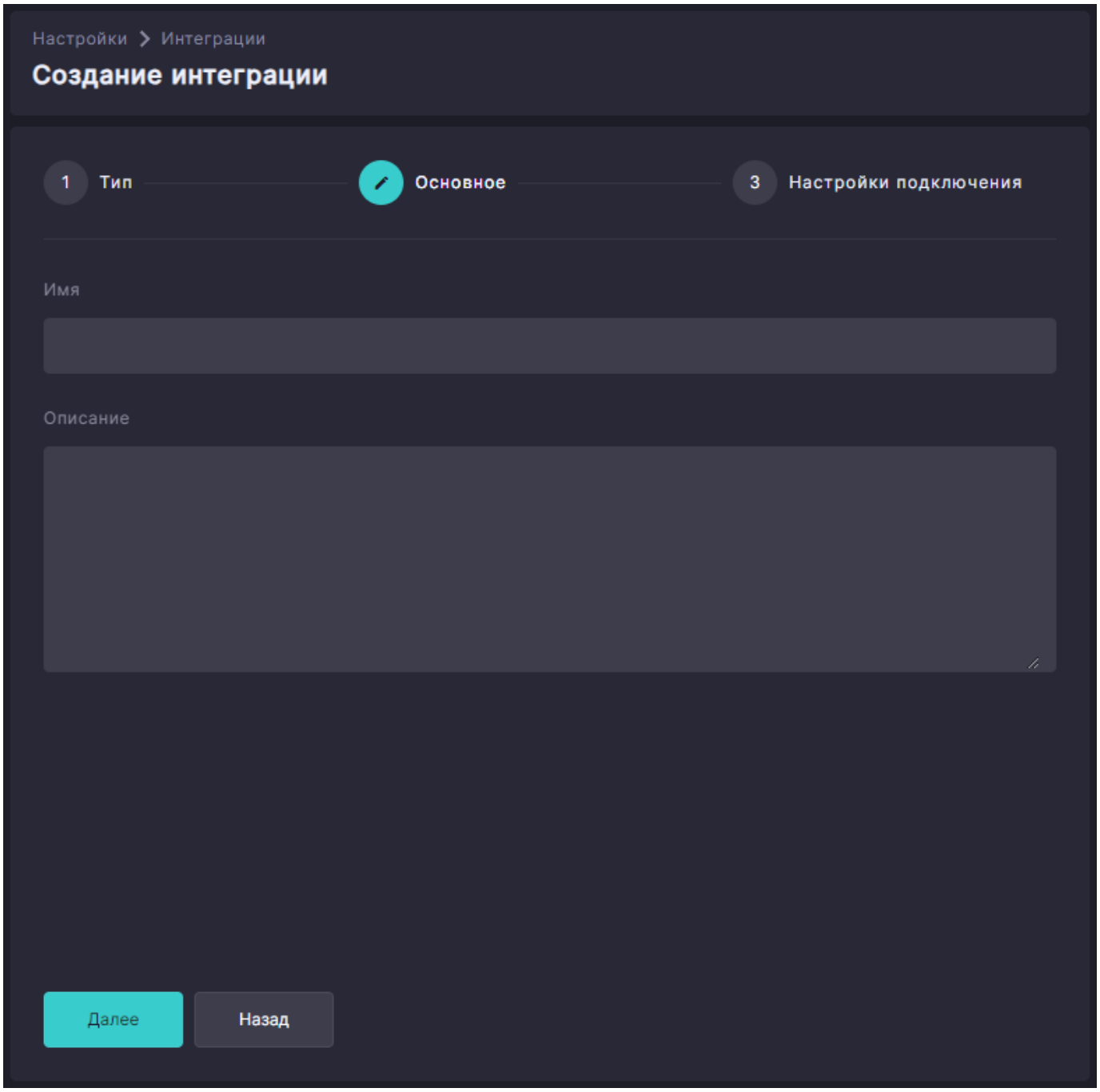
Выберите тип создаваемой интеграции нажатием на соответствующий элемент-шаблон в представленном на странице списке.



В текущей версии Системы доступно создание и использование REST Client и E-mail Client интеграций. В следующих версиях будут поддерживаться остальные типы интеграций.

Нажмите кнопку «Далее» для перехода на следующую страницу мастера конфигурации.

СТРАНИЦА «ОСНОВНОЕ»



Задайте параметры:

- Имя.

  Введите уникальное имя для идентификации интеграции в интерфейсе Системы.

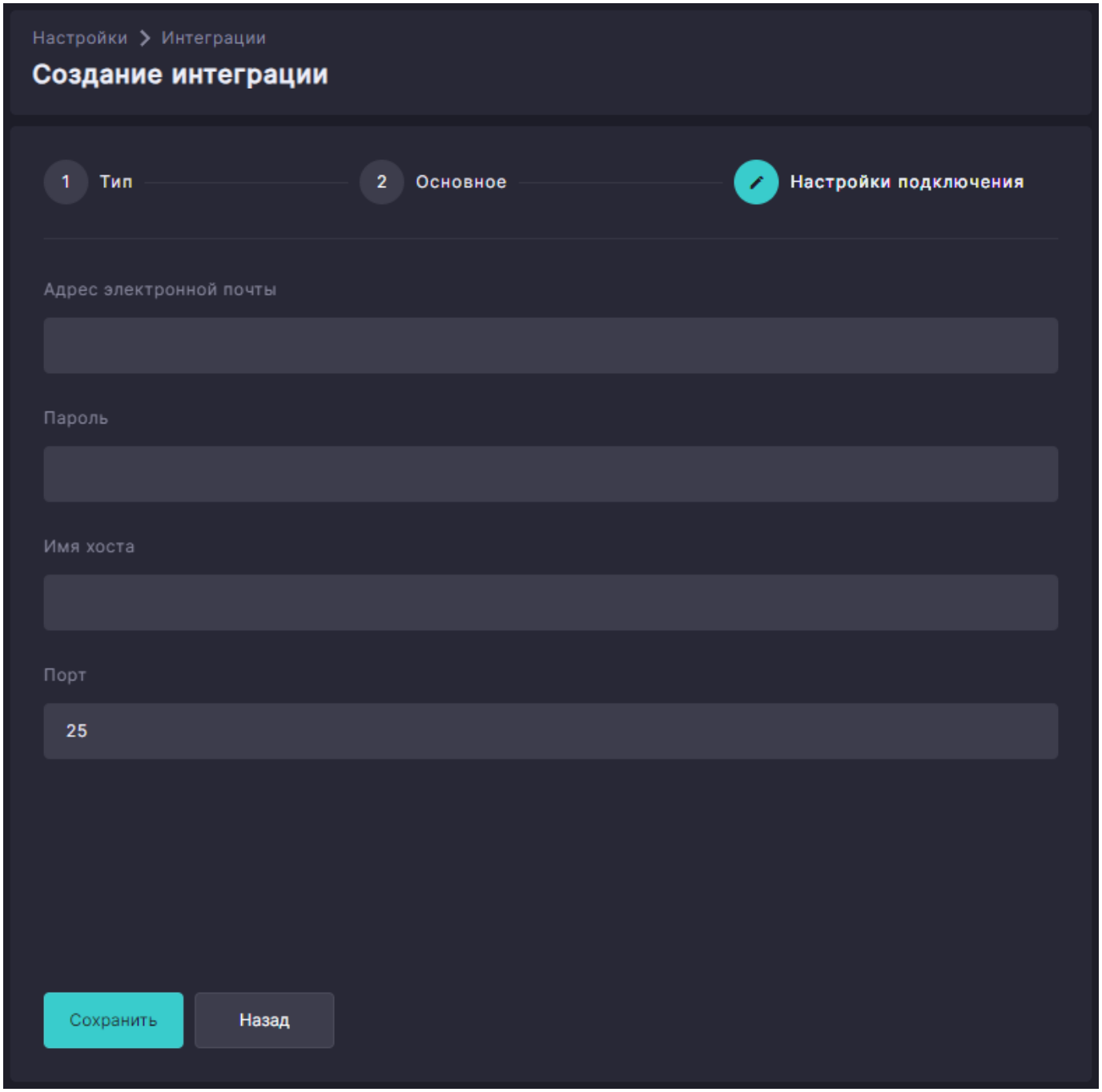
- Описание.

  При необходимости введите описание интеграции.

Нажмите кнопку «Далее» для перехода на следующую страницу мастера конфигурации.

СТРАНИЦА «НАСТРОЙКИ ПОДКЛЮЧЕНИЯ»

Система предоставляет настройку специфичных для типа интеграции параметров. Содержимое данной страницы варьируется в зависимости от типа интеграции. Ниже представлены параметры для типа интеграции «E-mail Client».

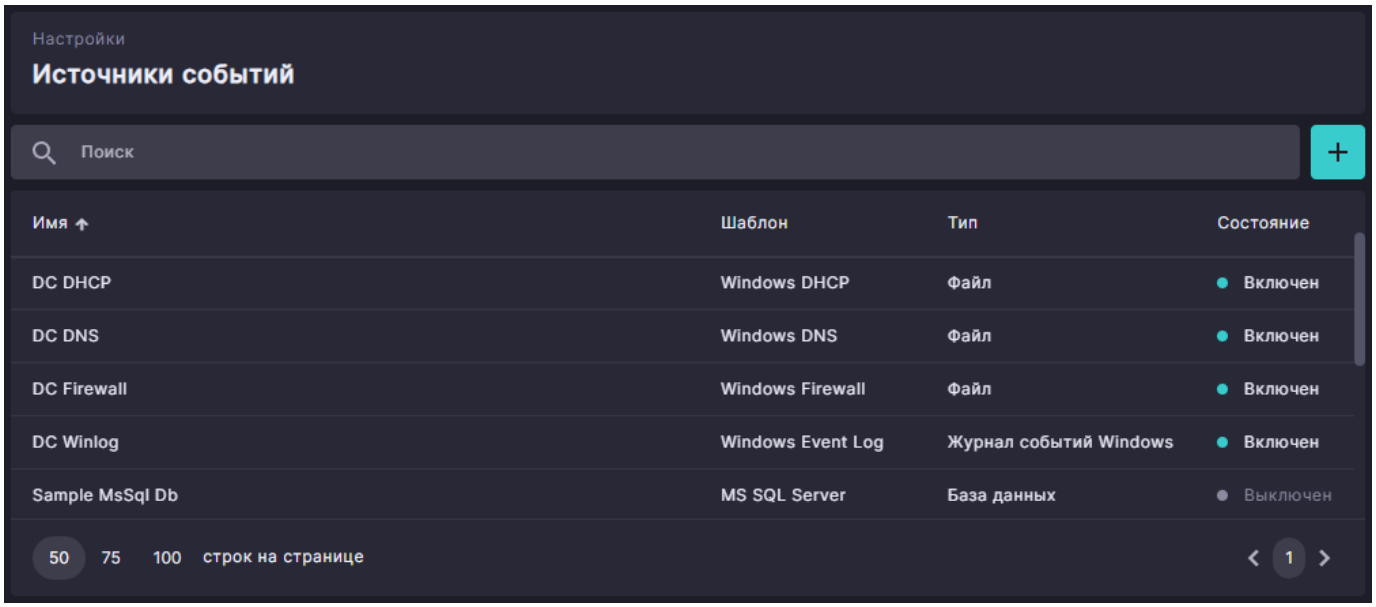


После введения параметров нажмите кнопку «Сохранить» для завершения работы мастера конфигурации. Окно «Создание интеграции» закроется, и созданный интеграция добавится в таблицу модуля.

8.2.4 Модуль «Источники событий»

Позволяет создавать и модифицировать источники в рамках процесса сбора событий из них.

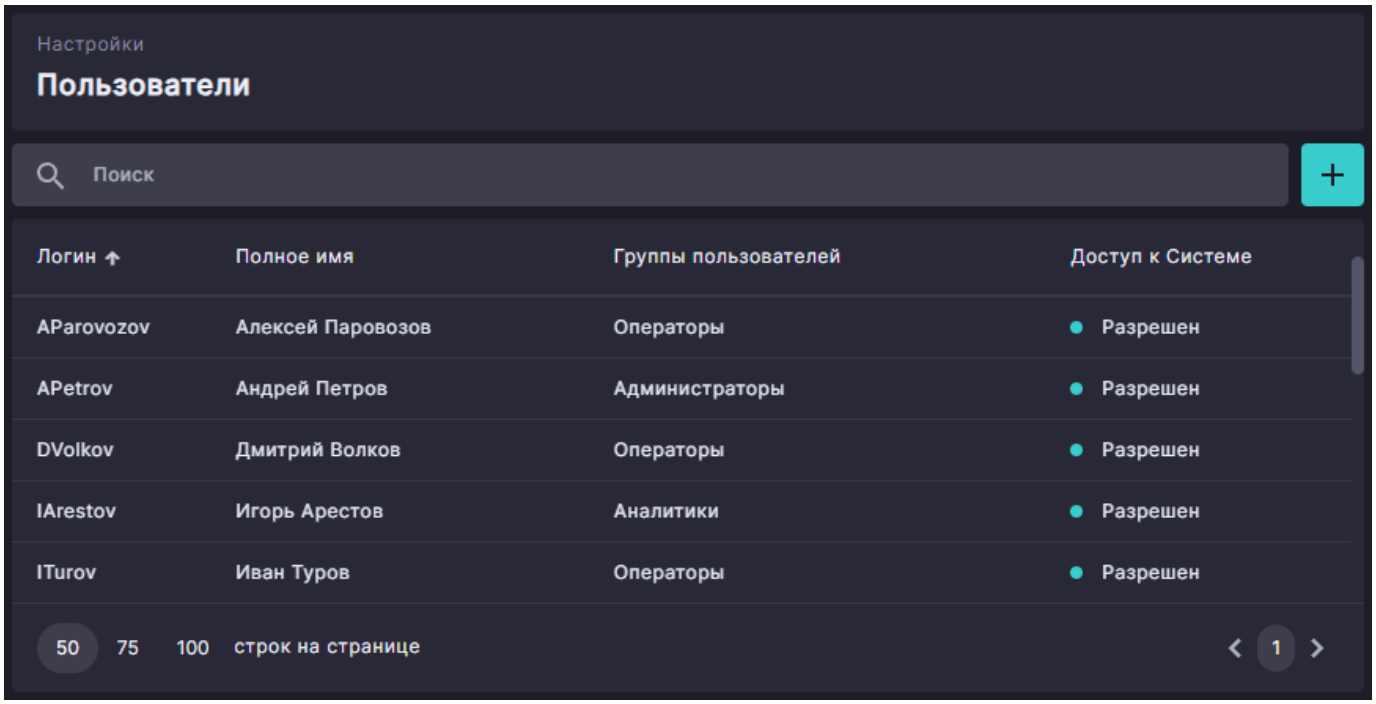
Для отображения созданных источников событий используется табличное представление.



8.2.5 Модуль «Пользователи»

Модуль используется для настройки пользователей Системы в рамках процесса мониторинга и контроля.

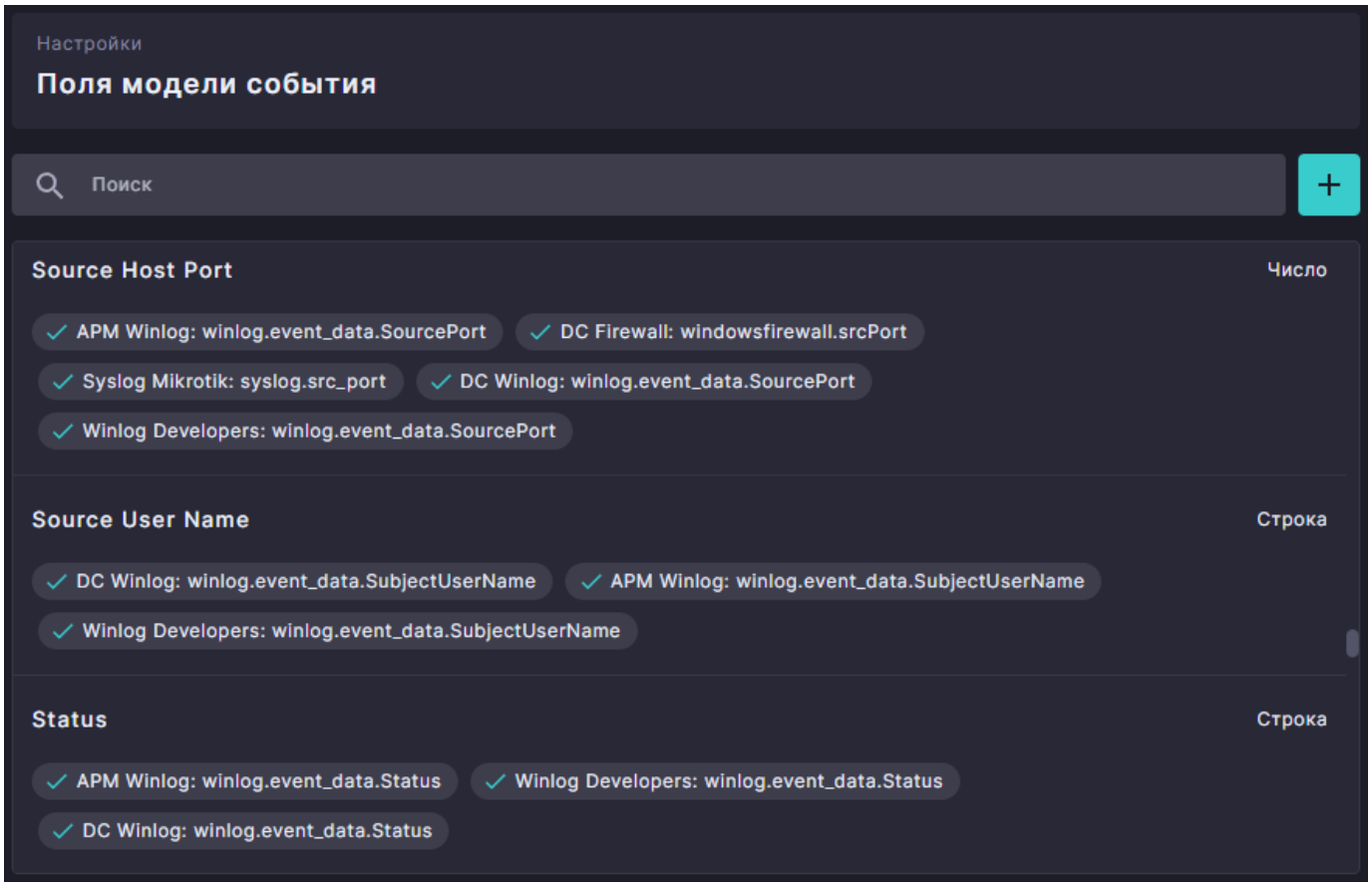
Для отображения зарегистрированных в Системе/созданных пользователей используется табличное представление.



8.2.6 Модуль «Поля модели события»

Позволяет создавать и модифицировать источники в рамках процесса сбора событий из них.

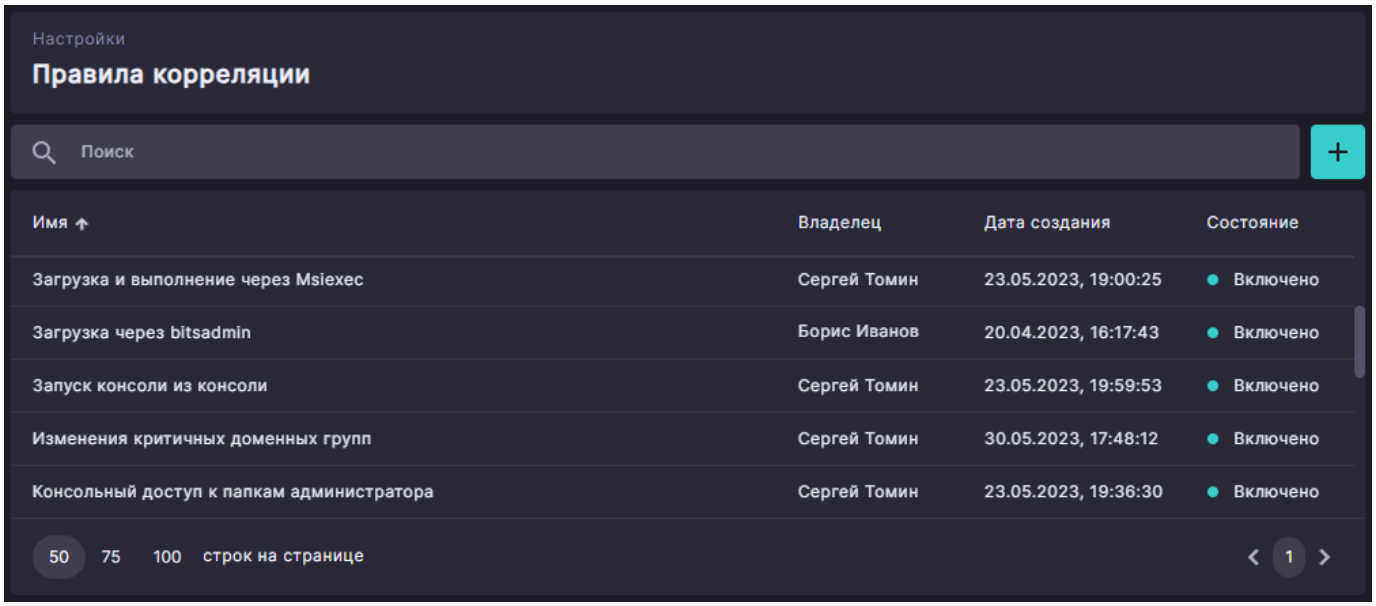
Для отображения созданных источников событий используется табличное представление.



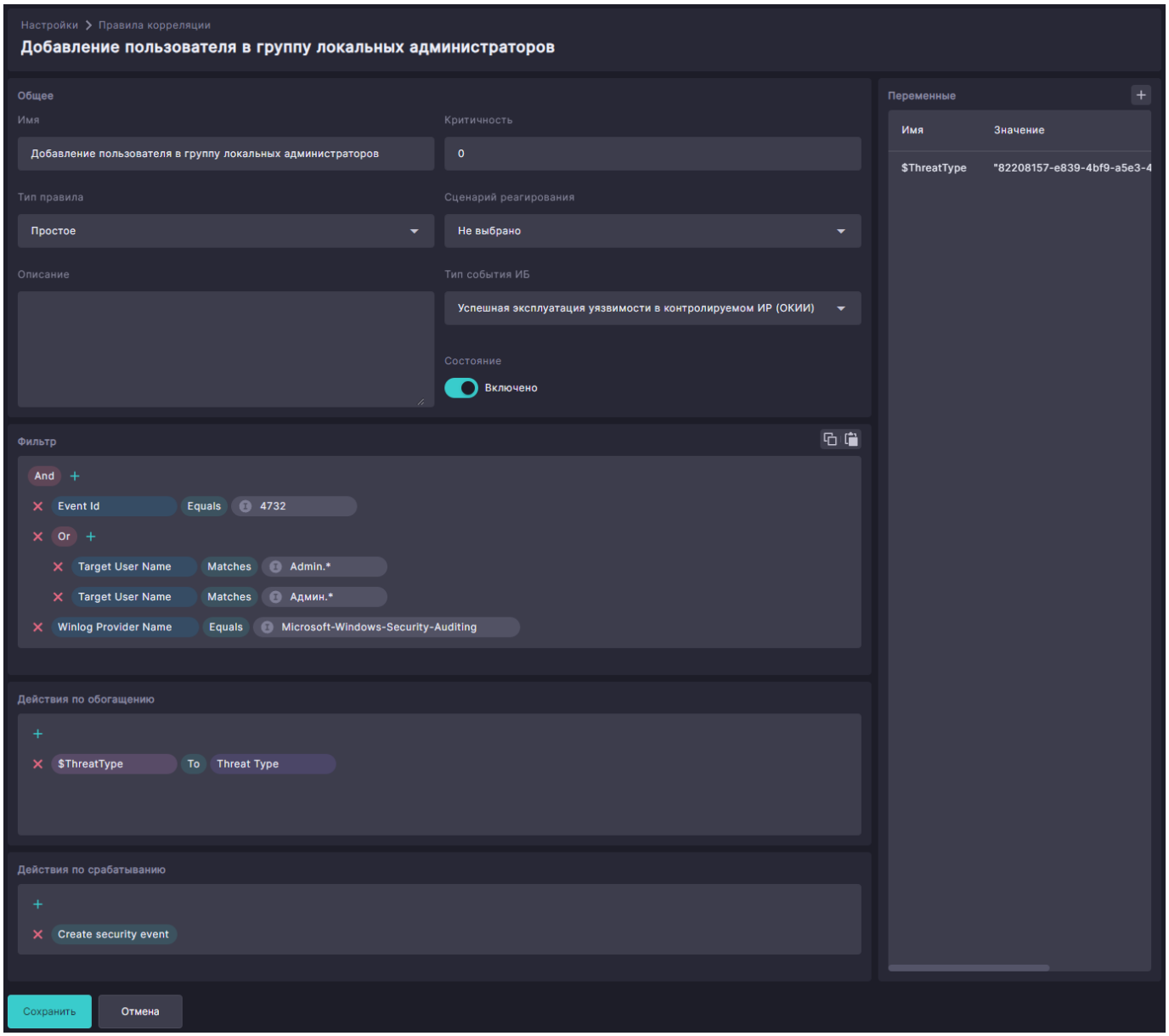
8.2.7 Модуль «Правила корреляции»

Позволяет управлять правилами корреляции и настраивать их в рамках процессов мониторинга и контроля и реагирования. Детальная информация по имеющимся возможностям управления и настройки приведена в этом разделе.

Для отображения созданных правил корреляции используется табличное представление.



Режим редактирования

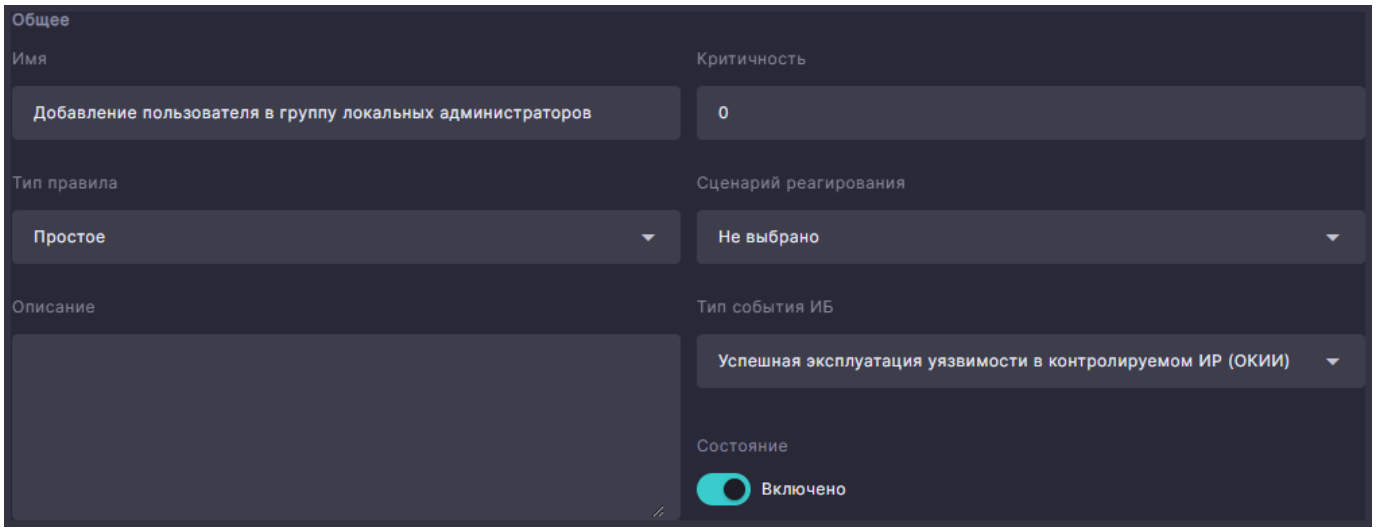


В режиме редактирования модуль предоставляет инструменты, позволяющие задать параметры правила корреляции. Инструменты расположены в следующих панелях:

- «Общее»;
- «Фильтр»;
- «Действия по обогащению»;
- «Параметры агрегации»;
- «Действия по срабатыванию»;
- «Переменные».

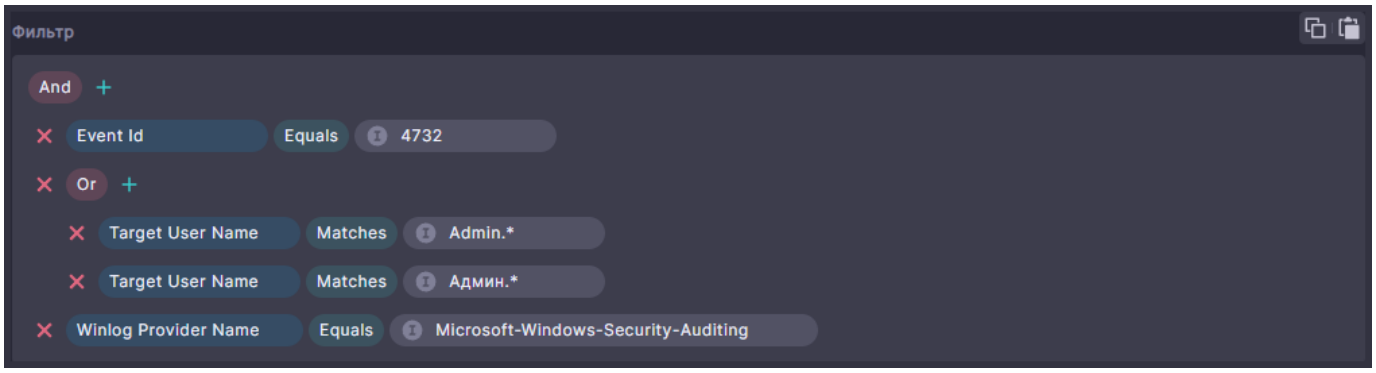
ПАНЕЛЬ «ОБЩЕЕ»

В этой панели можно задать имя правила, его тип, связанный сценарий реагирования и другие параметры. Также здесь можно производить запуск и останов правила.



ПАНЕЛЬ «ФИЛЬТР»

Позволяет настроить критерии поиска целевых событий, к которым будет применено правило корреляции. Вы можете задать критерии на основе полей событий, значений полей и переменных, используя графический конструктор.

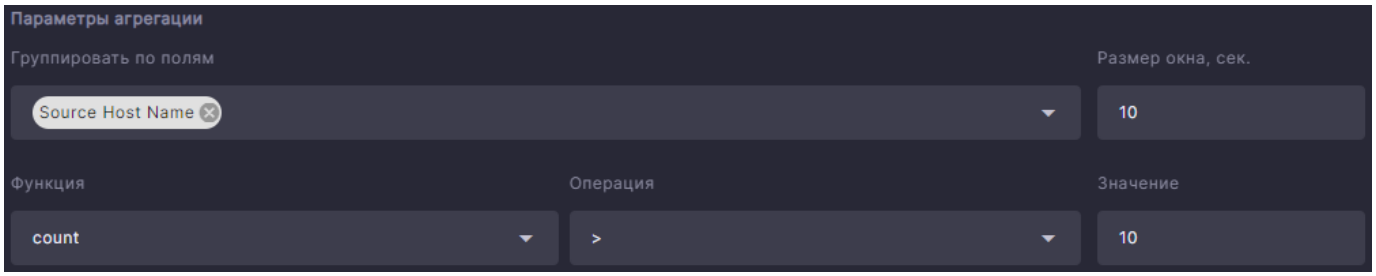


ПАНЕЛЬ «ДЕЙСТВИЯ ПО ОБОГАЩЕНИЮ»

В этой панели можно задать действия, производимые с удовлетворяющими фильтру целевыми событиями.

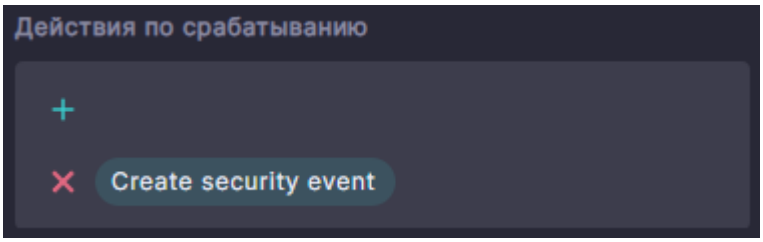
ПАНЕЛЬ «ПАРАМЕТРЫ АГРЕГАЦИИ»

Позволяет задать параметры, определяющие условие срабатывания правила на основе выявленной последовательности целевых событий, удовлетворяющих критериям фильтра. Панель отображается, если выбран тип правила «С агрегированием».



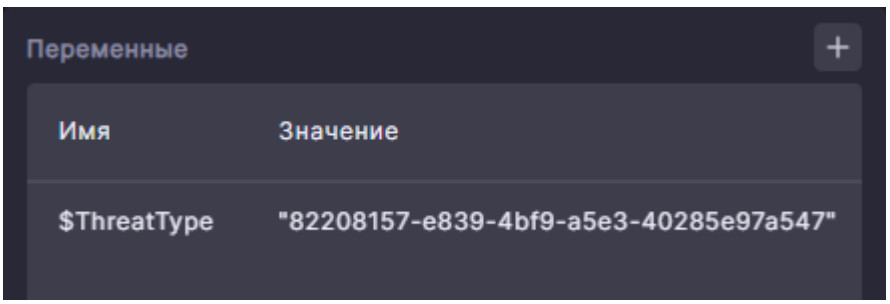
ПАНЕЛЬ «ДЕЙСТВИЯ ПО СРАБАТЫВАНИЮ»

Панель позволяет задать действия, производимые по срабатыванию правила.



ПАНЕЛЬ «ПЕРЕМЕННЫЕ»

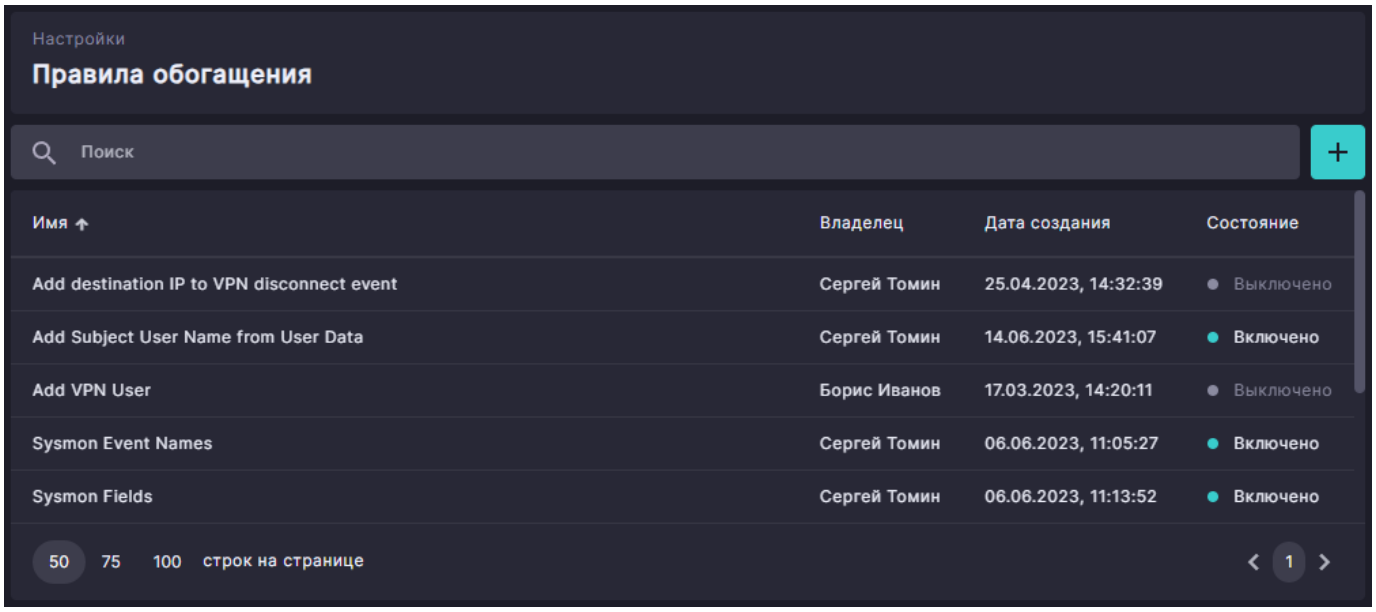
Здесь можно задать переменные для использования в правиле.



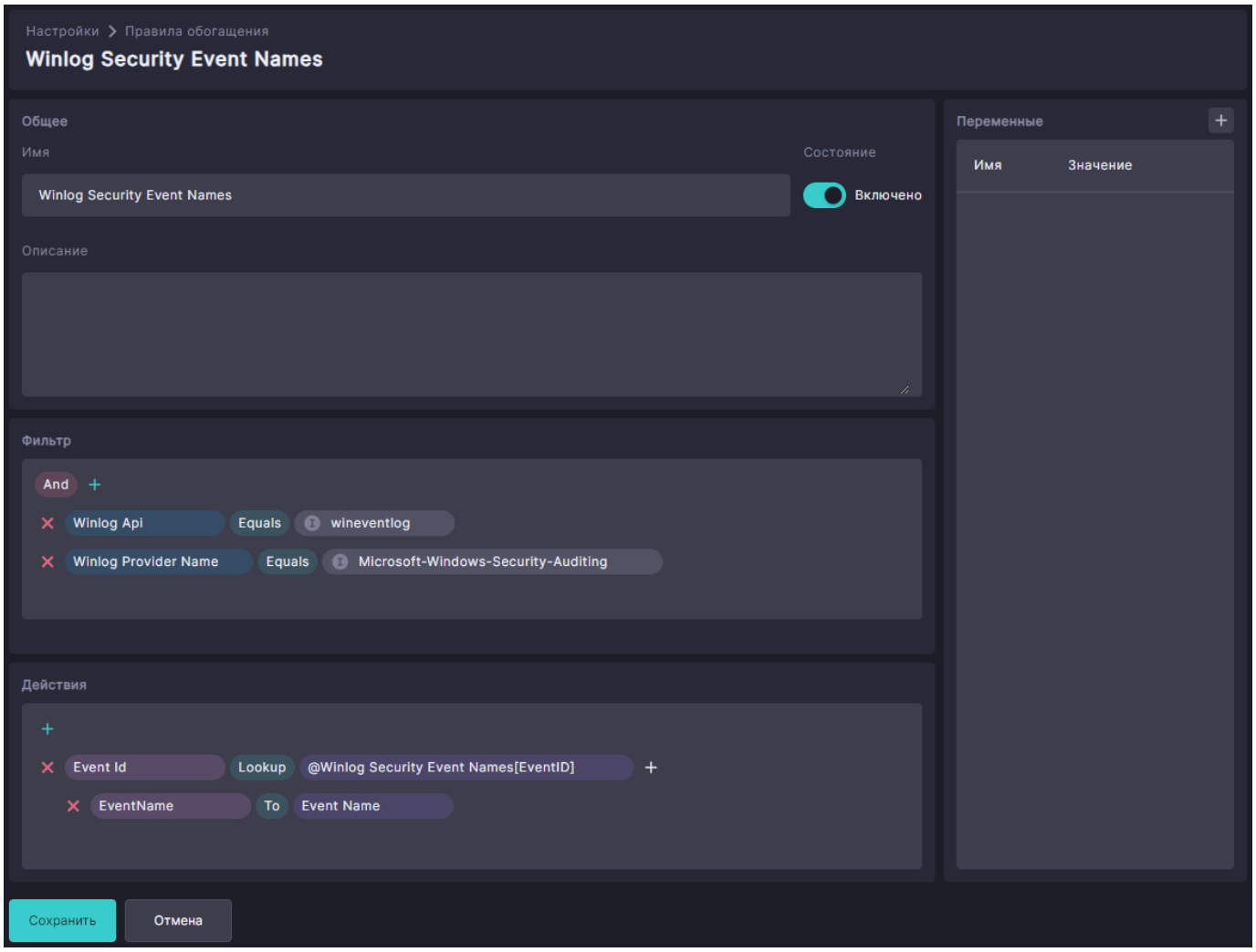
8.2.8 Модуль «Правила обогащения»

Позволяет настраивать правила обогащения событий в рамках процесса их сбора.

Для отображения созданных правил обогащения используется табличное представление.



Режим редактирования



В режиме редактирования модуль предоставляет инструменты, позволяющие задать параметры правила обогащения. Инструменты расположены в следующих панелях:

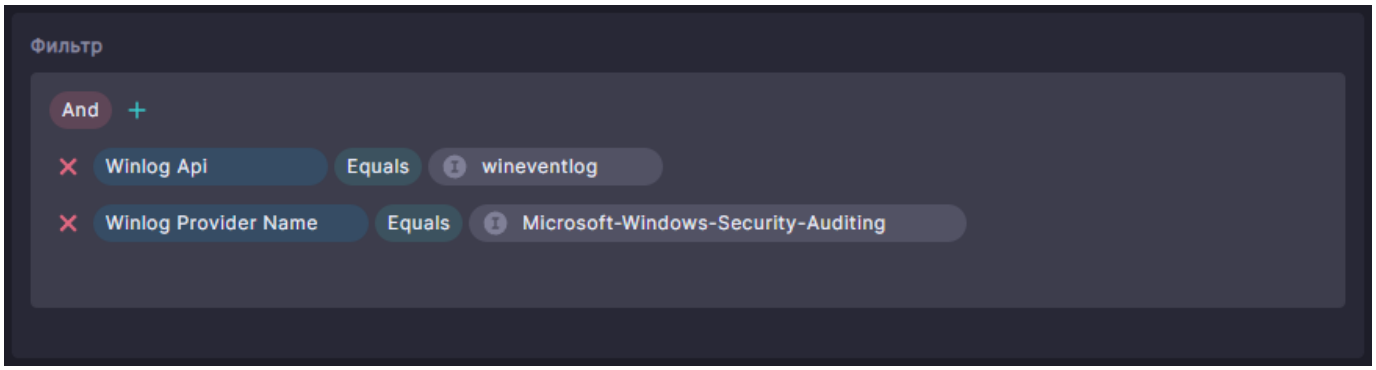
- «Общее»;
- «Фильтр»;
- «Действия по обогащению»;
- «Переменные».

ПАНЕЛЬ «ОБЩЕЕ»

В этой панели можно задать имя правила и его описание. Также здесь можно производить запуск и останов правила.

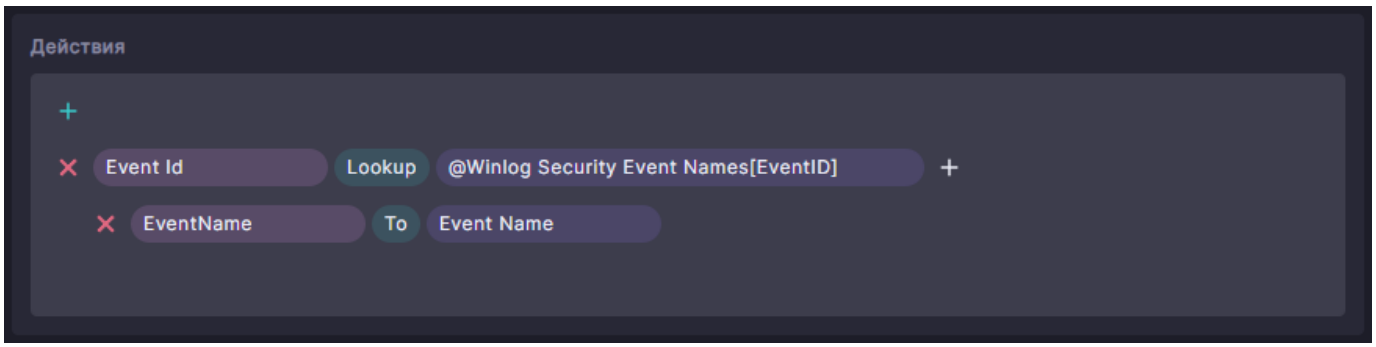
ПАНЕЛЬ «ФИЛЬТР»

Позволяет настроить критерии поиска целевых событий, к которым будет применено правило обогащения. Вы можете задать критерии на основе полей событий, значений полей и переменных, используя графический конструктор.



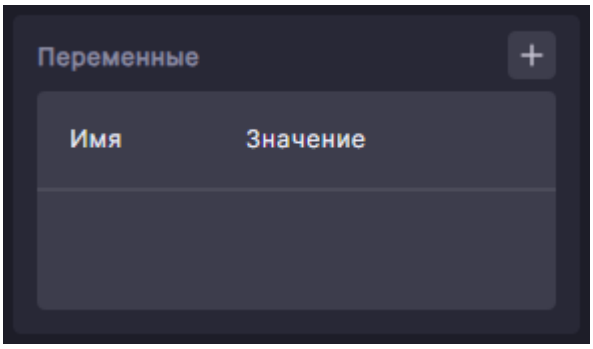
ПАНЕЛЬ «ДЕЙСТВИЯ ПО ОБОГАЩЕНИЮ»

Здесь можно задать действия по обогащению, производимые с удовлетворяющими фильтру целевыми событиями.



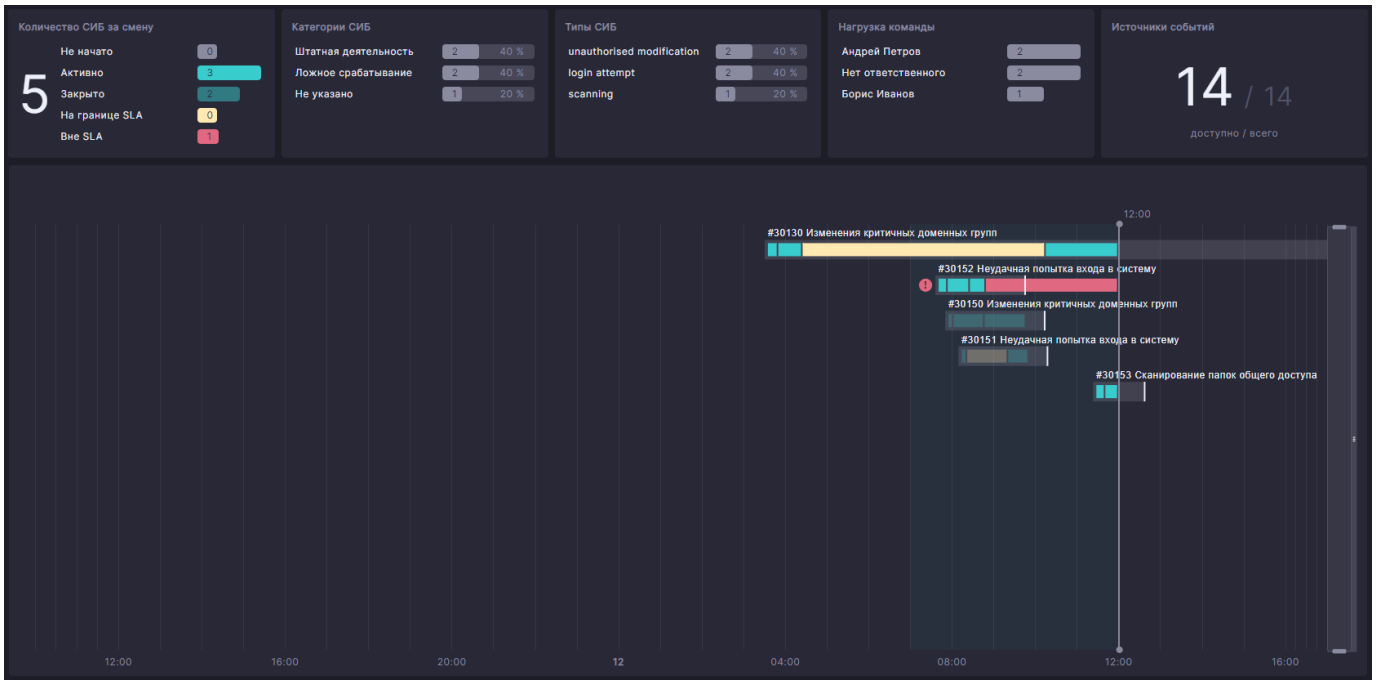
ПАНЕЛЬ «ПЕРЕМЕННЫЕ»

В этой панели можно задать переменные для использования в правиле.



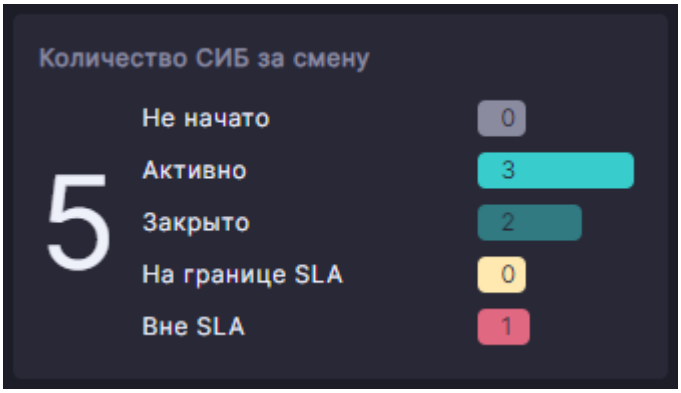
8.2.9 Модуль «Работа смены»

Модуль используется для контроля состояния процесса мониторинга.



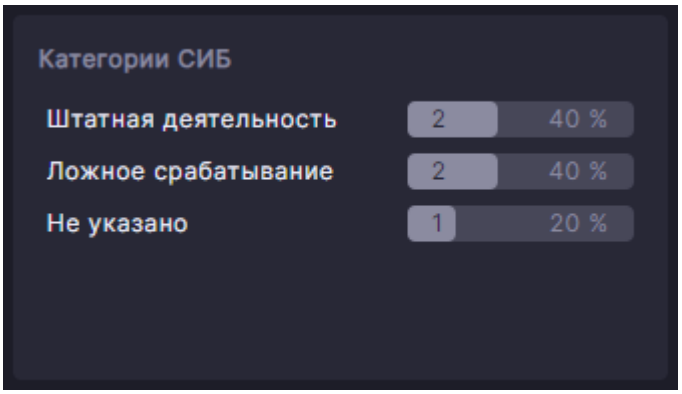
Для отображения информации используются следующие панели.

Панель «Количество СИБ за смену»



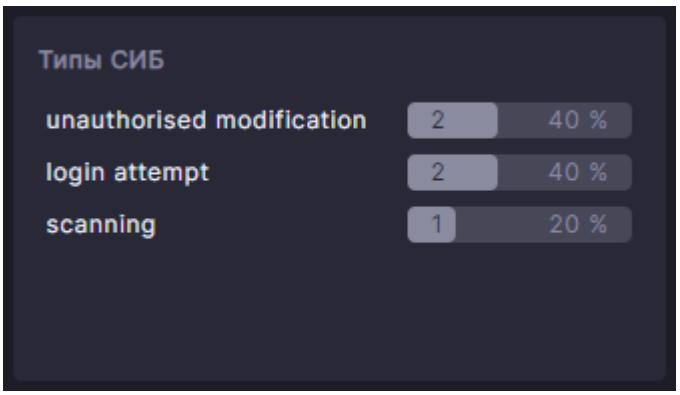
Отображает количественные характеристики событий и инцидентов ИБ, созданных в период текущей смены и сгруппированных по статусу обработки и исполнению SLA. Панель позволяет изменять критерий фильтра.

Панель «Категории СИБ»



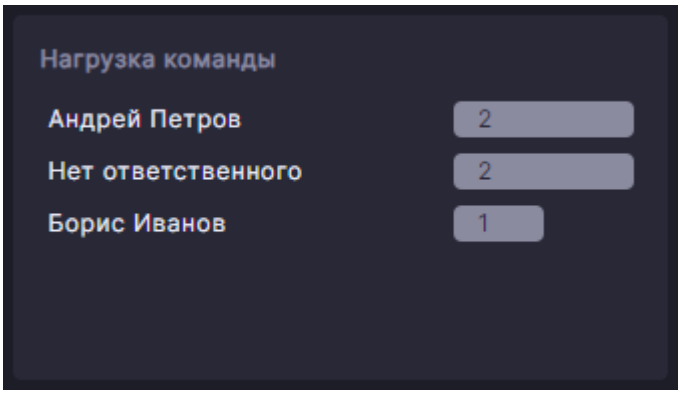
Отображает количественные характеристики событий и инцидентов ИБ, созданных в период текущей смены и сгруппированных по категориям. Панель позволяет изменять критерий фильтра и управлять настройками фильтра. Элементы панели (категории) отсортированы в порядке убывания их значений. Панель ограничена показом первых пяти элементов. Полный список элементов можно отобразить в боковой панели «Настройки фильтра».

Панель «Типы СИБ»



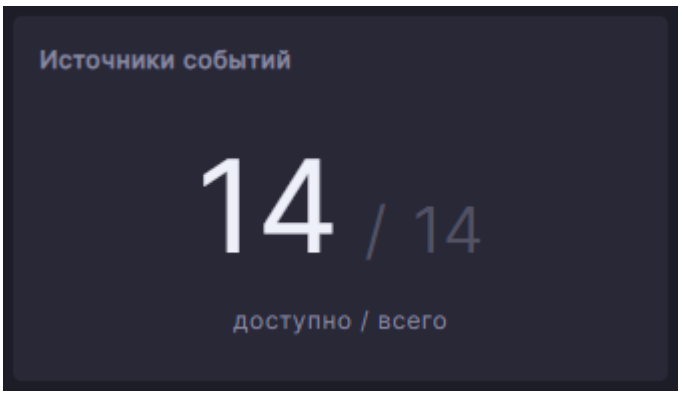
Отображает количественные характеристики событий и инцидентов ИБ, созданных в период текущей смены и сгруппированных по типам. Панель позволяет изменять критерий фильтра и управлять настройками фильтра. Элементы панели (типы) отсортированы в порядке убывания их значений. Панель ограничена показом первых пяти элементов. Полный список элементов можно отобразить в боковой панели «Настройки фильтра».

Панель «Нагрузка команды»



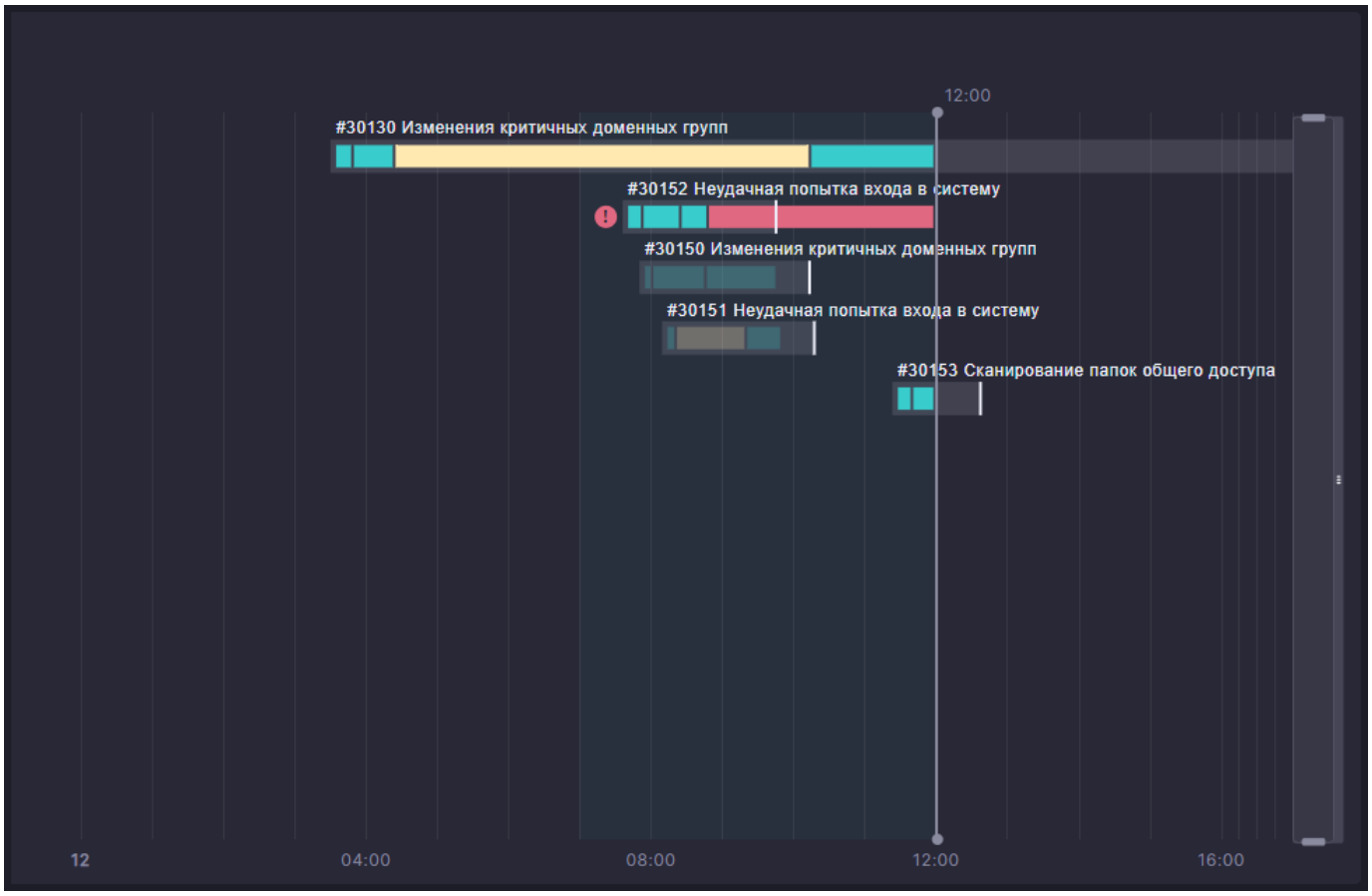
Отображает количественные характеристики событий и инцидентов ИБ, созданных в период текущей смены и сгруппированных по сотрудникам. Панель позволяет изменять критерий фильтра и управлять настройками фильтра. Элементы панели (имена сотрудников) отсортированы в порядке убывания их значений. Панель ограничена показом первых пяти элементов. Полный список элементов можно отобразить в боковой панели «Настройки фильтра».

Панель «Источники событий»



Отображает количественные характеристики источников событий, сгруппированных по доступности для Системы.

Панель «Хронология обработки СИБ»



Отображает события и инциденты ИБ, созданные в период текущей смены и отфильтрованные по критериям, заданным в других панелях. Вы можете изучить детали любого отображенного в панели события или инцидента ИБ, нажав на его графический элемент.

Боковая панель «Настройки фильтра»

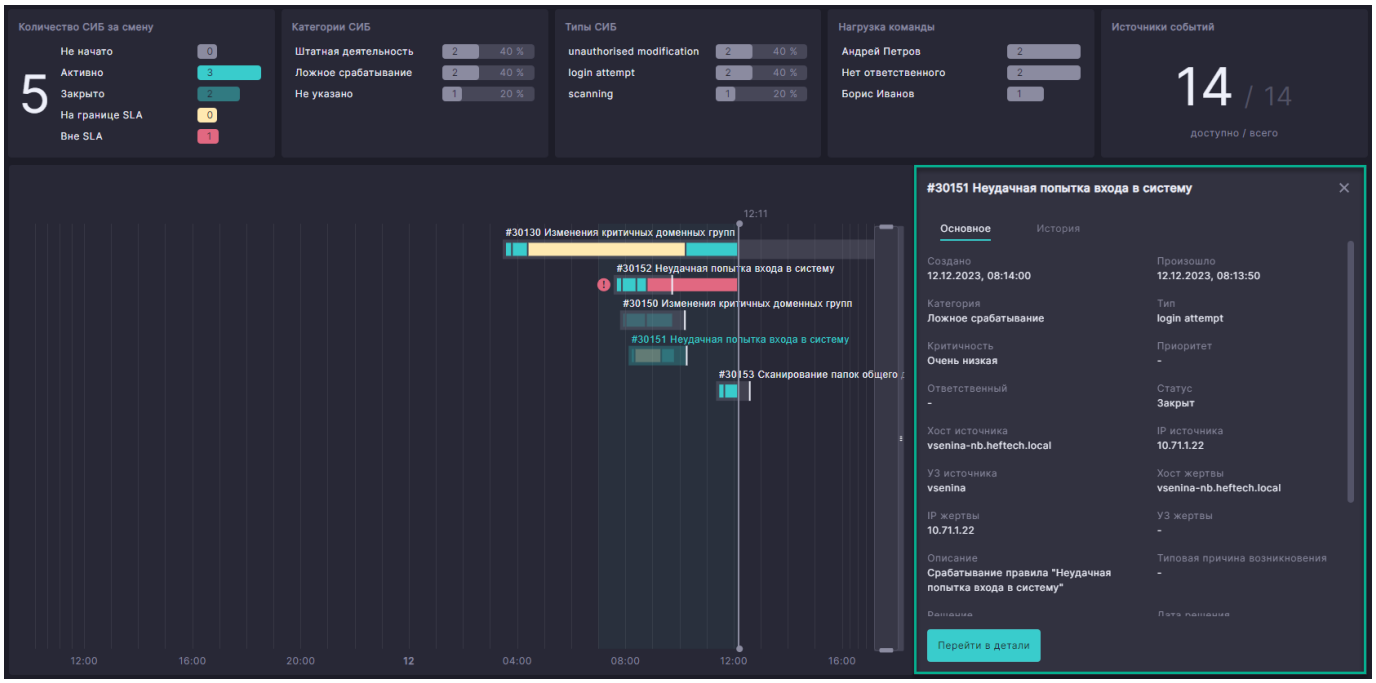
Позволяет просмотреть полный список доступных элементов другой панели (источника), минуя ограничение в пять элементов. Боковую панель можно отобразить нажатием контекстного значка («Показать настройки фильтра») в панели-источнике при управлении ее настройками фильтра.

Содержимое боковой панели включает в себя:

- имя панели-источника;
- все ее элементы, доступные для фильтрации представленных в панели «Хронология обработки СИБ» событий и инцидентов ИБ.

Вы можете нажать элемент в этой боковой панели, чтобы изменить соответствующий критерий фильтра.

Боковая панель «Детальная информация по СИБ»



Отображает детальную информацию по выбранному в панели «Хронология обработки СИБ» событию/инциденту ИБ. Нажмите кнопку «Перейти в детали», чтобы перейти в модуль «События ИБ» для просмотра карточки этого события/инцидента ИБ.

Настройка фильтра данных хронологии обработки СИБ

Система предоставляет возможность отфильтровать данные, представленные в панели «Хронология обработки СИБ», описанными ниже способами.

ИЗМЕНЕНИЕ КРИТЕРИЯ ФИЛЬТРА

Доступно в следующих панелях:

- «Количество СИБ за смену»;
- «Категории СИБ»;
- «Типы СИБ»;
- «Нагрузка команды»;
- «Настройки фильтра».

Нажмите на элемент панели, чтобы добавить соответствующий критерий к фильтру данных, представленных в панели «Хронология обработки СИБ».

Каждая панель может создать только один критерий фильтра, поэтому добавляемый критерий заместит существующий от этой панели.

Элемент, используемый в фильтре, выделится цветом. Для удаления критерия из фильтра выберите один из следующих вариантов:

- Нажмите на выделенный цветом элемент панели.
- Наведите указатель мыши на панель и нажмите значок  («Очистить»), отображаемый в ее правом верхнем углу.

УПРАВЛЕНИЕ НАСТРОЙКАМИ ФИЛЬТРА

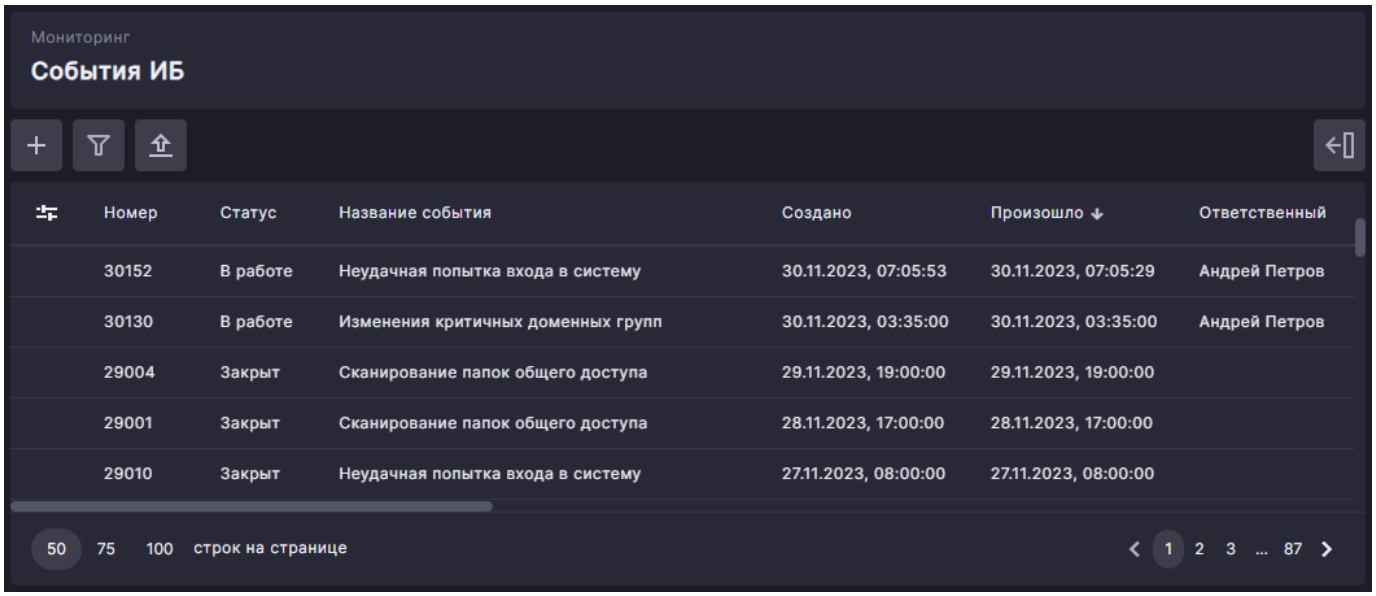
Доступно в следующих панелях:

- «Категории СИБ»;
- «Типы СИБ»;
- «Нагрузка команды».

Наведите указатель мыши на панель и нажмите контекстный значок («Показать настройки фильтра»), отображаемый в ее правом верхнем углу. Панель «Настройки фильтра» отобразится сбоку от панели «Хронология обработки СИБ». Повторное нажатие значка закроет панель с настройками фильтра.

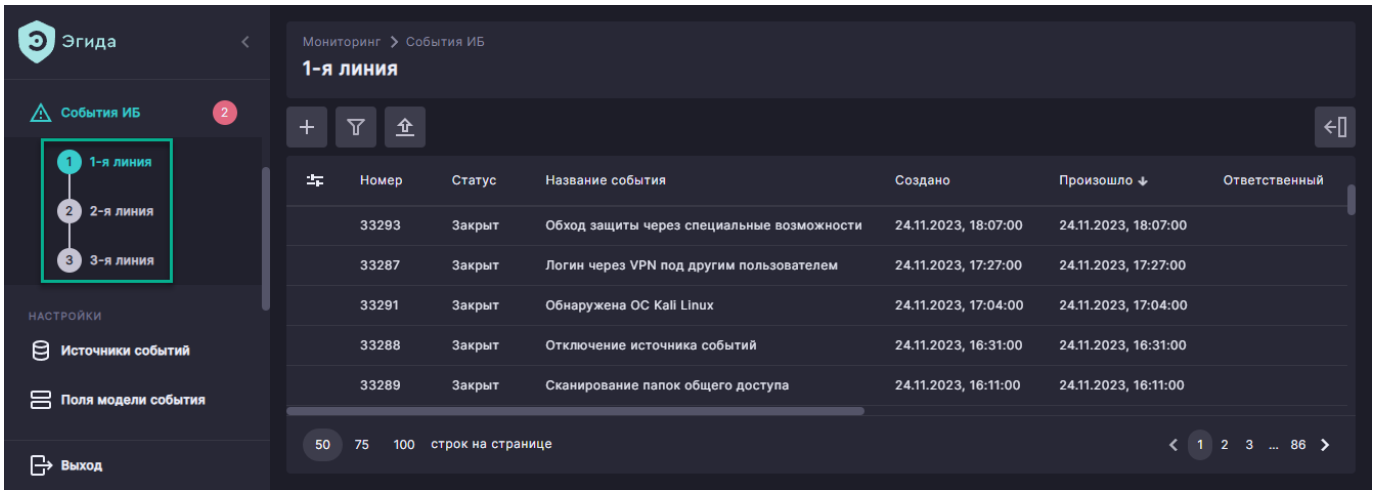
8.2.10 Модуль «События ИБ»

Позволяет регистрировать, изучать и обрабатывать события и инциденты ИБ в рамках процессов мониторинга и контроля, расследования и исследования. Для отображения зарегистрированных событий и инцидентов ИБ используется табличное представление.



Фильтрация событий/инцидентов ИБ

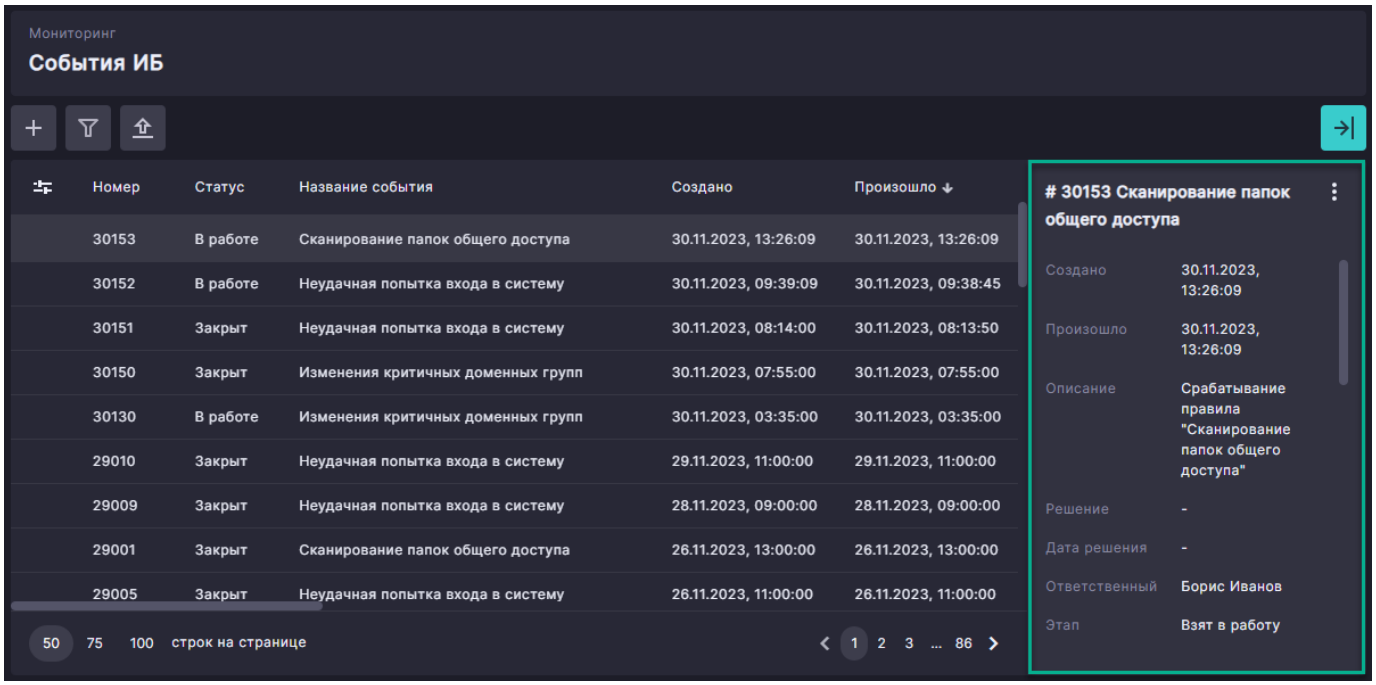
Система предоставляет возможность отображать в таблице события и инциденты ИБ общим списком и отфильтрованными по заданным в конфигурации Системы параметрам. В поставляемой с Системой базовой реализацией процессной модели заданы линии обработки событий/инцидентов ИБ и правила их перевода между линиями. В графическом интерфейсе доступна фильтрация отображаемых событий/инцидентов ИБ по линиям обработки. Для отображения событий/инцидентов ИБ на определенной линии обработки нажмите на ее имени в списке модулей Системы.



Вы можете также использовать дополнительную фильтрацию событий/инцидентов ИБ, предоставляемую таблицей.

Панель с деталями события/инцидента ИБ

Отображает в виде списка поля события/инцидента ИБ и их значения, а также позволяет настроить видимость этих полей.



Данные полей идентичны отображаемым в карточке события/инцидента ИБ на странице «Основная панель».

Режим редактирования

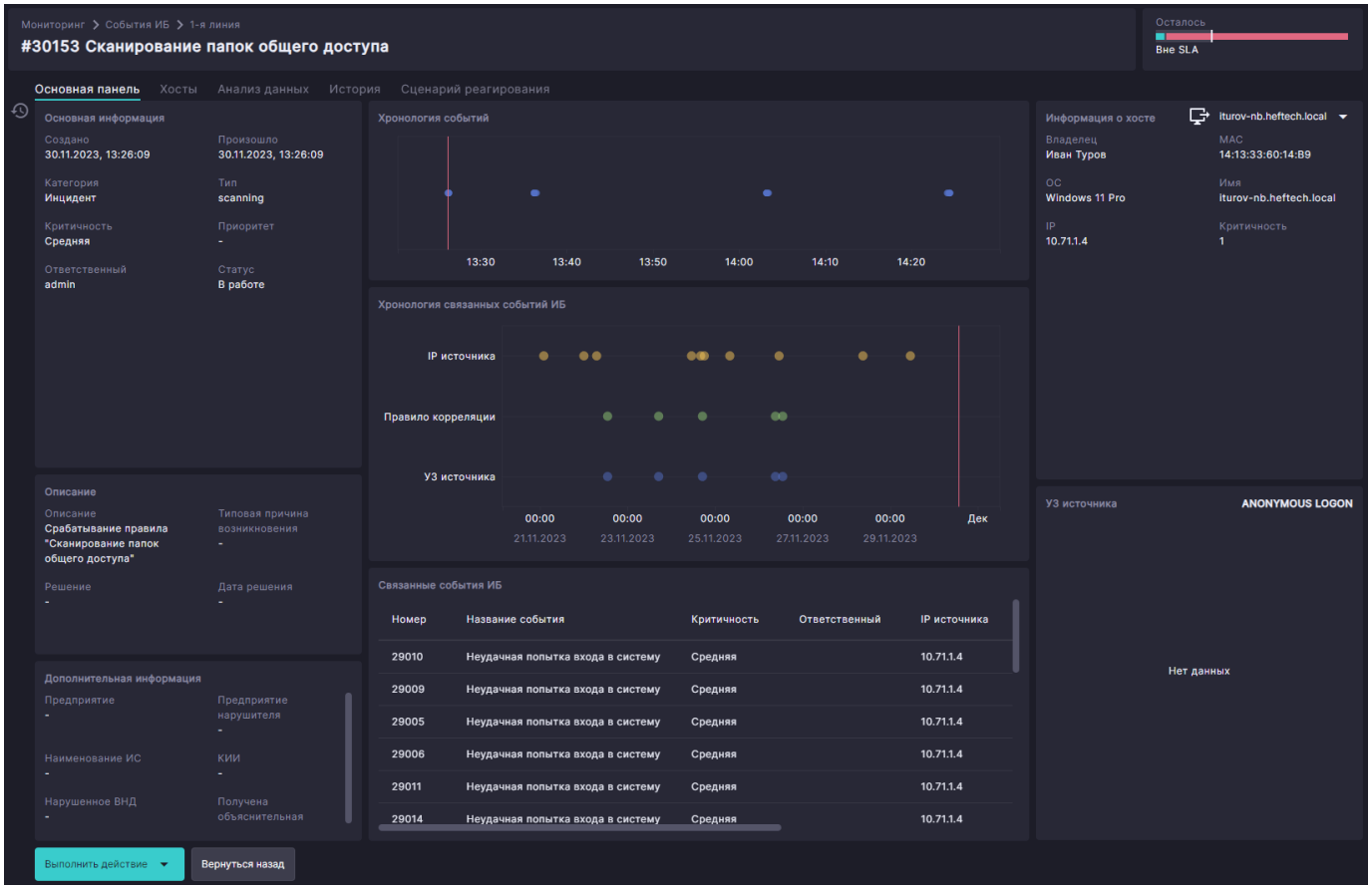
В режиме редактирования модуль отображает карточку события/инцидента ИБ, которая отображает его данные и предоставляет инструменты для их анализа и обработки. Карточка содержит следующие элементы:

- информацию, помогающую определить наличие угрозы в событии ИБ;
- данные расширенного контекста, помогающие определить масштабы и иные характеристики угрозы;
- инструменты, позволяющие произвести обработку события/инцидента ИБ согласно процессной модели.

Данные сгруппированы в панели и распределены по страницам, описанным в разделах ниже. Отображаемые в панелях данные, состав и расположение панелей на страницах и другие настройки карточки входят в конфигурацию Системы.

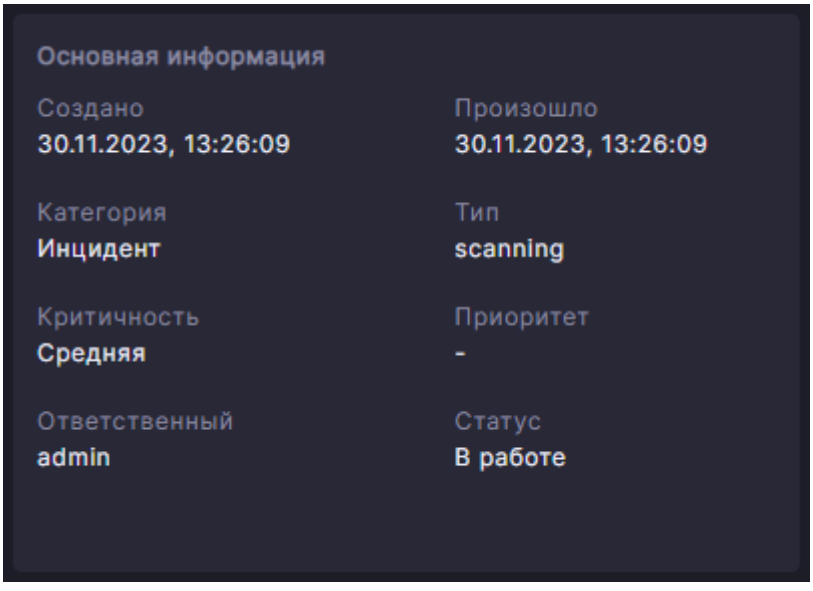
СТРАНИЦА «ОСНОВНАЯ ПАНЕЛЬ»

Содержит ключевую информацию об изучаемом событии/инциденте ИБ.



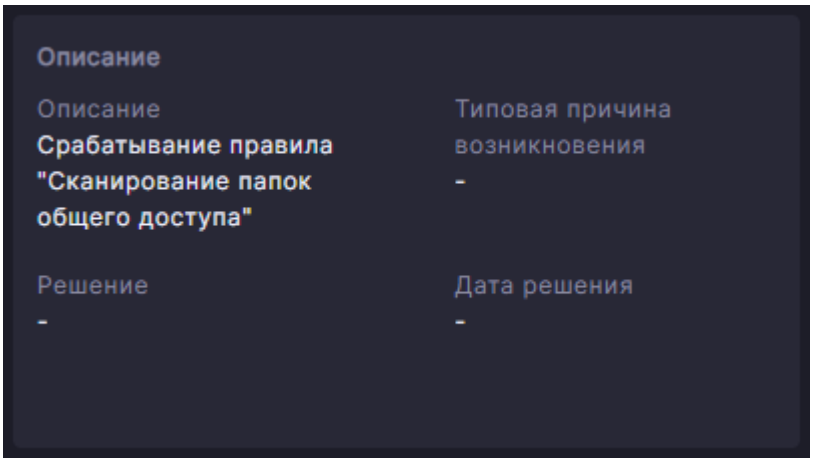
Информация размещена на следующих панелях.

Панель «Основная информация»



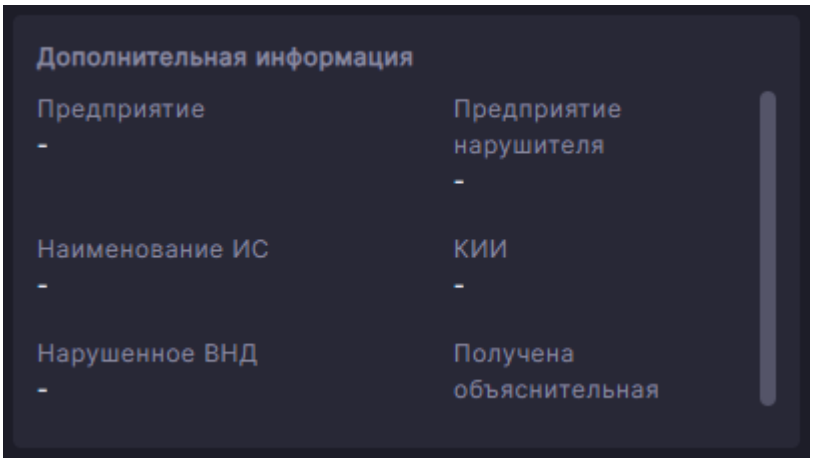
Позволяет ознакомиться с основными параметрами события/инцидента ИБ.

Панель «Описание»



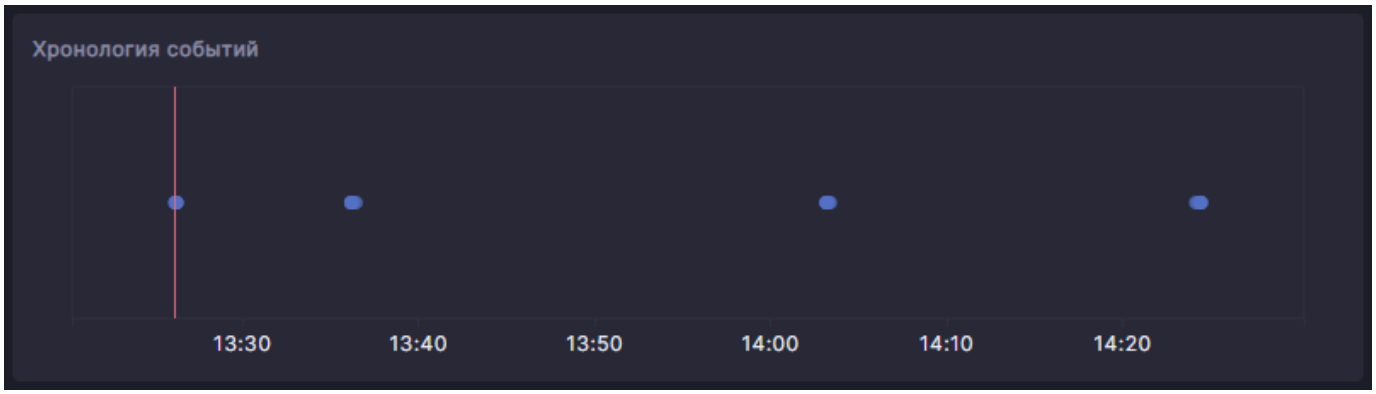
В этой панели можно ознакомиться с причинами возникновения события/инцидента ИБ. После выработки/нахождения решения здесь также будут отражены его дата и описание.

Панель «Дополнительная информация»



Позволяет изучить дополнительные данные о событии/инциденте ИБ.

Панель «Хронология событий»



В этой панели можно просмотреть последовательность событий, связанных с изучаемым событием/инцидентом ИБ, и ознакомиться с их подробностями. Для отображения используется хронологический график. На графике изучаемое событие/инцидент ИБ выделяется вертикальной чертой.

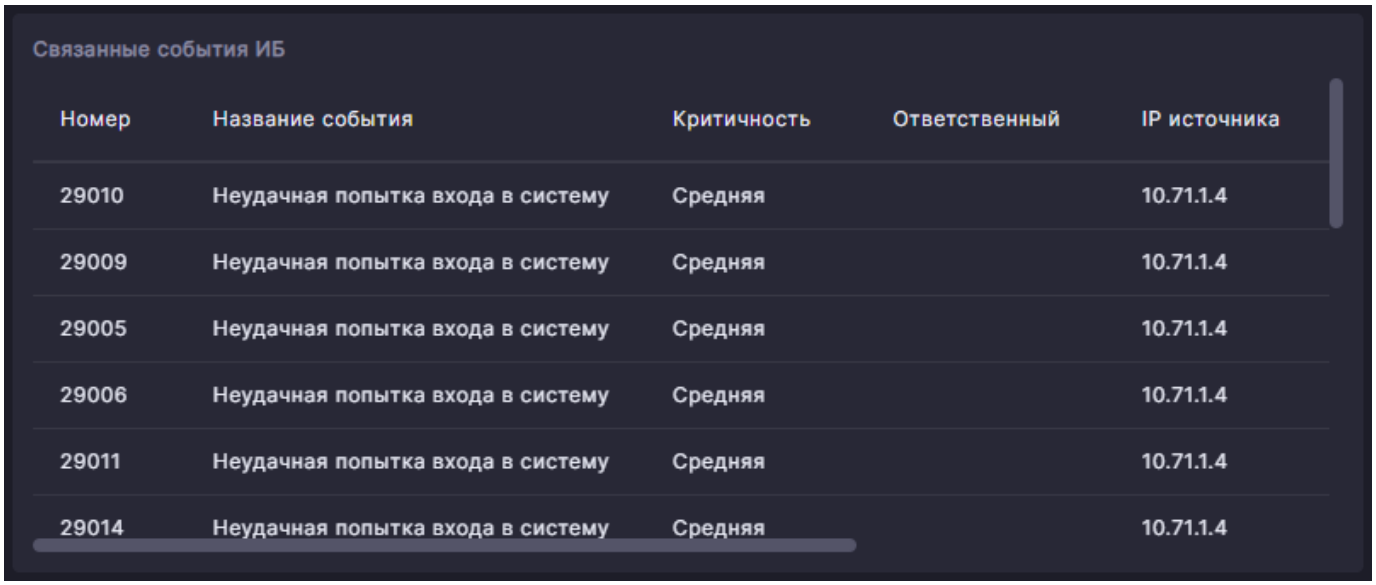
Панель «Хронология связанных событий ИБ»

Отображает хронологический график событий и инцидентов ИБ, когда их параметры совпадали с параметрами изучаемого события/инцидента ИБ. Таким образом по графику можно определить их возможную связь или подобие. На графике изучаемое событие/инцидент ИБ выделяется вертикальной чертой.

В поставляемой с Системой базовой конфигурации заданы следующие параметры:

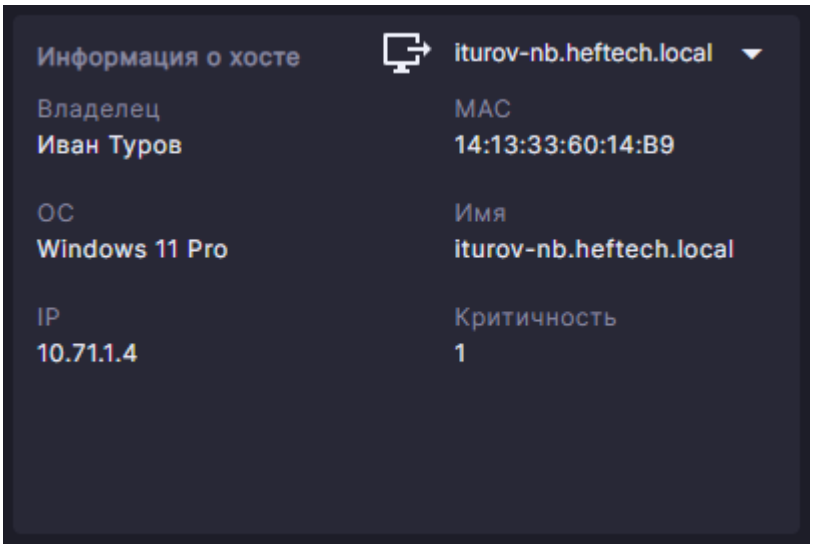
- Период, в рамках которого производится поиск связанных событий и инцидентов ИБ, составляет 14 дней до и после даты создания изучаемого события/инцидента ИБ.
- Для графика задано ограничение: 3 одновременно изображаемых параметра вдоль вертикальной оси, остальные параметры объединяются под именем «Другие».

Панель «Связанные события ИБ»



Отображает события и инциденты ИБ, связанные с изучаемым событием/инцидентом ИБ, в виде таблицы. Ее состав идентичен хронологии связанных событий/инцидентов ИБ.

Панель «Информация о хосте»



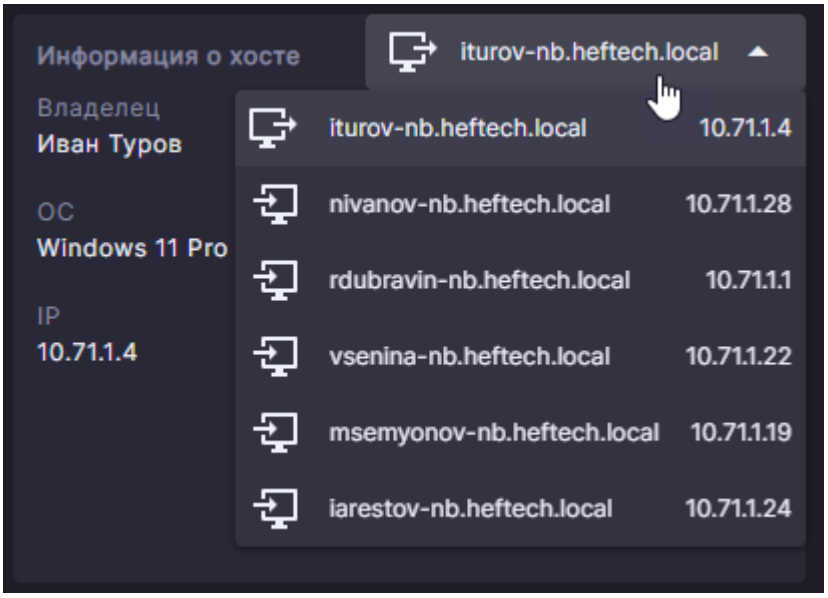
Позволяет просмотреть следующую информацию:

- Хосты, связанные с изучаемым событием/инцидентом ИБ.

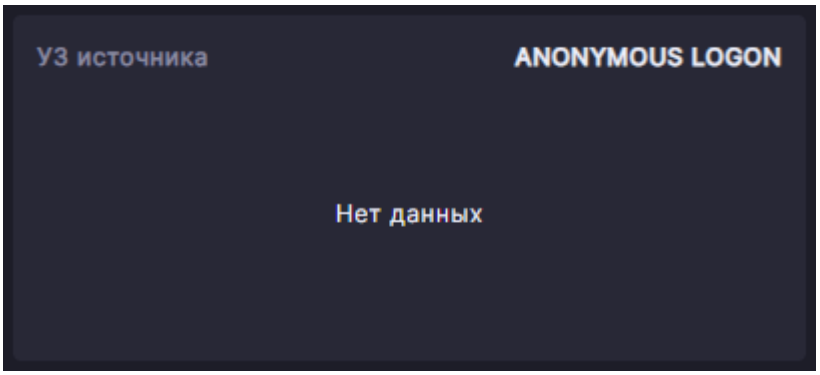
  Отображаются элементами в выпадающем списке с индикацией типа хоста: источник ( ) или жертва ( ). По умолчанию выбран первый элемент списка.

- Данные инвентаризации по выбранному хосту.

  Чтобы сменить выбранный хост, нажмите на его имя в правом верхнем углу панели и из выпадающего списка выберите другой хост.



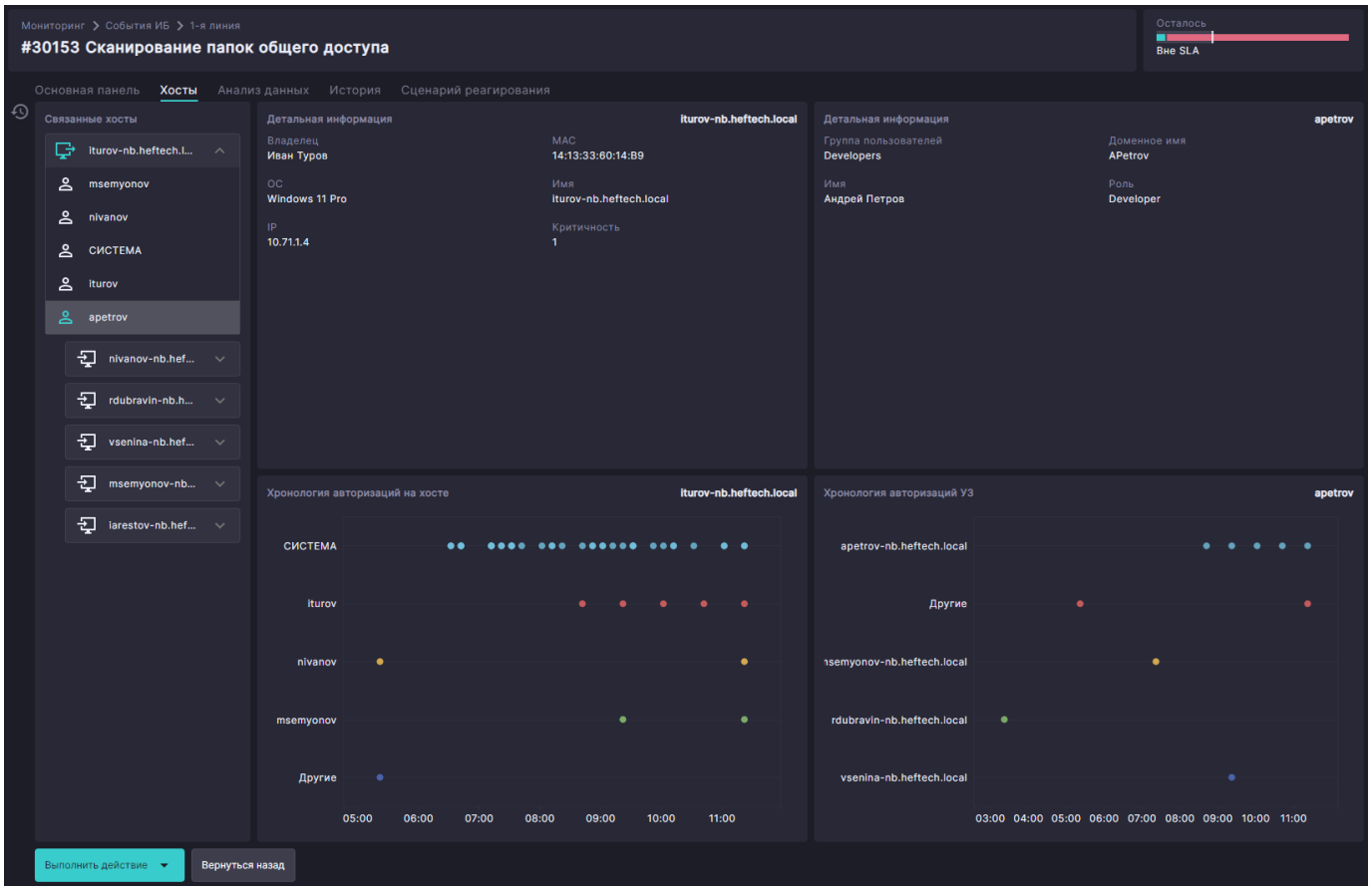
Панель «УЗ источника»



Позволяет изучить данные инвентаризации (если есть) по УЗ источника.

СТРАНИЦА «ХОСТЫ»

Позволяет изучить данные об УЗ и их авторизациях, осуществленных в рамках определенного периода на хостах, непосредственно связанных с изучаемым событием/инцидентом ИБ, а также иных хостах.



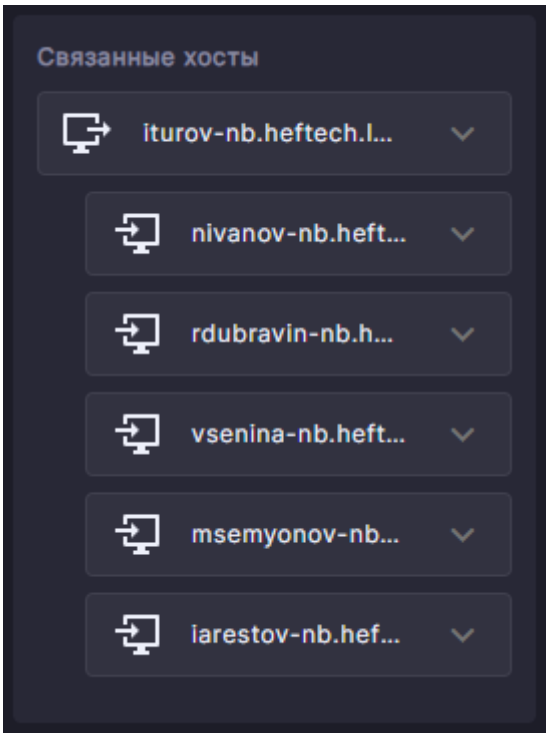
Представленная информация позволяет видеть более полный контекст изучаемого события/инцидента ИБ и включить в анализ обнаруженную активность УЗ, косвенно связанную с ним.

В поставляемой с Системой базовой конфигурации заданы следующие параметры:

- Индикатором авторизации УЗ служит событие Системы журналирования Windows (Windows Event Log) Event ID 4624 с параметром Logon Type не равным 5.
- Период поиска таких событий составляет 12 часов до и после времени создания изучаемого события/инцидента ИБ.

Информация размещена на следующих панелях.

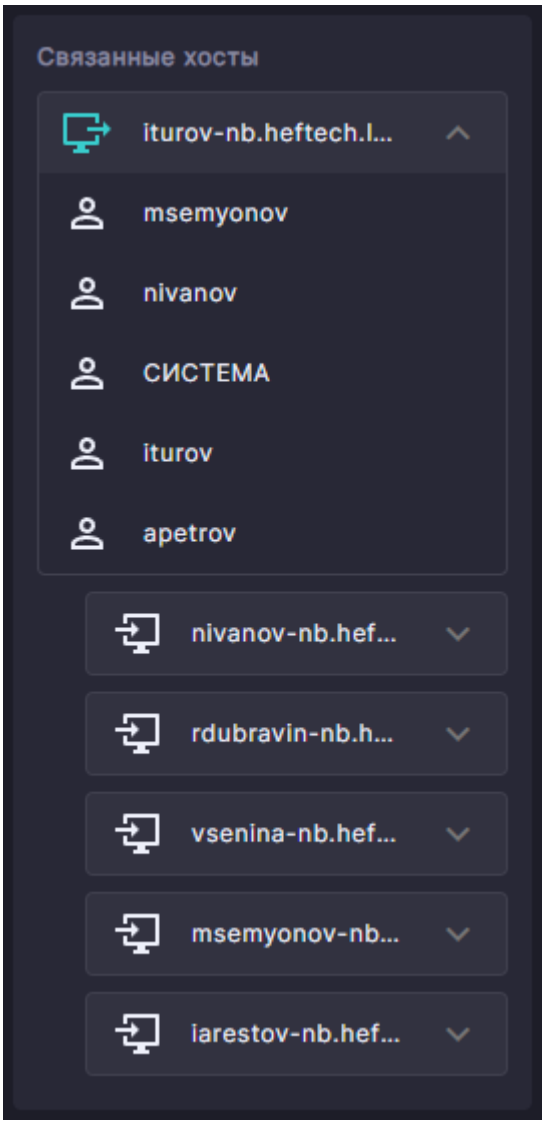
Панель «Связанные хосты»



Здесь отображены хосты, связанные с изучаемым событием/инцидентом ИБ, с индикацией их типа: источник ( ) или жертва ( ). Хосты жертвы располагаются под соответствующим хостом источником.

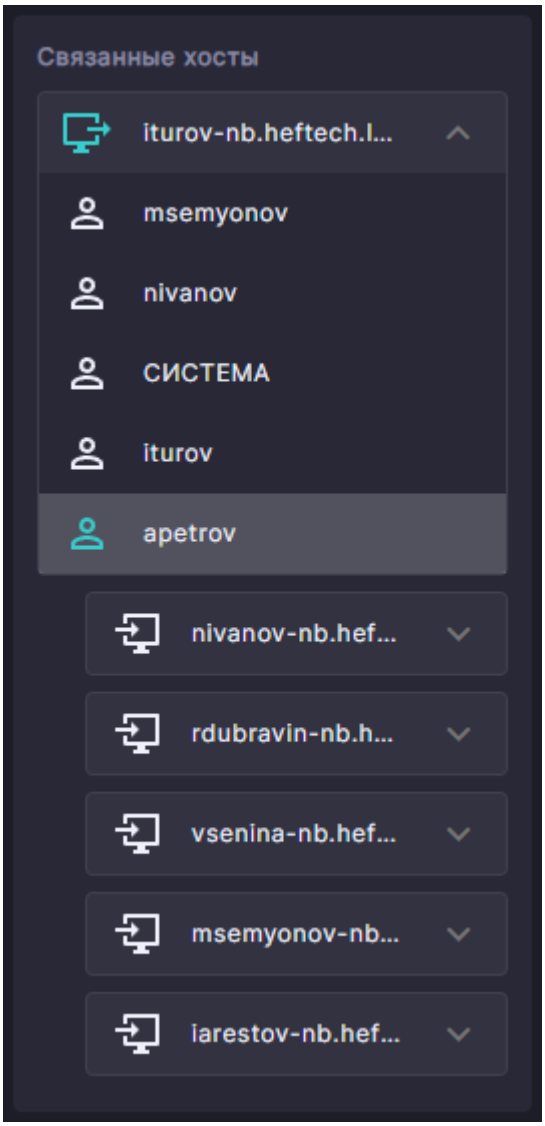
Чтобы отобразить дополнительную информацию, нажмите на нужный хост для его выбора. В результате выполнятся следующие действия:

- Под хостом распахнется список УЗ, осуществивших авторизацию на нем в рамках заданного в конфигурации периода.



- Панель «Детальная информация» заполнится данными инвентаризации по выбранному хосту.
- Информация по авторизациям, перечисленных в списке УЗ, отобразится в панели «Хронология авторизаций на хосте».

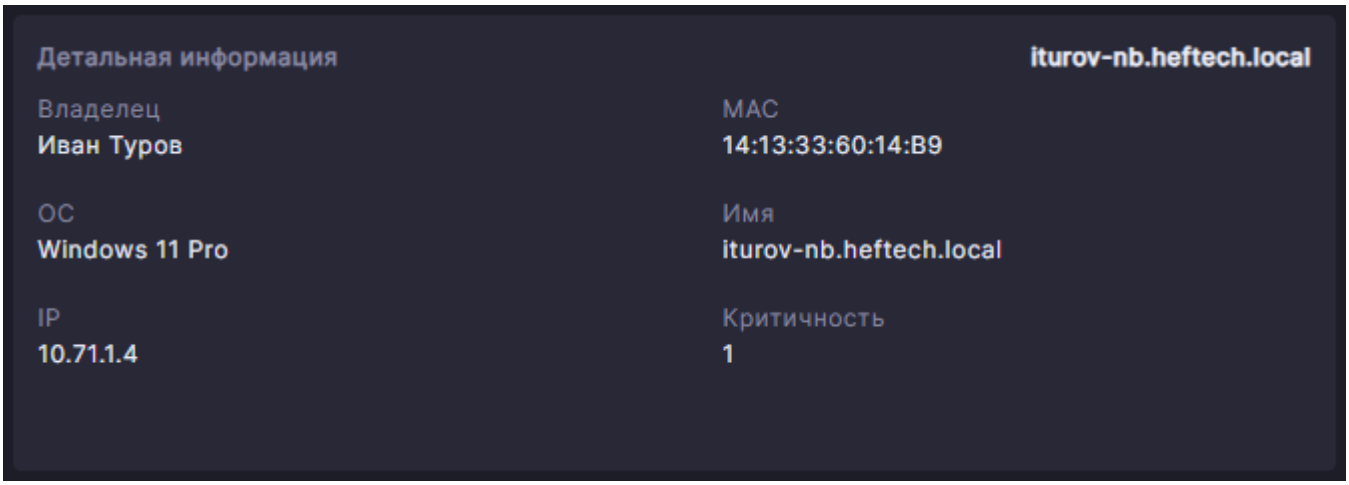
Чтобы просмотреть дополнительную информацию по любой УЗ из списка под выбранным хостом, нажмите на УЗ для ее выбора.



В результате выполнятся следующие действия:

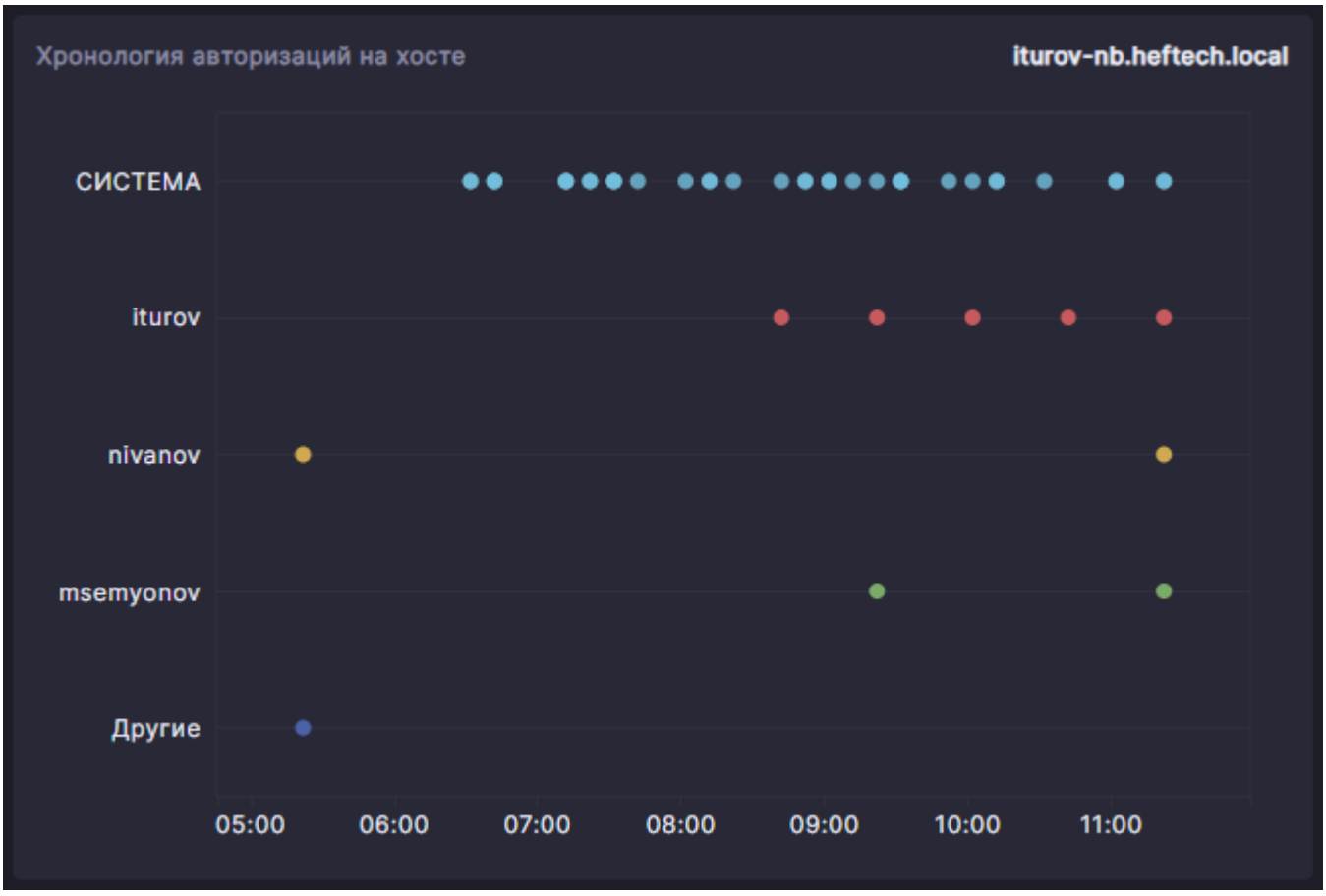
- Панель «Детальная информация» заполнится данными инвентаризации по выбранной УЗ.
- Информация по авторизациям выбранной УЗ отобразится в панели «Хронология авторизаций УЗ».

Панель «Детальная информация (по выбранному хосту)»



Отображает имя выбранного хоста и данные инвентаризации по нему.

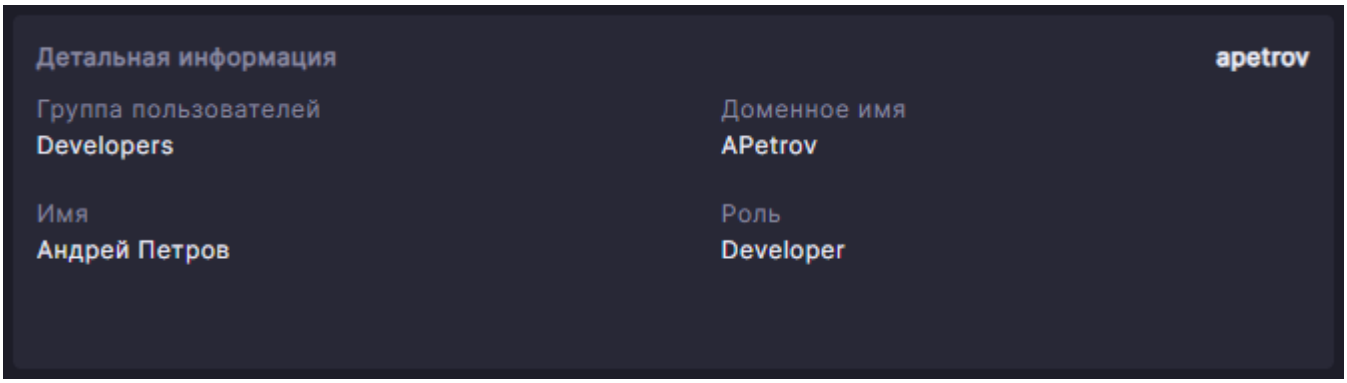
Панель «Хронология авторизаций на хосте»



Здесь отображаются имя выбранного хоста и хронологический график авторизаций УЗ, осуществленных на этом хосте в рамках заданного в конфигурации периода.

В поставляемой с Системой базовой конфигурации для графика задано ограничение: 4 одновременно изображаемых УЗ вдоль вертикальной оси, остальные УЗ объединяются под именем «Другие».

Панель «Детальная информация (по выбранной УЗ)»



Отображает имя выбранной УЗ и данные инвентаризации по ней.

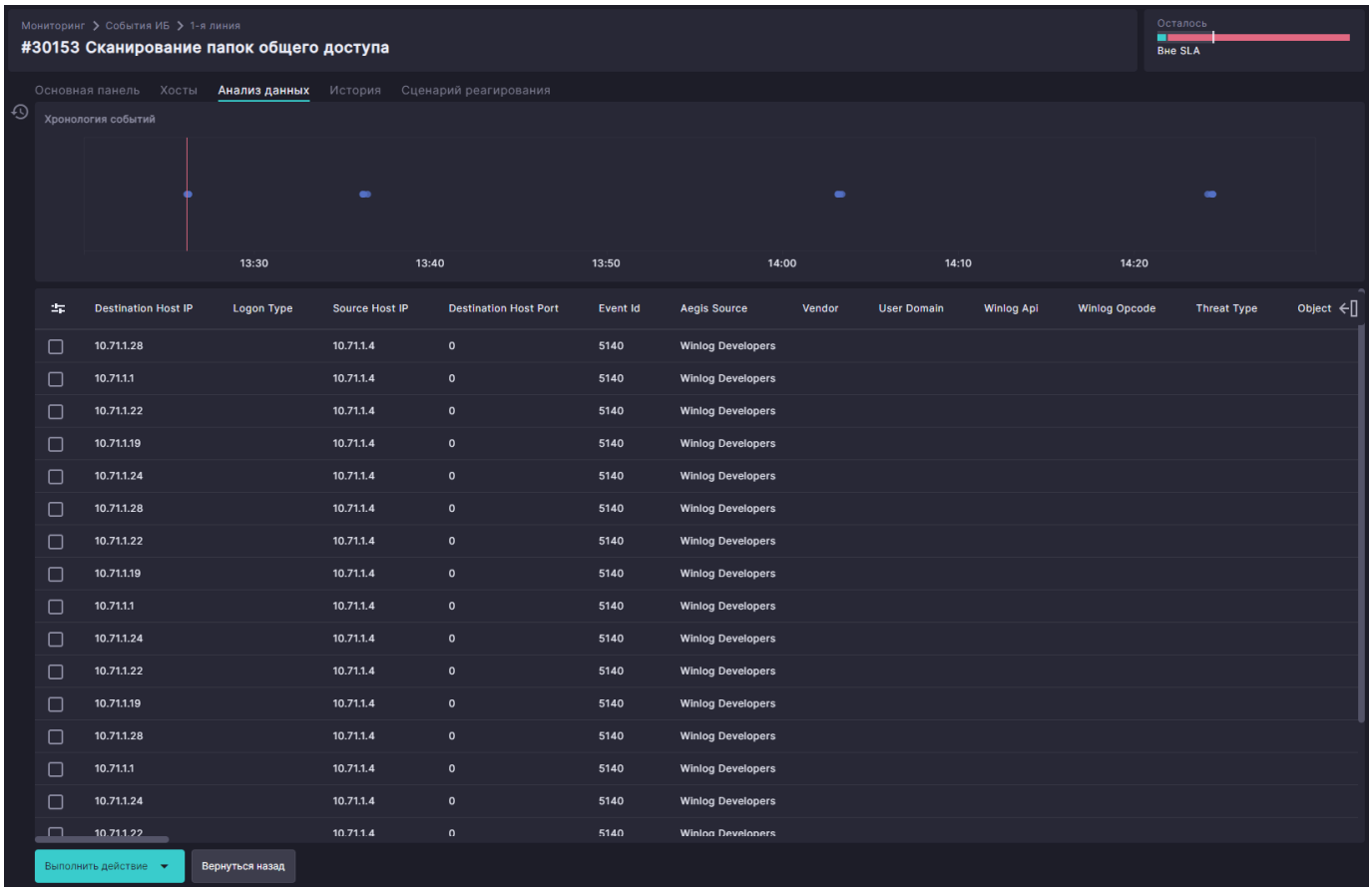
Панель «Хронология авторизаций УЗ»

Отображает имя выбранной УЗ и хронологический график авторизаций УЗ, осуществленных на хостах в рамках заданного в конфигурации периода.

В поставляемой с Системой базовой конфигурации для графика задано ограничение: 4 одновременно изображаемых хоста вдоль вертикальной оси, остальные хосты объединяются под именем «Другие».

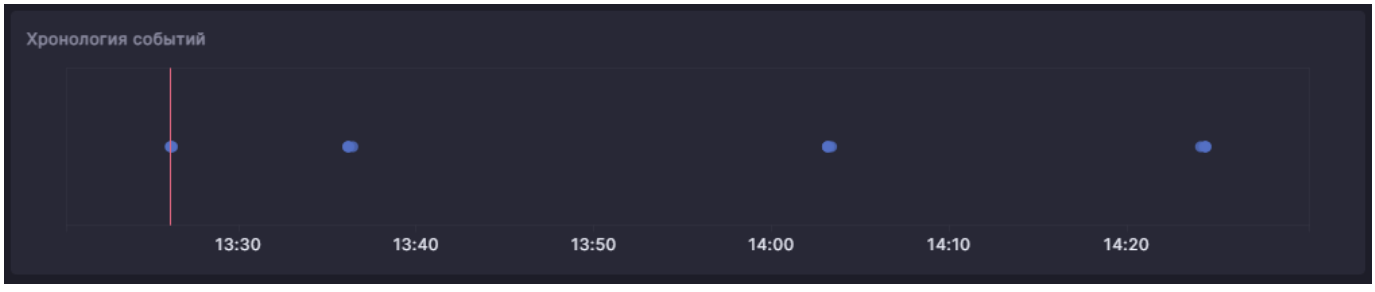
СТРАНИЦА «АНАЛИЗ ДАННЫХ»

Позволяет изучить данные о подготовленных и исходных событиях, связанных с изучаемым событием/инцидентом ИБ.



Информация размещена на следующих панелях.

Панель «Хронология событий»



Отображает хронологический график событий, связанных с изучаемым событием/инцидентом ИБ, который на графике выделяется вертикальной чертой. Содержимое панели идентично хронологии событий, изображенной на странице «Основная панель».

Таблица связанных событий

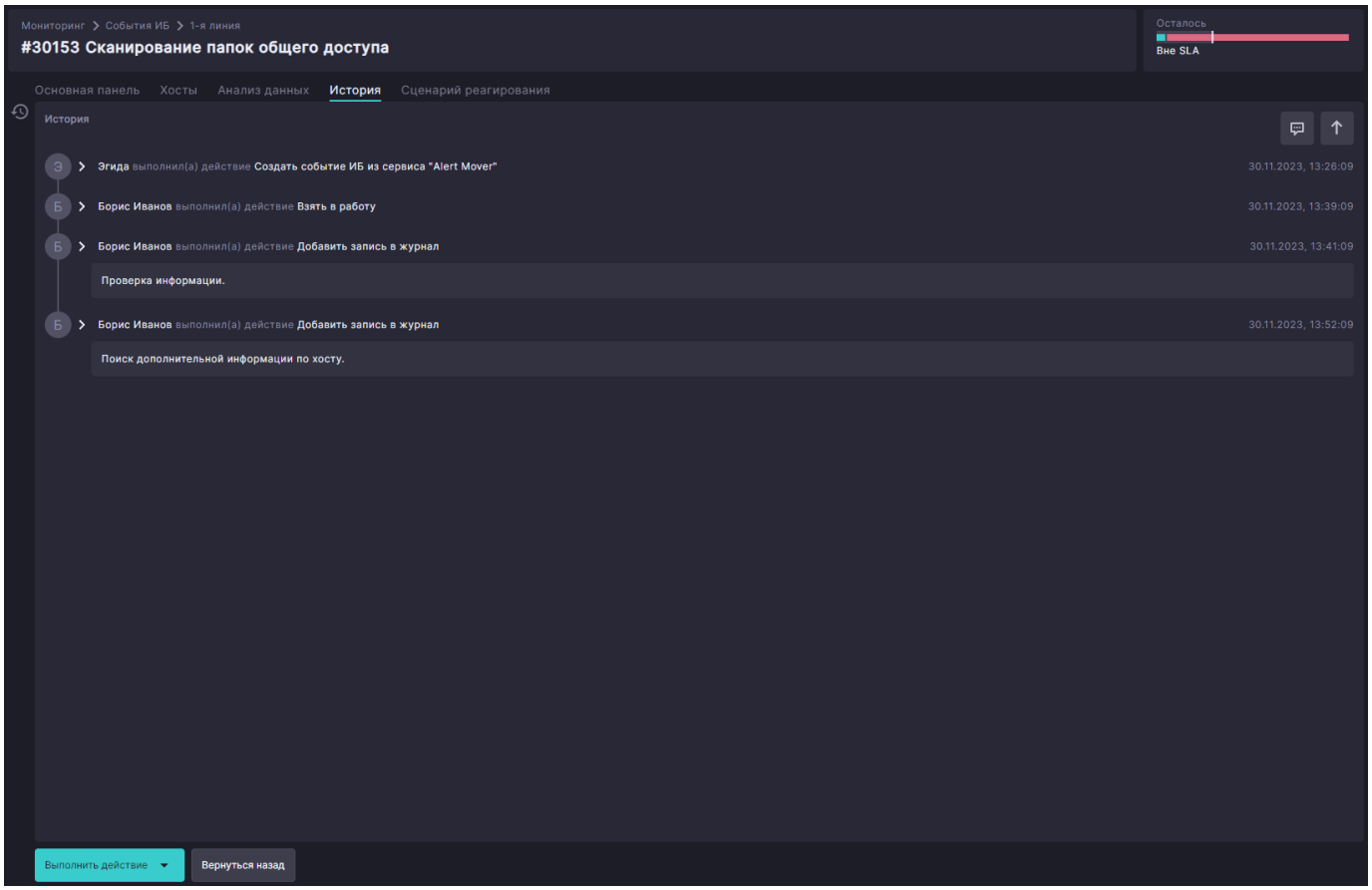
В таблице отображены подготовленные события, связанные с изучаемым событием/инцидентом ИБ.

Destination Host IP	Logon Type	Source Host IP	Destination Host Port	Event Id	Aegis Source	Vendor
10.71.1.28		10.71.1.4	0	5140	Winlog Developers	
10.71.1.1		10.71.1.4	0	5140	Winlog Developers	
10.71.1.22		10.71.1.4	0	5140	Winlog Developers	
10.71.1.19		10.71.1.4	0	5140	Winlog Developers	
10.71.1.24		10.71.1.4	0	5140	Winlog Developers	
10.71.1.28		10.71.1.4	0	5140	Winlog Developers	
10.71.1.22		10.71.1.4	0	5140	Winlog Developers	
10.71.1.19		10.71.1.4	0	5140	Winlog Developers	

Состав таблицы идентичен хронологии событий, изображенной в панели выше. Для просмотра и анализа данных событий используйте функции таблицы, которые аналогичны представленным в модуле «Анализ данных». Для удобства можно отобразить данные подготовленного и исходного событий, используя боковую панель с подробностями события.

СТРАНИЦА «ИСТОРИЯ»

Содержит информацию о всех действиях, произведенных с изучаемым событием/инцидентом ИБ, в виде журнала.



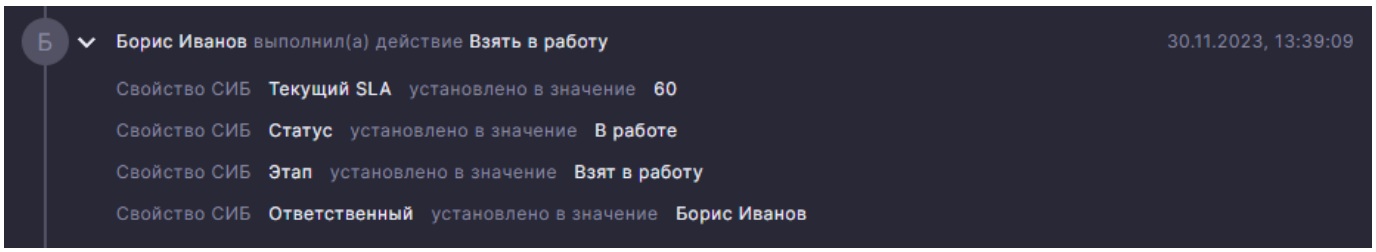
Записи журнала отображаются в хронологическом порядке. Каждая из них содержит описание действия, дата и время его регистрации в журнале аудита Системы. Также запись может содержать:

- данные аудита изменений значений полей изучаемого события/инцидента ИБ;
- пользовательские комментарии и файлы, приложенные к ним.

Журнал предоставляет следующие возможности настройки отображения записей.

Управление видимостью детальной информации о произведенном действии

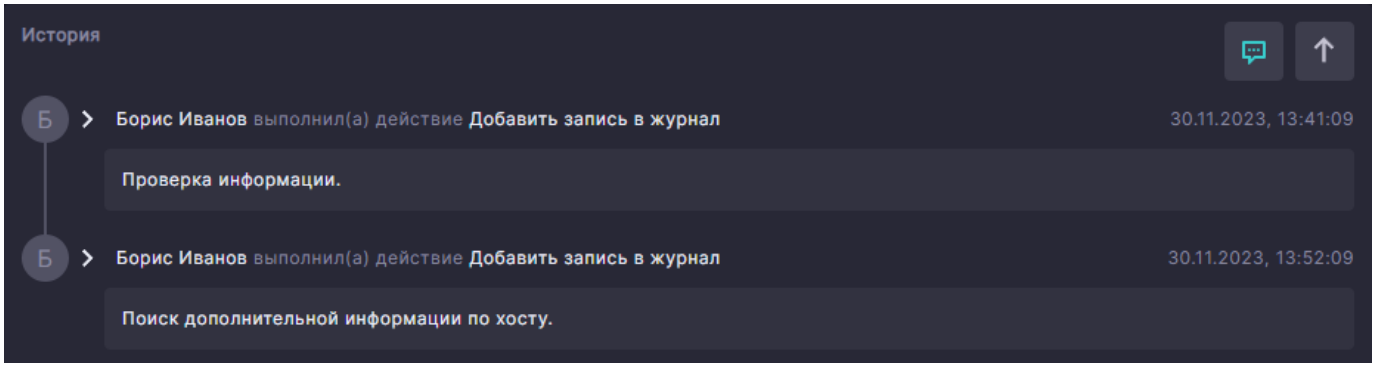
По умолчанию детальная информация скрыта. Нажмите значок > («Показать детали действия»), расположенный слева от описания действия, чтобы распахнуть список с детальной информацией о произведенных этим действием изменениях значений полей изучаемого события/инцидента ИБ.



Нажмите значок ⌄ («Скрыть детали действия»), расположенный слева от описания действия, чтобы свернуть список.

Управление видимостью записей без комментариев

По умолчанию журнал отображает все записи. Вы можете настроить отображение только записей, содержащих комментарии, нажав значок 💬 («Скрыть действия без комментариев»).



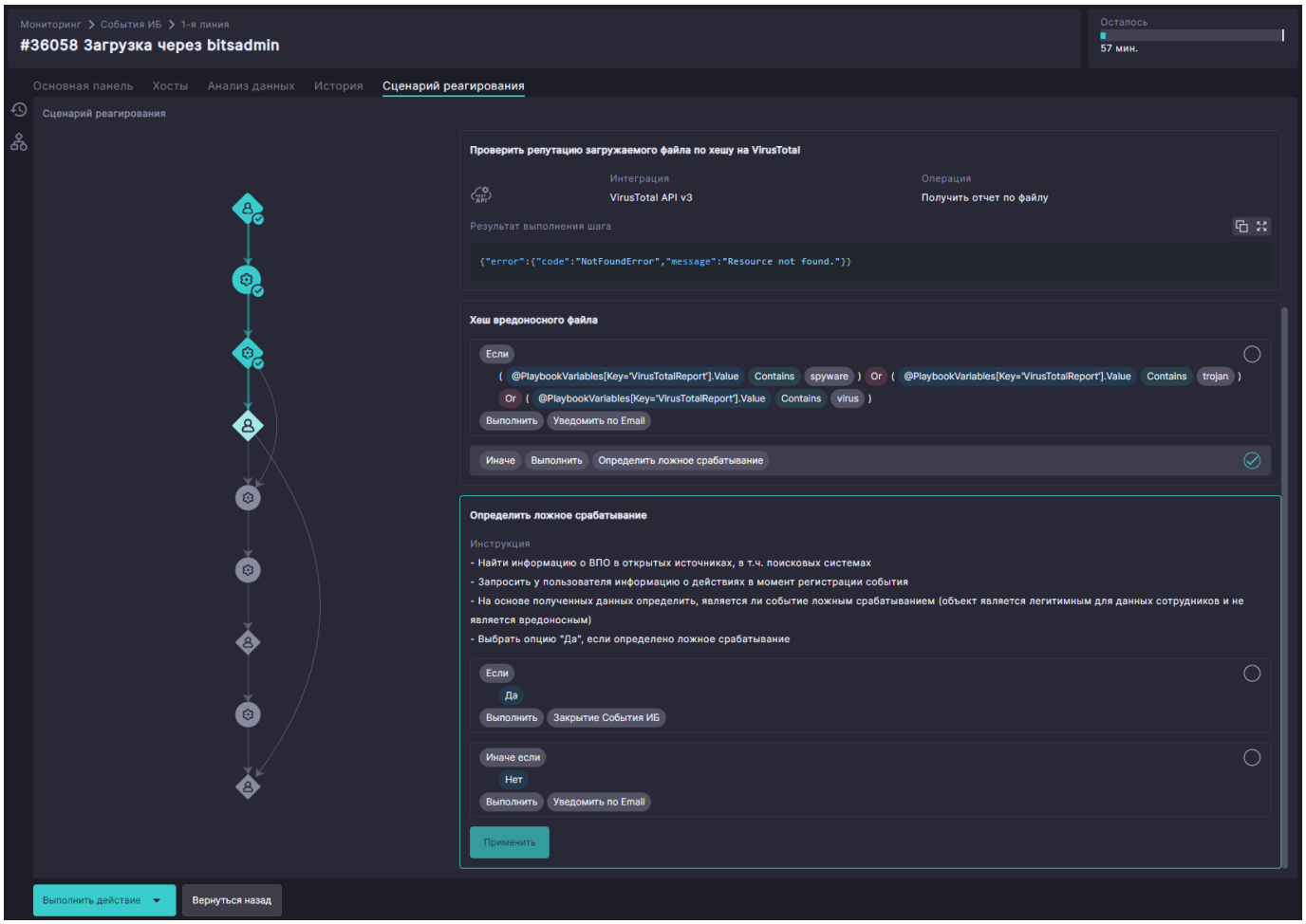
Повторное нажатие значка вернет отображение всех записей.

Изменение порядка следования записей

По умолчанию записи следуют сверху вниз, от старых к новым. Вы можете изменить порядок следования записей на обратный, нажав значок ↑ («Показать сначала новые действия»). Чтобы вернуться к исходному порядку следования записей, нажмите значок ↓ («Показать сначала старые действия»).

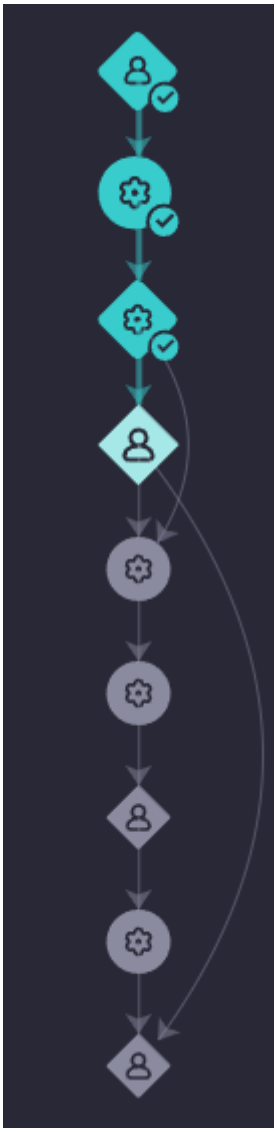
СТРАНИЦА «СЦЕНАРИЙ РЕАГИРОВАНИЯ»

Отображает сценарий реагирования, связанный с изучаемым событием/инцидентом ИБ, и позволяет выполнить предлагаемые сценарием шаги.

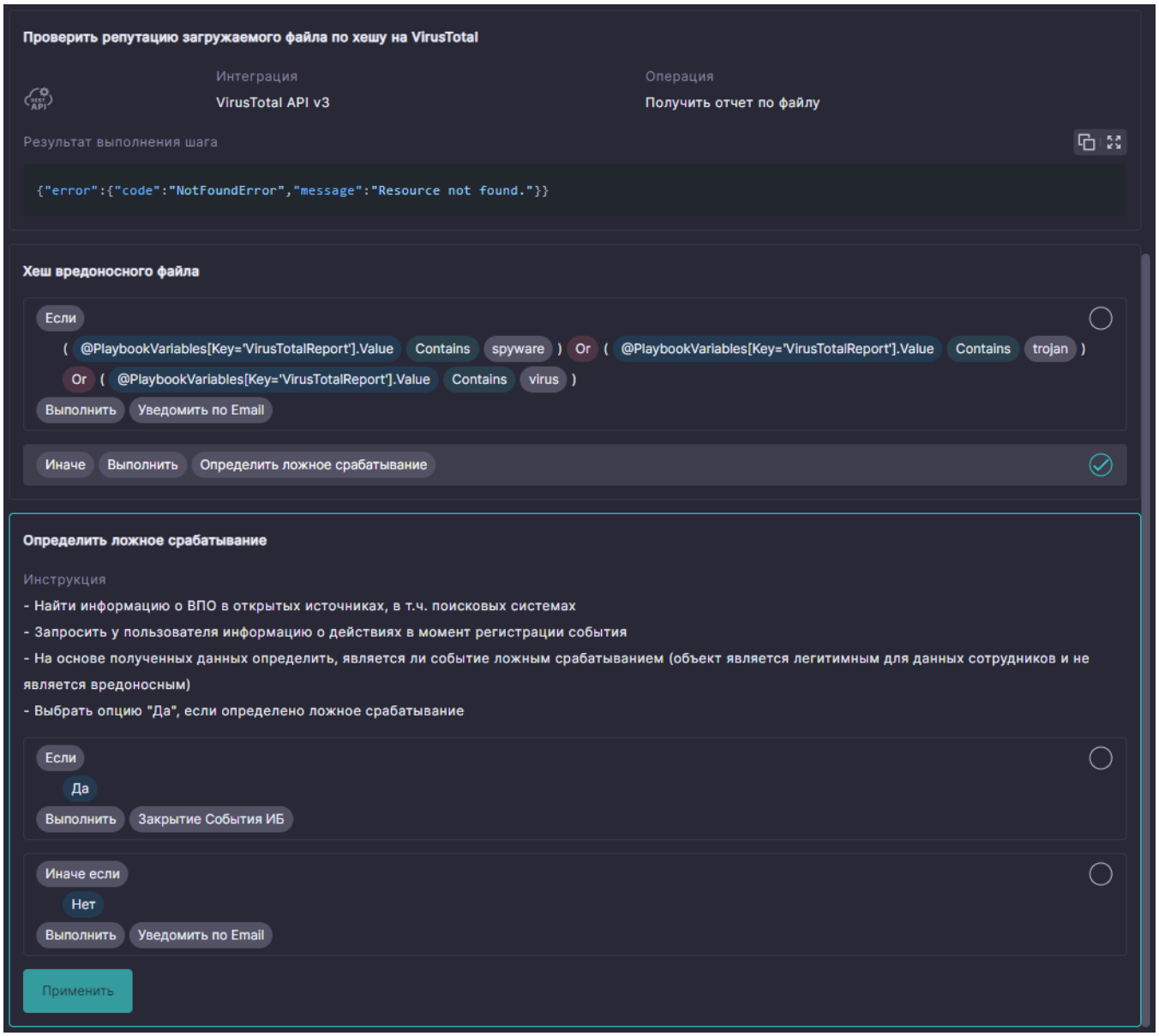


Содержит следующие элементы:

- диаграмма сценария реагирования;



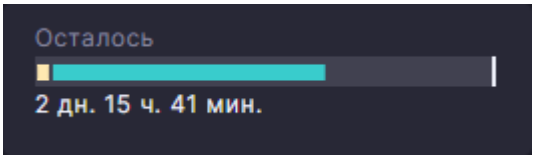
- список выполненных и доступных для выполнения шагов.



ПАНЕЛЬ С ПОКАЗАТЕЛЕМ SLA

Включает в себя сам показатель SLA и время, оставшееся до истечения норматива завершения обработки события/инцидента ИБ. Норматив определяется ближайшей из перечисленных ниже временных точек:

- время завершения текущего этапа обработки события/инцидента;
- время завершения обработки и закрытия события/инцидента.



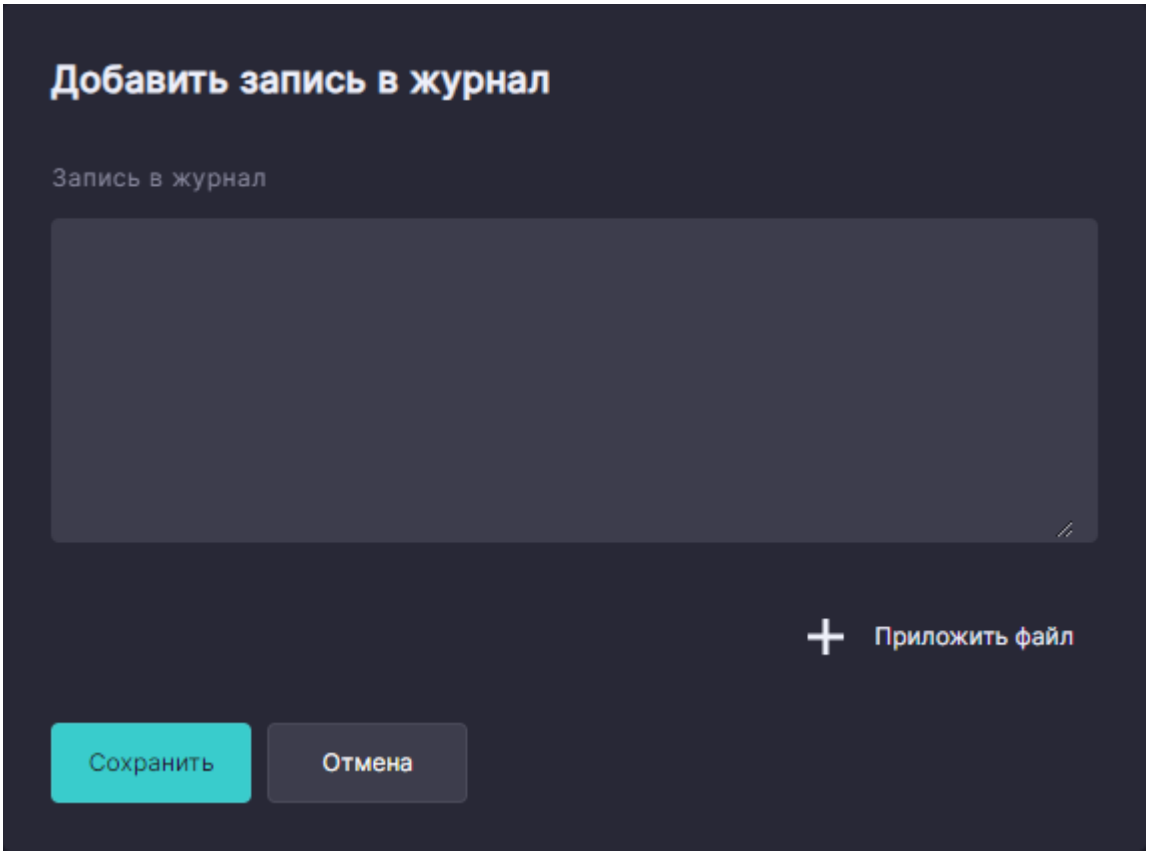
Выполнение управляющих действий с событием/инцидентом ИБ

Набор действий, доступных для выполнения, определяется процессной моделью и текущим этапом обработки события/инцидента ИБ.

Модуль «События ИБ» предоставляет следующие возможности для отображения доступных действий:

- В таблице, отображающей зарегистрированные события и инциденты ИБ, нажмите значок () («Выполнить действие»).
- В карточке события/инцидента ИБ нажмите кнопку «Выполнить действие».

Далее в выпадающем списке с набором управляющих действий нажмите на нужном действии для его выполнения. После этого откроется окно для задания параметров выполняемого действия. Одним из таких действий является добавление записи в журнал.



Если в процессной модели задано обязательное добавление комментариев (примечаний, пояснений или выводов) и иной дополнительной информации по выполняемому действию, оно также будет сопровождаться добавлением записи в журнал. При этом в окне для задания параметров выполняемого действия будут присутствовать параметры добавляемой записи.

Возможности по добавлению записи описаны в разделе ниже.

ДОБАВЛЕНИЕ ЗАПИСИ В ЖУРНАЛ

1. Введите текст записи в поле «Запись в журнал».
2. При необходимости приложите один или более файлов, как описано ниже.
3. Для завершения добавления записи в журнал выберите один из следующих вариантов:

    - Нажмите кнопку «Сохранить», чтобы добавить запись с заданными параметрами.

      Окно задания параметров выполняемого действия закроется, и журнал будет обновлен.

    - Нажмите кнопку «Отмена», чтобы отказаться от добавления записи.

      Окно задания параметров выполняемого действия закроется, введенный в окне текст будет утерян, и будут удалены копии файлов, приложенные к записи. Непосредственно сами файлы не удаляются из файловой системы.

Приложение файлов к добавляемой записи

Нажмите кнопку « + Приложить файл» и выберите нужный файл в открывшемся окне. При этом создастся одноименная копия этого файла, которая и приложится к записи. Имена приложенных файлов (их копий) отображаются под полем «Запись в журнал».

Удаление приложенных к записи файлов

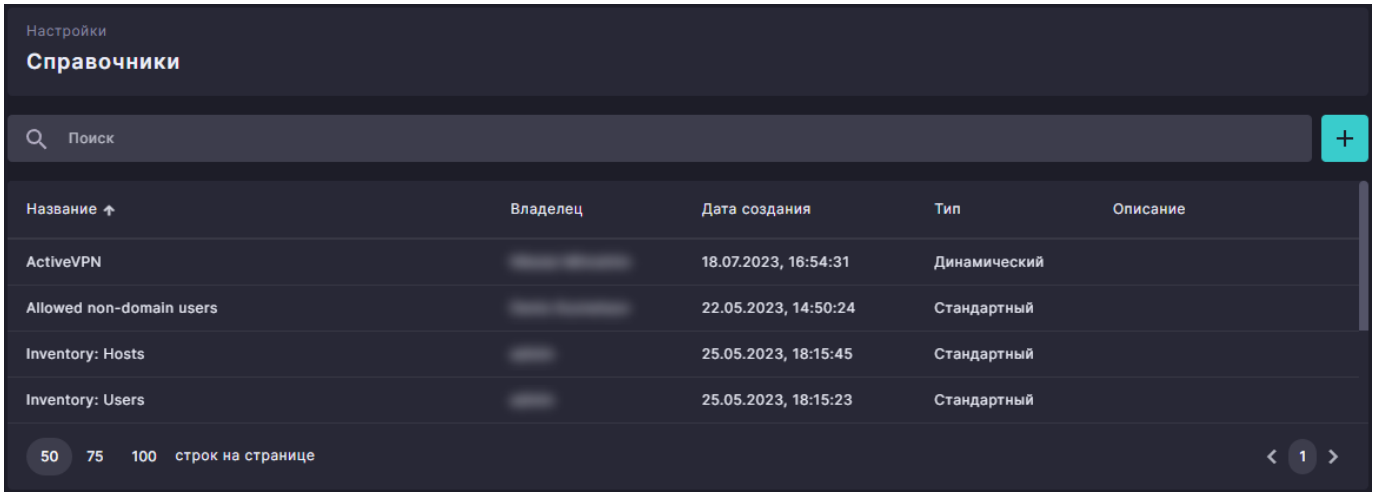
Вы можете удалить любую приложенную копию файла до сохранения записи, нажав значок ✕ («Удалить приложенный файл»), отображающийся справа от имени файла. Непосредственно сами файлы не удаляются из файловой системы.

8.2.11 Модуль «Справочники»

Позволяет создавать и модифицировать справочники, используемые при задании:

- правил обогащения событий в рамках процесса их сбора;
- правил корреляции событий в рамках процесса мониторинга и контроля;
- критериев поиска событий, событий ИБ и инцидентов ИБ при проведении сбора событий, мониторинга и контроля, расследований и исследований.

Для отображения созданных справочников используется табличное представление.

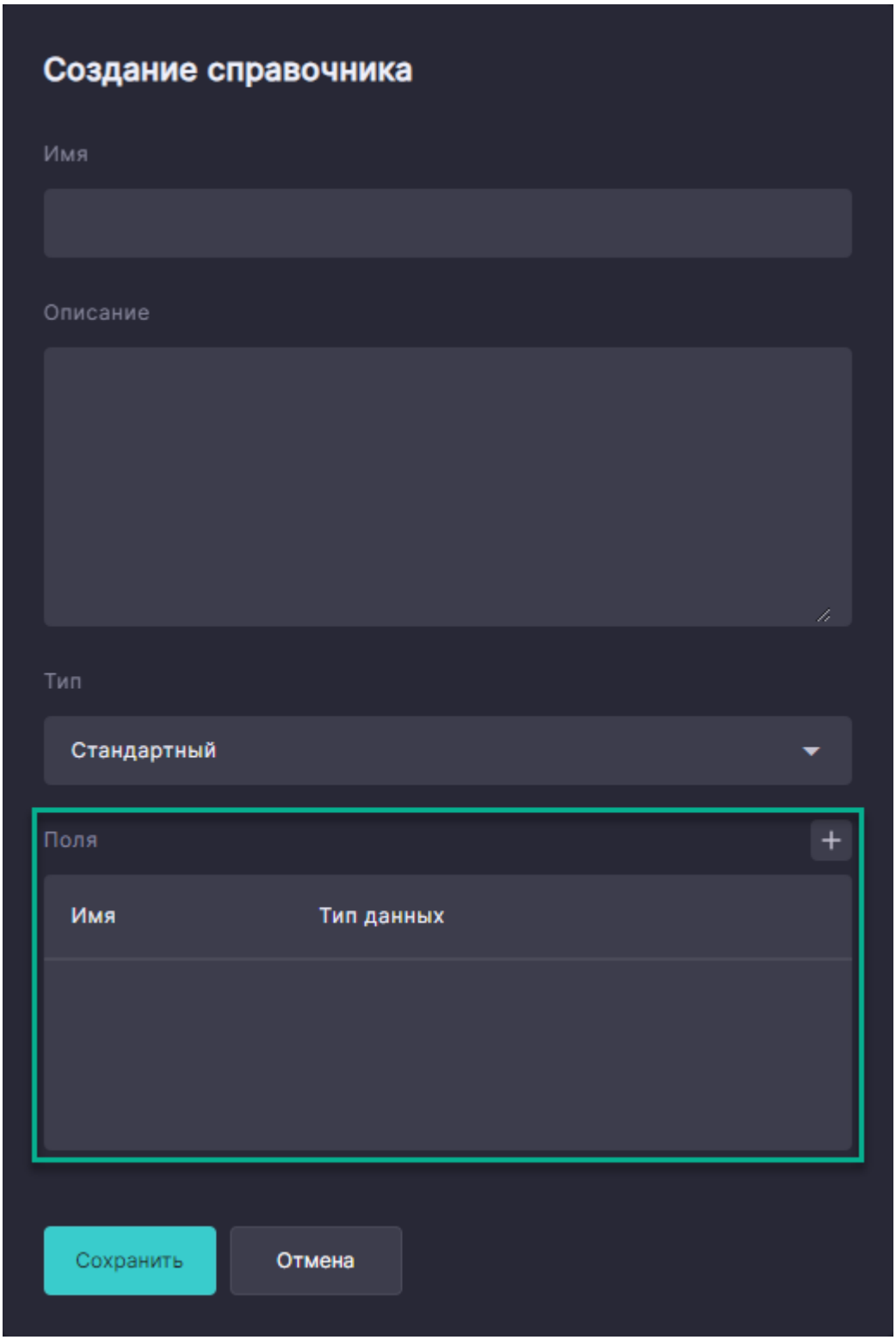


Настройки справочника

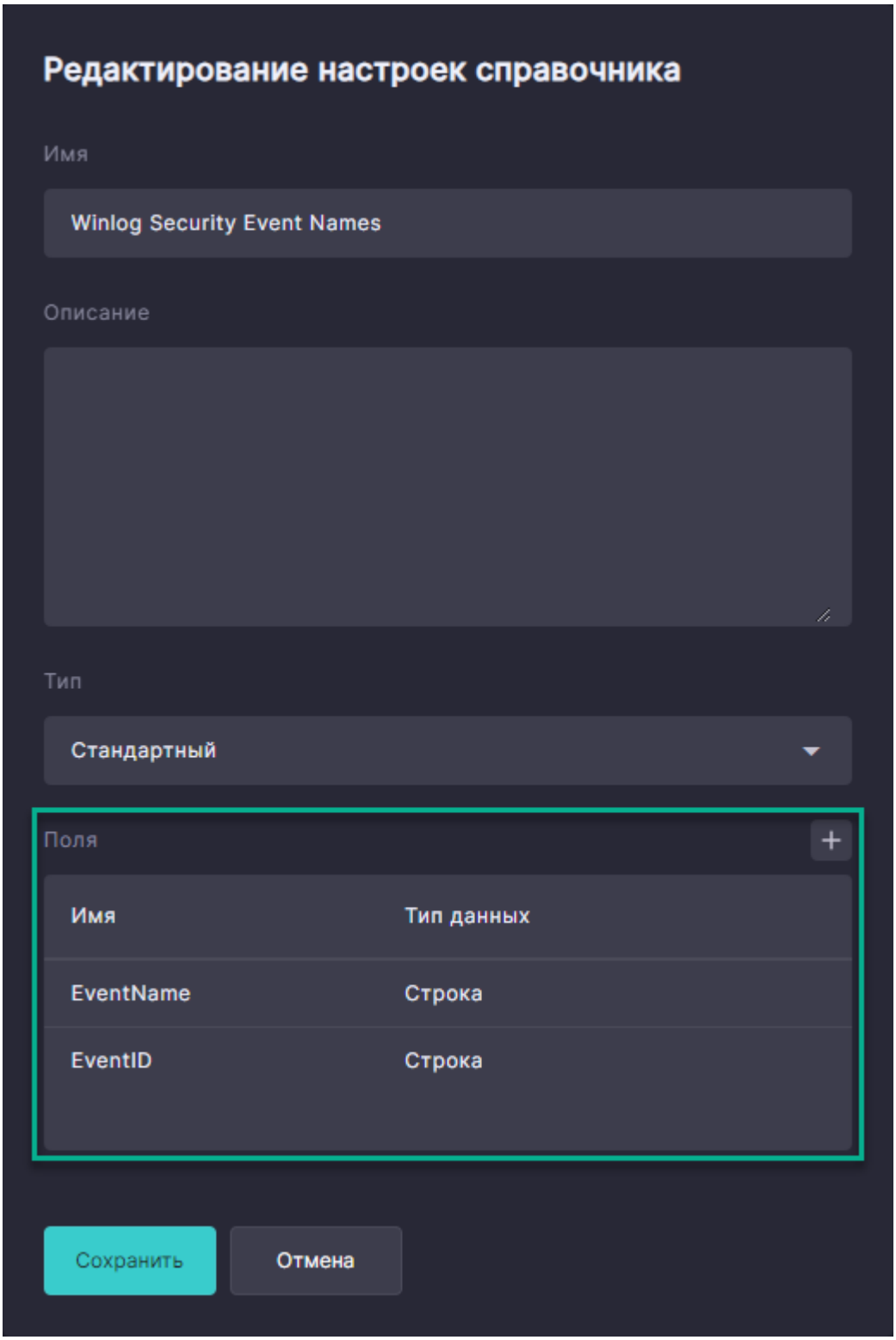
ТАБЛИЦА «ПОЛЯ»

Элемент настроек справочника, отображающий поля справочника и позволяющий их создавать, редактировать и удалять в следующих окнах модуля «Справочники»:

- окно «Создание справочника»;

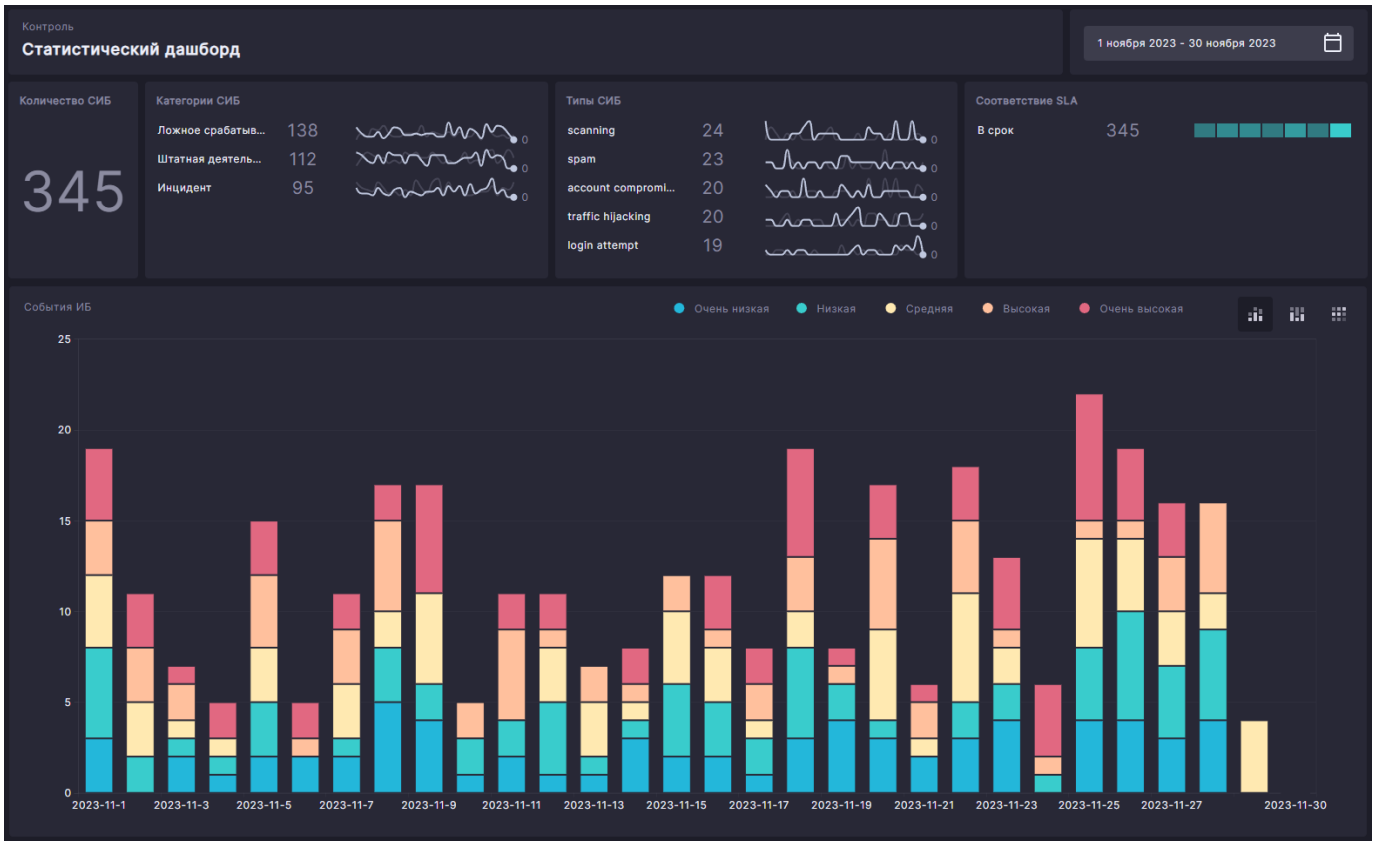


- окно «Редактирование настроек справочника».



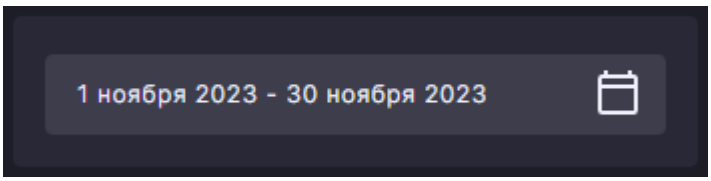
8.2.12 Модуль «Статистический дашборд»

Модуль используется для контроля состояния процесса мониторинга.

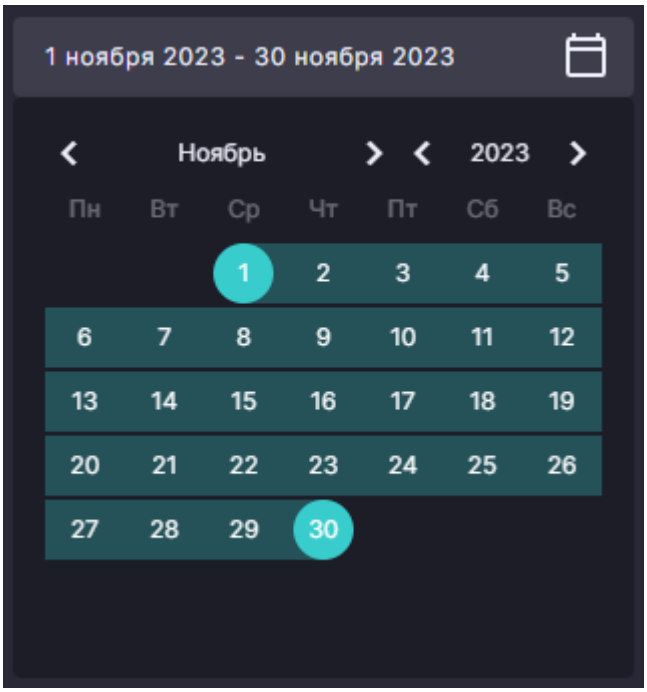


Для отображения информации используются следующие панели.

Панель редактора временного диапазона

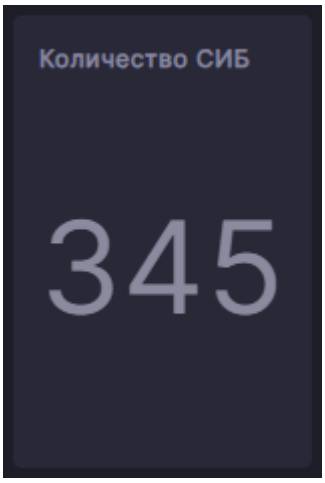


Позволяет задать диапазон выборки событий и инцидентов ИБ для получения статистических данных. Для задания диапазона нажмите в области редактора и в открывшемся окне календаря нажмите в любом порядке на начальную и конечную даты.



Содержимое остальных панелей будет обновлено данными из выбранного диапазона.

Панель «Количество СИБ»

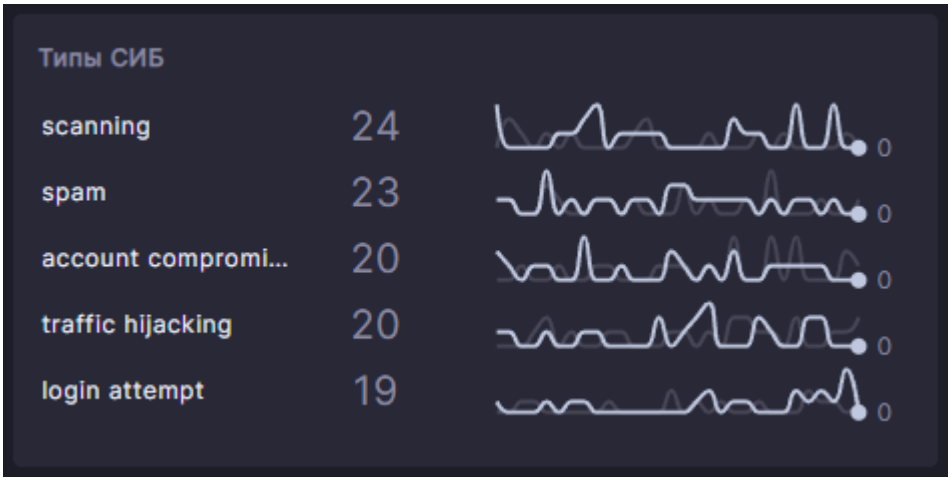


Отображает общее количество событий и инцидентов ИБ, созданных в заданный временной диапазон.

Панель «Категории СИБ»

Отображает количественные характеристики событий и инцидентов ИБ, созданных в заданный временной диапазон и сгруппированных по категориям. Панель позволяет изменять критерий фильтра и управлять настройками фильтра. Элементы панели (категории) отсортированы в порядке убывания их значений. Панель ограничена показом первых пяти элементов. Полный список элементов можно отобразить в боковой панели «Настройки фильтра».

Панель «Типы СИБ»

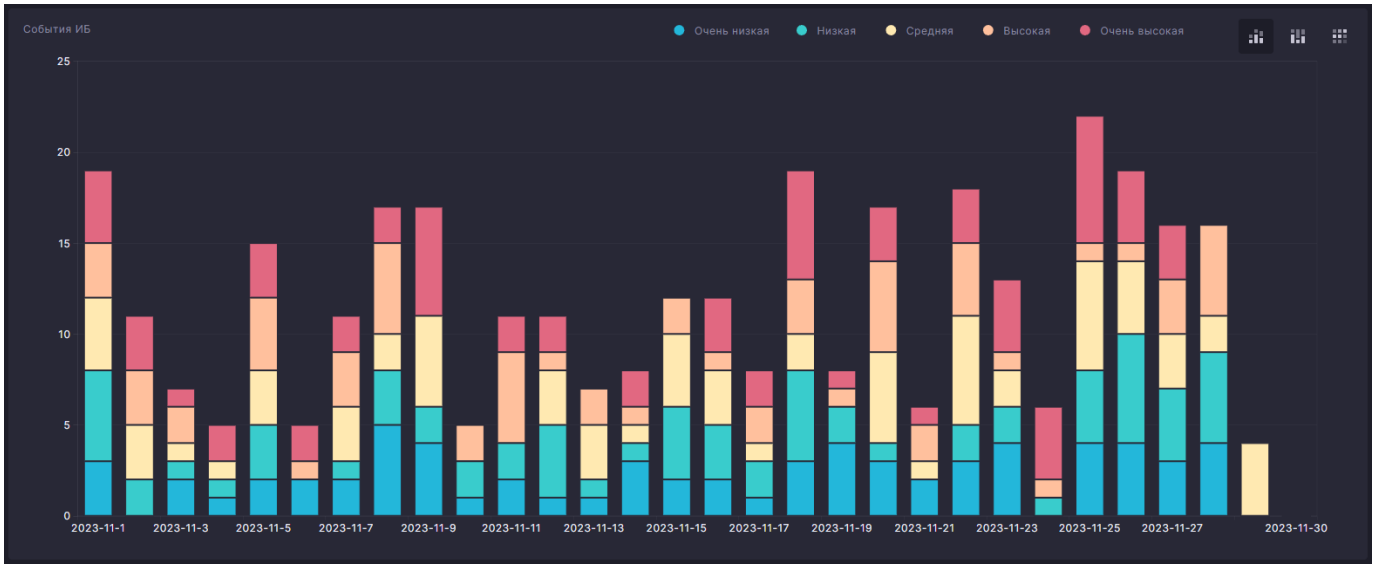


Отображает количественные характеристики событий и инцидентов ИБ, созданных в заданный временной диапазон и сгруппированных по типам. Панель позволяет изменять критерий фильтра и управлять настройками фильтра. Элементы панели (типы) отсортированы в порядке убывания их значений. Панель ограничена показом первых пяти элементов. Полный список элементов можно отобразить в боковой панели «Настройки фильтра».

Панель «Соответствие SLA»

Отображает количественные характеристики событий и инцидентов ИБ, созданных в заданный временной диапазон и сгруппированных по исполнению SLA. Панель позволяет изменять критерий фильтра и управлять настройками фильтра. Элементы панели (результаты исполнения) отсортированы в порядке убывания их значений. Панель ограничена показом первых пяти элементов. Полный список элементов можно отобразить в боковой панели «Настройки фильтра».

Панель «События ИБ»

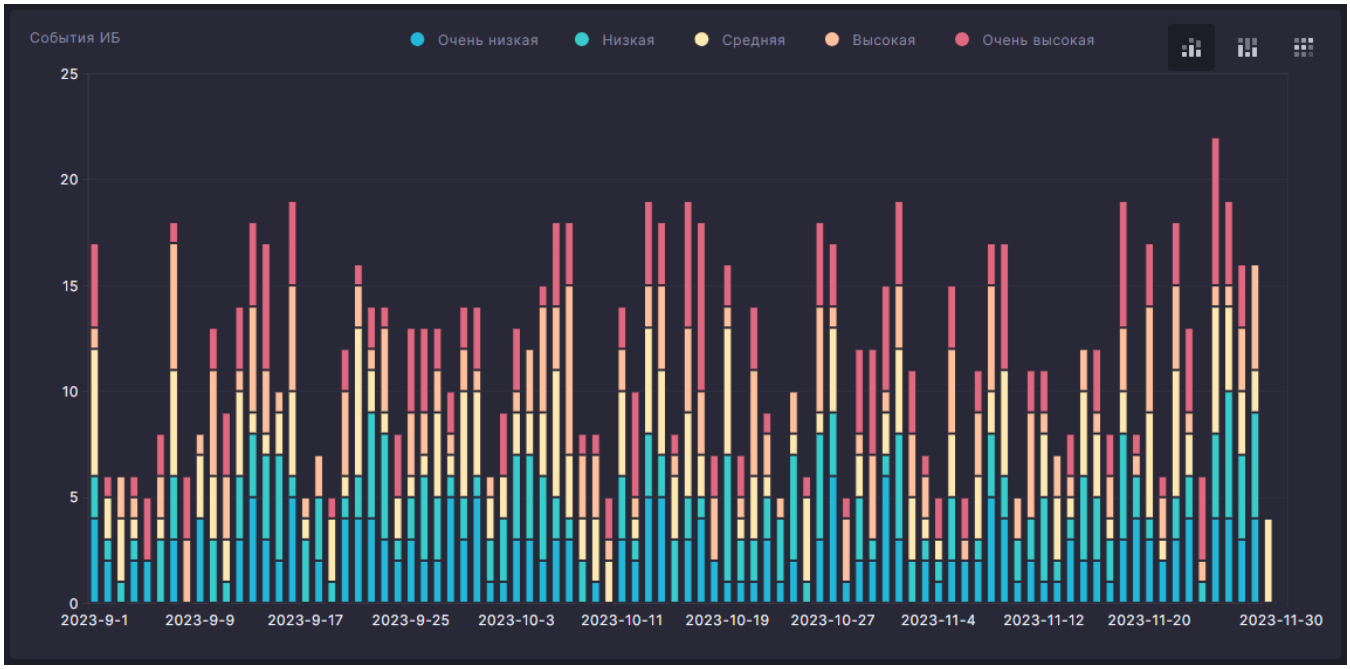


Отображает в виде диаграммы хронологию создания событий и инцидентов ИБ в заданном временном диапазоне. Данные диаграммы отфильтрованы по критериям, заданным в других панелях. Цвет сегментов диаграммы отражает критичность событий/инцидентов ИБ.

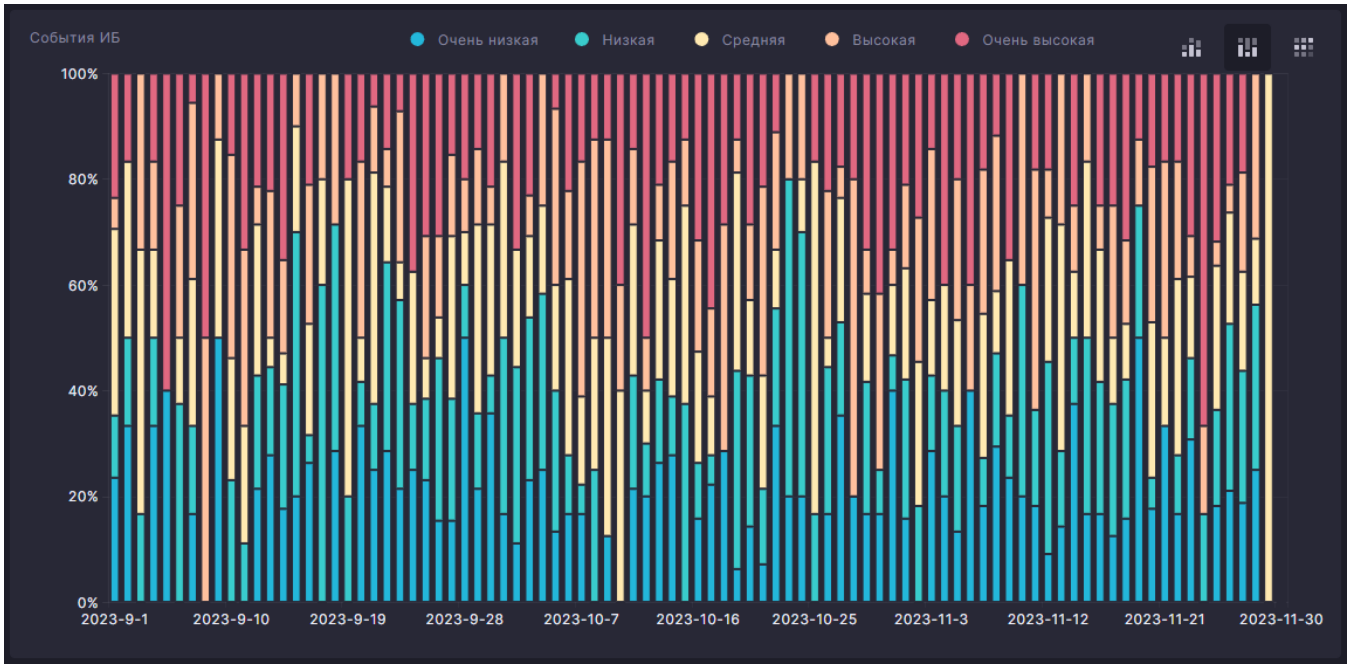
ВЫБОР ТИПА ДИАГРАММЫ

Нажмите на соответствующий значок в правом верхнем углу диаграммы для смены ее типа:

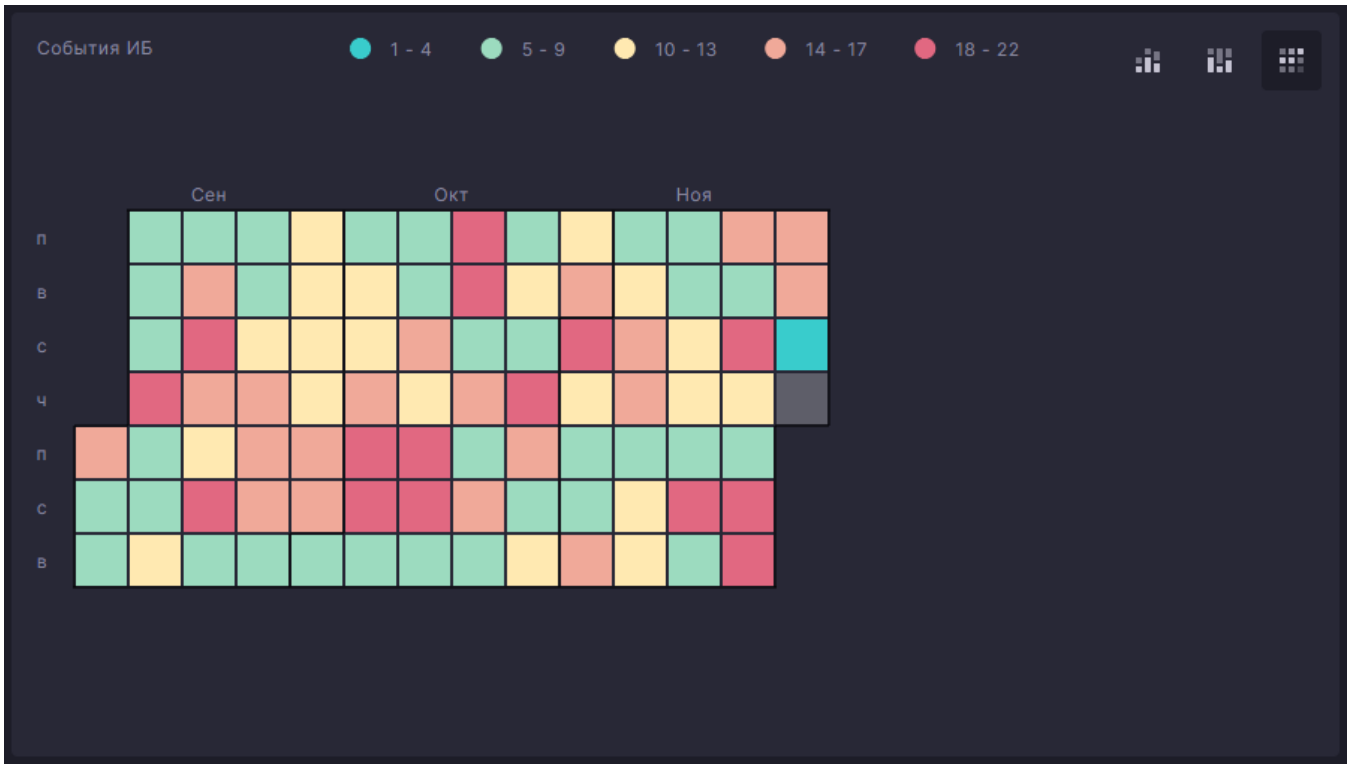
- Столбчатая диаграмма с накоплением ( ).



- Нормированная столбчатая диаграмма с накоплением ( ).

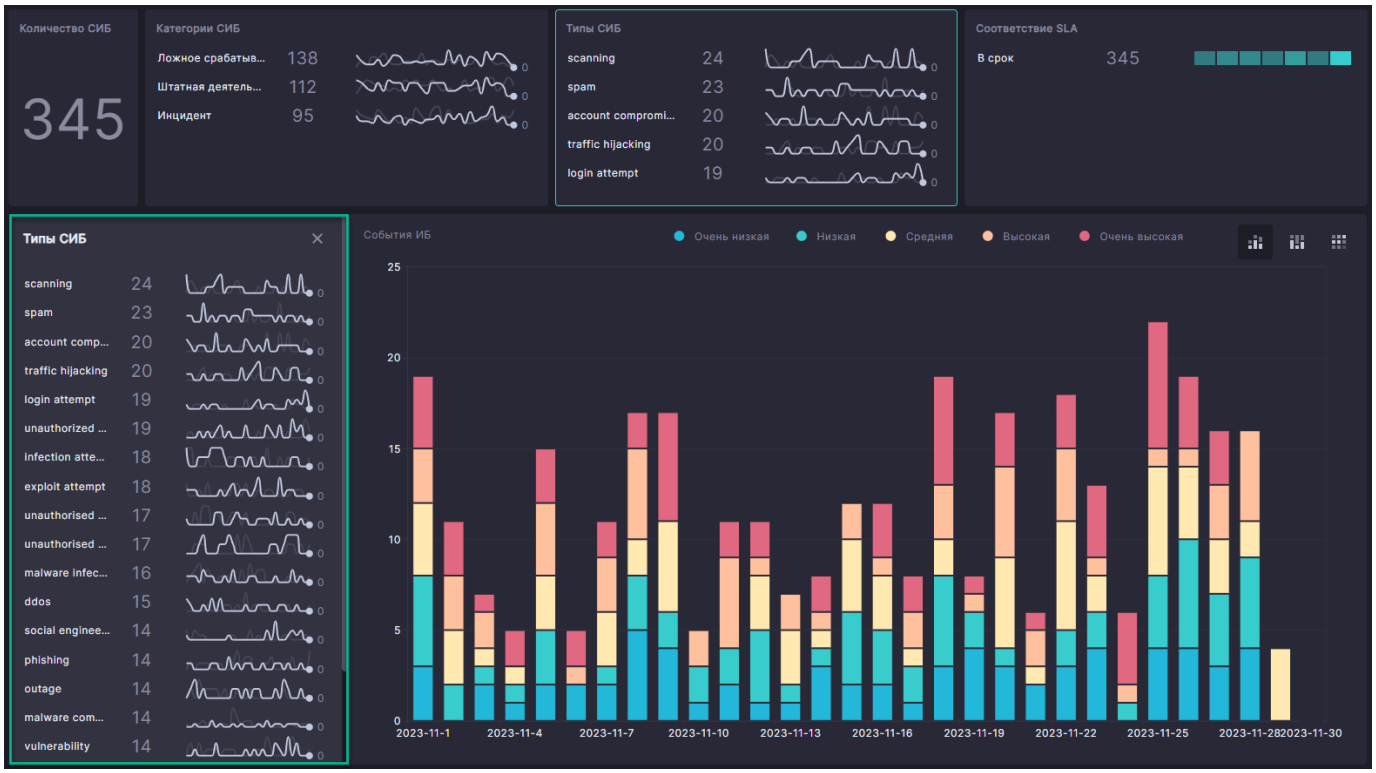


- Диаграмма интенсивности ( ).



Также вы можете просмотреть список событий и инцидентов ИБ в любом отображенном в панели единичном временном периоде, нажав на его графический элемент (столбец или ячейку).

Боковая панель «Настройки фильтра»



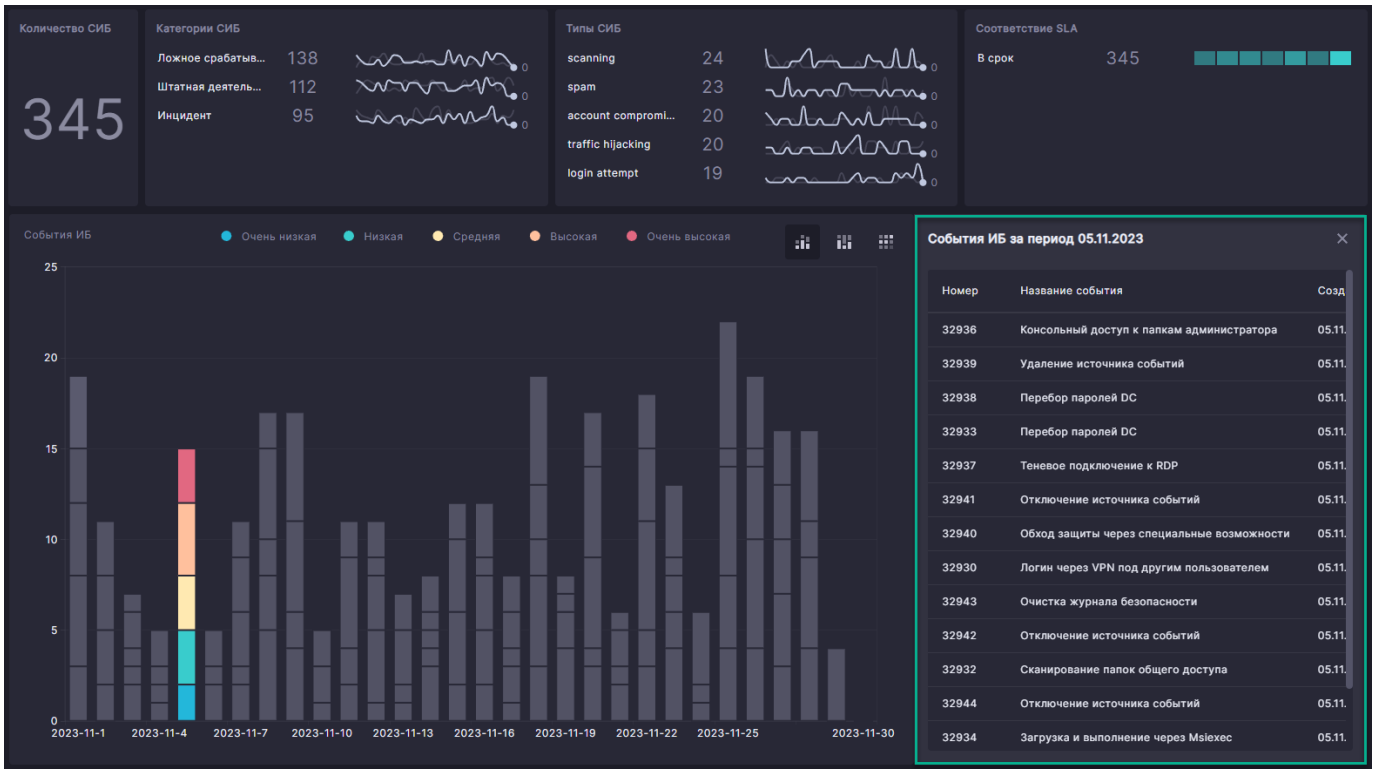
Позволяет просмотреть полный список доступных элементов другой панели (источника), минуя ограничение в пять элементов. Боковую панель можно отобразить нажатием контекстного значка («Показать настройки фильтра») в панели-источнике при управлении ее настройками фильтра.

Содержимое боковой панели включает в себя:

- имя панели-источника;
- все ее элементы, доступные для фильтрации представленных в панели «События ИБ» событий и инцидентов ИБ.

Вы можете нажать элемент в этой боковой панели, чтобы изменить соответствующий критерий фильтра.

Боковая панель «События ИБ за период»



Отображает в виде таблицы события и инциденты ИБ, созданные в выбранном в панели «События ИБ» временном периоде. Этот период указан в заголовке панели.

Настройка фильтра данных хронологии создания СИБ

Система предоставляет возможность отфильтровать данные, представленные в панели «События ИБ», описанными ниже способами.

ИЗМЕНЕНИЕ КРИТЕРИЯ ФИЛЬТРА

Доступно в следующих панелях:

- «Категории СИБ»;
- «Типы СИБ»;
- «Соответствие SLA»;
- «Настройки фильтра».

Нажмите на элемент панели, чтобы добавить соответствующий критерий к фильтру данных, представленных в панели «События ИБ».

Каждая панель может создать только один критерий фильтра, поэтому добавляемый критерий заместит существующий от этой панели.

Элемент, используемый в фильтре, выделится цветом. Для удаления критерия из фильтра выберите один из следующих вариантов:

- Нажмите на выделенный цветом элемент панели.
- Наведите указатель мыши на панель и нажмите значок  («Очистить»), отображаемый в ее правом верхнем углу.

УПРАВЛЕНИЕ НАСТРОЙКАМИ ФИЛЬТРА

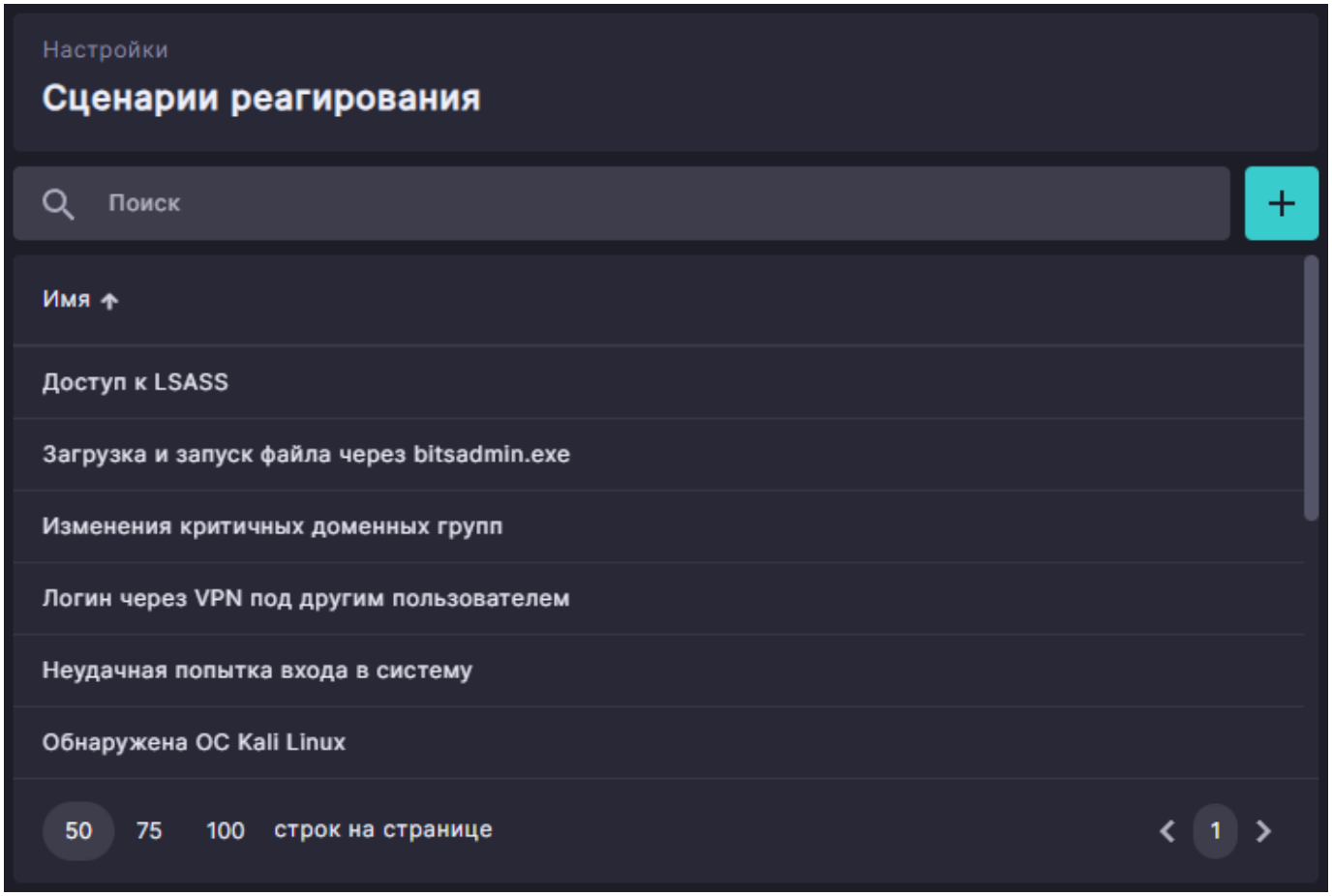
Доступно в следующих панелях:

- «Категории СИБ»;
- «Типы СИБ»;
- «Соответствие SLA».

Наведите указатель мыши на панель и нажмите контекстный значок («Показать настройки фильтра»), отображаемый в ее правом верхнем углу. Панель «Настройки фильтра» отобразится сбоку от панели «События ИБ». Повторное нажатие значка закроет панель с настройками фильтра.

8.2.13 Модуль «Сценарии реагирования»

Позволяет создавать сценарии реагирования для обработки событий ИБ и устранению инцидентов ИБ в автоматическом и полуавтоматическом режимах.

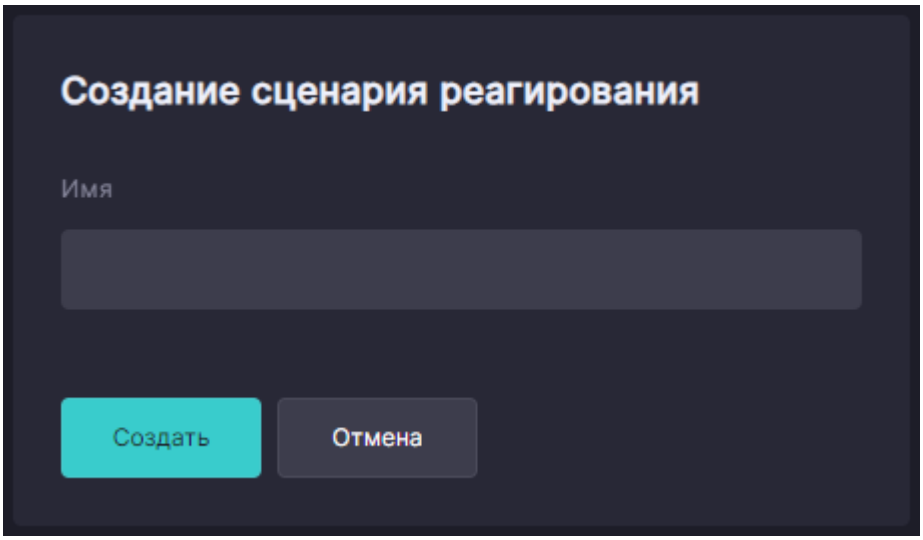


Для отображения созданных сценариев реагирования используется табличное представление.

Управление сценариями реагирования

СОЗДАНИЕ СЦЕНАРИЯ РЕАГИРОВАНИЯ

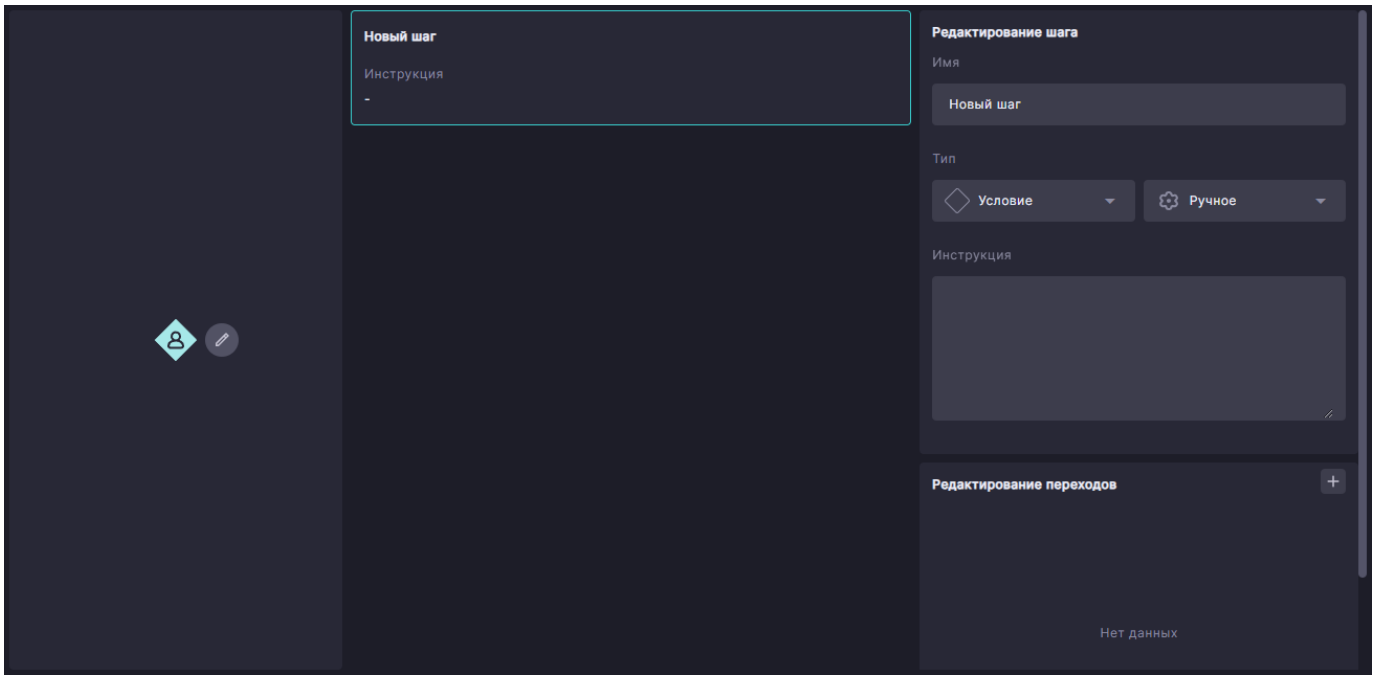
Нажмите значок + («Создать сценарий реагирования»). В открывшемся окне «Создание сценария реагирования» введите уникальное имя для идентификации сценария реагирования в интерфейсе Системы.



Нажмите кнопку «Создать», чтобы завершить создание сценария. Окно закроется, и созданный сценарий будет автоматически переведен в режим редактирования.

Чтобы закрыть окно и отказаться от создания сценария реагирования, нажмите кнопку «Отмена».

Созданный сценарий будет содержать единственный шаг.



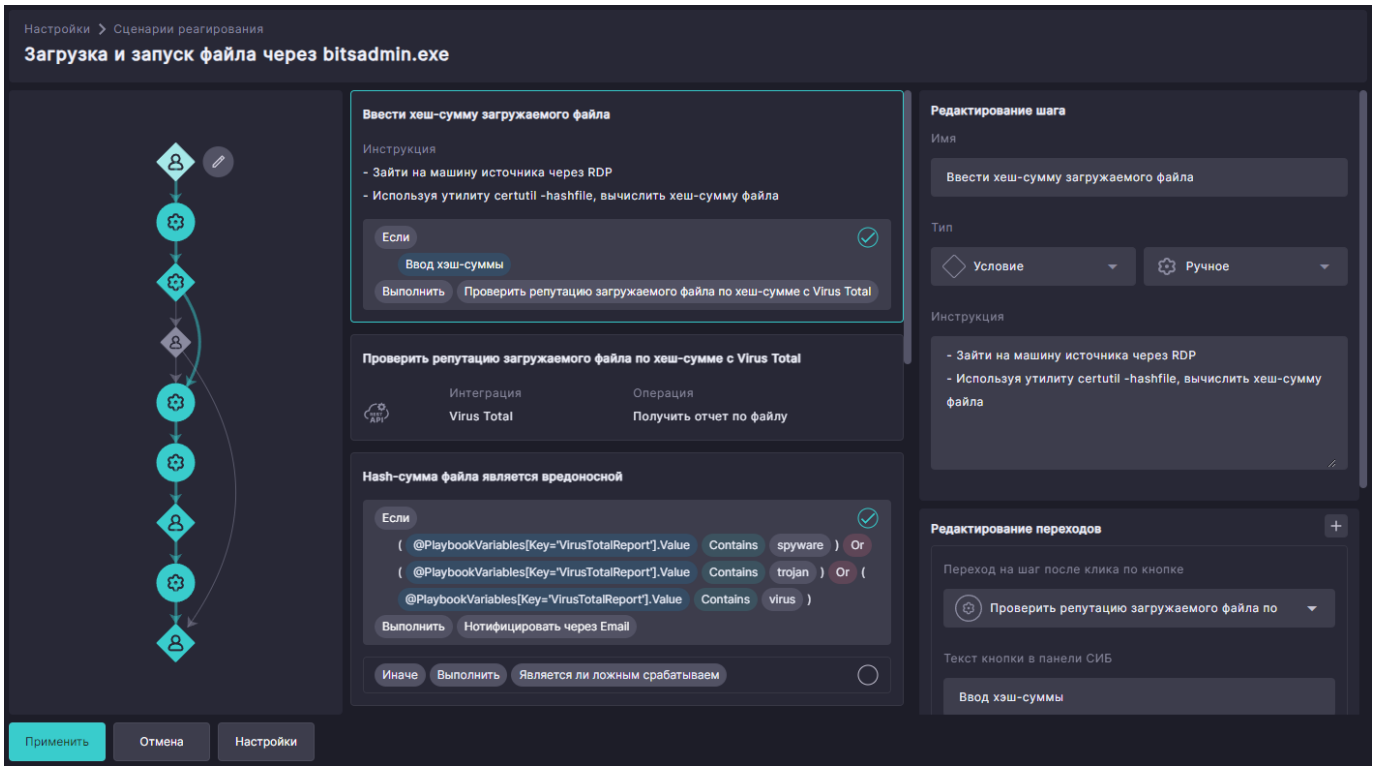
Вы можете продолжить работу в режиме редактирования либо вернуться к таблице сценариев модуля, нажав кнопку «Отмена».

РЕДАКТИРОВАНИЕ СЦЕНАРИЯ РЕАГИРОВАНИЯ

Найдите в таблице запись с требуемым сценарием реагирования и переведите его в режим редактирования одним из следующих способов:

- Дважды щелкните мышью по записи.
- Наведите указатель мыши на запись и нажмите контекстный значок () («Открыть детальную информацию»).

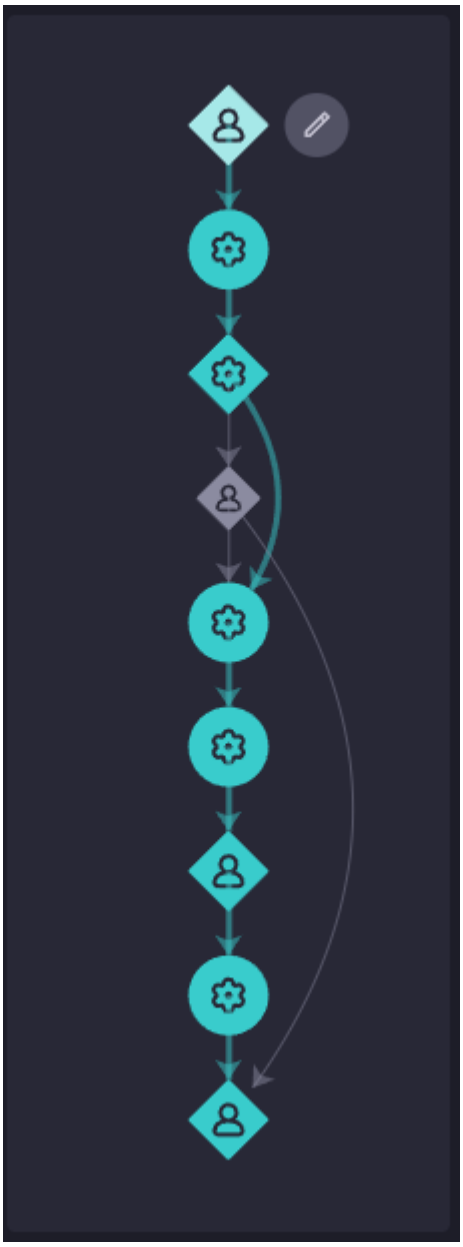
Режим редактирования



В режиме редактирования модуль предоставляет следующие инструменты настройки сценария реагирования.

ДИАГРАММА

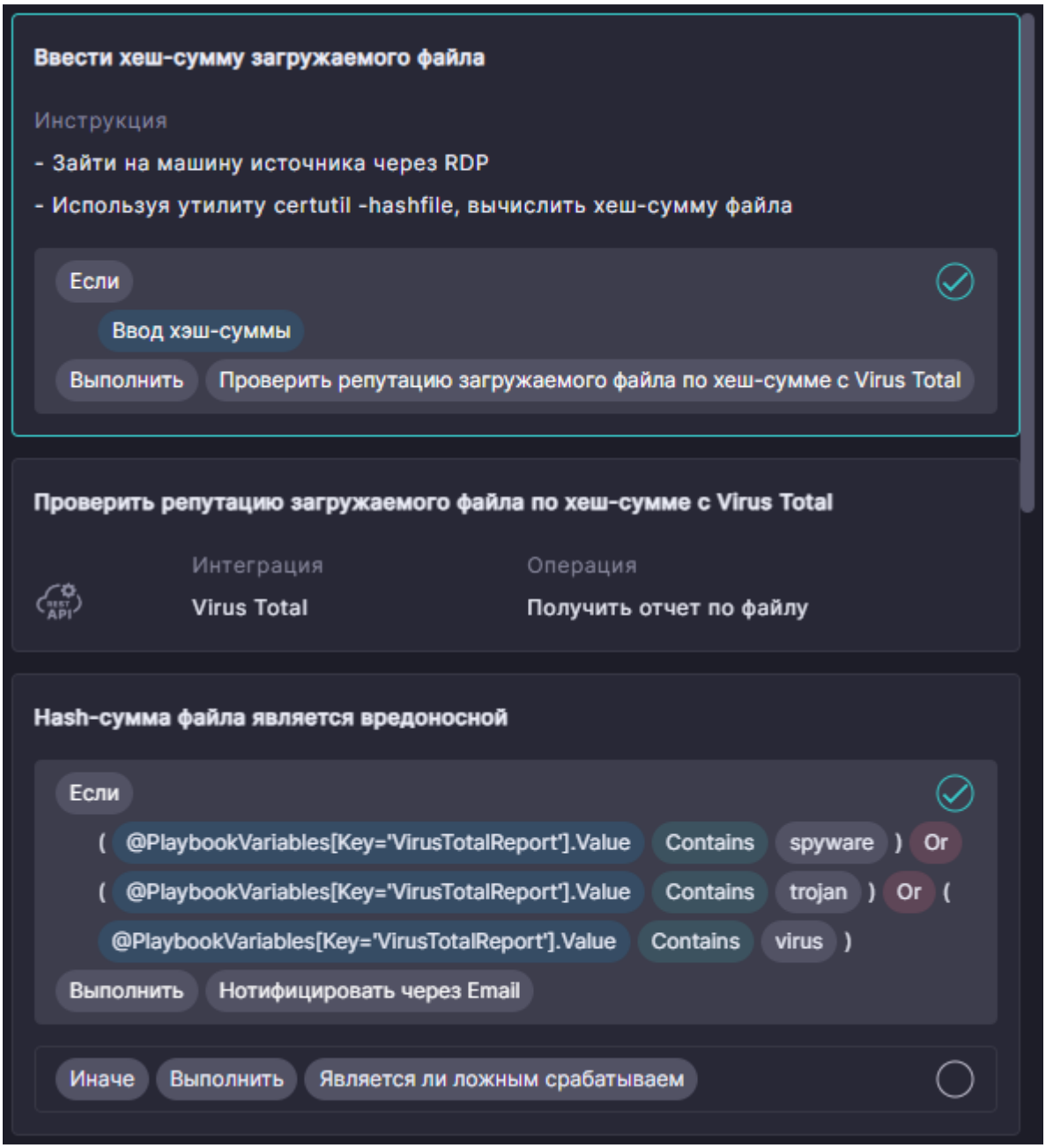
Является визуальным представлением редактируемого сценария реагирования, его шагов (узлов) и переходов (направленных линий).



Список предоставляет следующие возможности:

- выбор шага для его быстрого нахождения в списке шагов и отображения параметров шага;
- выполнение действий с выбранным шагом.

СПИСОК ШАГОВ

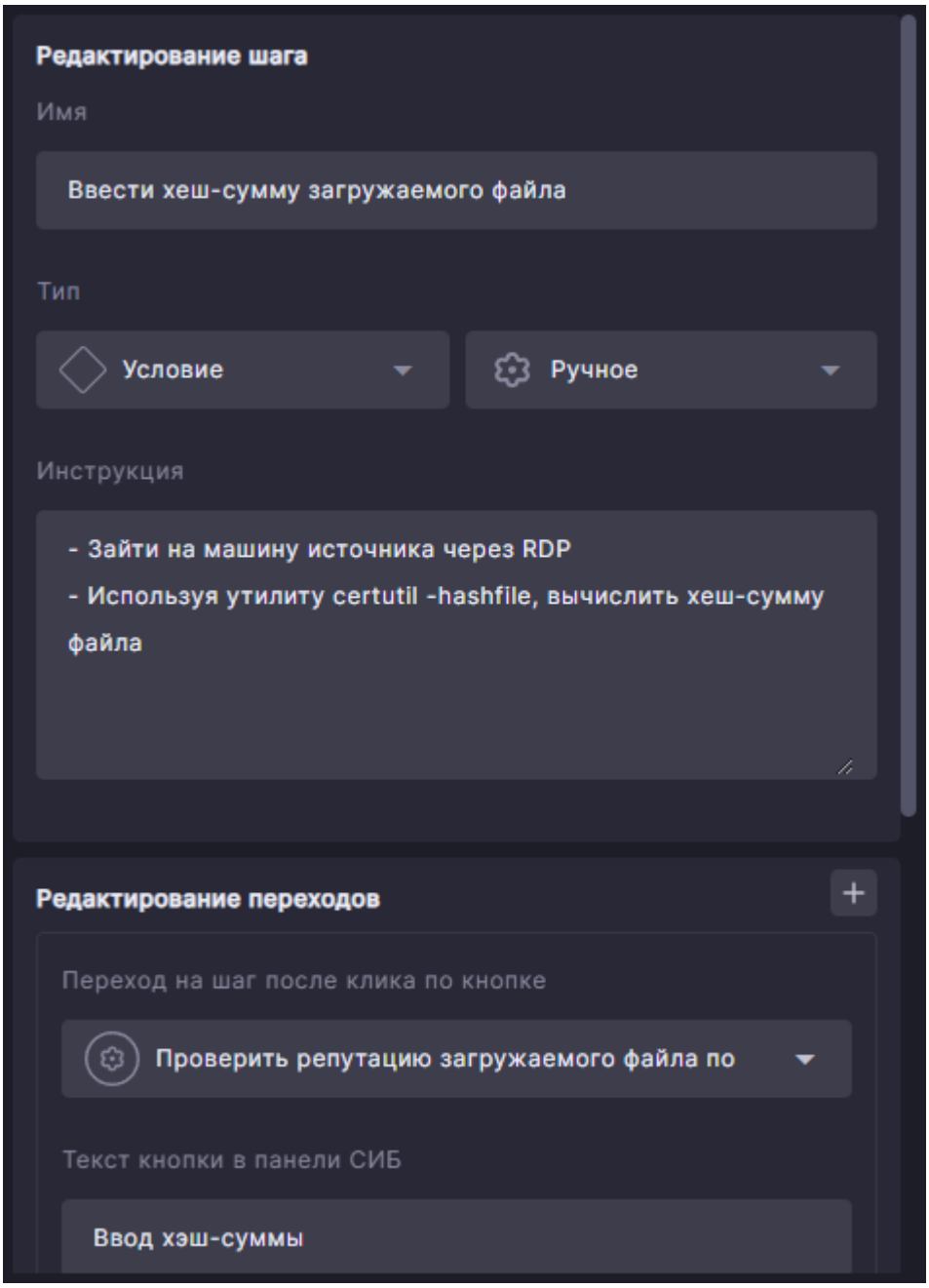


Список предоставляет следующие возможности:

- выбор шага для его быстрого нахождения в диаграмме и отображения его параметров;
- выбор ветки сценария для отображения в списке шагов и диаграмме.

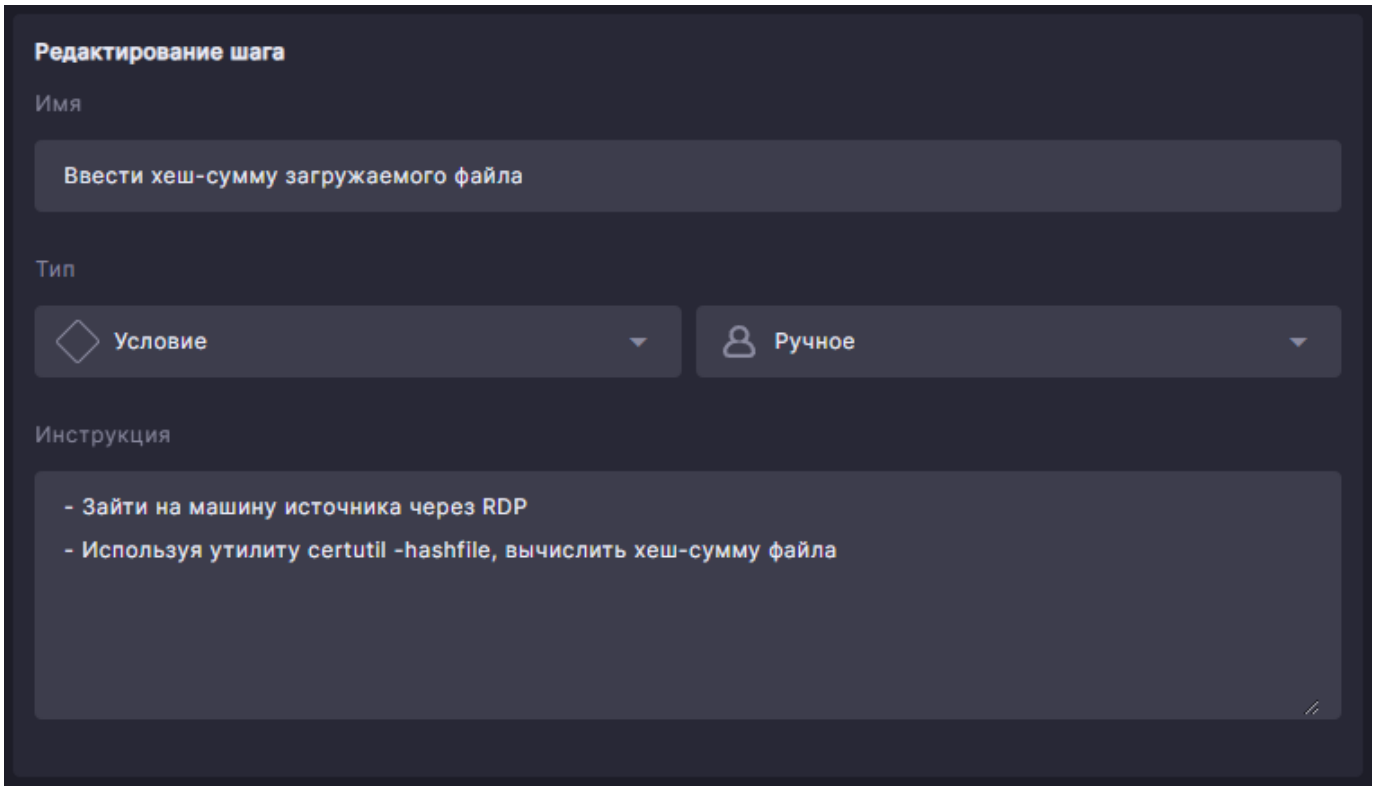
СПИСОК ПАРАМЕТРОВ ШАГА

Отображает параметры выбранного шага.



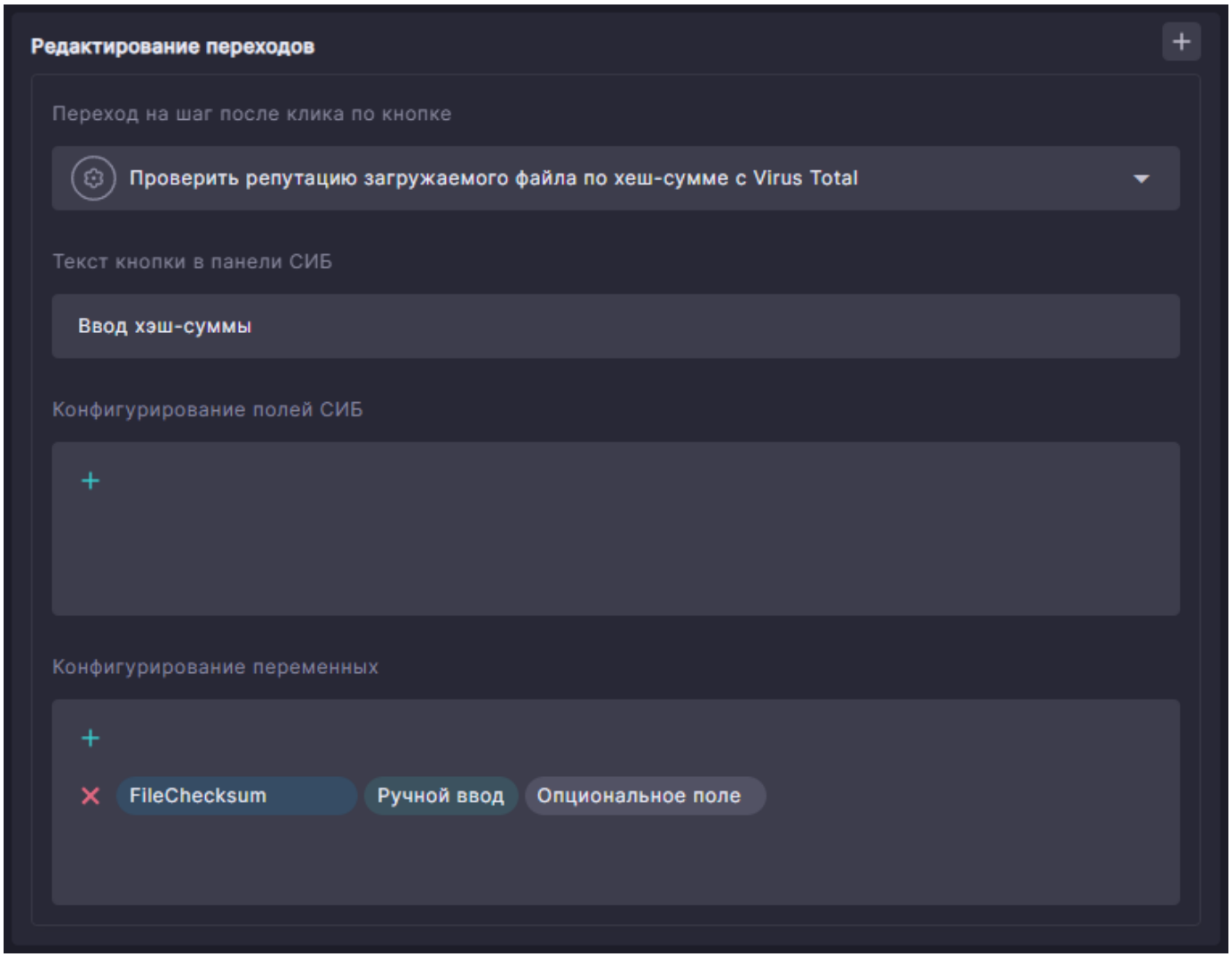
Панель «Редактирование шага»

Позволяет задать имя, тип и другие параметры выбранного шага.



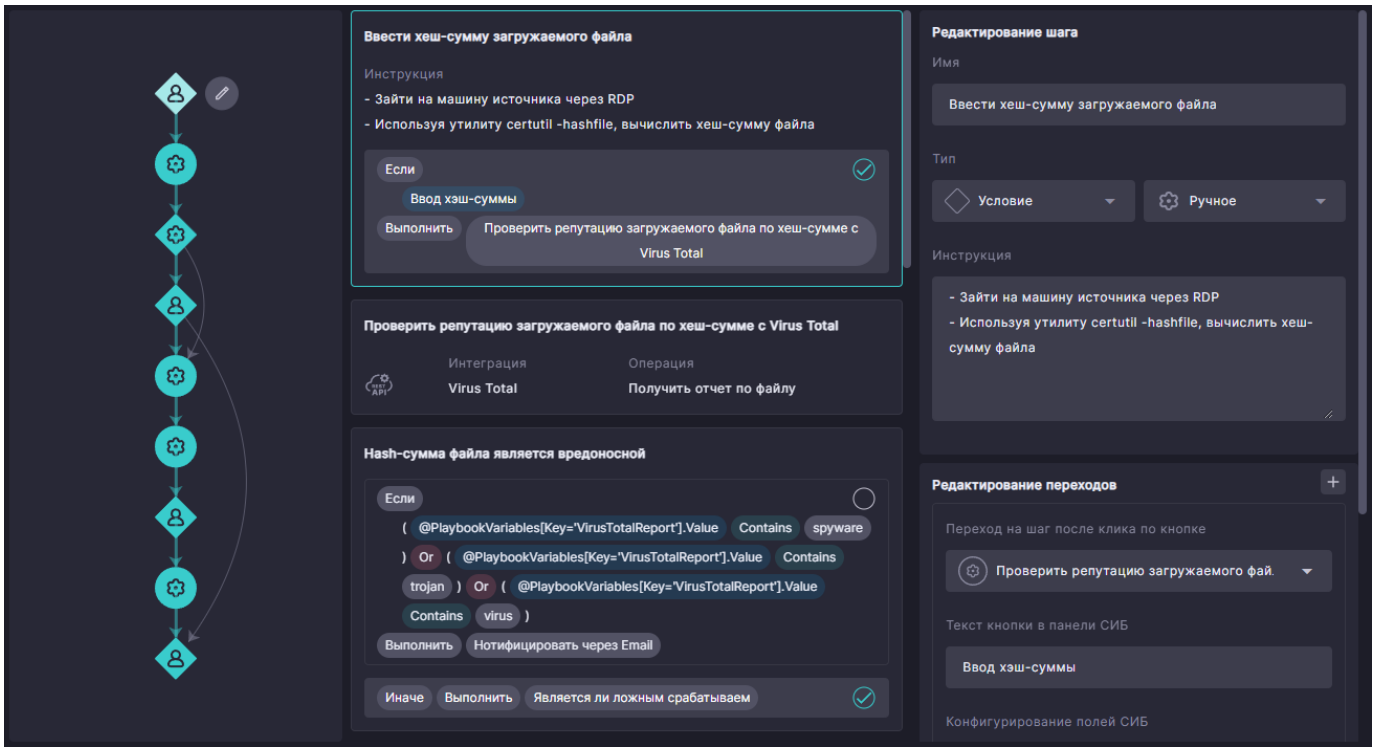
Панель «Редактирование переходов»

Позволяет управлять переходами из выбранного шага и настраивать их параметры, включая конфигурации полей сценария и события или инцидента ИБ, который будет связан с этим сценарием.



ВЫБОР ШАГА ДЛЯ ПРОСМОТРА ПАРАМЕТРОВ

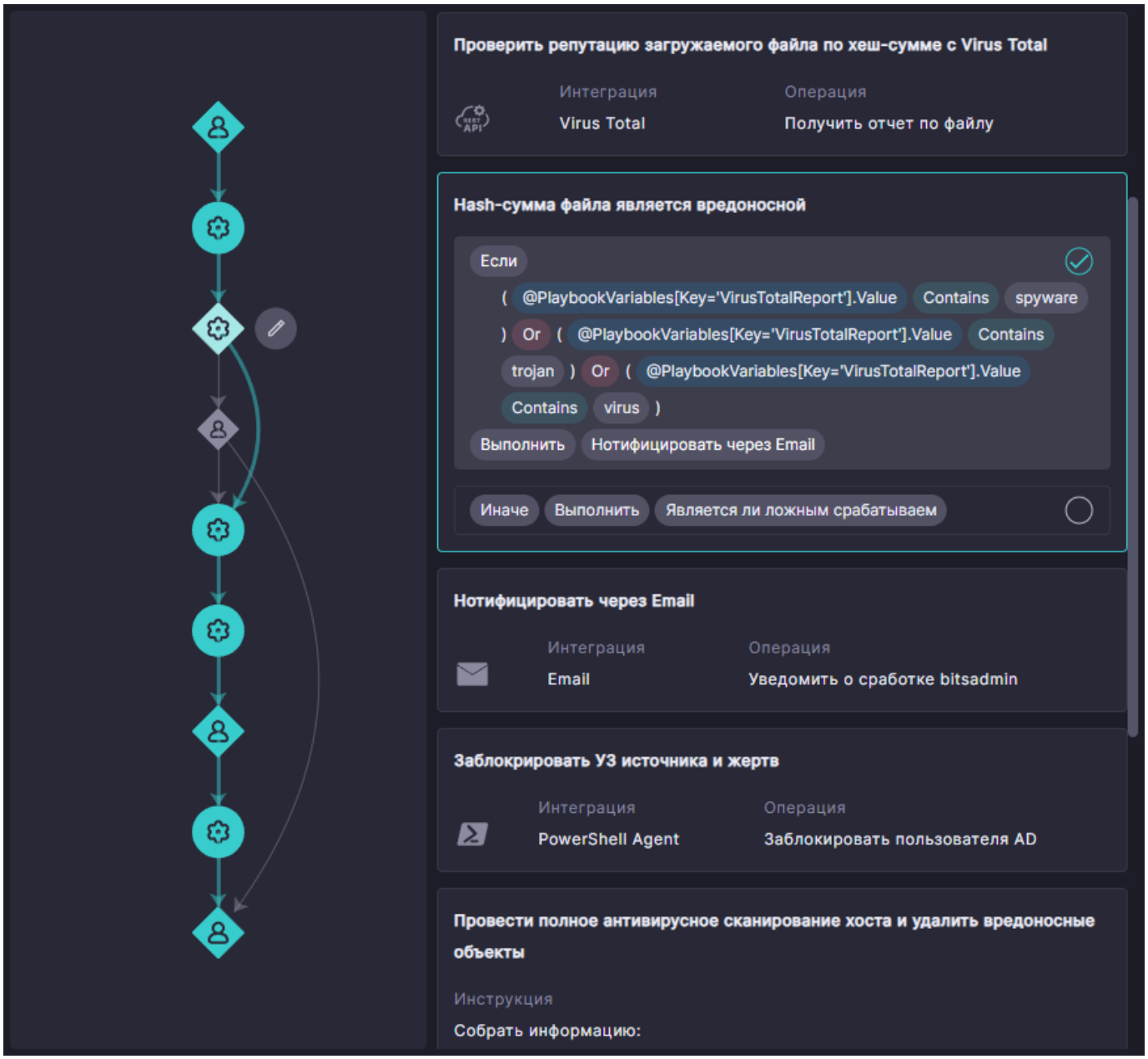
Для выбора шага нажмите на него в диаграмме или в списке шагов. Этот шаг будет выделен более ярким цветом, а также будет обведен рамкой в списке шагов.



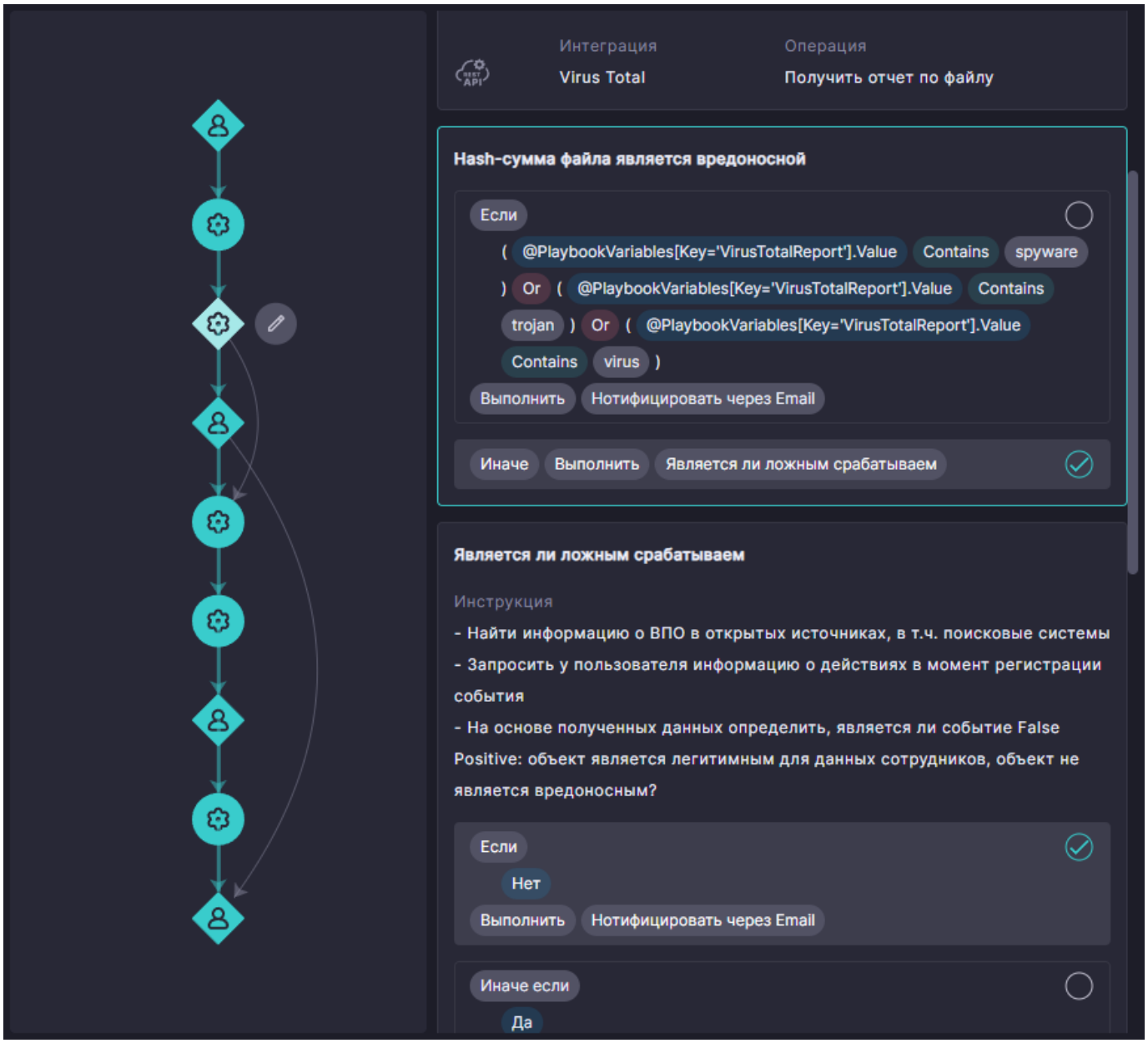
В диаграмме рядом с выбранным шагом будет отображен значок , позволяющий раскрыть меню с доступными для выполнения с этим шагом действиями.

ВЫБОР ВЕТКИ СЦЕНАРИЯ

Шаг-условие отображает все шаги, на которые из него имеются прямые переходы.

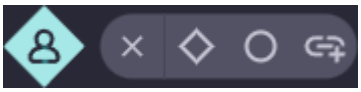


Для выбора ветки нажмите на соответствующий шаг из них. Выбранный шаг будет отмечен значком . При этом список шагов обновится и отобразит шаги выбранной ветки, а диаграмма выделит цветом шаги и переходы, относящиеся к этой ветке.



ВЫПОЛНЕНИЕ ДЕЙСТВИЯ С ВЫБРАННЫМ ШАГОМ

Нажмите значок ✎ для показа раскрывающегося меню с доступными действиями.



Доступные действия представлены в меню следующими значками:

-  - Закрыть меню.
-  - Добавить переход на новое условие.
-  - Добавить переход на новую автоматизацию.
-  - Добавить переход на существующий шаг.
-  - Удалить шаг.

Нажмите на значок для выполнения соответствующего действия.

9. Глоссарий

9.1 Группа компьютеров

Логическое объединение компьютеров с установленным специализированным ПО (агентом), предназначенное для унификации процесса сбора событий из источников, находящихся на этих компьютерах. Группы компьютеров задаются в конфигурации Системы.

9.2 Инцидент ИБ

Событие ИБ, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ.

9.3 Исходное событие

Событие, полученное из источника событий. Данные исходного события являются основой для его подготовки к использованию в Системе. Исходное событие хранится в Системе совместно с подготовленным событием.

9.4 Конфигурация Системы

Набор настроек, определяющих рабочие процессы, параметры функционирования модулей, роли и группы пользователей, а также функции и действия, доступные пользователям в рамках Системы.

В последующих версиях Системы будут предоставляться средства настройки конфигурации.

9.5 Корреляция

Производимый в реальном времени анализ подготовленных событий на наличие признаков угроз ИБ. В анализе могут участвовать данные справочников и переменных.

Полученные результаты анализа применяются для выполнения следующих задач:

- выявление в рамках мониторинга событий, удовлетворяющих заданным пользователем критериям;
- обогащение выявленных событий дополнительными данными;
- реагирование на выявленные события, включая создание событий ИБ и управление содержимым динамических справочников.

Корреляция событий выполняется специализированным компонентом Системы (коррелятором) на основе заданных пользователем правил.

9.6 Модель события

Универсальная совокупность полей, необходимых для хранения данных исходных событий, подготовленных к использованию в Системе. Каждое созданное на основе модели событие содержит все определенные в ней поля.

Модель события можно динамически расширять новыми полями в соответствии с созданием и модификацией ресурсов Системы (источников событий, правил обогащения, корреляции и других).

9.7 Нормализованное событие

Нормализация начинает процесс подготовки события к использованию в Системе. При нормализации создается экземпляр события на основе модели события и его поля заполняются данными исходного события на основе правил нормализации. Правилами нормализации служат все включенные для этих полей сопоставления, заданные в источнике исходного события. Полю модели могут сопоставляться несколько полей из разных источников событий.

За нормализацией события следует его обогащение.

9.8 Обогащенное событие

Обогащение расширяет контекст события дополнительными данными на основе правил обогащения и справочников. Правило обогащения включает в себя:

- критерии выборки целевых событий, которые будут обогащаться;
- описания действий, которые необходимо выполнить для этих событий.

Можно обогащать следующие события:

- События, прошедшие нормализацию (нормализованные) события.

  Обогащение завершает процесс подготовки этих событий к использованию в Системе.

- Подготовленные события, которые удовлетворяют критериям, указанным в правилах корреляции.

  Обогащение производится на основе описаний действий по обогащению, заданных в этих правилах.

9.9 Подготовленное событие

Подготовка является одним из этапов сбора событий. Она преобразует данные исходного события в универсальный формат модели события, чьи поля будут хранить данные для дальнейшего использования в Системе при визуализации, анализе, создании отчетов и других операциях.

При подготовке события производятся:

- нормализация события с заполнением его полей на основе правил нормализации;
- обогащение нормализованного события с заполнением его полей на основе правил обогащения.

Подготовленное событие хранится в Системе совместно с исходным событием.

9.10 Поддерживаемые типы данных

Тип данных определяет формат их представления и диапазон возможных значений. Система поддерживает работу со следующими типами данных:

- строка;
- число (целое);
- дата.

9.11 Показатель SLA

Индикатор качества исполнения временных нормативов, определенных в соглашении об уровне обслуживания (SLA) для каждого этапа обработки события ИБ или инцидента ИБ.

Параметры SLA задаются в конфигурации Системы.

9.12 Поле модели события

Предназначено для хранения данных элемента структуры модели события в подготовленном событии после нормализации и обогащения. Поле модели может использоваться в нескольких правилах нормализации и/или обогащения.

Поле имеет следующие характеристики:

- Имя.

  Идентифицирует данные поля в модели и графическом интерфейсе Системы. Является уникальным в модели. Допускает использование пробелов.

- Тип данных.

  Определяет формат представления и диапазон значений данных поля.

9.13 Правило корреляции

Правило корреляции позволяет автоматизировать выявление и реагирование на события, свидетельствующие о возможных угрозах ИБ. Правило корреляции определяет действия, выполняемые коррелятором при анализе подготовленных событий.

Правило корреляции позволяет задать:

- Критерии поиска подготовленного события или последовательности таких событий.

  События, удовлетворяющие этим критериям, называются корреляционными.

- Опциональные действия по обогащению каждого корреляционного события дополнительными данными.

  Эти действия выполняются до срабатывания правила.

- Действия по реагированию на корреляционные события.

  Эти действия выполняются по срабатыванию правила.

Иными словами, правило корреляции срабатывает при выявлении одного или нескольких корреляционных событий и выполняет с ними заданные действия по реагированию.

9.13.1 Типы правил

Поддерживаются следующие типы правил корреляции:

- Простое.

  Срабатывает при каждом выявлении корреляционного события.

- С агрегированием (оконное).

  Срабатывает при возникновении последовательности корреляционных событий в течение установленного временного интервала. Данный интервал определяет «окно» срабатывания правила, поэтому такое правило также называется «оконным». В критериях срабатывания такого правила можно использовать функции вычисления агрегированных значений по корреляционным событиям, вошедшим в последовательность.

9.14 Процессная модель

Описывает последовательность процессов (действия/операции и исполнители/участники) обработки событий и инцидентов ИБ организации. С Системой поставляется базовая реализация процессной модели, включающая в себя:

- три линии обработки событий и инцидентов ИБ;
- правила перевода событий и инцидентов ИБ между линиями.

Настройки процессной модели входят в конфигурацию Системы.

9.15 Событие ИБ

Регистрируется во время проведения мониторинга или исследования при выявлении у подготовленного события признаков угрозы ИБ.

9.16 Сопоставление

Отражает общность данных поля модели события и элемента исходного события, полученного из источника событий. Сопоставления задаются в источнике событий и служат правилами нормализации событий.

Сопоставление задается следующими характеристиками:

- Путь в источнике.

  Представляет собой строковый ключ, назначенный элементу исходного события парсером (обработчиком формата) этого события. Ключ обычно содержит имя парсера и идентификатор элемента. Поставляемые с Системой парсеры названы в соответствии с типами источников событий, чей формат они обрабатывают.

  После нормализации данные элемента исходного события будут храниться в сопоставленном ему поле модели события. Если элементу не сопоставлено поле модели события, то данные этого элемента будут храниться в поле с именем, идентичным назначенному ключу.

- Имя поля модели события.

  Тип данных поля определяется из модели события.

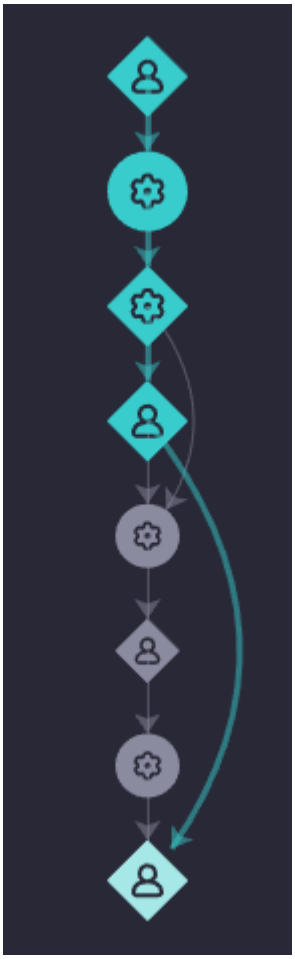
- Состояние (Включено/Выключено).

  Показывает, используется ли сопоставление при нормализации. Правилами нормализации могут служить только сопоставления включенных источников.

В графическом интерфейсе Системы данные исходного события будут представлены в сопоставленных полях модели события. Одно поле модели события может использоваться в нескольких сопоставлениях.

9.17 Сценарий реагирования (playbook)

Набор действий по устранению конкретного типа инцидента ИБ. Визуально представляется в виде диаграммы, состоящей из последовательности шагов (узлов) и направленных линий переходов между ними.



9.18 CSV-файл

Формат CSV - универсальный формат хранения табличных данных в текстовых файлах. CSV-файл содержит строку заголовка с именами полей и следующие за ней строки со значениями полей. Файл имеет кодировку UTF-8.

При сохранении данных в файл производятся следующие операции:

- Имена и значения полей в строках разделяются запятыми.
- К символу кавычки (") добавляется еще один символ кавычки (").
- Если имена полей или их значения содержат символы запятой или кавычек (, и "), они заключаются в кавычки (").

10. Юридическая информация

10.1 Авторские права

Материалы, приведенные в настоящем документе, являются собственностью ООО «Гефест Технолоджиз» и могут быть использованы только для целей экспертной проверки Системы в рамках процедуры включения в Единый реестр российских программ для электронных вычислительных машин и баз данных, а также для личных целей приобретателей программного комплекса автоматизации ситуационного центра информационной безопасности «Эгида».

Запрещается воспроизведение отдельных частей документа, внесение правок в него, размещение на сетевых ресурсах, распространение в любой форме (в том числе в переводе) на бумажных и электронных носителях, посредством каналов связи и средств массовой информации или каким-либо другим способом без специального письменного разрешения ООО «Гефест Технолоджиз» и ссылки на источник.

Программный комплекс автоматизации ситуационного центра информационной безопасности «Эгида» и товарные знаки, указанные в настоящем документе зарегистрированы ООО «Гефест Технолоджиз» и охраняются законом.

10.2 Содержание документа

Содержание данного документа может изменяться без предварительного уведомления. ООО «Гефест Технолоджиз» не несет ответственности за неточности и/или ошибки, допущенные в данном документе, и возможный ущерб, связанный с этим.