



Т Р А Н С С Е Т Ь

**АКЦИОНЕРНОЕ ОБЩЕСТВО «ТРАНССЕТЬ»
(АО «Т р а н с с е т ь»)**

**ПРОГРАММА ДЛЯ ЭВМ «ПРОГРАММНЫЙ КОМПЛЕКС
АВТОМАТИЧЕСКОЙ ФИЛЬТРАЦИИ, АНАЛИЗА СОБЫТИЙ И
ФОРМИРОВАНИЯ ИНЦИДЕНТОВ»**

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Листов 49

АННОТАЦИЯ

Данное руководство разработано для пользователей Программы для ЭВМ «Программный комплекс автоматической фильтрации, анализа событий и формирования инцидентов» (далее – Программный комплекс анализа событий).

Основная цель настоящего документа заключается в обеспечении пользователя необходимой информацией для самостоятельной работы с Программным комплексом анализа событий, выполняющего автоматизацию процессов фильтрации дублирующей и незначимой информации, корреляции связанных событий и передачи управляющих команд в производственную систему для формирования листов регистрации инцидентов (далее – ЛР И) для их учета в рабочих процессах.

Правообладатель вправе вносить изменения в настоящий документ.

СОДЕРЖАНИЕ

1	Общие сведения	5
1.1	Основные сведения о системе	5
1.2	Область применения	5
1.3	Краткое описание возможностей	5
1.4	Уровень подготовки пользователей	6
1.5	Перечень эксплуатационной документации	7
1.6	Служба технической поддержки	7
2	Назначение и условия применения	8
2.1	Назначение системы	8
2.2	Условия применения системы	8
3	Подготовка к работе	10
3.1	Состав и содержание дистрибутивного носителя данных	10
3.2	Порядок загрузки данных и программ	10
3.3	Порядок проверки работоспособности системы	11
3.4	Порядок доступа к системе	11
4	Описание операций	12
4.1	Выполняемые функции и задачи	12
4.2	Описание интерфейса	13
4.2.1	Интерфейсные формы	15
4.2.2	Общий инструментарий	17
4.2.2.1	Сортировка записей в реестровом представлении	18
4.2.2.2	Поиск записей в реестровом представлении	19
4.2.2.3	Фильтрация данных по количеству отображаемых строк в реестровом представлении	20
4.2.2.4	Выгрузка данных в файл формата «xlsx» / «csv»	20
4.2.2.5	Переход в полноэкранный режим	21
4.2.2.6	Просмотр учетной карточки	22
4.2.2.7	Создание учетной карточки	22
4.2.2.8	Редактирование учетной карточки	23
4.2.2.9	Удаление учетной карточки	25
4.2.2.10	Элементы управления, используемые в системе	25
4.3	Описание операций пользователя	26

4.3.1	Управление коррелятором событий	26
4.3.1.1	Реестр правил коррелятора.....	28
4.3.1.2	Учетная карточка правила коррелятора	32
4.3.2	Настройка правил коррелятора событий	39
4.3.2.1	Настройка правила объединения событий	39
4.3.2.2	Настройка правила объединения часто повторяющихся событий 41	
4.3.2.3	Настройка правила фильтрации событий.....	42
4.3.2.4	Настройка правила автоматического создания ЛР И	42
5	Аварийные ситуации	44
6	Рекомендации по освоению	45
	Обозначения и сокращения	46
	Приложение 1 Порядок применения специализированных имитационных компонентов для демонстрации сквозного бизнес-процесса обработки событий и формирования инцидентов.....	47

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Основные сведения о системе

Полное наименование системы: Программа для ЭВМ «Программный комплекс автоматической фильтрации, анализа событий и формирования инцидентов».

Условное наименование системы: Программный комплекс анализа событий.

Разработчик: Акционерное общество «Транссеть».

Почтовый адрес: г. Нижний Новгород, 603002, ул. Литвинова, дом 74, корп. 30, этаж 5, офис 55.

Телефон: +7 (831) 272-88-88.

Адрес в Интернете: <https://transset.ru/>.

1.2 Область применения

Программа для ЭВМ «Программный комплекс автоматической фильтрации, анализа событий и формирования инцидентов» (далее – Программный комплекс анализа событий) – это система интеллектуальной обработки событийных потоков. Программный комплекс анализа событий используется для обеспечения непрерывности работы, оперативного выявления сбоев и координации действий инженерно-технического персонала.

Программный комплекс анализа событий позволяет применять гибкие правила анализа для выявления первопричин сбоев и передавать управляющие команды в производственную систему для формирования листов регистрации инцидентов (далее – ЛР И) и их учета в рабочих процессах, а также для отображения результатов обработки событий в оперативном режиме диспетчера.

1.3 Краткое описание возможностей

С помощью Программного комплекса анализа событий обеспечивается:

- управление реестром правил фильтрации, объединения и формирования ЛР И через визуальный конструктор;

- автоматическое объединение часто повторяющихся событий с одинаковыми параметрами в структуру «родитель-дочерние» с определением первопричины;
- объединение дочерних событий в рамках родительского события (первопричины);
- фильтрация незначимых событий в реальном времени с исключением их из рабочей области диспетчера;
- передача управляющих команд в производственную систему для автоматической генерации ЛР И с предварительным заполнением параметров учетной карточки и установлением связи между сформированными ЛР И и исходными событиями;
- ведение детальной истории изменений правил и обработки событий с возможностью аудита;
- отказоустойчивая обработка очереди событий с возможностью передачи необработанных данных в ручной режим при неуспешной идентификации.

1.4 Уровень подготовки пользователей

В автоматизированной деятельности Программного комплекса анализа событий принимают участие следующие пользователи, изучившие требования эксплуатационной документации:

- авторизированный пользователь – пользователь, успешно прошедший процедуру авторизации и идентифицированный системой;
- администратор, отвечающий за бесперебойное функционирование системы и управляющий программно-аппаратным комплексом, на котором установлена система.

Пользователь должен иметь:

- знание соответствующей предметной области;
- базовую квалификацию по работе с операционными системами, а также навыки работы с комплектом программного и аппаратного обеспечения, приведенном в п. 2.2;
- учетную запись с назначенными соответствующими правами доступа.

Требования к квалификации администратора:

- опыт сопровождения и администрирования ЛВС, знание протоколов сетевого и транспортного уровня;

- опыт решения вопросов инсталляции, общесистемного сопровождения и администрирования;
- опыт работы с системами виртуализации и контейнеризации;
- опыт администрирования систем и Web-приложений, разработанных на C#.

1.5 Перечень эксплуатационной документации

Для самостоятельной работы с Программным комплексом анализа событий пользователям необходимо ознакомиться с Руководством пользователя (настоящий документ) и Руководством администратора.

1.6 Служба технической поддержки

Фактический адрес размещения инфраструктуры службы поддержки: филиал АО «Транссеть» в г. Нижнем Новгороде, 603002, ул. Литвинова, дом 74, корп. 30, этаж 5, офис 55.

Связаться со специалистами службы технической поддержки можно одним из следующих способов:

- Телефон: +7 (831) 272-88-88.
- E-mail: inform@transset.ru.

При обращении в службу технической поддержки необходимо представить следующую информацию:

- наименование системы и вариант её исполнения;
- чёткое описание возникшей проблемы;
- наименование и версию используемого программного обеспечения;
- тип компьютера и сведения о его конфигурации;
- название используемой операционной системы и номер её версии.

2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

2.1 Назначение системы

Программный комплекс анализа событий предназначен для автоматизированной обработки событийных потоков. Программный комплекс анализа событий используется для обеспечения непрерывности работы, оперативного выявления сбоев и координации действий инженерно-технического персонала.

Основными функциями Программного комплекса анализа событий являются:

- фильтрация шумовых сигналов и незначимых сообщений;
- корреляция и анализ: выявление причинно-следственных связей, группировка связанных событий, определение первопричин отказов;
- передача управляющих команд в производственную систему для формирования ЛР И для их учета в рабочих процессах;
- отображение статистической информации о текущей ситуации и истории обработки событий.

2.2 Условия применения системы

Для успешной работы с Программным комплексом анализа событий необходимо выполнение следующих требований:

- рабочая станция пользователя должна иметь доступ к серверу системы по протоколу межсетевого взаимодействия – ТСР/ІР;
- пользователь рабочей станции должен быть зарегистрирован в качестве пользователя Программного комплекса анализа событий с соответствующими его роли полномочиями;
- на рабочей станции пользователя должна быть установлена ОС, имеющая графический интерфейс;
- на рабочей станции пользователя должен быть установлен Microsoft Office 2010 или выше;
- на рабочей станции пользователя должен быть установлен Yandex браузер не ниже 20 версии.

Минимальные требования к оборудованию и программному обеспечению Программного комплекса анализа событий указаны в Руководстве администратора.

Программный комплекс анализа событий предназначен для эксплуатации в составе распределенной инфраструктуры Заказчика, представляющей собой

согласованно функционирующий контур, объединяющий системы технического мониторинга, аналитические системы управления инцидентами и т.п. В рамках данного контура реализуется непрерывный обмен данными от источников событий до систем принятия управленческих решений, что обеспечивает целостность жизненного цикла события от момента выявления до закрытия.

Для обеспечения корректного функционирования Программного комплекса анализа событий и выполнения заявленных функций необходимо обеспечить взаимодействие с производственной системой Заказчика в части:

- получения событийных потоков для последующего их анализа и применения настроенных правил коррелятора;
- передачи управляющих команд на автоматическое формирование ЛР И, а также на отображение результатов обработки событий в оперативном режиме диспетчера.

В целях верификации сквозных бизнес-процессов и проверки Программного комплекса анализа событий в изолированных (тестовых или демонстрационных) средах допускается применение специализированных имитационных компонентов, в частности: генераторов синтетических событий, эмуляторов модулей управления инцидентами и систем оперативного отображения данных. Описание порядка применения специализированных имитационных компонентов для демонстрации сквозного бизнес-процесса обработки событий и формирования инцидентов приведено в приложении (Приложение 1).

Указанные специализированные имитационные компоненты носят вспомогательный характер, не входят в состав поставляемого Программного комплекса и не оказывают влияния на его базовую функциональность в эксплуатационных условиях. Порядок их конфигурирования, развёртывания и эксплуатации выходит за рамки настоящего Руководства пользователя и регламентируется в соответствующих технических спецификациях или методических указаниях, поставляемых отдельно.

3 ПОДГОТОВКА К РАБОТЕ

3.1 Состав и содержание дистрибутивного носителя данных

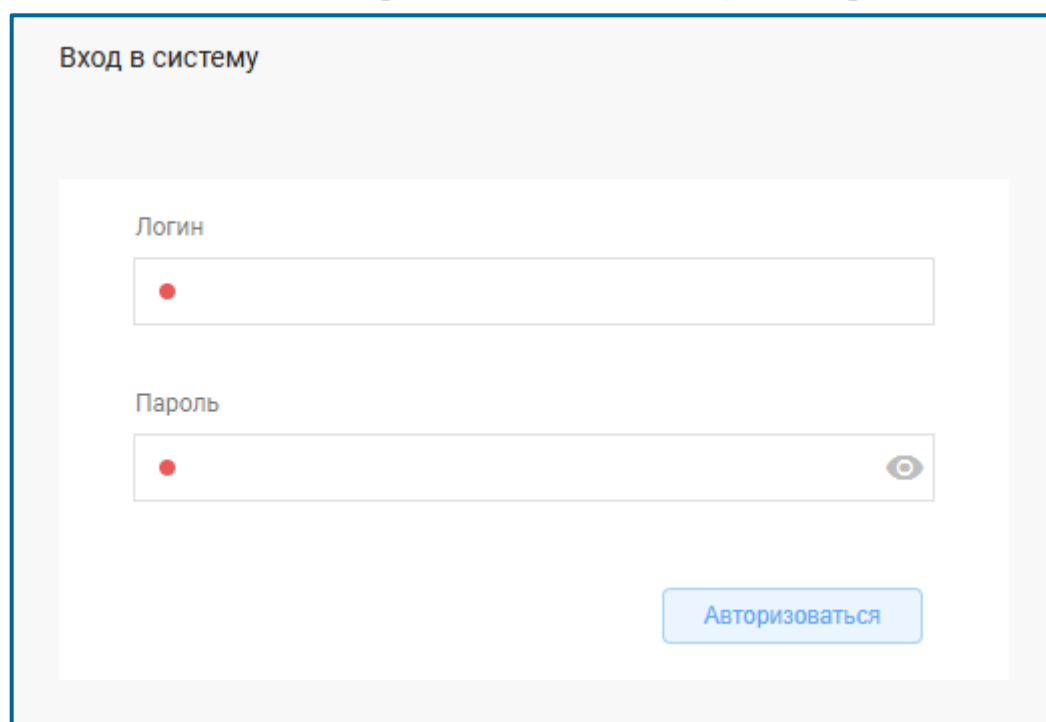
Описание состава и содержания дистрибутивного носителя данных указано в Руководстве администратора.

3.2 Порядок загрузки данных и программ

Порядок установки и настройки Программного комплекса анализа событий на узлах Заказчика, предполагаемых к использованию, определяется условиями договора. В рамках установки и настройки Программного комплекса должны быть выполнены работы по передаче учетных данных пользователей и их прав доступа из производственной системы в Программный комплекс анализа событий. Этапы работ и ответственные исполнители определяется условиями договора.

Взаимодействие пользователя с Программным комплексом анализа событий осуществляется посредством веб-интерфейса.

Для начала работы в Программном комплексе анализа событий необходимо запустить интернет-браузер и в адресной строке ввести адрес сервера. Далее откроется окно авторизации (Рисунок 3.1), в котором необходимо ввести учётные данные пользователя (логин и пароль) и нажать кнопку «Авторизоваться».



Вход в систему

Логин

Пароль

Авторизоваться

Рисунок 3.1 – Окно авторизации Программного комплекса анализа событий

После успешной авторизации и аутентификации пользователя отобразится Главная страница Программного комплекса анализа событий (Рисунок 3.2).

При отсутствии доступа пользователя к странице на экране будет выведено сообщение У вас нет прав для просмотра данной страницы.

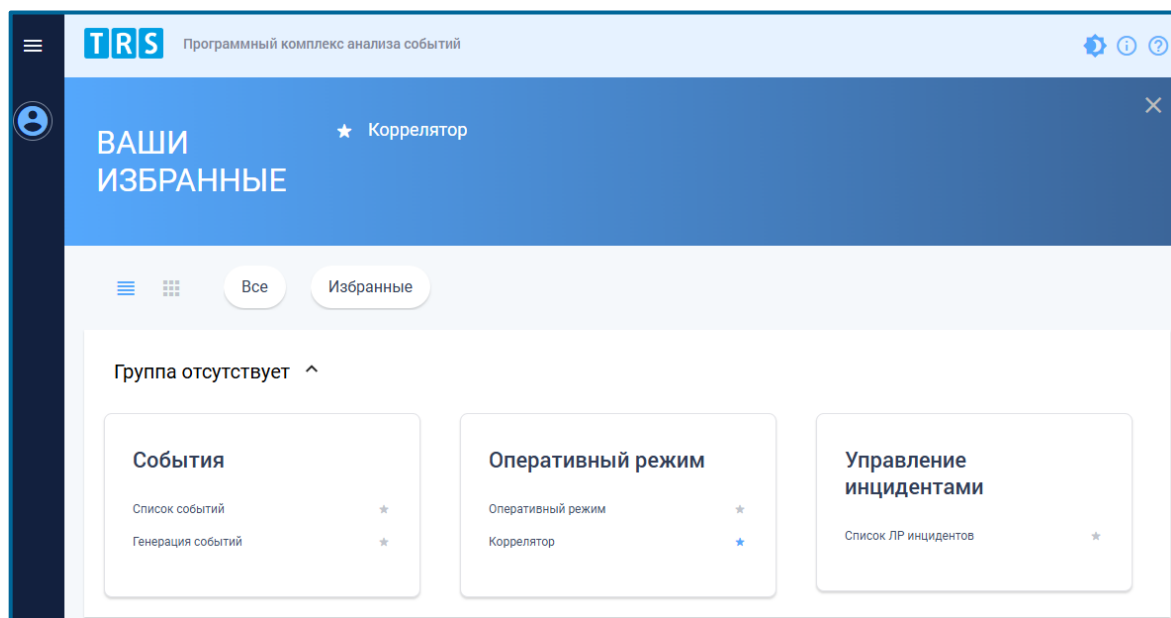


Рисунок 3.2 – Главная страница Программного комплекса анализа событий

3.3 Порядок проверки работоспособности системы

Программный комплекс анализа событий работоспособен, если в результате действий пользователя, изложенных в п. 3.2 и 4, на экране монитора пользователю не выданы сообщения о сбое в работе.

В случае если Программный комплекс анализа событий не запускается (на странице сервера пользователь видит уведомление об ошибке), следует обратиться в службу технической поддержки (п. 1.6).

3.4 Порядок доступа к системе

Доступ к работе с Программным комплексом анализа событий производится под учетными записями, созданными администратором производственной системы. В Программном комплексе анализа событий авторизация возможна только под учетными записями пользователей, ведение которых осуществляется в производственной системе.

4 ОПИСАНИЕ ОПЕРАЦИЙ

4.1 Выполняемые функции и задачи

Программный комплекс анализа событий выполняет следующие функции и задачи:

- управление правилами обработки событий, включая:
 - ведение реестра правил, содержащего правила объединения повторяющихся событий, фильтрации шума, корреляции (объединения родительских и дочерних событий) и создания ЛР И;
 - создание и редактирование правил с помощью визуального конструктора с заданием условий по параметрам событий;
 - определение периода выполнения, а также порядка (приоритета) их запуска для обработки событий;
 - передачу управляющих команд в производственную систему для автоматического заполнения полей УК ЛР И при срабатывании правил;
 - активацию и деактивацию правил в рабочем режиме;
 - ведение истории изменений правил с фиксацией действий пользователей.
- автоматическая обработка очереди событий, включая:
 - автоматическое формирование очереди обработки событий;
 - идентификацию событий из очереди в соответствии с активными правилами в порядке их приоритета;
 - автоматическое принятие решений по обработке (объединение, фильтрация или создание ЛР И) при успешной идентификации;
 - передачу необработанных событий в оперативный режим для ручной обработки диспетчером при неуспешной идентификации;
 - логирование процесса принятия решений по каждому событию.
- применение правил фильтрации и анализа событий, включая:
 - автоматическое исключение событий, попадающих под правила фильтрации (незначимые события);
 - автоматическое объединение часто повторяющихся событий с одинаковыми параметрами в структуру «родитель-дочерние»;
 - объединение дочерних событий в рамках родительского события

(первопричины).

- применение правил формирования ЛР И, включая:
 - передача управляющих команд в производственную систему для автоматического:
 - создания ЛР И при срабатывании соответствующих правил;
 - заполнения полей учетной карточки (далее – УК) ЛР И на основе параметров исходных событий;
 - установления связи между сформированным ЛР И и событиями, послужившими основанием для его создания.
- визуализация данных, включая:
 - ведение истории обработки событий для оперативного реагирования и аудита.
- интеграция и обмен данными, включая:
 - прием событийных потоков;
 - передача управляющих команд в производственную систему для автоматического:
 - отображения событий (в том числе родительских со ссылками на подчиненные) в рабочей области диспетчера после применения правил объединения и объединения часто повторяющихся событий;
 - скрывание событий из рабочей области диспетчера после применения правила фильтрации.
 - поддержку работы в среде отечественных операционных систем и СУБД, включённых в реестр Минцифры.

Описание операций, осуществляемых пользователем в Программном комплексе анализа событий и необходимых для выполнения вышеуказанных функций и задач, приведено в соответствующих пунктах настоящего руководства, а также в Руководстве администратора.

4.2 Описание интерфейса

Интерфейс пользователя реализован с использованием технологии построения Web-ориентированного интерфейса, он позволяет применить для работы с данными стандартные программы просмотра Web-страниц (интернет-браузеры), обеспечить доступ к Программному комплексу анализа событий с любой рабочей станции, подключенной к сети передачи данных.

Web-интерфейс реализован по технологии «тонкого клиента», которая обладает следующими преимуществами:

- централизация основного объема вычислений и операций над объектами на стороне сервера;
- при обновлении Программного комплекса анализа событий не требуется переустанавливать ПО на рабочих станциях пользователей;
- соответствие самым высоким требованиям обеспечения целостности данных, доступности и безопасности.

Интерфейс Программного комплекса анализа событий разделен на 3 фрейма, предназначенных для одновременного отображения экранных форм различного функционального назначения.

Схема взаимодействия фреймов в Программном комплексе анализа событий приведена на рисунке (Рисунок 4.1).

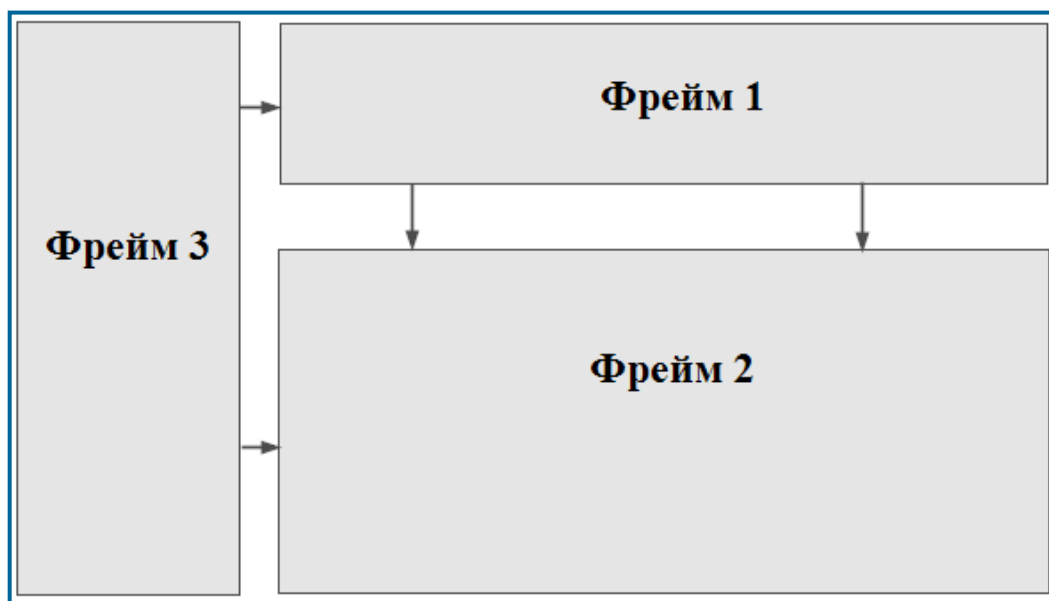


Рисунок 4.1– Схема взаимодействия фреймов

Внешний вид фреймов Программного комплекса анализа событий представлен на рисунке (Рисунок 4.2).

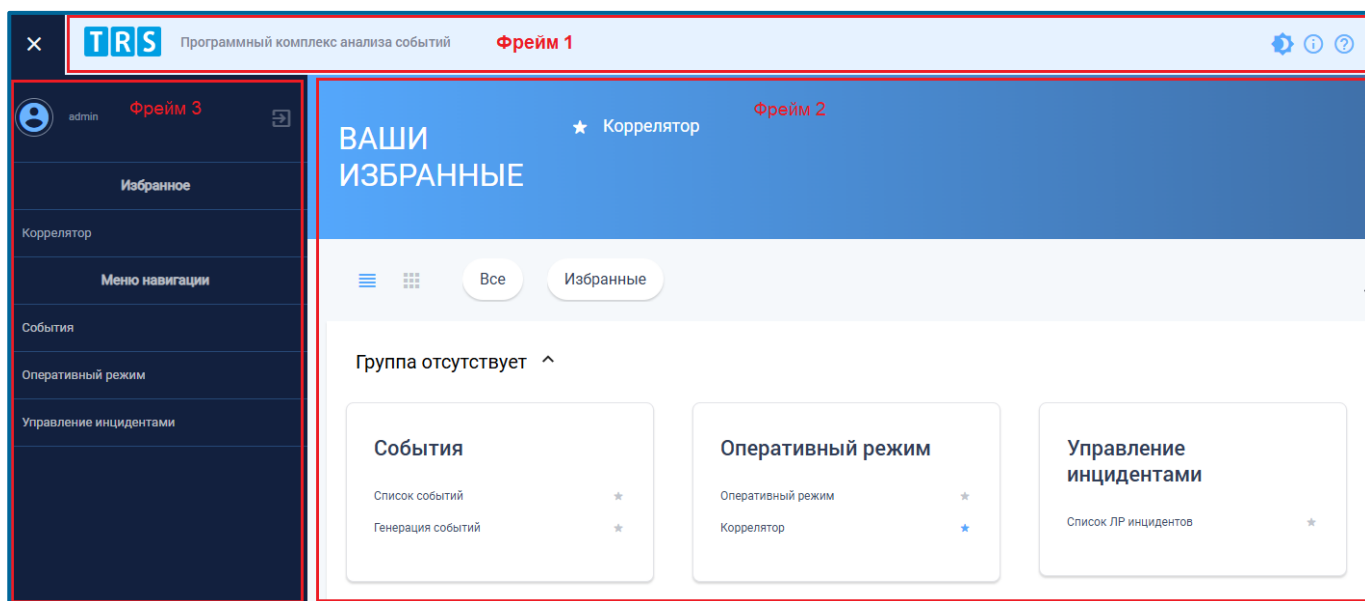


Рисунок 4.2 – Интерфейс Программного комплекса анализа событий

4.2.1 Интерфейсные формы

Фрейм 1 содержит:

- логотип и название программного комплекса (по нажатию на логотип осуществляется переход к главной странице);
- пиктограмму смены темы интерфейса  (возможные варианты – светлая и темная тема);
- пиктограмму  для перехода к просмотру вкладок: «Компоненты TRS», «OpenSource компоненты».

Внешний вид фрейма 1 приведен на рисунке (Рисунок 4.3).

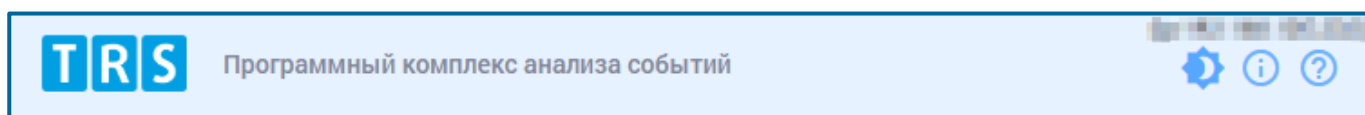


Рисунок 4.3 – Фрейм 1. Внешний вид

Фрейм 2 является областью отображения данных, соответствующих параметрам настройки фильтрации в фрейме 3.

Фрейм 2 состоит из следующих компонентов (Рисунок 4.4):

- реестровое представление данных: представлено в виде таблицы с полями (реестра) и предназначено для хранения УК;
- УК, переход в которую осуществляется из реестра.

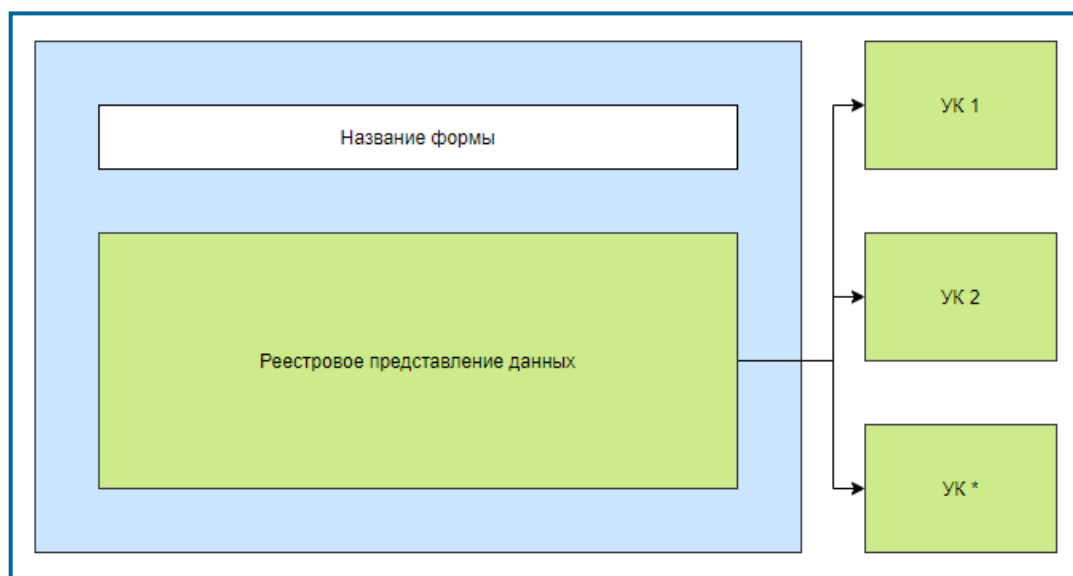


Рисунок 4.4 – Фрейм 2

Фрейм 3 является панелью навигации, с помощью которой происходит перемещение между пунктами меню Программного комплекса анализа событий и представляет собой выдвигающееся боковое меню с двумя уровнями вложенности (Рисунок 4.5):

- первый уровень содержит наименование разделов (если данный уровень имеет связанный с ним второй уровень вложенности, то при нажатии на наименование первого уровня откроется расширяющийся список с дочерним вторым уровнем).
- второй уровень включает в себя ссылки для перехода на определенную страницу раздела.

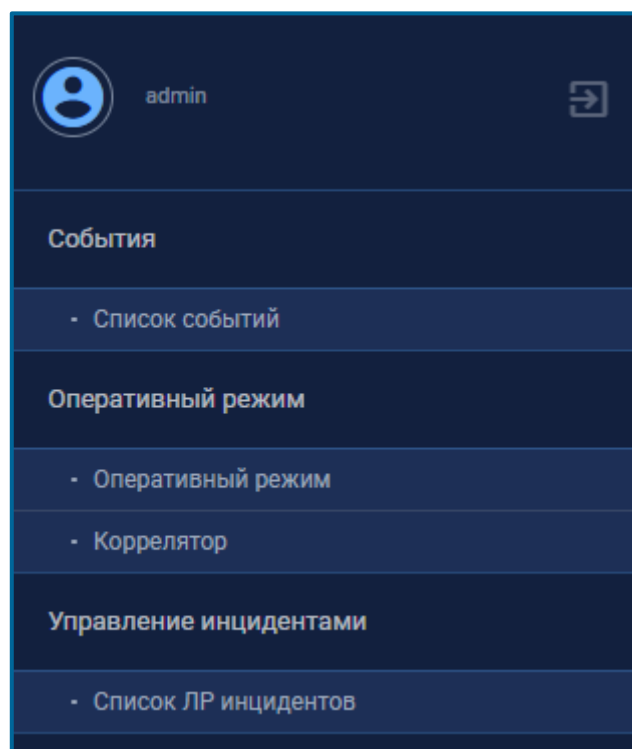


Рисунок 4.5 – Фрейм 3. Внешний вид

По кнопкам и пиктограмм в Фрейме 3 доступны операции, описанные в таблице (Таблица 4.1).

Таблица 4.1 – Пиктограммы Фрейма 3

Пиктограмма	Описание
	Переход в профиль/ личный кабинет пользователя Программного комплекса анализа событий.
	Сворачивание/ разворачивание Фрейма 3.
	Выход из Программного комплекса анализа событий.

4.2.2 Общий инструментарий

В данном пункте приводится описание инструментов, используемых в интерфейсных формах Программного комплекса анализа событий:

- сортировки записей в реестровом представлении (п. 4.2.2.1);
- поиска записей в реестровом представлении (п. 4.2.2.2);
- фильтрации данных по количеству отображаемых строк в реестровом представлении (п. 4.2.2.3);
- выгрузки данных в файл формата «xlsx» / «csv» (п. 4.2.2.4);

- переход в полноэкранный режим (п. 4.2.2.5);
- просмотра учетной карточки (п. 4.2.2.6);
- создания учетной карточки (п. 4.2.2.7);
- редактирования учетной карточки (п. 4.2.2.8);
- удаления учетной карточки (п. 4.2.2.9);
- элементов управления - кнопок, используемых в интерфейсе системы (п. 4.2.2.10).

4.2.2.1 Сортировка записей в реестровом представлении

По всем полям реестров предусмотрена сортировка, осуществляемая с помощью пиктограммы , рядом с наименованием поля (Рисунок 4.6). Возможны следующие варианты установки сортировки (переход между ними осуществляется последовательным кликом на пиктограмму):

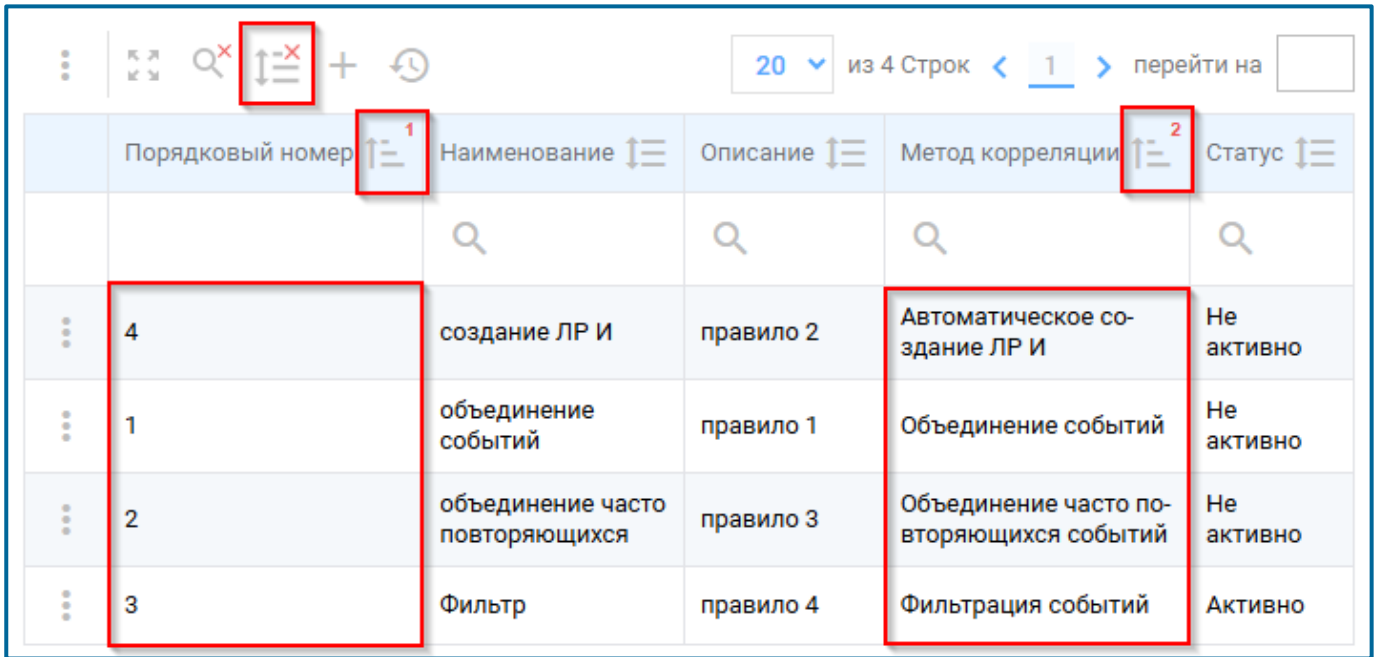
- сортировка в порядке возрастания ;
- сортировка в порядке убывания ;
- сортировка отключена .

Также предусмотрена возможность установки порядка сортировки по нескольким столбцам таблицы реестра.

Для этого необходимо:

- 1) отсортировать значения необходимых столбцов по возрастанию нажатием по пиктограмме  (или всех столбцов по убыванию – ).
- 2) определить порядок сортировки столбцов (первый, второй и т.д.) и нажать в соответствующем порядке по пиктограмме столбца (.

Таким образом, записи в столбцах сортируются в соответствии с указанным в них порядком. Отмена сортировки доступна по нажатию на пиктограмму .



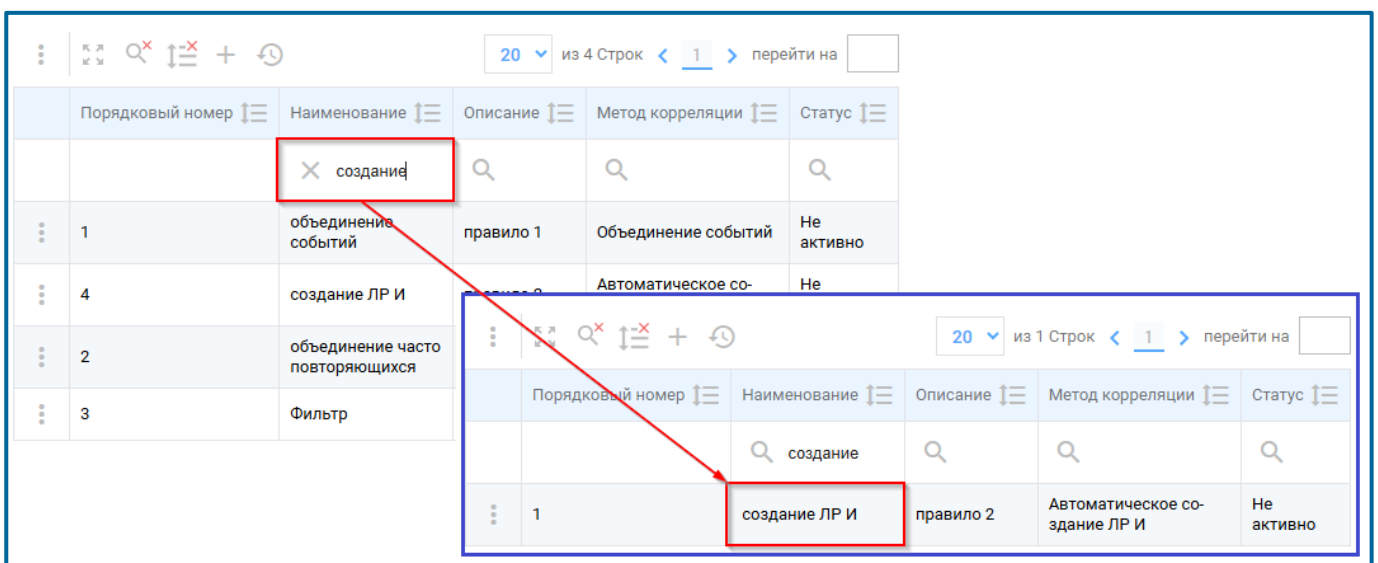
	Порядковый номер	Наименование	Описание	Метод корреляции	Статус
	4	создание ЛР И	правило 2	Автоматическое создание ЛР И	Не активно
	1	объединение событий	правило 1	Объединение событий	Не активно
	2	объединение часто повторяющихся	правило 3	Объединение часто повторяющихся событий	Не активно
	3	Фильтр	правило 4	Фильтрация событий	Активно

Рисунок 4.6 – Сортировка записей в реестровом представлении

4.2.2.2 Поиск записей в реестровом представлении

По всем полям таблицы предусмотрены поиск и фильтрация значений.

Для поиска записей в столбце таблицы необходимо в поле поиска столбца реестра внести значение (Рисунок 4.7) и нажать на пиктограмму  («Искать») или кнопку *Enter* на клавиатуре. Для сброса значений нажать на пиктограмму  («Очистить») или , размещенную над таблицей реестра.



	Порядковый номер	Наименование	Описание	Метод корреляции	Статус
		× создание			
	1	объединение событий	правило 1	Объединение событий	Не активно
	4	создание ЛР И	правило 2	Автоматическое со-	Не
	2	объединение часто повторяющихся			
	3	Фильтр			

	Порядковый номер	Наименование	Описание	Метод корреляции	Статус
		создание			
	1	создание ЛР И	правило 2	Автоматическое создание ЛР И	Не активно

Рисунок 4.7 – Поиск записей в реестровом представлении

4.2.2.3 Фильтрация данных по количеству отображаемых строк в реестровом представлении

В Программном комплексе анализа событий реализована фильтрация данных по количеству отображаемых строк. В результате фильтрации возможно отображение следующего количества строк на странице: 10, 20, 40, 60, 100.

Для фильтрации данных необходимо выбрать в выпадающем списке количество отображаемых строк на странице (Рисунок 4.8).

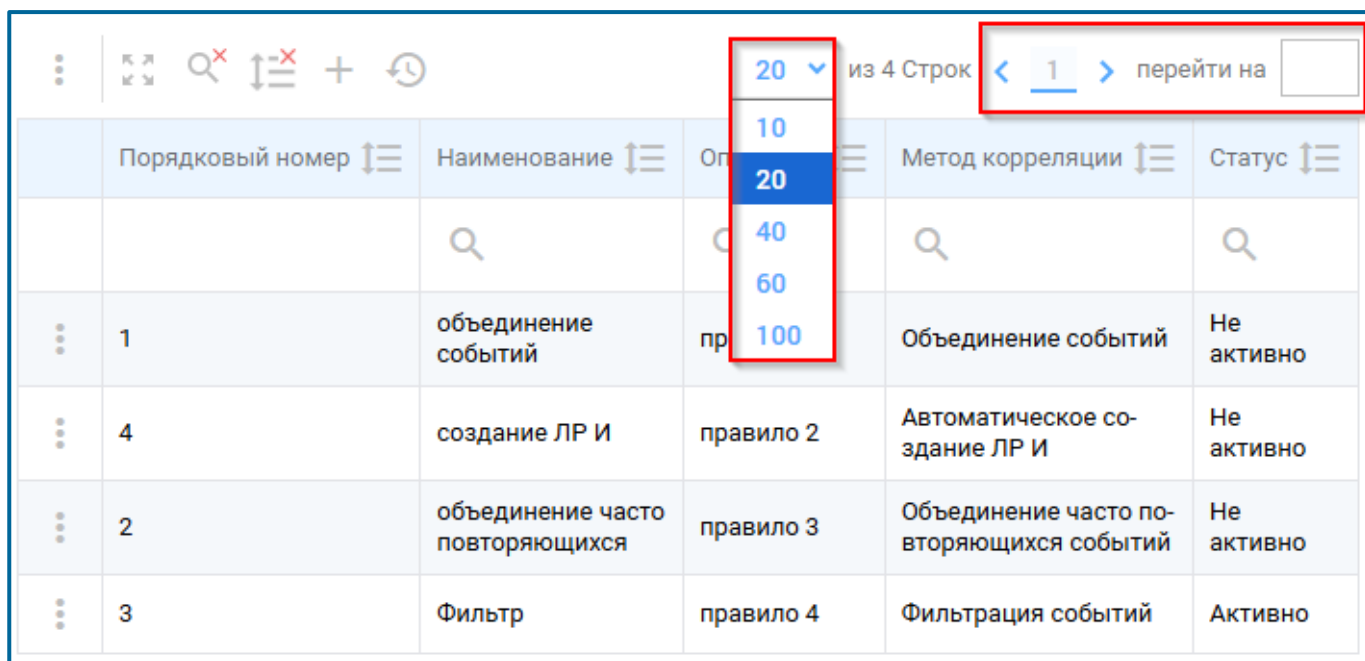


Рисунок 4.8 – Фильтрация по количеству строк в реестровом представлении

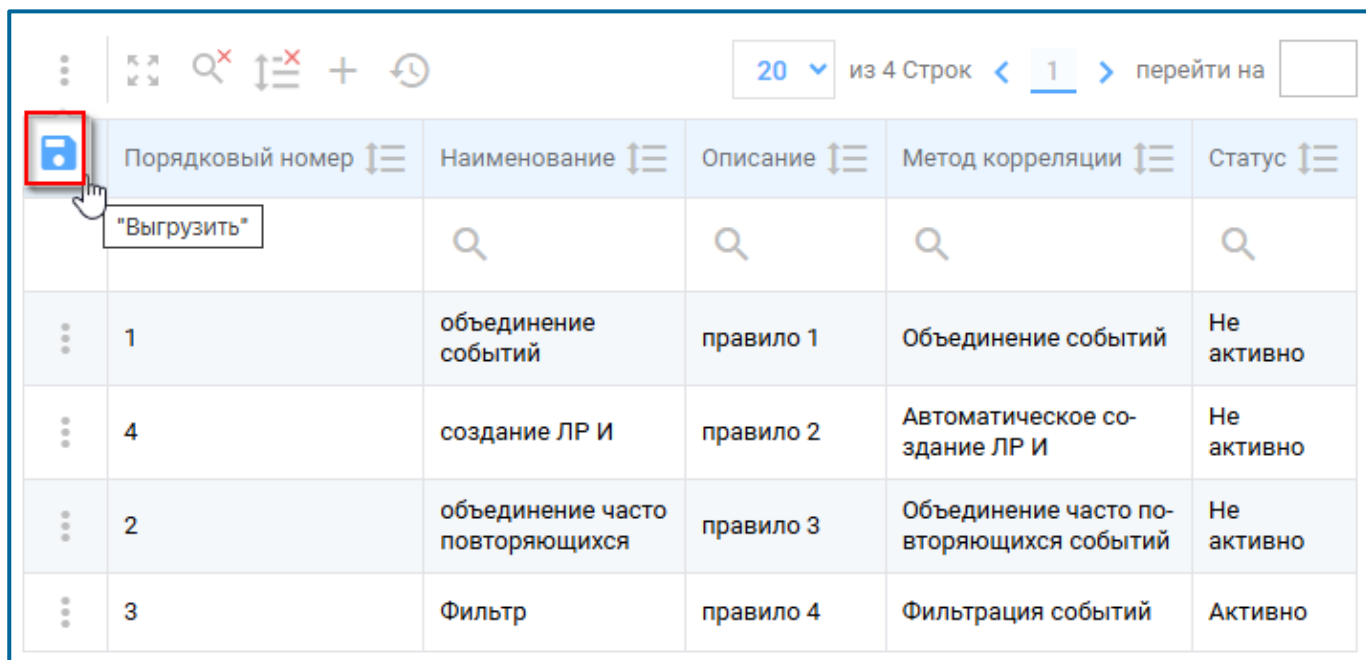
Последовательный переход между страницами осуществляется при помощи пиктограмм («Перейти на страницу назад»)/ («Перейти на страницу вперед») (Рисунок 4.8).

Для перехода к конкретной странице необходимо указать её номер в поле «перейти на» и нажать кнопку *Enter* на клавиатуре (Рисунок 4.8).

4.2.2.4 Выгрузка данных в файл формата «xlsx» / «csv»

У пользователя есть возможность экспортировать реестровое представление в файл формата «xlsx» / «csv». При этом все установленные ранее настройки по сортировке, поиску и фильтрации сохраняются, и информация в выгруженном файле будет представлена с их учётом.

Для этого необходимо нажать на пиктограмму («Выбор из дополнительного меню») над таблицей, затем на («Выгрузить») (Рисунок 4.9).



Порядковый номер	Наименование	Описание	Метод корреляции	Статус
1	объединение событий	правило 1	Объединение событий	Не активно
4	создание ЛР И	правило 2	Автоматическое создание ЛР И	Не активно
2	объединение часто повторяющихся	правило 3	Объединение часто повторяющихся событий	Не активно
3	Фильтр	правило 4	Фильтрация событий	Активно

Рисунок 4.9 – Выгрузка данных в файл формата «xlsx» / «csv»

4.2.2.5 Переход в полноэкранный режим

Для удобства пользователя реализована возможность разворачивать страницы интерфейса Программного комплекса анализа событий, содержащие большой объем информации, в полноэкранный режим.

Переход в полноэкранный режим страниц производится по пиктограмме , выход из него – с помощью пиктограммы  (Рисунок 4.10).

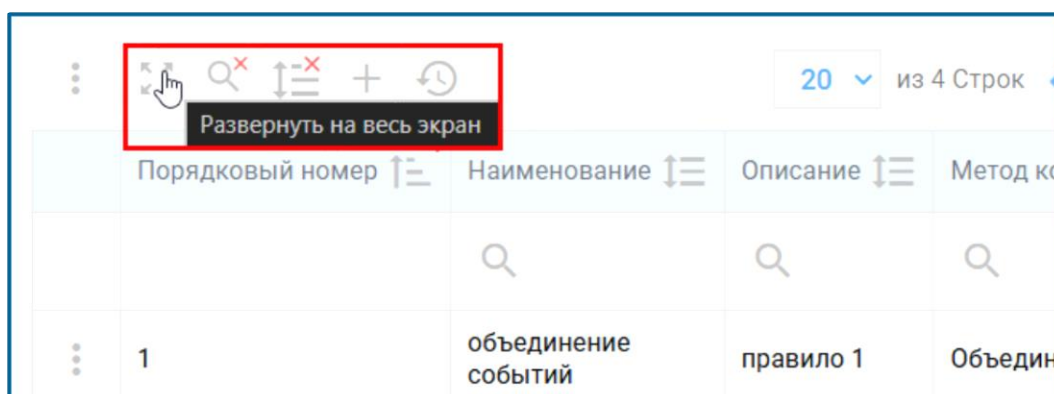


Рисунок 4.10 – Переход в полноэкранный режим

4.2.2.6 Просмотр учетной карточки

Переход к просмотру учетной карточки (УК) осуществляется по нажатию на пиктограмму  («Выбор из дополнительного меню») и при последующем выборе действия «Открыть» в реестре (Рисунок 4.11).

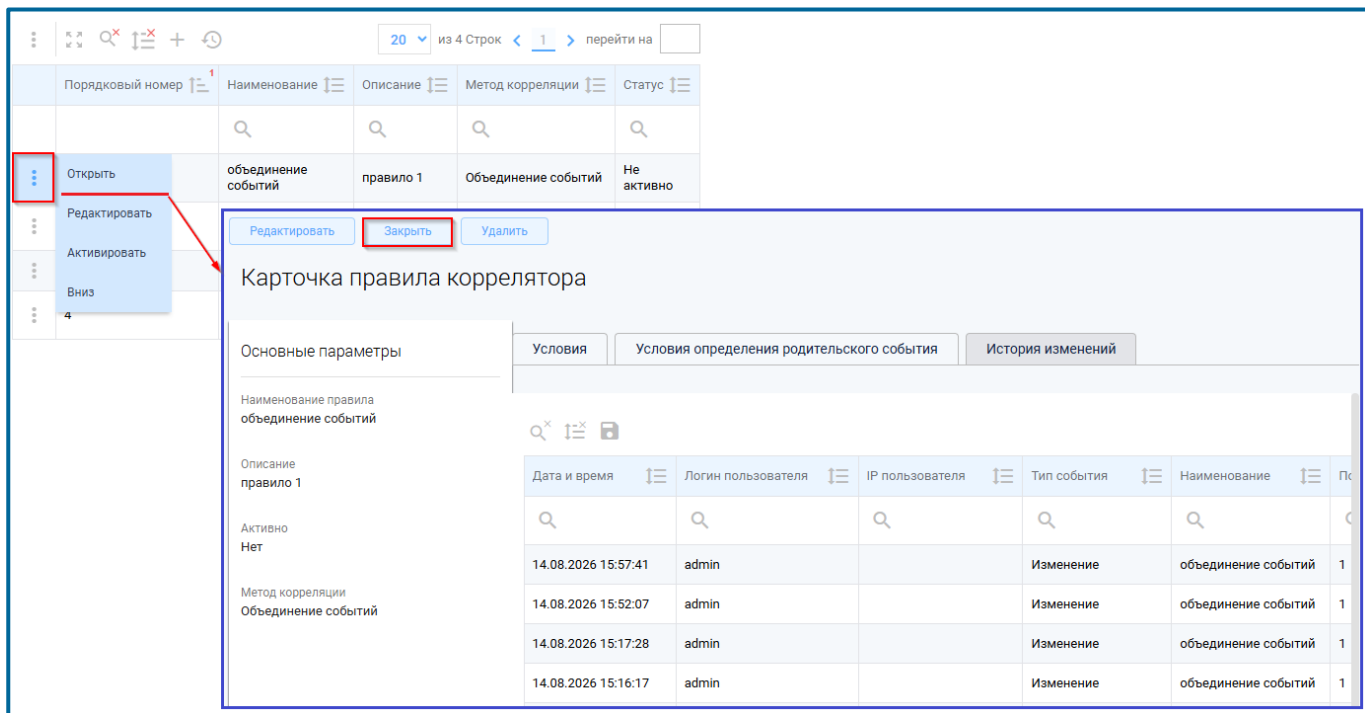


Рисунок 4.11 – Переход к просмотру УК

Для возврата в предыдущее окно нажать на кнопку «Закреть».

4.2.2.7 Создание учетной карточки

Для создания УК необходимо нажать на пиктограмму  («Добавить») в реестровом представлении над таблицей. В открывшейся форме внести данные и подтвердить их, нажав на кнопку «Создать». Для возврата в предыдущее окно нажать на кнопку «Отмена» (Рисунок 4.12).

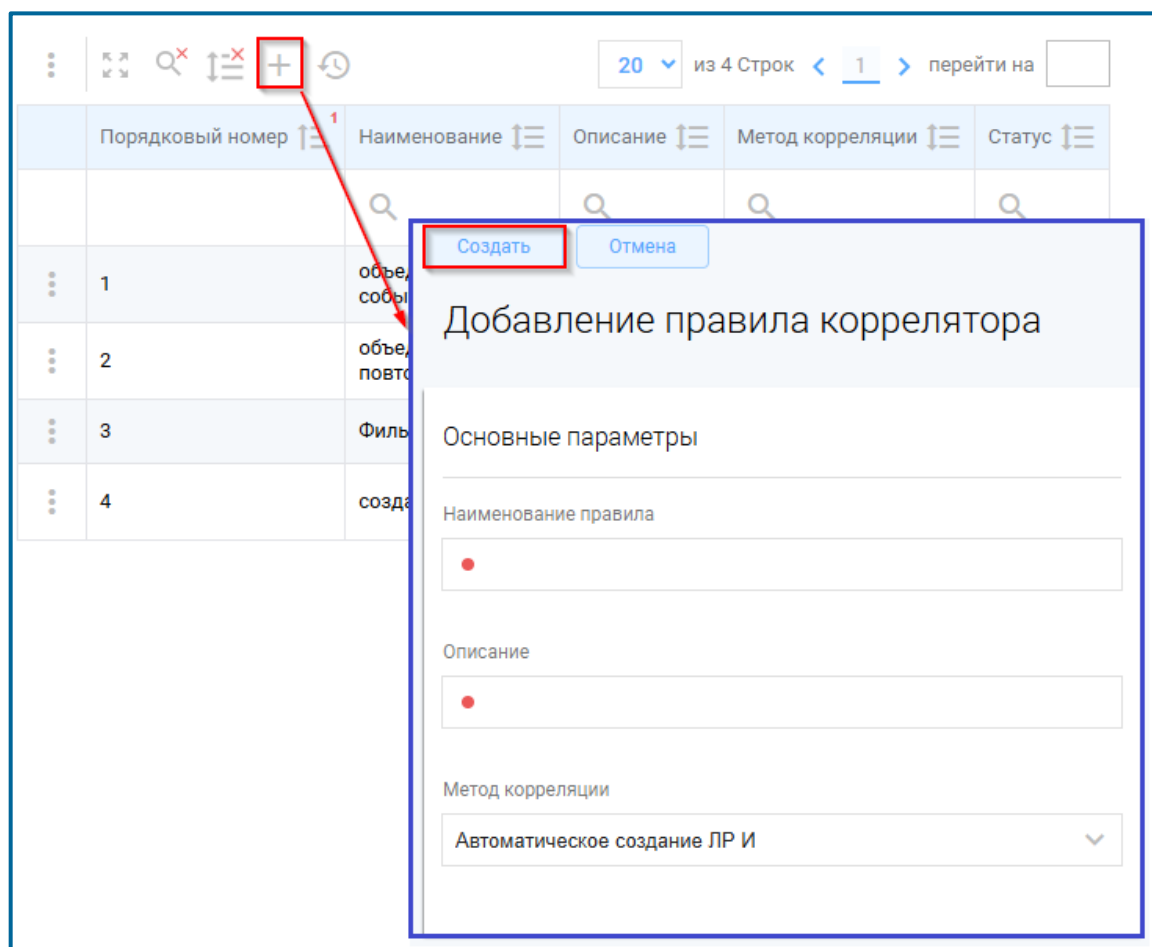


Рисунок 4.12 – Создание УК

Примечание – Обязательные для заполнения поля помечены . Без заполнения хотя бы одного из этих полей сохранение УК невозможно.

После сохранения УК будет доступна в реестровом представлении.

4.2.2.8 Редактирование учетной карточки

Переход к редактированию УК возможен следующими способами:

- из реестра по нажатию на пиктограмму  («Выбор из дополнительного меню») и последующем выборе в выпадающем меню пункта «Редактировать» (Рисунок 4.13);

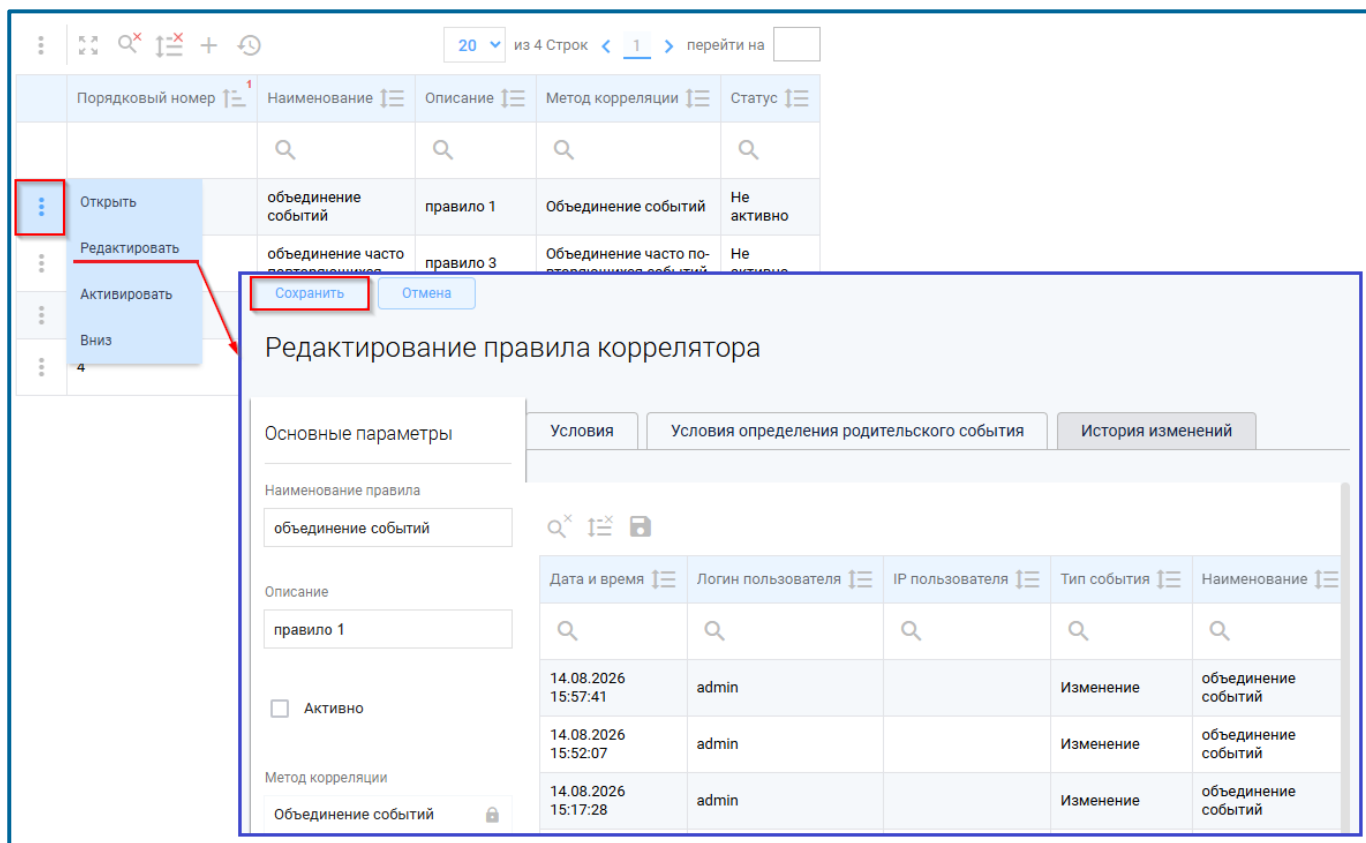


Рисунок 4.13 – Переход к редактированию из реестра (меню)

- из режима просмотра УК по нажатию на кнопку «Редактировать» (Рисунок 4.14).

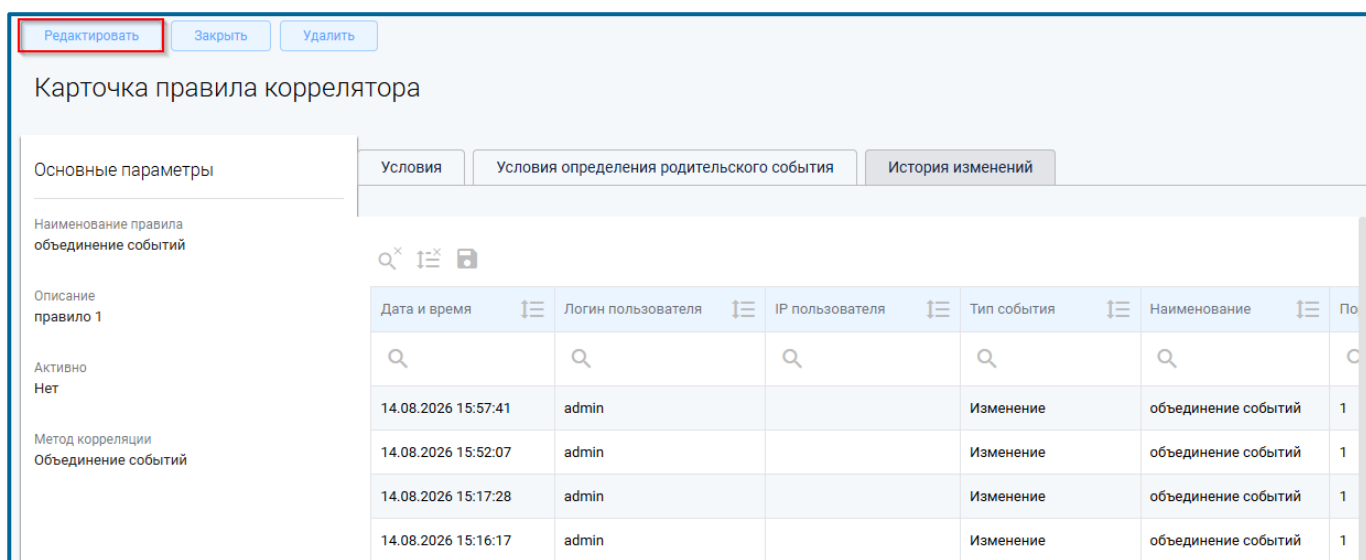


Рисунок 4.14 – Переход к редактированию из режима просмотра УК

Для редактирования необходимо выбрать УК и перейти к редактированию: в открывшемся окне внести необходимые изменения и подтвердить их нажав на кнопку «Сохранить». Для возврата в предыдущее окно нажать на кнопку «Отмена».

4.2.2.9 Удаление учетной карточки

Переход к удалению УК осуществляется из режима просмотра УК по нажатию на кнопку «Удалить» (Рисунок 4.15).

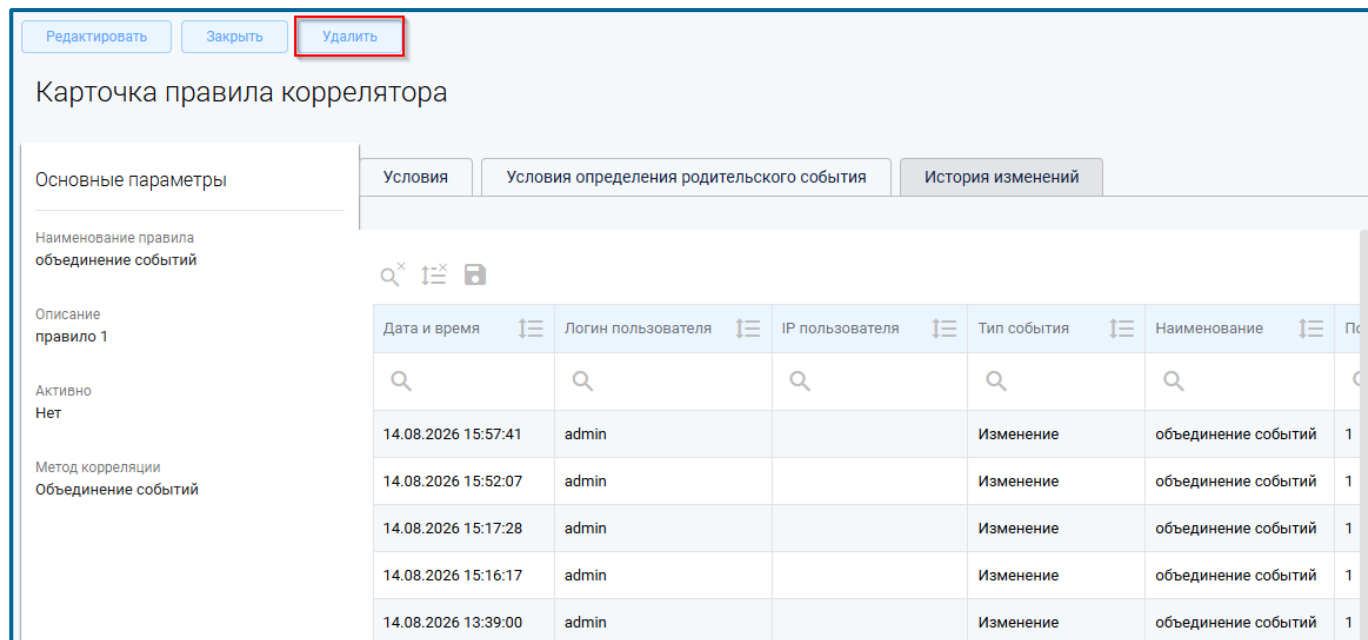


Рисунок 4.15 – Переход к удалению из режима просмотра УК

Для удаления выбрать УК и перейти к удалению.

Требуется дополнительное подтверждение для удаления УК: будет выведено сообщение: «Удалить карточку?», в котором необходимо выбрать «Да» для удаления карточки или «Нет» для отмены удаления.

4.2.2.10 Элементы управления, используемые в системе

Элементы управления, используемые в Программном комплексе анализа событий, представлены в таблице (Таблица 4.2).

Таблица 4.2 – Элементы управления

Графический объект	Описание
☒ / ☐	Выбор значения с помощью чек-бокса (Да/ Нет)
	Развернуть на весь экран
	Выйти из полноэкранного режима
	Выбрать значение из справочника

Графический объект	Описание
	Выбрать из календаря дату и/или время
	Вызвать дополнительное меню
	Выйти из системы
	Заккрыть окно/ Очистить фильтр, поле
	Обязательное поле
	Перейти на уровень (страницу) влево/ Перейти на уровень (страницу)вправо
	Раскрыть боковое меню/ Скрыть боковое меню
	Редактировать объект
	Создать (добавить) объект
	Переместить на уровень вверх/ вниз.
	Переход к просмотру истории изменений
	Сортировать значения в таблице (по возрастанию/ убыванию)
	Отменить условия сортировки
	Фильтрация по столбцам реестрового представления
	Сбросить все фильтры

4.3 Описание операций пользователя

4.3.1 Управление коррелятором событий

Коррелятор – это рабочее наименование раздела пользовательского интерфейса, реализующего функциональность Программного комплекса автоматической фильтрации, анализа событий и формирования инцидентов.

Коррелятор – механизм автоматической обработки событийных потоков по установленным пользователем правилам и условиям.

Для обработки входящих сообщений применяется следующий алгоритм:

- входящие сообщения от систем мониторинга инфраструктуры поступают в производственную систему Заказчика и регистрируются в ней в стандартизированном формате;

- из производственной системы Заказчика данные о событиях поступают в Программный комплекс анализа событий:
 - данные о событиях передаются в очередь обработки коррелятора событий;
 - коррелятор последовательно проверяет событие на соответствие условиям активных правил (в порядке их расположения в реестре);
 - при совпадении выполняется действие, указанное в правиле;
 - если событие не удовлетворяет ни одному из активных правил, оно передаётся в производственную систему для ручной обработки диспетчером.

Правила создаются пользователем с помощью конструктора правил.

В результате работы коррелятора выполняется:

- автоматическое объединение/фильтрация событий;
- передача управляющих команд в производственную систему для автоматического:
 - отображения событий (в том числе родительских со ссылками на подчиненные) в рабочей области диспетчера после применения правил объединения и объединения часто повторяющихся событий;
 - скрывания событий из рабочей области диспетчера после применения правила фильтрации;
 - создания ЛР И из события.

Коррелятор содержит следующий набор функциональностей:

- управление правилами автоматической фильтрации, анализа событий и формирования ЛР И;
- автоматическая обработка очереди событий в соответствии с настроенными правилами;
- применение правил автоматической фильтрации и корреляции событий;
- применение правил автоматического формирования ЛР И.

Переход к разделу «Коррелятор» доступен с главной страницы Программного комплекса анализа событий в пункте меню «Оперативный режим» (Рисунок 4.16), а также через панель навигации во Фрейме 3.

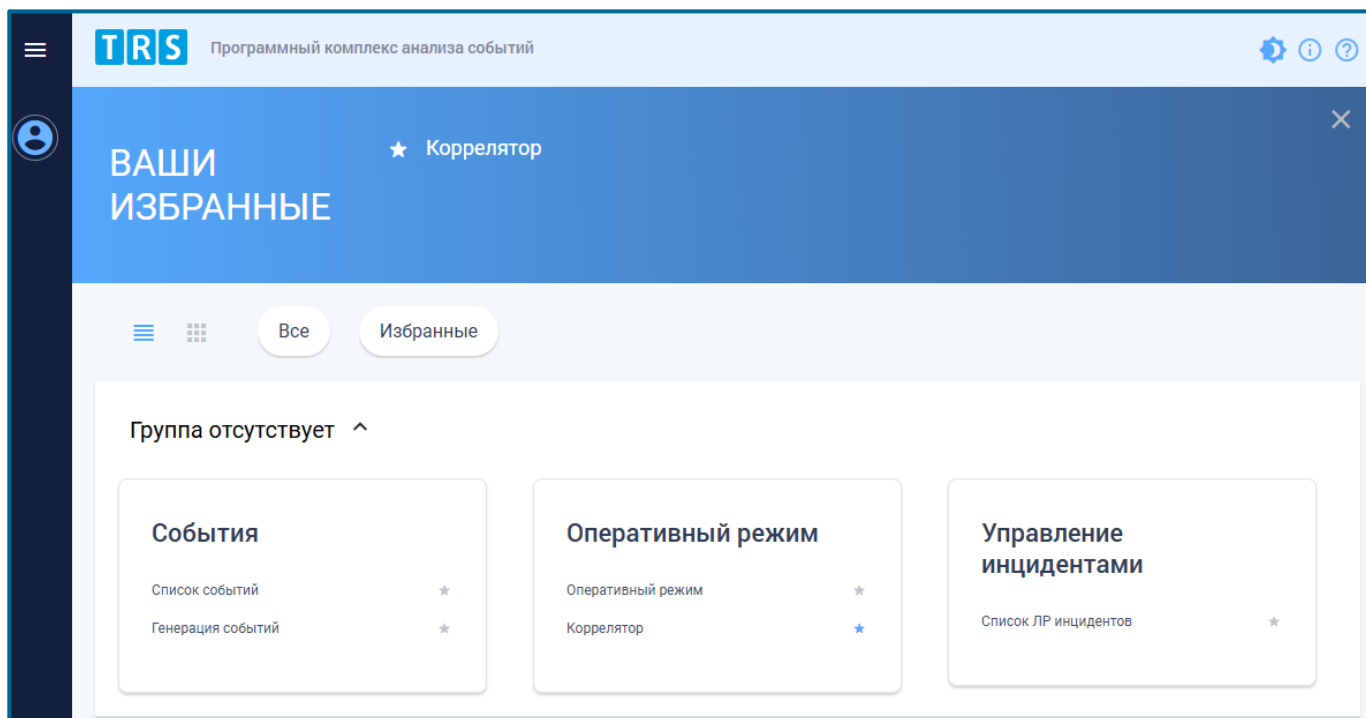


Рисунок 4.16 – Переход к разделу «Коррелятор»

Раздел «Коррелятор» состоит из следующих компонентов:

- Реестр (список) правил коррелятора (п. 4.3.1.1);
- Учетная карточка правила коррелятора (УК правила коррелятора) (п. 4.3.1.2).

4.3.1.1 Реестр правил коррелятора

Реестр (список) правил коррелятора содержит подробную информацию о созданных правилах коррелятора событий и представлен в виде таблицы с полями. Заполнение таблицы производится автоматически на основании данных соответствующих полей УК правил коррелятора событий и недоступно для редактирования пользователем.

Внешний вид страницы «Реестр правил коррелятора» представлен на рисунке (Рисунок 4.17):

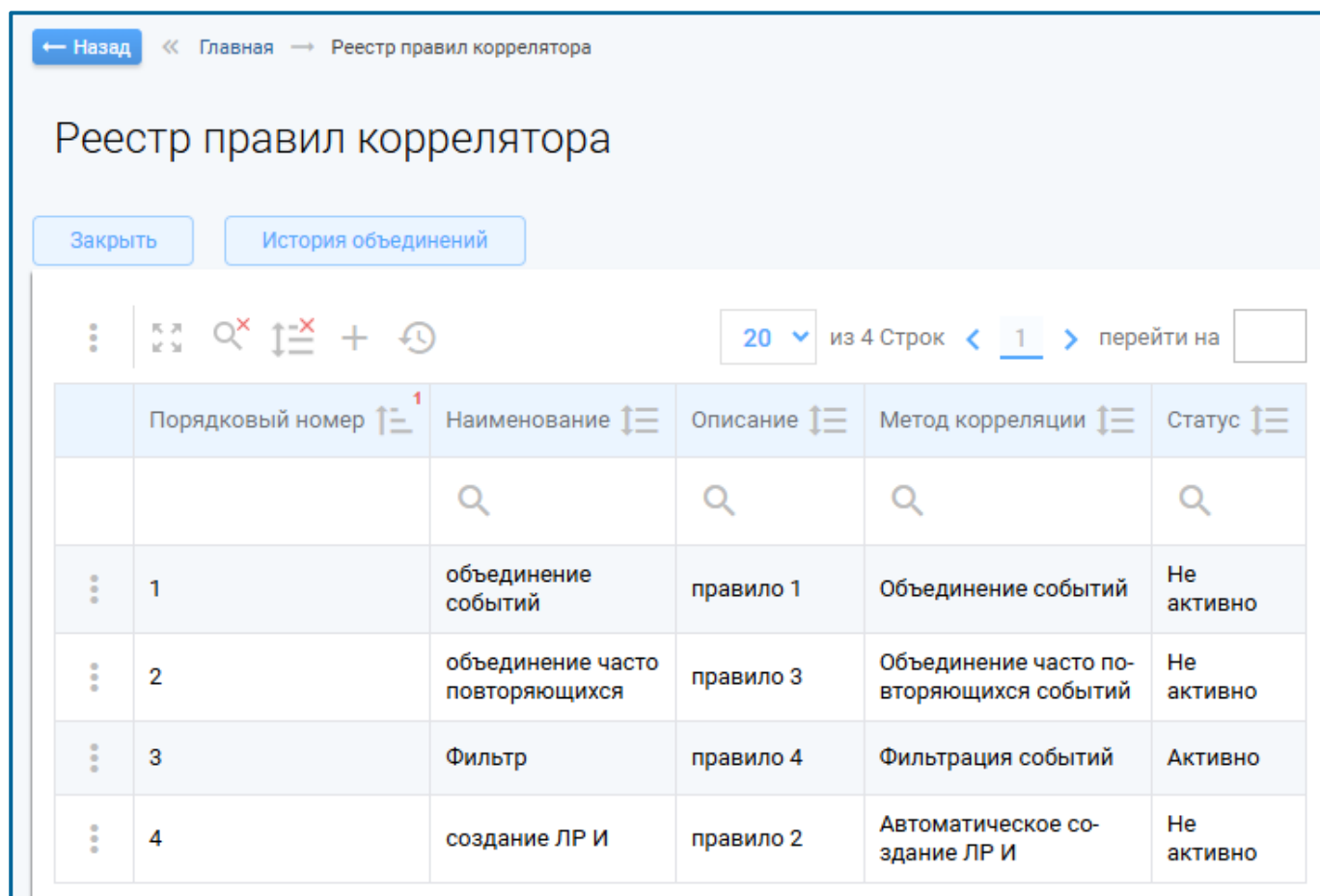


Рисунок 4.17 – Внешний вид страницы «Реестр правил коррелятора»

По реестру правил коррелятора доступны следующие операции:

- сортировка значений (аналогично п. 4.2.2.1);
- поиск информации по столбцам таблицы (аналогично п. 4.2.2.2);
- фильтрация данных по количеству отображаемых строк (аналогично п. 4.2.2.3);
- выгрузка данных в файл формата «csv»/ «xlsx» (аналогично п. 4.2.2.4);
- переход к просмотру УК правила коррелятора (аналогично п. 4.2.2.5);
- переход к созданию УК правила коррелятора (аналогично п. 4.2.2.7);
- переход к редактированию УК правила коррелятора (аналогично п. 4.2.2.8);
- переход к удалению УК правила коррелятора (аналогично п. 4.2.2.9);
- активация/деактивация правил (п. «Активация/деактивация правил»);
- сортировка порядка расположения правил (п. «Сортировка порядка запуска правил»);
- просмотр истории объединений (п. «Просмотр истории объединений»);

- просмотр истории изменений (доступно по пиктограмме  в реестре (Рисунок 4.17).

Активация/деактивация правил

Активация/деактивация осуществляется из Реестра правил коррелятора по нажатию на пиктограмму  → «Активировать/Деактивировать» (Рисунок 4.18). Также активировать/деактивировать правило можно в блоке «Основные параметры» учетной карточки правила коррелятора путем установки/снятия чек-бокса в поле «Активно». Если правило находится в статусе «Неактивно», то оно не применяется при анализе событий коррелятором.

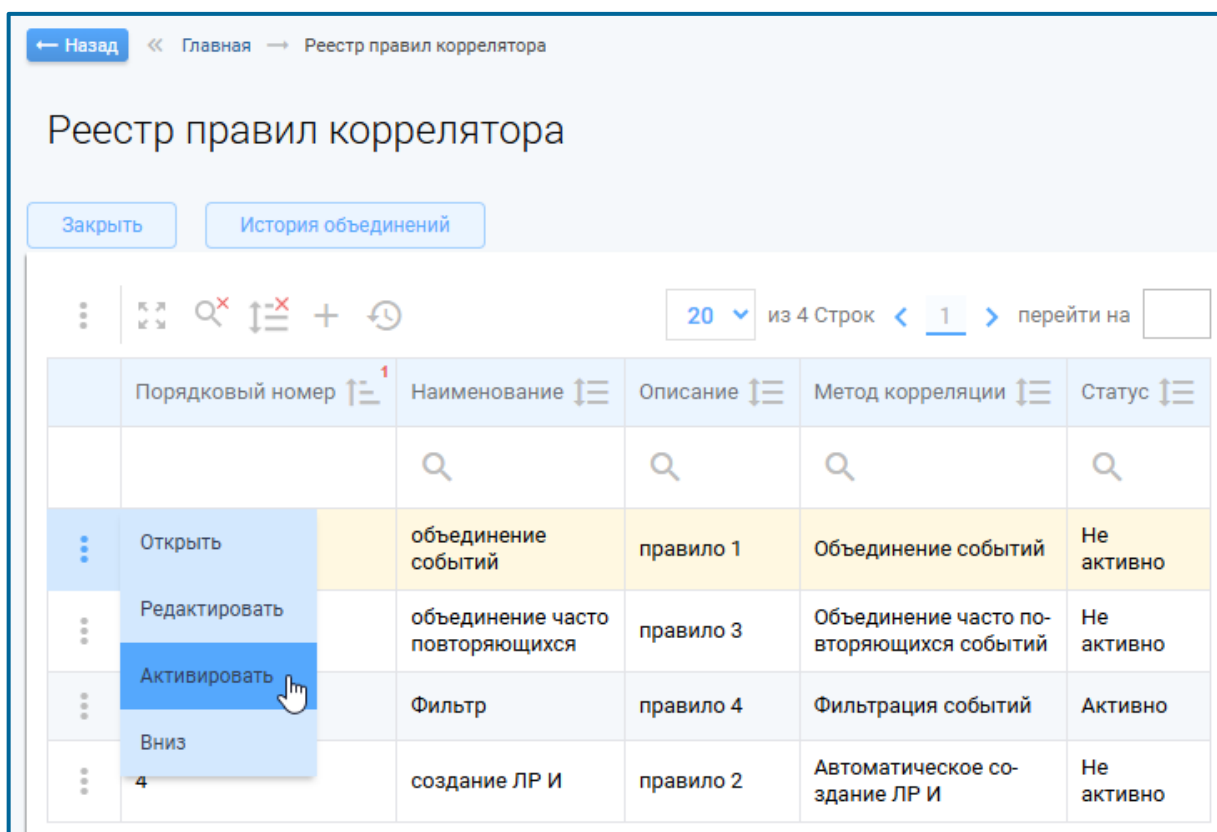


Рисунок 4.18 – Активация/Деактивация правила

Сортировка порядка запуска правил

Правила коррелятора событий, находящиеся в статусе «Активен», применяются в последовательности их расположения в реестре правил коррелятора событий в соответствии с порядковым номером правила. Перемещение правила реестра вверх/вниз (изменения порядкового номера запуска правила) осуществляется из Реестра правил коррелятора по нажатию на пиктограмму  → «Вверх», «Вниз».

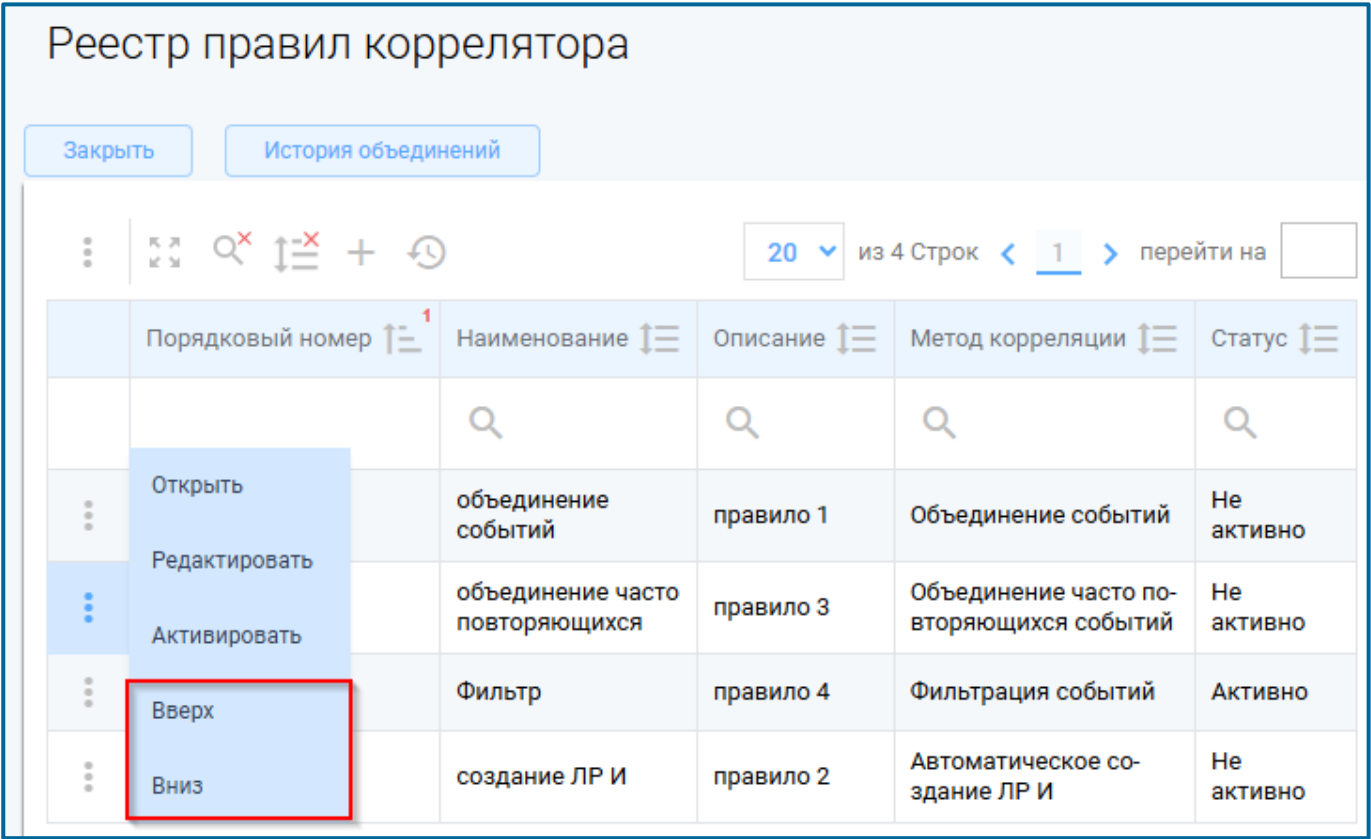


Рисунок 4.19 – Сортировка порядка запуска правил коррелятора

Просмотр истории объединений

При нажатии на кнопку «История объединений» осуществляется переход к просмотру результатов обработки событий, согласно правил (Рисунок 4.20).

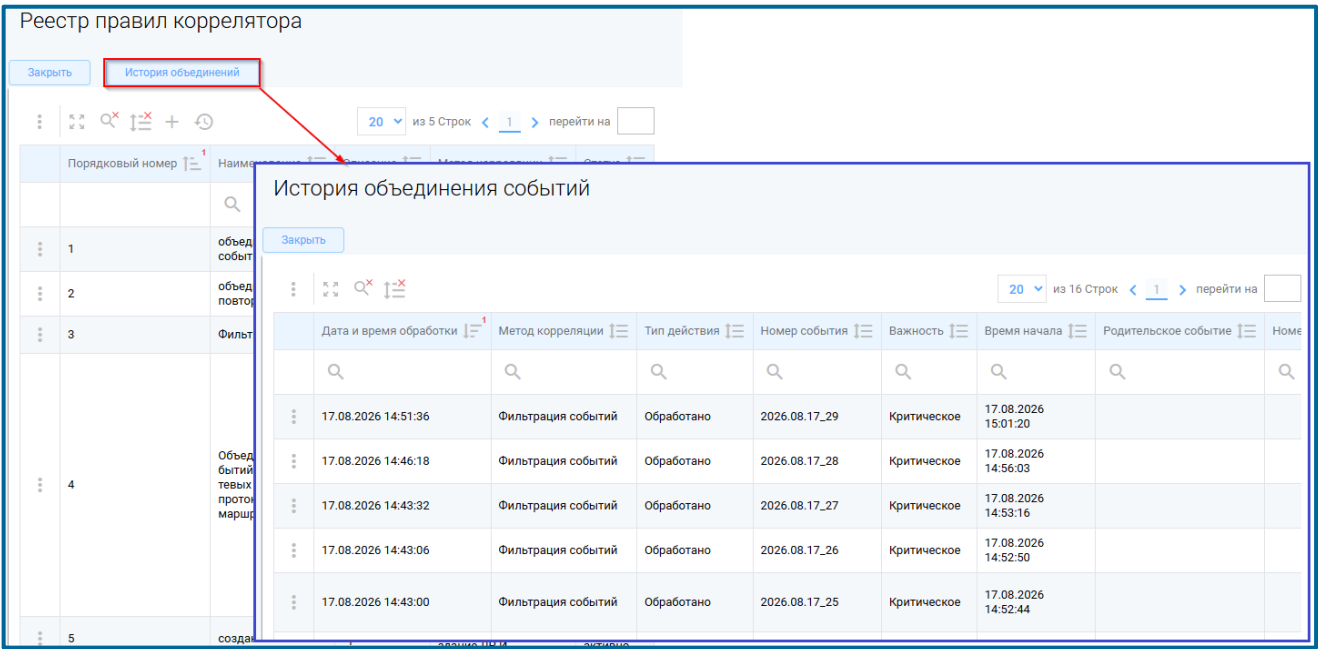


Рисунок 4.20 – Переход к просмотру результатов обработки событий

В интерфейсе истории объединения событий доступны следующие операции:

- сортировка значений (аналогично п. 4.2.2.1);
- навигация по страницам (аналогично п. 4.2.2.3);
- поиск информации по столбцам таблицы (аналогично п. 4.2.2.2);
- выгрузка данных в файл формата «csv»/ «xlsx» (аналогично п. 4.2.2.4) по пиктограмме ;
- вернуть событие (п. «Возврат события»).

Возврат события в оперативный режим

Для возврата события в оперативный режим нажать на пиктограмму «Вызвать дополнительное меню» () и выбрать в меню пункт «Вернуть событие» (Рисунок 4.21).

История объединения событий

Заккрыть

20 из 16 Строк < 1 > перейти на

	Дата и время обработки	Метод корреляции	Тип действия	Номер события	Важность	Время начала	Родительское событие	Номер
	🔍	🔍	🔍	🔍	🔍	🔍	🔍	🔍
	Вернуть событие	Фильтрация событий	Обработано	2026.08.17_29	Критическое	17.08.2026 15:01:20		
	17.08.2026 14:46:18	Фильтрация событий	Обработано	2026.08.17_28	Критическое	17.08.2026 14:56:03		
	17.08.2026 14:43:32	Фильтрация событий	Обработано	2026.08.17_27	Критическое	17.08.2026 14:53:16		

Рисунок 4.21 – Переход к возврату события в оперативный режим

Данное действие возврата события отменяет объединение или фильтрацию событий, выполненных с помощью коррелятора, и возвращает эти события в оперативный режим для дальнейшей ручной обработки. При этом у события разрываются все связи (объединение с другими событиями и связь с ЛР) и сбрасывается его статус. Запись об этом отражается в истории объединении событий с значением в поле «Тип действия» = «Возвращено в ОР».

4.3.1.2 Учетная карточка правила коррелятора

Учетная карточка правила коррелятора предназначена для регистрации правил и условий коррелятора в Программном комплексе анализа событий. Переход к УК правила коррелятора осуществляется из реестра правил коррелятора по нажатию на пиктограмму  → «Открыть».

Внешний вид УК правила коррелятора представлен на рисунке:

Дата и время	Логин пользователя	IP пользователя	Тип события	Наименование	Порядок	Метод корреляции
14.08.2026 15:57:41	admin		Изменение	объединение событий	1	Объединение событий
14.08.2026 15:52:07	admin		Изменение	объединение событий	1	Объединение событий
14.08.2026 15:17:28	admin		Изменение	объединение событий	1	Объединение событий
14.08.2026 15:16:17	admin		Изменение	объединение событий	1	Объединение событий
14.08.2026 13:39:00	admin		Изменение	объединение событий	1	Объединение событий
14.08.2026 13:14:18	admin		Изменение	объединение событий	1	Объединение событий
14.08.2026 10:21:20	admin		Изменение	объединение событий	1	Объединение событий
14.08.2026 10:20:05	admin		Изменение	основное правило	1	Объединение событий
13.08.2026 14:19:25	admin		Создание	основное правило	1	Объединение событий

Рисунок 4.22 – УК правила коррелятора

УК правила коррелятора имеет следующую структуру (Рисунок 4.22):

- наименование формы – «Карточка правила коррелятора» и блок кнопок (1);
- блок «Основные параметры» (2);
- блок вкладок (3).

Для УК правила коррелятора доступны операции:

- просмотр (п. 4.2.2.5);
- создание (п. 4.2.2.7)
- редактирование (п. 4.2.2.8);
- удаление (п. 4.2.2.9).

Блок «Основные параметры»

В блоке «Основные параметры» вводятся и размещаются первоначальные данные по правилу коррелятора.

Описание блока «Основные параметры» УК правила коррелятора представлено в таблице:

Таблица 4.3 – Описание блока «Основные параметры» УК правила коррелятора

Наименование	Описание
Наименование правила	Название правила. Ручной ввод.

Наименование	Описание
Описание	Описание правила. Ручной ввод.
Активно	Признак активности правила. Заполняется установкой чек-бокса.
Метод корреляции	Выбор из списка следующих значений: – Объединение событий; – Объединение часто повторяющихся событий; – Фильтрация событий; – Автоматическое создание ЛР И. Недоступно к редактированию после создания и сохранения УК.

Вкладка «Условия»

Вкладка «Условия» предназначена для настройки условий правила коррелятора.

Настройка условий – это создание логических выражений, отражающих условия объединения или фильтрации событий, условия автоматического создания ЛР И при активации правила.

Внешний вид вкладки представлен на рисунках (Рисунок 4.23, Рисунок 4.24):

Условия История изменений

Интервал появления однотипных событий, сек
4

Анализируемое время, мин
2

Полученное выражение ?

События.Тип аварийного сообщения = Данные

Рисунок 4.23 – Вкладка «Условия», режим просмотра

Условия История изменений

Интервал появления однотипных событий, сек

4

Анализируемое время, мин

2

Условия сохранены

Добавить параметры запроса

☐ Без учета регистра

☐ События.Тип аварий... = Данные ☐

Полученное выражение

События.Тип аварийного сообщения = Данные

Рисунок 4.24 – Вкладка «Условия», режим редактирования

Описание полей вкладки «Условия» представлены в таблице:

Таблица 4.4 – Описание полей вкладки «Условия» УК правила коррелятора

Наименование	Описание
Интервал появления однотипных событий, сек	Интервал появления однотипных событий. Заполняется вручную положительным целым числом, отличным от нуля. Поле отображается при условии, что в УК правила коррелятора указан метод «Объединение часто повторяющихся событий».
Анализируемое время, сек	Задается время, в течении которого должно производиться объединение Коррелятором зависимых событий в рамках родительского. Заполняется вручную положительным целым числом, отличным от нуля. Поле отображается при условии, что в УК правила коррелятора указан метод «Объединение событий» или «Автоматическое создание ЛР И».
Блок параметров запроса	
Переменная	Выпадающий список атрибутов события.
Условие отбора записей	Выпадающий список доступных операций в зависимости от типа данных выбранной переменной.
Значение	Ввод текстового или числового значения, либо выбор из модального окна в зависимости от типа данных выбранной переменной.

Наименование	Описание
Логическое условие	Выбор логического условия «И» /«ИЛИ»

Добавление параметров запроса по пиктограмме . При этом нужно выбрать логическое условие: И, ИЛИ.

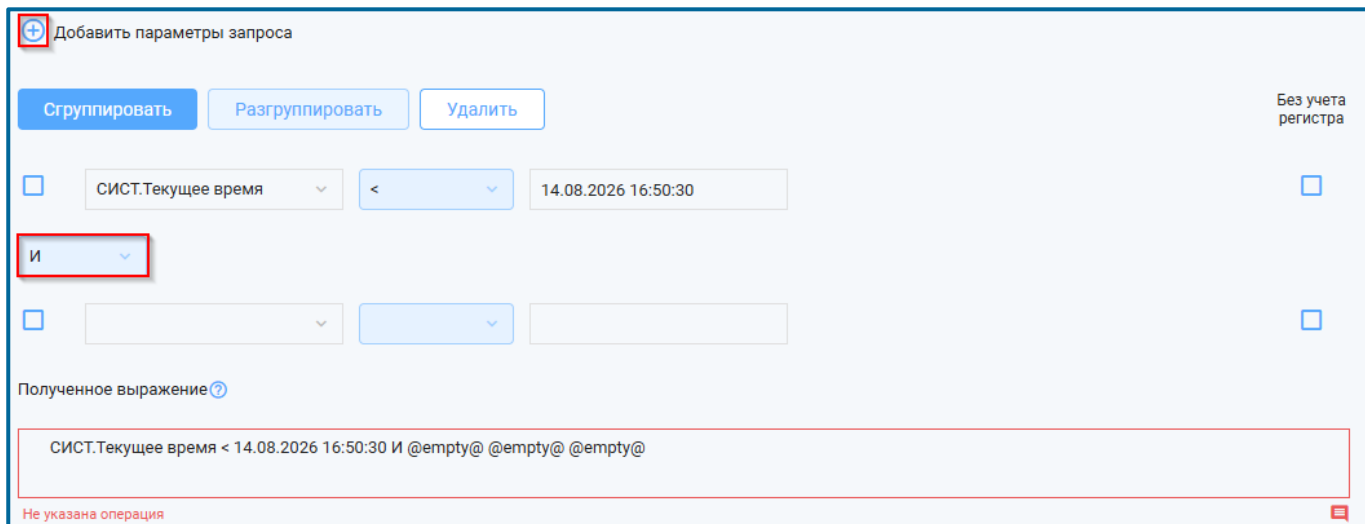


Рисунок 4.25 – Добавление параметров запроса

Также у пользователя есть возможность создавать группы условий. Для этого нужно установить чек-бокс напротив нужных блоков параметров и нажать на кнопку «Сгруппировать»:

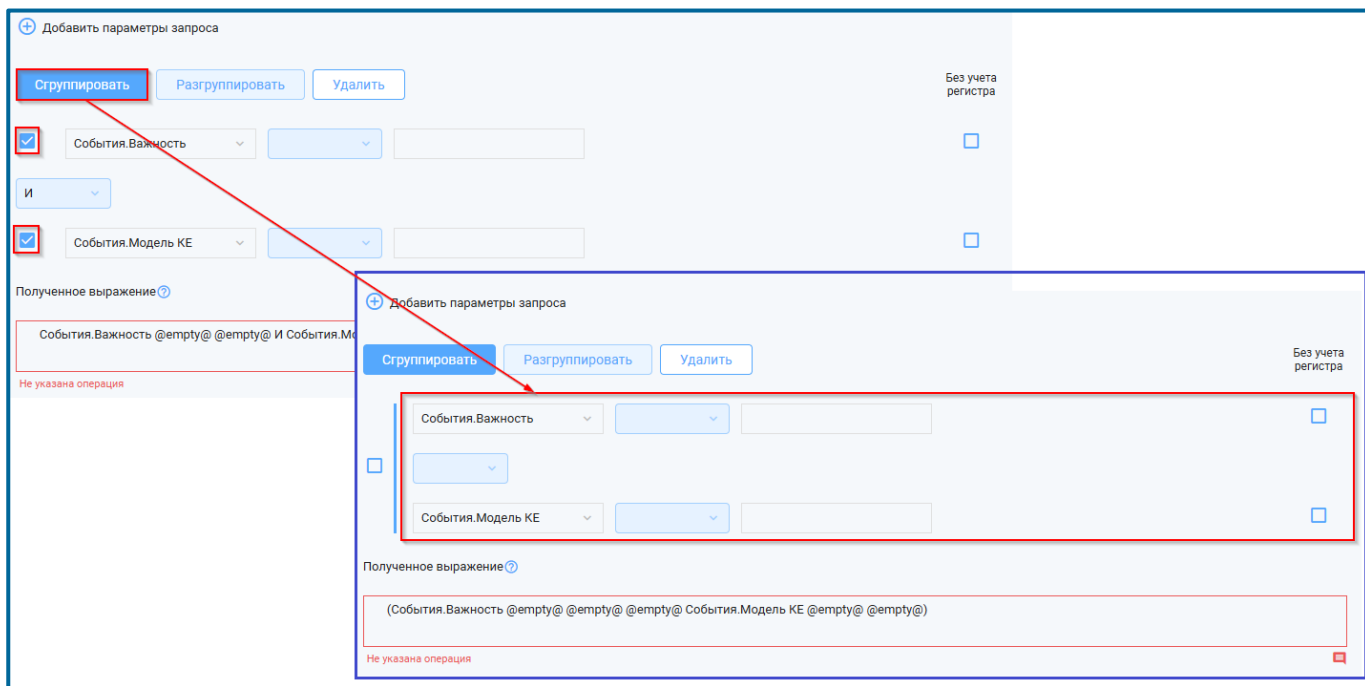


Рисунок 4.26 – Группировка блоков параметров. Формирование группы

Таким образом параметры будут объединены в одну группу, между переменными которой установить логическое условие «И/ИЛИ». Далее, при необходимости, можно сформировать еще одну группу параметров, а затем установить логическое условие «И/ИЛИ» между переменными внутри группы и т.д.

Добавить параметры запроса

Сгруппировать Разгруппировать Удалить

Без учета регистра

События.Важность = Важное

И

СИСТ.Текущее время из списка

ИЛИ

События.Важность = Существенное

И

СИСТ.Текущее время не пусто

Полученное выражение ?

Рисунок 4.27 – Две группы параметров с логическим условием «ИЛИ»

Для разгруппировки установить чек-бокс напротив группы параметров, нажать на кнопку «Разгруппировать».

Для удаления блока параметров условий установить чек-бокс напротив блока параметров, нажать на кнопку «Удалить».

В нижней части экранной формы условий запроса отображается блок с логическим выражением, полученным на основании настроенного блока условий в правиле:

Полученное выражение ?

События.Описание неисправности содержит BGP is down ИЛИ События.Описание неисправности содержит OSPF is down

Рисунок 4.28 – Логическое выражение правила

Вкладка «Условия определения родительского события»

Вкладка доступна, если в поле «Метод корреляции» основных параметров УК было выбрано значение «Объединение событий», и нужна для настройки условий определения родительского события.

Внешний вид вкладки представлен на рисунке:

The screenshot shows a web interface for editing a rule. At the top are three buttons: 'Редактировать', 'Закрыть', and 'Удалить'. Below them is the title 'Карточка правила коррелятора'. The main area has three tabs: 'Условия', 'Условия определения родительского события' (which is active), and 'История изменений'. On the left is a sidebar with 'Основные параметры' containing fields for 'Наименование правила' (объединение событий), 'Описание' (правило 1), 'Активно' (Нет), and 'Метод корреляции' (Объединение событий). The main content area under the active tab shows 'Полученное выражение' with a text box containing 'События.Описание неисправности содержит главная проблема'.

Рисунок 4.29 – Вкладка «Условия определения родительского события», режим просмотра

Описание полей вкладки «Условия определения родительского события» представлено в таблице:

Таблица 4.5 – Описание полей вкладки «Условия определения родительского события» УК правила коррелятора

Наименование	Описание
Блок условий запроса	
Переменная	Выпадающий список атрибутов события.
Условие отбора записей	Выпадающий список доступных операций в зависимости от типа данных выбранной переменной.
Значение	Ввод текстового или числового значения, либо выбор из модального окна в зависимости от типа данных выбранной переменной.
Логическое условие	Выбор логического условия «И» / «ИЛИ»

Вкладка «История изменений»

На вкладке «История изменений» хранятся и отображаются изменения, внесенные в основные параметры УК правила. Вкладка «История изменения» представлена в виде реестра и носит информационный характер. Все поля в реестре заполняются автоматически при выполнении действия с записью.

Внешний вид представлен на рисунке (Рисунок 4.30).

Условия

История изменений

🔍

🔍

📄

20 из 8 Строк

<

1

>

перейти

Дата и время	Логин пользователя	IP пользователя	Тип события	Наименование	Порядок	Метод корреляции
17.08.2026 12:07:54	admin		Изменение	объединение часто повторяющихся	2	Объединение часто повторяющихся событий
17.08.2026 12:04:46	admin		Изменение	объединение часто повторяющихся	2	Объединение часто повторяющихся событий
17.08.2026 12:00:02	admin		Изменение	объединение часто повторяющихся	2	Объединение часто повторяющихся событий
17.08.2026 11:58:08	admin		Изменение	объединение часто повторяющихся	2	Объединение часто повторяющихся событий
17.08.2026 11:57:33	admin		Изменение	объединение часто повторяющихся	2	Объединение часто повторяющихся событий
17.08.2026 11:57:03	admin		Изменение	объединение часто повторяющихся	2	Объединение часто повторяющихся событий
14.08.2026 10:21:55	admin		Изменение	объединение часто повторяющихся	2	Объединение часто повторяющихся событий
14.08.2026 10:20:54	admin		Создание	объединение часто повторяющихся	2	Объединение часто повторяющихся событий

Рисунок 4.30 – Вкладка «История изменения»

В интерфейсе вкладки доступны следующие операции:

- сортировка значений (аналогично п. 4.2.2.1);
- навигация по страницам (аналогично п. 4.2.2.3);
- поиск информации по столбцам таблицы (аналогично п. 4.2.2.2);
- выгрузка данных в файл формата «csv»/ «xlsx» (аналогично п. 4.2.2.4) по пиктограмме .

4.3.2 Настройка правил коррелятора событий

4.3.2.1 Настройка правила объединения событий

Для настройки правила объединения событий пользователю необходимо:

- 1) указать условия определения родительского события в УК правила коррелятора на вкладке «Условия определения родительского события» (подробнее п. Вкладка «Условия определения родительского события»);
- 2) задать условия отбора дочерних событий в УК правила коррелятора на вкладке «Условия» (подробнее п. Вкладка «Условия»).

После сохранения настроек коррелятор будет автоматически искать родительское событие и объединять с ним все поступающие дочерние события, соответствующие заданным правилам. Подробное описание механизма применения правила приведено ниже.

При поступлении нового события в очередь обработки коррелятора событий производится его сравнение с заданными условиями в настройках УК правила коррелятора:

- 1) Если событие удовлетворяет условиям, заданным в настройках УК правила коррелятора на вкладке «Условия определения родительского события» (п. Вкладка «Условия определения родительского события»), то событие считается первопричинным (родительским) и выполняется передача управляющих команд в производственную систему для отображения события в оперативном режиме без объединения. При попадании под условия на вкладке «Условия определения родительского события», более 1 события в качестве родительского выбирается событие с наименьшей датой и временем начала события. Остальные найденные события считаются вторичными (дочерними) по отношению к нему.
- 2) Если событие не удовлетворяет условиям, заданным в настройках УК правила коррелятора на вкладке «Условия определения родительского события» (п. Вкладка «Условия определения родительского события»), то проверяются условия, заданные на вкладке «Условия» (п. Вкладка «Условия»). Если событие удовлетворяет условиям, заданным в настройках УК правила коррелятора на вкладке «Условия», то событие считается вторичным (дочерним) и объединяется с родительским событием, найденным по условиям в рамках проверяемого правила на вкладке «Условия определения родительского события». Вносится запись в «Историю объединения событий» (дата и время обработки, метод корреляции, родительское событие).
- 3) Если событие удовлетворяет условиям, заданным в настройках УК правила коррелятора на вкладке «Условия» (п. Вкладка «Условия»), но при этом в системе отсутствует событие, заданное в настройках УК правила коррелятора на вкладке «Условия определения родительского события» (п. Вкладка «Условия определения родительского события»), то выполняется передача управляющих команд в производственную систему для отображения события в оперативном режиме без автоматической обработки и последующей ручной обработки диспетчером.
- 4) Если событие не удовлетворяет условиям, заданным в настройках УК правила коррелятора на вкладке «Условия определения родительского события» (п. Вкладка «Условия определения родительского события») и на вкладке «Условия» (п. Вкладка «Условия»), то

выполняется передача управляющих команд в производственную систему для отображения события в оперативном режиме без автоматической обработки и последующей ручной обработки диспетчером.

Объединение зависимых событий производится в течение времени, заданного в поле «Анализируемое время, мин» на вкладке «Условия».

4.3.2.2 Настройка правила объединения часто повторяющихся событий

Для настройки правила объединения часто повторяющихся событий пользователю необходимо указать условия определения однотипных событий в УК правила коррелятора на вкладке «Условия» (подробнее п. Вкладка «Условия») и временной интервал, в течение которого поступающие события будут накапливаться для их последующего объединения в рамках первоначально поступившего (первопричинного) события.

После сохранения настроек коррелятор будет автоматически выполнять объединение однотипных событий в рамках первоначально поступившего (первопричинного) события в течение указанного интервала появления событий (поле «Анализируемое время, мин» на вкладке «Условия»). Подробное описание механизма применения правила приведено ниже.

При поступлении нового события в очередь обработки коррелятора событий производится его сравнение с заданными условиями в настройках УК правила коррелятора:

- 1) Если событие удовлетворяет временному интервалу и условиям, заданных в настройках УК правила коррелятора, то событие, поступившее в обработку, объединяется с уже существующим событием, удовлетворяющим тому же временному интервалу и тем же условиям в настройках УК правила коррелятора (становится дочерним к первопричинному событию - событию с наименьшей датой и временем начала события) и вносится запись в «Историю объединения событий» (дата и время обработки, метод корреляции, родительское событие).
- 2) Если событие не удовлетворяет временному интервалу и условиям, заданным в настройках УК правила коррелятора, то выполняется передача управляющих команд в производственную систему для отображения события в оперативном режиме без автоматической обработки и последующей ручной обработки диспетчером.

4.3.2.3 Настройка правила фильтрации событий

Для настройки правила фильтрации событий пользователю необходимо указать условия фильтрации событий в УК правила коррелятора на вкладке «Условия» (подробнее п. Вкладка «Условия»).

После сохранения настроек коррелятор будет автоматически проверять поступающие события на соответствие заданным условиям и при совпадении передавать управляющие команды в производственную систему для исключения их из оперативного режима. Подробное описание механизма применения правила приведено ниже.

При поступлении нового события в очередь обработки коррелятора событий производится его сравнение с заданными условиями в настройках УК правила коррелятора:

- 1) Если событие удовлетворяет условиям фильтрации, заданным в настройках УК правила коррелятора, то выполняется передача управляющих команд в производственную систему для скрывания события из оперативного режима и вносится запись в «Историю объединения событий». При этом в истории объединения поля Родительское событие и Номер ЛР остаются не заполненными.
- 2) Если событие не удовлетворяет условиям фильтрации, заданным в настройках УК правила коррелятора, то выполняется передача управляющих команд в производственную систему для отображения события в оперативном режиме без автоматической обработки и последующей ручной обработки диспетчером.

4.3.2.4 Настройка правила автоматического создания ЛР И

Для настройки правила автоматического создания ЛР И пользователю необходимо указать условия отбора событий в УК правила коррелятора на вкладке «Условия» (подробнее п. Вкладка «Условия»).

После сохранения настроек коррелятор будет автоматически проверять поступающие события на соответствие заданным условиям и при совпадении передавать управляющие команды в производственную систему для автоматического создания связанного ЛР И. Подробное описание механизма применения правила приведено ниже.

При поступлении нового события в очередь обработки коррелятора событий производится его сравнение с заданными условиями в настройках УК правила коррелятора:

-
- 1) Если событие удовлетворяет условиям, заданным в настройках УК правила автоматического создания ЛР И, то выполняется передача управляющих команд в производственную систему для автоматического открытия ЛР И, при этом поля в созданном ЛР И заполняются данными из события, вносится запись в историю ЛР с пометкой о создании ЛР И и вносится запись в «Историю объединения событий» (дата и время обработки, метод корреляции, номер событие и номер созданного ЛР И). Событие, поступившее в обработку, привязывается к созданному ЛР И и вносится запись в «Историю установления статусов» (дата и время, отметка об автоматической привязке).
 - 2) Если событие не удовлетворяет условиям, заданным в настройках УК правила автоматического создания ЛР И, то выполняется передача управляющих команд в производственную систему для отображения события в оперативном режиме без автоматической обработки и последующей ручной обработки диспетчером.

5 АВАРИЙНЫЕ СИТУАЦИИ

В случае возникновения ошибок при работе с Программным комплексом анализа событий, не описанных ниже в данном разделе, или в случае, невозможности самостоятельного решения проблемы, необходимо обратиться в службу технической поддержки (п. 1.6).

Таблица 5.1 – Перечень неисправностей и способы их устранения

Ошибка / Неисправность	Действия пользователя при возникновении ошибки / неисправности
Сервер не найден. Невозможно отобразить страницу входа. Система недоступна	1. Убедиться в том, что соединение компьютера с Интернетом установлено. Попробовать загрузить несколько сетевых сервисов высокой надежности, например, http://yandex.ru , http://rbc.ru и т.п. 2. Убедиться в правильности ввода доменной части адреса системы. 3. Очистить кэш обозревателя.
Сбой аутентификации. Пользователь не может войти в систему	1. Повторить ввод имени пользователя и пароля. 2. Если учетная запись пользователя заблокирована, нужно обратиться к администратору системы.
Сбой в электропитании рабочей станции. Рабочая станция выключилась или перезагрузилась	1. Перезагрузить рабочую станцию. 2. Проверить доступность сервера. Должна быть доступна страница входа в систему. 3. Повторить попытку подключения (входа) в систему, введя логин и пароль пользователя.
Сбой локальной сети. Отсутствует возможность начала (продолжения) работы с системой. Нет сетевого подключения к серверу системы	1. Перезагрузить рабочую станцию. 2. Проверить доступность сервера. Должна быть доступна страница входа в систему. 3. После восстановления работы локальной сети повторить попытку подключения (входа) в систему, введя логин и пароль пользователя.
Получение сообщения об ошибке и/или невозможности выполнения действия в системе непосредственно на той странице, на которой эта ошибка была вызвана	Устранить ошибку, исключив препятствие, указанное в сообщении об ошибке.

6 РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ

Для успешного освоения Программного комплекса анализа событий необходимо:

- иметь навыки работы с ПК, а также интернет-браузерами;
- ознакомиться с настоящим руководством пользователя.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ЛВС	– Локальная вычислительная сеть
ЛР И	– Лист регистрации инцидента
ОС	– Операционная система
ПК	– Персональный компьютер
ПО	– Программное обеспечение
Программный комплекс анализа событий	– Система
УК	– Учетная карточка
ЭВМ	– Электронная вычислительная машина

ПРИЛОЖЕНИЕ 1

ПОРЯДОК ПРИМЕНЕНИЯ СПЕЦИАЛИЗИРОВАННЫХ ИМИТАЦИОННЫХ КОМПОНЕНТОВ ДЛЯ ДЕМОНСТРАЦИИ СКВОЗНОГО БИЗНЕС-ПРОЦЕССА ОБРАБОТКИ СОБЫТИЙ И ФОРМИРОВАНИЯ ИНЦИДЕНТОВ

Порядок применения правила объединения событий

- 1) Запустить интернет-браузер и в строке «адрес» набрать адрес сервера;
- 2) В форме авторизации ввести учетные данные пользователя Программного комплекса анализа событий и нажать на кнопку «Авторизация»;
- 3) Перейти в раздел «События»/«Генерация событий»;
- 4) Выбрать вид генерации: Объединение событий;
- 5) Нажать на кнопку «Сгенерировать» и закрыть форму;
- 6) Перейти в раздел «Оперативный режим»/«Коррелятор»;
- 7) Перейти в реестр правил, нажать на кнопку «История объединений» и найти родительское событие;
- 8) Проверить заполнение истории объединений после обработки событий правилом объединения событий:
 - для родительского события тип действия «Обработано»;
 - для подчиненного события тип действия «Обработано» и заполнено поле «Родительское событие».
- 9) Открыть УК родительского события и убедиться, что количество подчиненных событий равно «1»;
- 10) Перейти в «Оперативный режим» и убедиться:
 - в отображении родительского события в статусе «Ожидает обработки» с количеством подчиненных событий, равным «1».
 - дочернее событие, привязанное к родительскому, не отображается в Оперативном режиме.

Порядок применения правила объединения часто повторяющихся событий

- 1) Запустить интернет-браузер и в строке «адрес» набрать адрес сервера;

- 2) В форме авторизации ввести учетные данные пользователя Программного комплекса анализа событий и нажать на кнопку «Авторизация»;
- 3) Перейти в раздел «События»/«Генерация событий»;
- 4) Выбрать вид генерации: Объединение часто повторяющихся событий;
- 5) Нажать на кнопку «Сгенерировать» и закрыть форму;
- 6) Перейти в раздел «Оперативный режим»/«Коррелятор»;
- 7) Перейти в реестр правил, нажать на кнопку «История объединений» и найти первопричинное событие;
- 8) Проверить заполнение истории объединений после обработки событий правилом объединения часто повторяющихся событий:
 - для первопричинного события тип действия «Обработано»;
 - для подчиненных событий тип действия «Обработано» и заполнено поле «Родительское событие» значением первопричинного события.
- 9) Открыть УК первопричинного события и убедиться, что количество подчиненных событий равно «2»;
- 10) Перейти в Оперативный режим и убедиться:
 - в отображении первопричинного события в статусе «Ожидает обработки» с количеством подчиненных событий, равным «2»;
 - подчиненные события, привязанные к первопричинному, не отображаются в Оперативном режиме.

Порядок применения правила фильтрации событий

- 1) Запустить интернет-браузер и в строке «адрес» набрать адрес сервера;
- 2) В форме авторизации ввести учетные данные пользователя Программного комплекса анализа событий и нажать на кнопку «Авторизация»;
- 3) Перейти в раздел «События»/«Генерация событий»;
- 4) Выбрать вид генерации: Фильтрация событий;
- 5) Нажать на кнопку «Сгенерировать» и закрыть форму;
- 6) Перейти в раздел «Оперативный режим»/«Коррелятор»;

- 7) Перейти в реестр правил, нажать на кнопку «История объединений» и найти сгенерированное событие;
- 8) Убедиться в корректном применении правила фильтрации событий;
- 9) Перейти в Оперативный режим и убедиться в отсутствии события, которое было обработано правилом фильтрации событий.

Порядок применения правила автоматического создания ЛР И

- 1) Запустить интернет-браузер и в строке «адрес» набрать адрес сервера;
- 2) В форме авторизации ввести учетные данные пользователя Программного комплекса анализа событий и нажать на кнопку «Авторизация»;
- 3) Перейти в раздел «События»/«Генерация событий»;
- 4) Выбрать вид генерации: Автоматическое создание ЛР И;
- 5) Нажать на кнопку «Сгенерировать» и закрыть форму;
- 6) Перейти в раздел «Оперативный режим»/«Коррелятор»;
- 7) Перейти в реестр правил, нажать на кнопку «История объединений» и найти сгенерированное событие;
- 8) Проверить заполнение истории объединений после обработки события правилом автоматического создания ЛР И: тип действия «Создан ЛР И» и заполнено поле «Номер ЛР И» значением созданного ЛР И.
- 9) Открыть УК сгенерированного события и убедиться в наличии связанного процесса: заполнено поле «Номер ЛР» номером созданного ЛР Инцидент;
- 10) Открыть УК созданного ЛР Инцидент, перейти на вкладку «События» и убедиться в наличии связанного события.