АКЦИОНЕРНОЕ ОБЩЕСТВО «ТРАНССЕТЬ»
(АО «Транссеть»)

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

РУКОВОДСТВО АДМИНИСТРАТОРА

Листов 11

2026

АННОТАЦИЯ

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

Документ содержит сборник описаний операций, выполняемых администратором.

Правообладатель вправе вносить изменения в настоящий документ.

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

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 Требования к оборудованию и программному обеспечению

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

- Операционная система на базе ядра GNU/Linux (предпочтение системам, находящимся в Едином реестре российского ПО Минцифры России);
- СУБД PostgreSQL версии не ниже 15;
- Совмещенный сервер бизнес-логики и СУБД: количество – 1, процессор – не менее 12 vCPU, оперативная память – не менее 24 Гб, дисковое пространство – не менее 64 GB.

Данная конфигурация предполагает количество одновременно работающих пользователей в системе – не более 100, ежедневный суточный прирост данных – не более 10Мб, отсутствие резервирования данных.

1.5 Задачи администратора

Администратор Программного комплекса анализа событий несет ответственность за бесперебойное функционирование системы, управляет программно-аппаратным комплексом, на котором установлена система.

Администратор должен иметь следующий опыт:

- 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#;
- знание принципов работы СУБД (PostgreSQL);
- навыки работы с системами логирования, мониторинга и управления сервисами.

Основными задачами администратора являются мониторинг состояния системы.

В обязанности администратора входит:

- обновление программного обеспечения (далее – ПО) и его компонентов;
- обеспечение бесперебойной работы системы и поддержание жизненного цикла ПО, а именно проведение на регулярной основе:
  - ежедневного мониторинга работы ПО;
  - контроля работы процедуры создания резервной копии данных.

2 ПОДГОТОВКА К РАБОТЕ

На узлах Заказчика, предполагаемых к использованию, администратором должен быть предустановлен набор ПО, необходимого для запуска компонентов Программного комплекса анализа событий.

Общий порядок работы в системе описан в Руководстве пользователя Программного комплекса анализа событий.

2.1 Установка, настройка и обновление ПО

Порядок установки и настройки Программного комплекса анализа событий на узлах Заказчика, предполагаемых к использованию, определяется условиями договора. В договоре определяются ответственные исполнители, этапы работ.

Установка производится методами (пакетными менеджерами), предусмотренными дистрибутивом – комплектом файлов (формат дистрибутива – *.tar.gz). Комплект файлов может быть предоставлен на портативном носителе данных (CD-диск/ DVD-диск/ Flash-носитель) или в виде ссылки на архивное хранилище файлов.

Архивное хранилище файлов в формате *.tar.gz включает в себя компоненты:

- компонент ядра и web-компоненты;
- набор пакетов первоначальной инициализации;
- набор базовых конфигурационных файлов;
- комплект ключей лицензирования.

Обновления компонентов ПО поставляются в виде архива в формате *.tar.gz и могут включать в себя:

- обновления web-компонентов и компонентов ядра;
- обновления пакетов функциональности.

Обновление web-компонентов и компонентов ядра производится администратором замещением соответствующих файлов из предоставленного архива. Для обновления необходимо:

1) выполнить копирование (с замещением) в соответствующие каталоги (/opt/core или /opt/web);
2) восстановить (в случае необходимости) права на измененные файлы.

Обновление пакетов функциональности производится администратором копированием файлов обновления из предоставленного архива на узел компонента ядра и последующим выполнением команды инициализации обновления.

2.2 Резервное копирование и восстановление

Автоматическое резервное копирование данных Программного комплекса анализа событий обеспечивается средствами системного и базового ПО (ОС, СУБД), входящего в состав программно-технического комплекса Заказчика.

С целью обеспечения надежного функционирования системы используются стандартные средства и встроенные механизмы СУБД, предусматривающие:

- контроль наличия ошибок при передаче информации;
- сохранение целостности данных в базе данных при нештатном завершении работы системы;
- сохранение работоспособности системы при некорректных действиях пользователя (ввод неверных по размеру и/или составу данных, нештатное завершение действия и т.п.);
- резервное копирование базы данных и файлов конфигураций.

Восстановление нормального функционирования Программного комплекса анализа событий обеспечивается администратором путем:

- перезапуска ПО при программных сбоях, не повлекших потерю данных;
- восстановления из резервной копии при аппаратных отказах или повреждении данных в течение одного рабочего дня, не считая времени восстановления аппаратного и системного ПО.

2.3 Мониторинг системы

В Программном комплексе анализа событий предусмотрен мониторинг ее функционирования путем ведения специализированных журналов (лог-файлов).

При возникновении аварийных ситуаций или ошибок в системе, диагностические инструменты позволяют сохранять полный набор информации, необходимой разработчику для идентификации проблемы.

Реализация журнала исключает возможность внесения пользователем правок.

Аварийными ситуациями являются:

- нарушение работоспособности ПО Программного комплекса анализа событий;
- нарушение работоспособности комплекса технических средств.

Для поддержания жизненного цикла ПО администратору необходимо проводить ежедневный мониторинг его работы на основании данных о состоянии сервера мониторинга, ПО, значений контролируемых параметров в части:

- потребления процессорной мощности и оперативной памяти;
- занятости дискового пространства;
- наличия критических ошибок в логах;
- наличия ошибок в работе серверного оборудования;
- контроля работы процедуры создания резервной копии данных.

3 АВАРИЙНЫЕ СИТУАЦИИ

В случае возникновения ошибок при работе Программного комплекса анализа событий, не описанных в Руководстве пользователя, или в случае, невозможности самостоятельного решения проблемы, необходимо обратиться в службу технической поддержки.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ЛВС	–	Локальная вычислительная сеть
ОС	–	Операционная система
ПО	–	Программное обеспечение
СУБД	–	Система управления базами данных
УК	–	Учетная карточка
Программный комплекс анализа событий	–	Система