kaspersky

Kaspersky Machine Learning for Anomaly Detection

© 2026 АО "Лаборатория Касперского"

Содержание

О Kaspersky Machine Learning for Anomaly Detection
- Комплект поставки
- Аппаратные и программные требования
- Рекомендации по обеспечению безопасной работы
- Устранение уязвимостей и установка критических обновлений
- Разделение доступа к функциям программы

Что нового

Архитектура Kaspersky MLAD

Типовые схемы развертывания

Схема потока данных телеметрии и событий

Порты, используемые Kaspersky MLAD

Установка и удаление программы
- Подготовка к установке программы
- Проверка целостности файлов архива Kaspersky MLAD
- Установка программы
- Обновление программы
- Проверка версии и состояния программы
- Резервное копирование программы
- Откат программы к предыдущей установленной версии
- Сценарий восстановления Kaspersky MLAD из резервной копии
- Добавление информации о предыдущей установленной версии программы
- Очистка программы
- Подготовка к работе
- Запуск, остановка и перезапуск Kaspersky MLAD
- Обновление сертификатов Kaspersky MLAD
- Первый запуск Kaspersky MLAD
- Удаление программы

Веб-интерфейс Kaspersky MLAD

Подключение к Kaspersky MLAD и завершение пользовательской сессии
- Подключение к веб-интерфейсу
- Завершение сессии подключения к Kaspersky MLAD

Изменение пароля учетной записи

Выбор языка веб-интерфейса Kaspersky MLAD

Лицензирование программы
- О Лицензионном соглашении
- О лицензии
- О лицензионном сертификате
- О лицензионном ключе
- О файле лицензионного ключа
- Доступная функциональность Kaspersky MLAD в зависимости от лицензии
- Добавление лицензионного ключа
- Просмотр информации о добавленном лицензионном ключе
- Удаление лицензионного ключа

Обработка и хранение данных в Kaspersky MLAD
О предоставлении данных
Директории для хранения данных программы
Задачи системного администратора
Управление учетными записями пользователей
Создание учетной записи пользователя
Изменение учетной записи пользователя
Отзыв токенов аутентификации для учетной записи пользователя
Просмотр прав доступа для учетной записи пользователя
Управление ролями
Создание роли
Изменение роли
Удаление роли
Просмотр прав доступа для роли
Управление уведомлениями
Управление подписками на уведомления
Создание подписки на уведомления
Изменение подписки на уведомления
Удаление подписки на уведомления
Работа с группами контактов
Поиск и фильтрация групп контактов
Создание группы контактов
Изменение группы контактов
Удаление группы контактов
Работа с дополнительными контактами
Создание дополнительного контакта
Изменение дополнительного контакта
Удаление дополнительного контакта
Настройка параметров Kaspersky MLAD
Настройка основных параметров Kaspersky MLAD
Настройка параметров безопасности Kaspersky MLAD
Настройка службы Anomaly Detector
Настройка службы Keeper
Настройка службы Mail Notifier
Настройка службы Similar Anomaly
Настройка службы Stream Processor
Настройка службы Trainer
Настройка коннектора HTTP Connector
Настройка коннектора MQTT Connector
Настройка коннектора AMQP Connector
Настройка коннектора KICS Connector
Настройка коннектора CEF Connector
Настройка коннектора WebSocket Connector
Настройка службы Event Processor
Настройка приоритетов, статусов и причин инцидентов
Настройка ведения журналов служб Kaspersky MLAD
Настройка временных интервалов отображения данных

- Настройка уровней критичности активов
- Настройка отображения пунктов меню Kaspersky MLAD
- Экспорт и импорт параметров Kaspersky MLAD
- Управление активами и тегами
  - Об иерархической структуре объекта мониторинга
  - О тегах и способах получения наблюдений по тегам
  - Поиск и фильтрация объектов в разделе Активы
  - Создание актива
  - Изменение параметров актива
  - Создание тега
  - Изменение тега
  - Перемещение активов и тегов
  - Удаление актива или тега
  - Проверка текущей структуры тегов
  - Загрузка конфигурации активов и тегов в систему
  - Сохранение конфигурации активов и тегов в файл
- Работа с основным меню
  - Сценарий: работа с Kaspersky MLAD
  - Просмотр сводных данных в разделе Информационная панель
  - Просмотр поступающих данных в разделе Мониторинг
    - Выбор элементов ML-моделей в разделе Мониторинг
    - Просмотр данных для определенного пресета в разделе Мониторинг
    - Выбор интервала времени в разделе Мониторинг
    - Настройка параметров отображения графиков в разделе Мониторинг
  - Просмотр данных в разделе История
    - Выбор элементов ML-модели в разделе История
    - Просмотр исторических данных для определенного пресета
    - Выбор даты и интервала времени в разделе История
    - Навигация по времени в разделе История
    - Настройка параметров отображения графиков в разделе История
  - Просмотр данных в разделе Временной срез
    - Выбор определенного элемента ML-модели в разделе Временной срез
    - Просмотр данных для определенного пресета в разделе Временной срез
    - Выбор даты и интервала времени в разделе Временной срез
    - Навигация по времени в разделе Временной срез
    - Настройка параметров отображения графиков в разделе Временной срез
  - Работа с процессором событий
    - О процессоре событий
      - О событиях
      - О паттернах
      - О механизме внимания
      - О режимах работы процессора событий
      - О мониторах
    - Настройка отображения параметров событий
    - Настройка параметров конфигурации внимания
      - Добавление головы внимания
      - Изменение головы внимания

Удаление головы внимания
Работа с мониторами
Создание монитора
Изменение монитора
Удаление монитора
Просмотр истории событий
Просмотр истории паттернов
Управление инцидентами и группами инцидентов
Об инцидентах
Об инцидентах, обнаруженных предиктивным элементом ML-модели
Об инцидентах, обнаруженных элементом ML-модели на основе диагностического правила
Об инцидентах, обнаруженных элементом ML-модели на основе эллиптического конверта
Об инцидентах, обнаруженных детектором Limit Detector
Об инцидентах, обнаруженных службой Stream Processor
Об аномалиях
Сценарий: анализ инцидентов
Просмотр инцидентов
Просмотр технических характеристик зарегистрированного инцидента
Исследование поведения объекта мониторинга в момент обнаружения инцидента
Изменение приоритета, статуса, причины, экспертных рекомендаций и комментариев к инциденту
Работа с группами инцидентов
Просмотр групп инцидентов
Добавление группы инцидентов
Изменение группы инцидентов
Изменение состава инцидентов в группе
Удаление групп инцидентов
Экспорт инцидентов в файл
Управление ML-моделями
Об ML-моделях
О предиктивных элементах ML-модели
Об элементах ML-модели на основе диагностического правила
Об элементах ML-модели на основе эллиптического конверта
О статусах и состояниях ML-моделей и их элементов
О шаблонах ML-моделей
О разметках
Об условиях в составе разметок и диагностических правил
О вычислимых тегах в составе разметок и диагностических правил
Операции в выражениях для расчета вычислимых тегов
Рекомендации по использованию элементов ML-моделей
Сценарий: работа с ML-моделями
Сценарий: работа с элементами ML-модели на основе диагностического правила
Сценарий: работа с элементами ML-модели на основе эллиптического конверта
Сценарий: работа с предиктивными элементами ML-модели
Поиск и фильтрация объектов в разделе Модели
Работа с разметками
Создание разметки
Просмотр графика разметок

Просмотр сведений об элементах, связанных с разметками
Копирование разметки
Изменение разметки
Удаление разметки
Работа с импортированными ML-моделями
Импорт ML-модели
Активация импортированной ML-модели
Изменение параметров элемента импортированной ML-модели
Работа с ML-моделями, созданными вручную
Создание ML-модели
Добавление предиктивного элемента ML-модели
Изменение предиктивного элемента ML-модели
Добавление элемента ML-модели на основе диагностического правила
Изменение элемента ML-модели на основе диагностического правила
Добавление элемента ML-модели на основе эллиптического конверта
Изменение элемента ML-модели на основе эллиптического конверта
Копирование элемента ML-модели
Удаление элемента ML-модели
Копирование ML-модели
Работа с шаблонами ML-моделей
Создание шаблона по ML-модели
Изменение шаблона ML-модели
Создание ML-модели по шаблону
Удаление шаблона ML-модели
Изменение параметров ML-модели
Обучение предиктивного элемента ML-модели
Обучение элемента ML-модели на основе эллиптического конверта
Просмотр результатов обучения элемента ML-модели
Оценка результатов обучения элемента ML-модели
Запуск и остановка инференса ML-модели
Оценка результатов исторического инференса ML-модели
Просмотр графа потока данных в ML-модели
Подготовка ML-модели к публикации
Публикация и снятие ML-модели с публикации
Удаление ML-модели
Управление пресетами
О пресетах
Поиск и фильтрация объектов в разделе Пресеты
Просмотр пресета
Создание пресета
Загрузка пресетов из файла
Изменение пресета
Сохранение пресетов в файл
Удаление пресетов
Управление службами
Просмотр статусов служб
Запуск, остановка и перезапуск служб

- Управление источниками данных
  - Создание карточки источника данных OPC UA
  - Копирование карточки источника данных
  - Изменение параметров источника данных
  - Подключение к источнику данных и отключение от него
  - Удаление карточки источника данных
- Устранение неисправностей
  - При подключении к Kaspersky MLAD браузер выводит предупреждение о сертификате
  - Заканчивается свободное пространство на жестком диске
  - Непредвиденная перезагрузка операционной системы
  - Не удается подключиться к веб-интерфейсу Kaspersky MLAD
  - Не отображаются графики данных или графические области в разделах История и Мониторинг
  - Не отображается результат применения разметки
  - Отображается сообщение об остановленной службе Trainer
  - Обучение элемента ML-модели завершилось с ошибкой
  - Не приходят уведомления об инцидентах по электронной почте
  - Отсутствует артефакт элемента ML-модели по результатам инференса
  - Не отображаются изменения параметров элемента на графике его артефакта
  - Время точки-индикатора инцидента не совпадает с временем инцидента
  - Не выполняется передача событий между Kaspersky MLAD и внешними системами
  - Невозможно загрузить данные для просмотра в разделе Процессор событий
  - Неправильно обрабатываются данные в разделе Процессор событий
  - Не отображаются события в разделе Процессор событий
  - Списки активаций мониторов пустые или частично отсутствуют после перезапуска службы Event Processor
  - Требуется изменить язык локализации Справки
- Обращение в Службу технической поддержки
- Список ограничений
- Приложения
  - Параметры конфигурационного файла .env
  - Параметры конфигурационного файла config.env
  - Параметры и пример Excel-файла, содержащего конфигурацию активов и тегов
  - Параметры и пример JSON-файла, описывающего пресеты
  - Параметры и пример JSON-файла, содержащего конфигурацию параметров для службы Event Processor
  - Параметры и пример JSON-файла, описывающего теги источника данных OPC UA
  - Просмотр журнала Kaspersky MLAD
    - Сценарий: просмотр журналов событий информационной безопасности
    - Сценарий: оценка основных метрик Kaspersky MLAD
    - Сценарий: просмотр метрик и журналов контейнера
  - Специальные символы регулярных выражений
  - Наборы шифров для защищенного TLS-соединения
  - Примеры вычисления комбинированных функций в выражениях для расчета вычислимых тегов
- Глоссарий
  - ML-модель
  - Актив
  - Аномалия
  - Артефакт
  - АСУ ТП

- Внимание
- Время данных
- Графическая область
- Иерархическая структура объекта мониторинга
- Индикатор инференса
- Индикатор обучения
- Инференс
- Инцидент
- Коннектор
- Монитор
- Паттерн
- Пресет
- Равноинтервальная временная сетка (РИВС)
- Разметка
- Роль учетной записи
- Семплирование
- Событие
- Тег
- Топ-тег
- Топик AMQP
- Топик MQTT
- Уведомление
- Эксфильтрация данных

Информация о стороннем коде

Уведомления о товарных знаках

О Kaspersky Machine Learning for Anomaly Detection

Система раннего обнаружения аномалий Kaspersky Machine Learning for Anomaly Detection (далее также Kaspersky MLAD, программа) – программное обеспечение, предназначенное для предотвращения сбоев, аварий или деградации промышленных установок, технологических процессов, сложных киберфизических систем. Анализируя данные телеметрии с помощью методов машинного обучения (искусственного интеллекта), Kaspersky MLAD выявляет признаки аномальной ситуации до того, как она будет обнаружена традиционными системами мониторинга.

Kaspersky MLAD обнаруживает аномалии в технологических процессах независимо от вызвавших их причин. Аномалии могут быть вызваны следующими причинами:

- Физические (например, поломка оборудования или выход из строя датчиков).
- Человеческий фактор (например, намеренные или ненамеренные, неверные действия оператора, настройка оборудования, смена режимов или установок или переход на ручное управление).
- Кибератаки.

Основные возможности Kaspersky MLAD:

- В реальном времени выявляет аномальное поведение объекта мониторинга.
- Определяет сигналы, в которых обнаружены наибольшие отклонения от нормального поведения.
- Позволяет анализировать инциденты с учетом информации о похожих инцидентах.
- Предоставляет возможность экспертной классификации и аннотации инцидентов.
- Предоставляет возможность уведомления об обнаружении инцидентов через веб-интерфейс, сообщения электронной почты, через отправку сообщений в Kaspersky Industrial CyberSecurity for Networks, а также через индустриальные протоколы передачи данных.
- Позволяет использовать модели на основе машинного обучения, произвольных правил и эллиптических конвертов для обнаружения аномалий.
- Отображает в виде графиков исторические данные и данные, поступающие в режиме реального времени, в соответствии с заданными наборами тегов, а также результаты обработки этих данных ML-моделями.
- Обеспечивает работу с журналом обнаруженных инцидентов.
- Позволяет создавать ML-модели и добавлять в нее предиктивные элементы, элементы на основе эллиптического конверта и элементы на основе диагностических правил.
- Предоставляет возможность обучения предиктивных элементов и элементов на основе эллиптических конвертов.
- Позволяет создавать шаблоны на основе добавленных ML-моделей и добавлять ML-модели в Kaspersky MLAD по созданным шаблонам.
- Позволяет определить способ организации данных объекта мониторинга в виде дерева активов.

- Предоставляет возможность получения данных телеметрии по протоколам HTTP, MQTT, AMQP, CEF и WebSocket, а также по специализированному протоколу поверх протокола HTTPS от программы Kaspersky Industrial CyberSecurity for Networks.
- Позволяет получать данные телеметрии по протоколу OPC UA от нескольких источников данных одновременно.
- Определяет и обрабатывает прекращения и/или прерывания потока поступающих данных, а также восстанавливает пропущенные наблюдения.
- На основе данных о событиях, полученных из внешних систем, распознает закономерности в виде повторяющихся событий и паттернов, а также выявляет новые события и паттерны в потоке событий.
- Отображает выявленные события в виде графа и таблицы, а также выявленные паттерны в виде послойной иерархии вложенных элементов.
- Отправляет оповещения об обнаружении определенных событий, паттернов или значений параметров событий, поступающих в процессор событий в потоке данных от объекта мониторинга.

Комплект поставки

Kaspersky MLAD поставляется в виде файла архива Kaspersky_MLAD_6.0.0.<номер сборки>_ru-RU_en-US.tar.xz, который содержит следующие файлы:

- утилита mladctl для проверки целостности дистрибутива, установки, обновления, резервного копирования, восстановления, запуска, остановки, очистки и удаления программы;
- файлы с текстом Лицензионного соглашения на русском и английском языках;
- файлы с информацией о программе (Release Notes) на русском и английском языках;
- файл с информацией о стороннем коде legal_notices.txt на английском языке;
- файл со списком отозванных сертификатов.

После того как вы распаковали архив, в директории legal будут расположены текстовые файлы license_ru.txt и license_en.txt, с помощью которых вы можете ознакомиться с Лицензионным соглашением. В Лицензионном соглашении указано, на каких условиях вы можете пользоваться программой.

Аппаратные и программные требования

Аппаратные требования для каждого защищаемого объекта нужно уточнять с учетом применяемой модели, количества обрабатываемых тегов и событий, средней скорости получения данных (количества наблюдений в секунду) и объема хранимых данных. Чем больше объем обрабатываемых данных и сложность используемой ML-модели, тем больше аппаратных ресурсов потребуется для установки серверной части Kaspersky MLAD.

Требования к серверу Kaspersky MLAD

Для функционирования программы сервер Kaspersky MLAD должен удовлетворять следующим минимальным требованиям.

Список поддерживаемых процессоров:

- процессор Intel® Xeon® E3 v3, v4, v5, v6;
- процессор Intel Xeon E5 v3, v4;
- процессор Intel Xeon E7 v3, v4;
- масштабируемые процессоры Intel Xeon;
- масштабируемые процессоры Intel Xeon 2-го и 3-го поколения;
- процессор Intel Xeon E;
- процессор Intel Xeon W;
- процессор Intel Xeon D;
- процессор Intel Core™ i5, i7 4-го поколения и выше;
- процессор Intel Core i9;
- процессор Intel Core M.

Минимальные аппаратные требования:

- 16 ядер;
- 32 ГБ оперативной памяти;
- 1 ТБ свободного пространства на жестком диске (рекомендуется использовать SSD-диск).

  Если в Kaspersky MLAD будет поступать большой поток данных, требуется увеличить объем свободного пространства на жестком диске.

Вы можете установить Kaspersky MLAD на сервер с другим 64-битным процессором архитектуры x86 2013 года выпуска и позже. Процессор должен соответствовать вышеперечисленным минимальным аппаратным требованиям и поддерживать следующие расширения, необходимые для библиотеки TensorFlow™ 2.20:

- Advanced Vector Extensions (avx);
- Advanced Vector Extensions 2 (avx2).

Поддерживаемые операционные системы:

- Ubuntu 22.04 LTS и выше;
- Astra Linux Common Edition 2.12.46 и выше.

До развертывания Kaspersky MLAD должно быть установлено следующее программное обеспечение:

- docker 24.0.9 или выше;
- docker compose 2.12.2 или выше.

Устанавливать программное обеспечение Docker на сервер Kaspersky MLAD требуется с официального Docker-репозитория.

Требования к компьютеру пользователя

Для работы с веб-интерфейсом Kaspersky MLAD компьютер пользователя должен удовлетворять следующим минимальным требованиям:

- процессор Intel Core™ i5;
- 8 ГБ оперативной памяти;
- 64-битная операционная система;
- установленный браузер Google Chrome™ версии 135 и выше или браузер Microsoft Edge версии 130 и выше;
- минимальное разрешение экрана монитора для правильного отображения веб-интерфейса – 1600x900.

Рекомендации по обеспечению безопасной работы

Для обеспечения безопасной работы Kaspersky MLAD на предприятии рекомендуется ограничить и контролировать доступ к оборудованию, на котором работает программа.

Физическая безопасность оборудования

При внедрении Kaspersky MLAD рекомендуется принять следующие меры по обеспечению безопасной работы:

- Ограничить доступ в помещение, в котором расположен сервер с установленной программой Kaspersky MLAD, а также к сетевому оборудованию выделенной сети. Доступ в помещение должен предоставляться только доверенными лицами, например персоналу, обладающему полномочиями по установке и настройке программы.
- Обеспечить контроль физического доступа к оборудованию, на котором работает программа, с помощью технических средств или службы охраны.
- Проводить мониторинг доступа в контролируемые помещения с помощью средств охранной сигнализации.
- Осуществлять видеонаблюдение в контролируемых помещениях.

Параметры ML-модели напрямую влияют на обнаружение аномалий, и поэтому изменять их могут только системные администраторы и пользователи с правами из группы прав **Управление ML-моделями**. История изменений доступна только в журналах программы, которые хранятся ограниченное время.

При использовании веб-интерфейса рекомендуется принять следующие меры по обеспечению информационной безопасности интранет-системы:

- Обеспечить пользователям доступ к программе только через веб-интерфейс.
- Установить сертификаты на компьютеры пользователей для авторизации сервера Kaspersky MLAD с браузером. Для использования доверенного сертификата вам нужно обратиться к квалифицированному техническому специалисту Заказчика, сотруднику АО "Лаборатория Касперского" или сертифицированному интегратору.
- Обеспечить защиту трафика внутри интранет-системы.
- Обеспечить защиту подключений к внешним сетям.
- Использовать защищенное TLS-соединение для передачи данных.
- Изменить адрес электронной почты и пароль первого пользователя программы с ролью системного администратора при установке программы.
- Изменять пароль учетной записи в соответствии со сроком его действия. Срок действия пароля задается при настройке параметров безопасности программы. По умолчанию срок действия пароля составляет 180 дней.
- Для подключений через веб-интерфейс использовать пароли, которые соответствуют следующим требованиям:
  - Не совпадают с предыдущими паролями учетной записи. Количество ранее использованных паролей, с которыми новый пароль не должен совпадать, задается при настройке параметров безопасности программы. По умолчанию пароль не должен совпадать с пятью предыдущими паролями.
  - Содержат не менее восьми символов.
  - Содержат одну или несколько прописных букв латинского алфавита.
  - Содержат одну или несколько строчных букв латинского алфавита.
  - Содержат одну или несколько цифр.
  - Содержат один или несколько следующих специальных символов: `_ ! @ # $ % ^ & *`.
- Обеспечивать конфиденциальность и уникальность паролей. При угрозе компрометации пароля изменить пароль.
- Установить ограничение времени жизни веб-сессии пользователя.
- После окончания работы в браузере принудительно завершать сессию подключения к программе с помощью пункта **Выход** в веб-интерфейсе.

- Периодически выполнять установку обновлений для операционной системы на сервере, на котором развернут Kaspersky MLAD.
- Использовать разграничение прав доступа пользователей к функциям программы.

Безопасность данных

В процессе работы с Kaspersky MLAD рекомендуется принять следующие меры по обеспечению безопасности данных:

- Выполнить настройку операционной системы и обеспечить доступ к файлам сервера, на котором установлен Kaspersky MLAD, согласно *Рекомендациям по безопасной настройке операционных систем Linux*, предоставляемых Федеральной службой по техническому и экспортному контролю (ФСТЭК) России.
- Выполнять периодическое резервное копирование данных сервера с установленной программой Kaspersky MLAD согласно внутреннему регламенту компании.
- Выполнять периодический контроль работоспособности интерфейса и служб программы. Особое внимание нужно уделять службе уведомлений и системе ведения журналов.
- Выполнять проверку каналов связи на исправность и безопасность.
- Выполнять периодический контроль работоспособности сервера:
  - контроль дисков по SMART;
  - наличие достаточного свободного места и памяти;
  - загруженность оперативной памяти.
- Контролировать протоколы сервера на отсутствие проблем, используя систему мониторинга.
- Хранить чувствительные данные в надежном хранилище.

Устранение уязвимостей и установка критических обновлений

"Лаборатория Касперского" может выпускать обновления программы, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений поставляются и устанавливаются в рамках действующего *Договора об оказании технической поддержки*. Уведомления о выпуске критических обновлений рассылаются по адресам электронной почты, указанным в действующем *Договоре об оказании технической поддержки*.

Рекомендуется, чтобы сотрудник, ответственный за эксплуатацию программы, также периодически (не реже одного раза в три месяца) проверял отсутствие обнаруженных уязвимостей в программе, используя веб-сайт "Лаборатории Касперского".

Вы можете сообщить об обнаруженных недостатках безопасности или уязвимостях программы по адресу электронной почты vulnerability@kaspersky.com, зашифровав письмо с помощью PGP™-ключа. В письме предоставьте следующую информацию:

- Контактную информацию.
- Название продукта, его версию и тип операционной системы вашего устройства, на котором найдена уязвимость.
- Подробное описание уязвимости.
- Планируете ли вы распространять информацию об уязвимости третьей стороне.

> Не публикуйте информацию об уязвимости, пока она не исправлена специалистами "Лаборатории Касперского".

Разделение доступа к функциям программы

В Kaspersky MLAD вы можете разграничить доступ пользователей к функциям программы в зависимости от задач пользователей, используя роли. *Роль* – это набор прав доступа к функциям программы, который вы можете назначить пользователю.

В зависимости от назначенной роли пользователям могут быть доступны следующие функции Kaspersky MLAD:

Доступные функции программы

Функциональная область	Системный администратор	Пользовательская роль
Управление лицензионными ключами: • Добавление лицензионных ключей. • Удаление лицензионных ключей.	✓	–
Управление учетными записями пользователей: • Создание и изменение учетной записи пользователя. • Отзыв токенов аутентификации для учетной записи пользователя. • Просмотр прав для учетной записи пользователя.	✓	–
Управление ролями: • Создание и изменение роли. • Удаление роли. • Просмотр прав доступа для роли.	✓	–
Просмотр прав пользователей	✓	–
Управление уведомлениями: • Управление подписками на уведомления. • Работа с группами контактов. • Работа с дополнительными контактами.	✓	✓ (по назначению)
Настройка параметров Kaspersky MLAD (кроме настройки уровней критичности активов)	✓	–

Функциональная область	Системный администратор	Пользовательская роль
Управление активами и тегами: • Поиск и фильтрация активов и тегов. • Создание и изменение актива. • Создание тега и добавление тега в актив. • Изменение тега. • Перемещение активов и тегов. • Удаление актива или тега. • Проверка текущей структуры тегов. • Импорт и экспорт конфигурации активов. • Настройка уровней критичности активов.	✓	✓ (по назначению)
Управление ML-моделями: • Управление разметками. • Импорт ML-модели. • Активация импортированной ML-модели. • Создание ML-модели. • Изменение ML-модели. • Добавление и изменение предиктивного элемента ML-модели. • Добавление и изменение элемента ML-модели на основе эллиптического конверта. • Добавление и изменение элемента ML-модели на основе диагностического правила. • Удаление элемента ML-модели. • Копирование ML-модели. • Создание и изменение шаблона по ML-модели. • Создание ML-модели по шаблону. • Удаление шаблона ML-модели. • Обучение предиктивных элементов и элементов на основе эллиптического конверта. • Оценка результатов обучения. • Просмотр результатов обучения элементов ML-модели. • Подготовка ML-модели к публикации. • Публикация ML-модели. • Удаление ML-модели.	✓	✓ (по назначению)
Управление службами Kaspersky MLAD: • Просмотр статусов служб. • Запуск, остановка и перезапуск служб.	✓	✓ (по назначению)
Управление источниками данных: • Создание и изменение источников данных. • Копирование источников данных. • Подключение к источнику данных и отключение от него. • Удаление источника данных.	✓	–
Работа с журналами программы	✓	✓ (по назначению)

Всем пользователям программы доступны следующие права по умолчанию:

- Просмотр сводных данных в разделе **Информационная панель**.
- Просмотр первичных и рабочих данных по тегам в разделах **История** и **Мониторинг**.
- Просмотр значений технологических параметров, полученных от датчиков объекта мониторинга в один и тот же момент времени, в разделе **Временной срез**.

- Работа с событиями и паттернами:
  - Настройка параметров конфигурации внимания и отображения параметров событий.
  - Создание и удаление мониторов.
  - Просмотр истории событий и истории паттернов.
- Работа с инцидентами и группами инцидентов:
  - Просмотр инцидентов и групп инцидентов.
  - Добавление статуса, причины, экспертных рекомендаций и комментариев к инциденту или группе инцидентов.
  - Экспорт инцидентов в файл.
- Следующие действия в разделе **Модели**:
  - Поиск и фильтрация объектов в разделе **Модели**.
  - Запуск и остановка инференса ML-модели.
  - Оценка результатов исторического инференса ML-модели.
  - Просмотр графа потока данных ML-модели.
- Управление пресетами:
  - Просмотр пресетов.
  - Поиск и фильтрация объектов в разделе **Пресеты**.
  - Создание, изменение, удаление пресетов.
  - Загрузка конфигурации пресетов из файла.
  - Сохранение конфигурации пресетов в файл.
- Изменение собственного пароля.

Вы также можете создать роль с правом **Права на все действия**. Пользователям, которым будет присвоена эта роль, будут доступны функции системного администратора.

Вы можете просмотреть доступные роли пользователей и их права доступа к функциям программы в разделе **Роли** в меню администратора.

Вы можете просмотреть права доступа к функциям программы для определенных пользователей в разделе **Пользователи** в меню администратора.

Что нового

В Kaspersky Machine Learning for Anomaly Detection 6.0 появились следующие возможности и доработки:

- Конструктор моделей – добавлена функциональность, позволяющая использовать вычислимые теги в разметках и элементах ML-модели на основе диагностического правила. Добавлена функциональность, позволяющая выполнять инференс на исторических и поступающих данных одновременно. Добавлена функциональность, позволяющая выполнять полный и быстрый инференс на исторических данных. Добавлена функциональность оценки результатов обучения и инференса ML-модели. Оптимизирован выбор входных и выходных тегов для элементов ML-модели. Добавлена функциональность, позволяющая указывать приоритет инцидента для инцидентов, зарегистрированных элементом ML-модели.

- Источники данных – добавлена функциональность, позволяющая получать данные по протоколу OPC UA от нескольких источников данных одновременно. Для этого вместо коннектора OPC UA Connector используется новая служба Data Source Manager.

- Активы – добавлены параметры, позволяющие перед загрузкой конфигурации активов и тегов указать типы разделителей в числовых значениях и необходимость учета регистра в именах тегов. Добавлена функциональность, позволяющая указывать уровень критичности актива. Улучшено отображение дерева активов: добавлена функциональность, позволяющая просмотреть сведения об активах и тегах, добавлена функциональность, позволяющая выполнять поиск и фильтрацию по активам и тегам.

- Пресеты – добавлена функциональность, позволяющая размещать пресеты в дереве активов. Добавлена функциональность, позволяющая выполнять поиск и фильтрацию по пресетам.

- Разделы **Мониторинг** и **История** – добавлена функциональность, позволяющая объединять входные и выходные теги элемента ML-модели, а также теги разметки элемента в динамический пресет и отображать его данные на графиках.

- Лицензирование – расширены виды коммерческой лицензии.

- Установка и удаление программы – установка, обновление, резервное копирование, проверка целостности дистрибутива, запуск, остановка и удаление программы выполняются с помощью единой утилиты mladctl. С помощью утилиты mladctl также можно выполнять проверку версии и состояния программы и очистку программы, а также добавлять информацию о предыдущих установленных версиях программы.

- Уведомления – расширена функциональность подписок на уведомления об инцидентах. В веб-интерфейсе добавлена возможность создавать дополнительные контакты и группы контактов.

- Процессор событий – добавлена функциональность, позволяющая отслеживать необычные часы активности и признаки DNS-эксфильтрации. Оптимизирована скорость работы мониторов и голов внимания. Оптимизирована работа с постоянной историей событий и работа процессора событий в режиме сна.

- Разделение доступа к функциям программы – добавлены права на управление активами и тегами, управление разметками и управление уведомлениями.

- Приоритет инцидентов – добавлена функциональность, позволяющая управлять типовыми приоритетами инцидентов.

- Уровень критичности активов – добавлена функциональность, позволяющая управлять типовыми уровнями критичности активов.

- Служба Mail Notifier – добавлены новые параметры для настройки службы Mail Notifier.
- Служба Trainer – добавлены параметры для настройки службы Trainer.
- Коннектор HTTP Connector – добавлены новые параметры для настройки коннектора HTTP Connector.

Архитектура Kaspersky MLAD

Kaspersky MLAD устанавливается на сервере, который соответствует аппаратным и программным требованиям. Сервер Kaspersky MLAD осуществляет функции централизованного хранения информации о службах и коннекторах программы и предоставляет единый пользовательский веб-интерфейс для управлениями ими.

Отдельный доступ к контейнерам установленных служб Kaspersky MLAD невозможен.

При установке Kaspersky MLAD все службы и коннекторы программы размещаются на одном сервере и взаимодействуют друг с другом через внутреннюю виртуальную сеть, изолированную от внешних систем.

Kaspersky MLAD включает в себя специально подготовленные ML-модели, а также следующие службы и коннекторы:

ML-модель

ML-модель – это модель, которая создается для конкретного объекта защиты на основе алгоритмов машинного обучения, диагностических правил и/или эллиптических конвертов с использованием данных телеметрии этого объекта. ML-модель обеспечивает обнаружение аномалий.

ML-модель может быть создана с помощью конструктора моделей или предоставлена в рамках *Услуги построения модели и внедрения Kaspersky MLAD*.

Службы Kaspersky MLAD

Службы Kaspersky MLAD – это набор основных служб программы, который поставляется на каждый объект мониторинга. Kaspersky MLAD включает в себя следующие службы:

- *Anomaly Detector*. Обнаруживает аномалии на основе обработки данных с помощью ML-модели.
- *Event Processor*. Выявляет паттерны и аномальные последовательности событий, используя методы машинного обучения на основе нейросемантической сети.
- *Stream Processor*. Обрабатывает данные телеметрии, поступающие от объекта мониторинга в произвольные моменты реального времени, и приводит их к равноинтервальной временной сетке.
- *Data Source Manager*. Обеспечивает получение данных от нескольких источников одновременно. Поддерживает получение данных по протоколу, который описан спецификацией OPC Unified Architecture (Унифицированная архитектура OPC).
- *Trainer*. Выполняет обучение ML-модели на основе данных телеметрии, полученных Kaspersky MLAD для конкретного объекта мониторинга.
- *Similar Anomaly*. Выявляет и группирует схожие инциденты.
- *Message Broker*. Выполняет обмен данными между службами Kaspersky MLAD.
- *Time Series Database*. Осуществляет хранение временных рядов наблюдаемых значений тегов, артефактов, связанных с тегами, и артефактов элементов ML-моделей.

- *Keeper*. Осуществляет маршрутизацию данных телеметрии, которые подлежат сохранению в базе данных.
- *Database*. Используется для хранения всех конфигурационных параметров работы Kaspersky MLAD.
- *API Server*. Обеспечивает работу внутренних интерфейсов Kaspersky MLAD.
- *Web Server*. Обеспечивает работу веб-интерфейса Kaspersky MLAD.
- *Logger*. Осуществляет хранение функциональных журналов работы Kaspersky MLAD.
- *Mail Notifier*. Выполняет рассылку по электронной почте уведомлений о регистрации инцидентов.
- *Docker API Server*. Обеспечивает взаимодействие между собой Docker-контейнеров, которые лежат в основе служб Kaspersky MLAD.
- *Migrations*. Обновляет сведения о параметрах работы Kaspersky MLAD в базе данных Database.
- *Push Server*. Обеспечивает обмен push-сообщениями между компонентами Kaspersky MLAD.

Коннекторы

Коннекторы – это службы, которые обеспечивают обмен данными с внешними системами. Для каждого объекта защиты требуется выбрать один из следующих коннекторов:

- *KICS Connector*. Обеспечивает взаимодействие с Kaspersky Industrial CyberSecurity for Networks версии 4.0 и выше.
- *CEF Connector*. Обеспечивает получение событий от внешних источников (промышленного интернета вещей, сетевых устройств и приложений) и отправку обратно сообщений в формате CEF (Common Event Format), зарегистрированных мониторами анализа событий.
- *MQTT Connector*. Обеспечивает получение тегов от систем АСУ ТП и отправку сообщений о возникновении инцидентов по протоколу MQTT (Message Queuing Telemetry Transport).
- *AMQP Connector*. Обеспечивает получение тегов от систем АСУ ТП и отправку сообщений о возникновении инцидентов по протоколу AMQP (Advanced Message Queuing Protocol).
- *WebSocket Connector*. Обеспечивает получение тегов от систем АСУ ТП и отправку сообщений о возникновении инцидентов по протоколу WebSocket.
- *HTTP Connector*. Обеспечивает получение данных телеметрии от систем АСУ ТП в виде CSV-файлов через POST-запросы по протоколу HTTP или HTTPS.

На рисунке ниже представлена схема взаимодействия служб Kaspersky MLAD.

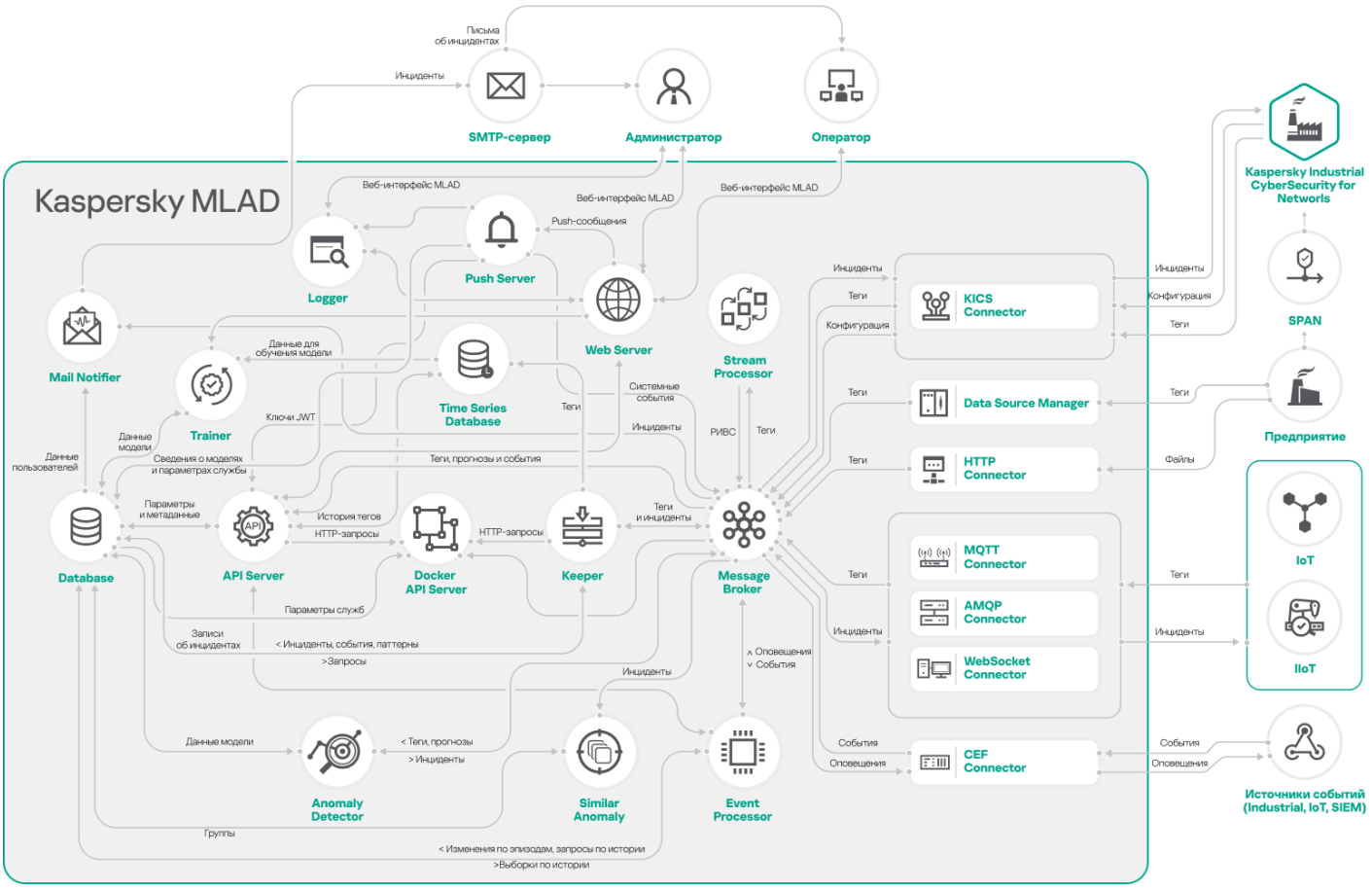


Схема взаимодействия служб Kaspersky MLAD

Типовые схемы развертывания

Этот раздел содержит описание стандартных схем развертывания Kaspersky MLAD в сети объекта мониторинга, а также описание особенностей интеграции Kaspersky MLAD с другими программами.

Kaspersky MLAD поддерживает следующие варианты установки:

- Одиночная установка.
- Установка с Kaspersky Industrial CyberSecurity for Networks версии 4.0 и выше.

Одиночная установка Kaspersky MLAD

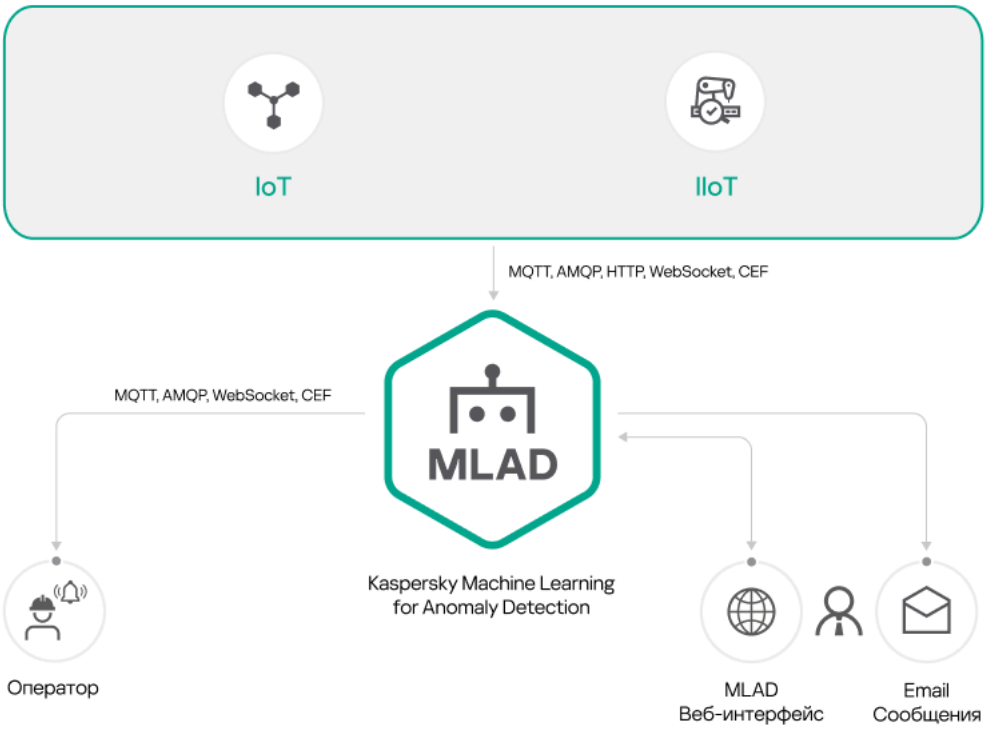
Вы можете установить только Kaspersky MLAD, если планируете использовать в качестве поставщика данных источники данных OPC UA или следующие коннекторы:

- MQTT Connector;
- AMQP Connector;
- CEF Connector;
- WebSocket Connector;
- HTTP Connector.

На рисунках ниже представлены примеры схем одиночной установки Kaspersky MLAD с использованием источников данных и перечисленных выше коннекторов. Вы можете использовать любые конфигурации источников данных и коннекторов, которые подходят для вашего объекта мониторинга.



Одиночная установка Kaspersky MLAD с использованием источников данных OPC UA и коннекторов: MQTT Connector, AMQP Connector, HTTP Connector, WebSocket Connector, CEF Connector



Одиночная установка Kaspersky MLAD с использованием коннекторов: MQTT Connector, AMQP Connector, HTTP Connector, WebSocket Connector, CEF Connector

Установка Kaspersky MLAD с Kaspersky Industrial CyberSecurity for Networks

Вы можете установить Kaspersky MLAD и Kaspersky Industrial CyberSecurity for Networks, если планируете использовать в качестве поставщика данных Kaspersky Industrial CyberSecurity for Networks (см. рисунок ниже).

Kaspersky Machine Learning for Anomaly Detection совместим с Kaspersky Industrial CyberSecurity for Networks версии 4.0 и выше.



Установка Kaspersky MLAD с Kaspersky Industrial CyberSecurity for Networks

Если вы хотите использовать этот вариант установки, сначала требуется установить Kaspersky Industrial CyberSecurity for Networks и добавить коннектор типа **Generic**. Для добавленного коннектора требуется создать файл свертки и указать в нем параметры подключения Kaspersky Industrial CyberSecurity for Networks к Kaspersky MLAD. Полученный файл свертки вам нужно загрузить в Kaspersky MLAD при настройке коннектора KICS Connector. Подробную информацию о создании и добавлении коннектора вы можете получить в разделе *Добавление коннектора* в *справке Kaspersky Industrial CyberSecurity for Networks*.

Компьютеры, на которых установлены Kaspersky MLAD и Kaspersky Industrial CyberSecurity for Networks, должны находиться в одной сети.

Схема потока данных телеметрии и событий

В Kaspersky MLAD обмен данными с внешними системами обеспечивается за счет коннекторов и источников данных. Для получения данных телеметрии (тегов) и/или событий от внешних систем требуется настроить коннекторы HTTP Connector, MQTT Connector, AMQP Connector, KICS Connector, CEF Connector и WebSocket Connector и создать карточки источников данных OPC UA.

Если в программе настроена передача событий и инцидентов в сторонние системы, программа отправляет зарегистрированные события и инциденты в сторонние системы по выбору системного администратора. Системный администратор программы самостоятельно выбирает сторонние системы и типы событий и инцидентов для передачи в сторонние системы. Обработка и сохранение полученных данных в сторонней системе выполняется в соответствии с ее функциональностью и назначением.

Данные телеметрии объекта мониторинга проходят первичную обработку в службе Stream Processor, которая приводит полученные теги к равноинтервальной временной сетке. При обнаружении нарушений потока данных телеметрии, а также наблюдений, поступивших в Kaspersky MLAD слишком рано или поздно, служба Stream Processor регистрирует инциденты.

Служба Stream Processor передает данные, приведенные к РИВС, в ML-модель службы Anomaly Detector. Если при обработке полученных данных элементы ML-моделей обнаруживают отклонения от нормального поведения объекта мониторинга, то служба Anomaly Detector регистрирует инциденты. Обнаруженные инциденты могут быть сгруппированы вручную или автоматически с помощью службы Similar Anomaly.

Вы можете просмотреть зарегистрированные инциденты и группы инцидентов в разделе **Инциденты**. Kaspersky MLAD также отправляет уведомления об инцидентах на адреса электронной почты контактов, указанных в подписках, и/или во внешние системы с помощью коннекторов.

События, поступившие в Kaspersky MLAD, проходят обработку в службе Event Processor. В качестве событий процессор событий также может обрабатывать инциденты, зарегистрированные службой Anomaly Detector. Процессор событий выявляет в потоке событий закономерности в виде повторяющихся событий и паттернов, новые и обобщенные события и паттерны, а также необычные часы активности и признаки DNS-эксфильтрации. При активации мониторов служба Event Processor также отправляет оповещения в соответствии с заданными критериями мониторинга во внешние системы с помощью коннектора CEF Connector. Вы также можете просмотреть информацию о событиях, паттернах и мониторах в разделе **Процессор событий**.

На рисунке ниже показан поток данных телеметрии и событий в Kaspersky MLAD.



Поток данных телеметрии и событий в Kaspersky MLAD

Порты, используемые Kaspersky MLAD

В таблице ниже перечислены порты, которые должны быть открыты на серверах, на которых установлен Kaspersky MLAD.

Порт	Протокол	Описание
443	TCP (HTTPS)	Используется для подключения к веб-интерфейсу Kaspersky MLAD.
3001	TCP (HTTPS)	Используется для подключения к системе ведения журналов (Grafana™).
4999	TCP (HTTP или HTTPS)	Используется для загрузки коннектором HTTP Connector CSV-файлов из внешних источников.
5518	TCP	Используется для подключения внешних источников событий к коннектору CEF Connector по умолчанию. Номер порта задается в конфигурационном файле .env.

Установка и удаление программы

Этот раздел содержит пошаговые инструкции по установке и удалению Kaspersky MLAD.

Подготовка к установке программы

Перед началом установки программы убедитесь, что сервер Kaspersky MLAD и программное обеспечение соответствуют аппаратным и программным требованиям. Также убедитесь, что соблюдаются рекомендации по обеспечению безопасной работы в отношении оборудования, аппаратного и программного обеспечения компьютеров, которые будут использоваться для подключения к веб-интерфейсу Kaspersky MLAD.

> Установка и использование Kaspersky MLAD возможны только на одном сервере. Установка и использование разных служб и коннекторов на нескольких серверах невозможны. Отдельный доступ к контейнерам установленных служб Kaspersky MLAD невозможен.

Перед установкой необходимо убедиться в наличии требуемого объема свободного места на жестком диске, на котором будет установлена программа. Если в разделе диска, в котором по умолчанию хранятся тома Docker, недостаточно места, их необходимо перенести в другой раздел диска, где места достаточно. Для этого необходимо указать путь к месту хранения томов в конфигурационном файле Docker.

Учетная запись пользователя в операционной системе сервера Kaspersky MLAD, от имени которого будет выполняться установка программы, должна обладать root-правами. Вы можете добавить нужную учетную запись с помощью стандартных средств операционной системы.

Установка программы, а также проверка целостности дистрибутива, обновление, резервное копирование, восстановление, запуск, остановка, очистка и удаление программы выполняются с помощью утилиты mladtctl, входящей в комплект поставки. Если требуется отобразить краткое описание функциональности утилиты, в командной строке выполните команду `mladctl help`. Если требуется отобразить информацию о версии утилиты, в командной строке выполните команду `mladctl version`.

Проверка целостности файлов архива Kaspersky MLAD

Проверка цифровой подписи и целостности файлов архива программы выполняется автоматически перед установкой или обновлением Kaspersky MLAD. Проверка целостности выполняется, чтобы убедиться, что дистрибутив выпущен "Лабораторией Касперского" и не был изменен после поставки или подменен в процессе поставки.

При необходимости, например, если требуется проверить дистрибутив, с помощью которого будет выполняться обновление программы, вы можете вручную проверить целостность файлов архива с помощью команды `checkintegrity` утилиты mladctl. В процессе работы утилита последовательно проверяет контрольные суммы файлов из архива программы.

Чтобы проверить целостность файлов архива Kaspersky MLAD:

1. Распакуйте архив Kaspersky_MLAD_6.0.0.<номер сборки>_ru-RU_en-US.tar.xz, входящий в состав комплекта поставки:

   `tar xf Kaspersky_MLAD_6.0.0.<номер сборки>_ru-RU_en-US.tar.xz`

   После распаковки архива появится директория mlad-release-6.0.0-<номер сборки>.

2. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

3. Выполните команду:

   `mladctl checkintegrity -f <полный путь к дистрибутиву программы>`

   где `-f <полный путь к дистрибутиву программы>` означает, что будет выполнена проверка целостности файлов дистрибутива в указанной директории.

Результаты проверки целостности файлов архива программы на компьютере признаются успешными, если утилита mladctl завершила работу с сообщением `SUCCEEDED`.

Установка программы

Этот раздел содержит пошаговое описание установки Kaspersky MLAD. Установка программы выполняется с помощью команды `install` утилиты mladctl.

Перед установкой программы требуется выполнить действия для подготовки к установке программы.

Установку Kaspersky MLAD выполняет квалифицированный технический специалист Заказчика, сотрудник "Лаборатории Касперского" или сертифицированный интегратор.
Установка Kaspersky MLAD выполняется в соответствии с описанной процедурой установки программы.
Установка Kaspersky MLAD будет прервана, если цифровая подпись дистрибутива не принадлежит "Лаборатории Касперского" или целостность архива программы нарушена (были изменены файлы или состав файлов). Для получения корректного архива программы обратитесь к специалистам "Лаборатории Касперского".

При установке Kaspersky MLAD создает первого пользователя программы с ролью системного администратора.

Чтобы установить Kaspersky MLAD:

1. Распакуйте архив Kaspersky_MLAD_6.0.0.<номер сборки>_ru-RU_en-US.tar.xz, входящий в состав комплекта поставки:

   `tar xf Kaspersky_MLAD_6.0.0.<номер сборки>_ru-RU_en-US.tar.xz`

   После распаковки архива появится директория mlad-release-6.0.0-<номер сборки>.

2. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

3. Перейдите в директорию mlad-release-6.0.0-<номер сборки>:

   `cd mlad-release-6.0.0-<номер сборки>`

4. Выполните команду:

   ```
   ./mladctl install
   ```

   Если требуется, вы можете выполнить команду установки программы со следующими ключами:

   - `--nointegrity` – выключает проверку целостности файлов архива программы при ее установке.
   - `--autostart` – автоматически запускает Kaspersky MLAD после установки.
   - `-f <полный путь к директории для установки программы>` – устанавливает программу в указанную директорию. Если при выполнении команды вы не использовали этот ключ, вы можете выбрать существующую пустую директорию во время установки программы.

     > Директория, выбранная для установки Kaspersky MLAD должна быть пустой или отсутствовать (директория будет автоматически создана в процессе установки программы).
     > При указании имени директории для установки программы используйте строчные буквы латинского алфавита, цифры и нижнее подчеркивание.

   - `-d <полный путь к дистрибутиву программы>` – устанавливает сборку программы из дистрибутива в указанной директории. Если при выполнении команды вы не использовали этот ключ, вы можете выбрать директорию с дистрибутивом во время установки программы.

5. Следуйте указаниям утилиты.

   Во время установки внимательно прочитайте Лицензионное соглашение. Согласие с условиями Лицензионного соглашения является обязательным условием для установки программы. Если вы не принимаете условия Лицензионного соглашения, установка программы будет прервана.

   Во время установки программы вы можете изменить адрес электронной почты и пароль первого пользователя программы с ролью системного администратора.

   По умолчанию программа устанавливается в директорию по умолчанию /opt/kaspersky/mlad. Во время установки вы можете указать другую директорию для установки Kaspersky MLAD.

Чтобы установить Kaspersky MLAD в неинтерактивном режиме:

1. Распакуйте архив Kaspersky_MLAD_6.0.0.<номер сборки>_ru-RU_en-US.tar.xz, входящий в состав комплекта поставки:

   `tar xf Kaspersky_MLAD_6.0.0.<номер сборки>_ru-RU_en-US.tar.xz`

2. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

3. Выполните команду:

   `mladctl install -q -e accept -f <полный путь к директории для установки программы> -d <полный путь к дистрибутиву программы>`

   где:

   `-q` означает, что программа будет установлена в неинтерактивном режиме. При установке программы в неинтерактивном режиме Kaspersky MLAD создает первого пользователя программы с ролью системного администратора и задает ему адрес электронной почты и пароль по умолчанию. Для получения адреса электронной почты и пароля пользователя, используемых по умолчанию, обратитесь к квалифицированному техническому специалисту Заказчика, сотруднику "Лаборатории Касперского" или сертифицированному интегратору.

   `-e accept` означает, что вы принимаете условия Лицензионного соглашения. Согласие с условиями Лицензионного соглашения является обязательным условием для установки программы. Если вы не указываете ключ `-e accept`, установка программы будет прервана.

   Прочитать текст Лицензионного соглашения можно в текстовых файлах license_ru.txt и license_en.txt, которые расположены в директории legal.

   `-f <полный путь к директории для установки программы>` означает, что программа будет установлена в указанную директорию. Если вы не указываете ключ `-f`, программа будет установлена в директорию по умолчанию /opt/kaspersky/mlad, которая если уже существует, должна быть пустой.

   > Директория, выбранная для установки Kaspersky MLAD должна быть пустой или отсутствовать (директория будет автоматически создана в процессе установки программы).
   > При указании имени директории для установки программы используйте строчные буквы латинского алфавита, цифры и нижнее подчеркивание.

   `-d <полный путь к дистрибутиву программы>` означает, что будет установлена сборка программы из дистрибутива, находящегося в указанной директории.

   Если требуется, вы можете выполнить команду установки программы со следующими ключами:

   - `--nointegrity` – выключает проверку целостности файлов архива программы при ее установке.
   - `--autostart` – автоматически запускает Kaspersky MLAD после установки.

Программа будет установлена на сервер. Если при запуске утилиты вы не указали ключ `--autostart`, запустите программу после ее установки.

До добавления лицензионного ключа часть функциональности будет недоступна.

Обновление программы

Обновление программы выполняется с помощью команды обновления `upgrade` утилиты mladctl. При обновлении Kaspersky MLAD будут сохранены все данные, загруженные, полученные и обработанные предыдущей версией Kaspersky MLAD: конфигурации тегов, пресеты, ML-модели и параметры Kaspersky MLAD.

Если требуется, при обновлении программы вы можете создать резервную копию предыдущей версии.

Перед началом обновления убедитесь, что на жестком диске имеется свободное место:

- Если обновление программы выполняется без выполнения резервного копирования, на жестком диске имеется свободное место в объеме, необходимом для установки Kaspersky MLAD.
- Если с обновлением программы одновременно выполняется резервное копирование и резервная копия сохраняется на том же диске, на этом диске имеется не менее 50% свободного места от общего объема жесткого диска.
- Если с обновлением программы одновременно выполняется резервное копирование и резервная копия сохраняется на другом диске, на диске для установки программы имеется свободное пространство в объеме, необходимом для установки Kaspersky MLAD, а на диске для хранения резервной копии имеется свободное пространство не менее объема занятого пространства на диске, на котором установлена программа.

Обновление Kaspersky MLAD возможно, начиная с версии программы 5.0.0-001. Перед обновлением программы, версия которой меньше 6.0.0-001, на версию 6.0.0-001 и выше необходимо добавить информацию о такой сборке программы в конфигурационный файл утилиты mladctl.

Во время обновления программа будет выключена. В Kaspersky MLAD не будут поступать данные и не будет выполняться их обработка.

Сервер Kaspersky MLAD и программное обеспечение, установленное на сервере, должны соответствовать аппаратным и программным требованиям.

Обновление Kaspersky MLAD выполняется для устранения недостатков безопасности и уязвимостей программы или при выпуске новых версий программы в рамках действующего *Договора об оказании технической поддержки*. Обновление программы выполняет квалифицированный технический специалист Заказчика, сотрудник "Лаборатории Касперского" или сертифицированный интегратор.

Обновление Kaspersky MLAD будет прервано, если цифровая подпись дистрибутива не принадлежит "Лаборатории Касперского" или целостность архива программы нарушена (были изменены файлы или состав файлов). Для получения корректного архива программы обратитесь к специалистам "Лаборатории Касперского".

Чтобы обновить Kaspersky MLAD:

1. Распакуйте архив mlad-6.0.0-<номер новой сборки>.tar.xz, входящий в состав комплекта поставки:

   `tar xf mlad-6.0.0-<номер новой сборки>.tar.xz`

2. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

3. Выполните обновление программы одним из следующих способов:

   - Если требуется выполнить резервное копирование предыдущей версии и сохранить резервную копию в директорию, в которой установлен Kaspersky MLAD, выполните команду:

     `mladctl upgrade`

     Резервная копия будет создана в директории с именем `mlad_backup-<номер версии>-<номер сборки>`. Директория будет создана внутри директории, в которой установлена программа.

   - Если требуется выполнить резервное копирование предыдущей версии и сохранить резервную копию в другой директории, выполните команду:

     `mladctl upgrade -b <полный путь к директории для хранения резервной копии>`

   - Если не требуется выполнять резервное копирование при обновлении программы, выполните команду:

     `mladctl upgrade --nobackup`

   При необходимости вы можете выполнить любую из вышеперечисленных команд со следующими ключами:

   - `--nointegrity` – выключает проверку целостности файлов архива программы при ее обновлении.
   - `--autostart` – автоматически запускает Kaspersky MLAD после обновления программы.
   - `-f <полный путь к директории, в которой установлена программа>` – обновляет программу, установленную в указанной директории. Если при выполнении команды вы не использовали этот ключ, вы можете выбрать директорию во время обновления программы.
   - `-d <полный путь к дистрибутиву с новой сборкой программы>` – устанавливает сборку из дистрибутива в указанной директории. Если при выполнении команды вы не использовали этот ключ, вы можете выбрать директорию с новой сборкой программы во время обновления программы.

4. Следуйте указаниям утилиты.

   Во время обновления программы примите условия Лицензионного соглашения. Согласие с условиями Лицензионного соглашения является обязательным условием для обновления программы. Если вы не принимаете условия Лицензионного соглашения, обновление программы будет прервано.

   Прочитать текст Лицензионного соглашения можно в текстовых файлах license_ru.txt и license_en.txt, которые расположены в директории legal.

Чтобы обновить Kaspersky MLAD в неинтерактивном режиме:

1. Распакуйте архив mlad-6.0.0-<номер новой сборки>.tar.xz, входящий в состав комплекта поставки:

   `tar xf mlad-6.0.0-<номер новой сборки>.tar.xz`

2. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

3. Выполните обновление программы одним из следующих способов:

   - Если требуется выполнить резервное копирование предыдущей версии и сохранить резервную копию в директории, в которой установлен Kaspersky MLAD, выполните команду:

     `mladctl upgrade -q -e accept -f <полный путь к директории, в которой установлена программа> -d <полный путь к новой сборке программы>`

     Резервная копия будет создана в директории с именем `mlad_backup-<номер версии>-<номер сборки>`. Директория будет создана внутри директории, в которой установлена программа.

   - Если требуется выполнить резервное копирование предыдущей версии и сохранить резервную копию в другой директории, выполните команду:

     `mladctl upgrade -q -e accept -b <полный путь к директории для хранения резервной копии> -f <полный путь к директории, в которой установлена программа> -d <полный путь к новой сборке программы>`

   - Если не требуется выполнять резервное копирование при обновлении программы, выполните команду:

     `mladctl upgrade -q -e accept --nobackup -f <полный путь к директории, в которой установлена программа> -d <полный путь к новой сборке программы>`

   где:

   `-q` означает, что программа будет обновлена в неинтерактивном режиме.

   `-e accept` означает, что вы принимаете условия Лицензионного соглашения. Согласие с условиями Лицензионного соглашения является обязательным условием для обновления программы. Если вы не указываете ключ `-e accept`, обновление программы будет прервано.

   Прочитать текст Лицензионного соглашения можно в текстовых файлах license_ru.txt и license_en.txt, которые расположены в директории legal.

   `-b <полный путь к директории для хранения резервной копии>` означает, что Kaspersky MLAD выполнит резервное копирование текущей версии программы и сохранит резервную копию в указанную директории.

   `--nobackup` означает, что Kaspersky MLAD выполнит обновление программы без резервного копирования текущей версии программы.

   `-f <полный путь к директории, в которой установлена программа>` означает, что будет обновлена программа, установленная в указанной директории.

   `-d <полный путь к дистрибутиву с новой сборкой программы>` означает, что будет выполнено обновление программы до сборки из указанной директории.

   При необходимости вы можете выполнить любую из вышеперечисленных команд со следующими ключами:

   - `--nointegrity`, если требуется выключить проверку целостности файлов архива программы при ее обновлении.

   - `--autostart`, если требуется автоматически запустить Kaspersky MLAD после обновления программы.

Kaspersky MLAD будет обновлен до версии, указанной в номере сборки. Все файлы программы будут расположены в директории, в которой установлен Kaspersky MLAD (по умолчанию – /opt/kaspersky/mlad).

Проверка версии и состояния программы

С помощью утилиты mladctl вы можете получить сведения о версии программы, объеме оперативной памяти, свободных объемах оперативной памяти и памяти в директориях томов (volumes) Docker, а также сведения о состоянии программы и контейнеров Docker.

Чтобы проверить состояние программы:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.
2. Выполните команду:

   ```
   mladctl status
   ```

   Отобразится информация о версии и состоянии программы.

Резервное копирование программы

Вы можете выполнять резервное копирование программы в соответствии с регламентом вашего предприятия. Если требуется, вы можете создать резервную копию Kaspersky MLAD при обновлении программы.

Резервное копирование программы выполняется с помощью команды `backup` утилиты mladctl. При резервном копировании Kaspersky MLAD будут сохранены все данные, загруженные, полученные и обработанные Kaspersky MLAD: конфигурации тегов, пресеты, ML-модели и параметры Kaspersky MLAD.

Перед началом резервного копирования необходимо убедиться, что на разделе диска свободно не менее 50% объема диска при сохранении резервной копии на жесткий диск, на котором установлена программа. Если резервная копия сохраняется на другой диск, необходимо убедиться, что на этом диске имеется свободное место в объеме, необходимом для установки Kaspersky MLAD.

Чтобы выполнить резервное копирование Kaspersky MLAD:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

2. Выполните резервное копирование программы одним из следующих способов:

   - Если требуется сохранить резервную копию в директории, в которой установлена программа, выполните команду:

     `mladctl backup`

     Резервная копия будет создана в директории с именем `mlad_backup-<номер версии>-<номер сборки>`. Директория будет создана внутри директории, в которой установлена программа.

   - Если требуется сохранить резервную копию в другую директорию, выполните команду:

     `mladctl backup -b <полный путь к директории для хранения резервной копии>`

   Если требуется, вы можете выполнить любую из вышеперечисленных команд со следующими ключами:

   - `--autostart` – автоматически запускает Kaspersky MLAD после резервного копирования программы.

   - `-f <полный путь к директории, в которой установлена программа>` – выполняет резервное копирование программы, установленной в указанной директории. Если при выполнении команды вы не использовали этот ключ, вы можете выбрать директорию во время резервного копирования программы.

3. Следуйте указаниям утилиты.

Чтобы выполнить резервное копирование Kaspersky MLAD в неинтерактивном режиме:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

2. Выполните резервное копирование программы одним из следующих способов:

   - Если требуется сохранить резервную копию в директории, в которой установлена программа, выполните команду:

     `mladctl backup -q -f <полный путь к директории, в которой установлена программа>`

     Резервная копия будет создана в директории с именем `mlad_backup-<номер версии>-<номер сборки>`. Директория будет создана внутри директории, в которой установлена программа.

   - Если требуется сохранить резервную копию в другую директорию, выполните команду:

     `mladctl backup -q -b <полный путь к директории для хранения резервной копии> -f <полный путь к директории, в которой установлена программа>`

   где:

   `-q` означает, что резервное копирование программы будет выполнено в неинтерактивном режиме.

   `-b <полный путь к директории для хранения резервной копии>` означает, что Kaspersky MLAD сохранит резервную копию в указанной директории.

   `-f <полный путь к директории, в которой установлена программа>` означает, что будет выполнено резервное копирование программы, установленной в указанной директории.

   Если требуется автоматически запустить Kaspersky MLAD после резервного копирования программы, вы можете выполнить любую из вышеперечисленных команд с ключом `--autostart`.

Откат программы к предыдущей установленной версии

Откат программы к предыдущей установленной версии выполняется с помощью команды `restore` утилиты mladctl.

Откат Kaspersky MLAD возможен, начиная с версии программы 5.0.0-001. Перед откатом программы к версии меньше 6.0.0-001 необходимо добавить информацию о сборке, к которой будет выполнен откат, в конфигурационный файл утилиты mladctl.

Во время выполнения отката к предыдущей версии программа будет выключена. В Kaspersky MLAD не будут поступать данные и не будет выполняться их обработка.

В результате выполнения отката Kaspersky MLAD к предыдущей установленной версии будут потеряны все данные, полученные и обработанные Kaspersky MLAD с момента обновления программы до момента отката к предыдущей версии. Рекомендуется проверить наличие полной резервной копии всех данных Kaspersky MLAD.

Чтобы откатить Kaspersky MLAD к предыдущей установленной версии:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.
2. Выполните команду:

   ```
   mladctl restore
   ```

   Если требуется, вы можете выполнить команду со следующими ключами:

   - `--autostart` – автоматически запускает Kaspersky MLAD после отката программы.
   - `-b <полный путь к резервной копии программы>` – выполняет откат программы к версии из указанной резервной копии. Если при выполнении команды вы не использовали этот ключ, вы можете выбрать директорию с резервной копией программы во время восстановления программы.
   - `-f <полный путь к директории, в которую требуется установить программу>` – устанавливает программу из резервной копии в указанную директорию. Если при выполнении команды вы не использовали этот ключ, вы можете выбрать директорию для установки программы во время восстановления программы.

     При указании имени директории для установки программы используйте строчные буквы латинского алфавита, цифры и нижнее подчеркивание.

3. Следуйте указаниям утилиты.

Будет выполнен откат Kaspersky MLAD к предыдущей установленной версии.

Чтобы откатить Kaspersky MLAD к предыдущей установленной версии в неинтерактивном режиме:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

2. Выполните команду:

   `mladctl restore -q -b <полный путь к резервной копии программы> -f <полный путь к директории, в которую требуется установить программу>`

   где:

   `-q` означает, что откат программы к предыдущей установленной версии будет выполнен в неинтерактивном режиме.

   `-b <полный путь к резервной копии программы>` означает, что будет выполнен откат программы к версии из указанной резервной копии.

   `-f <полный путь к директории, в которую требуется установить программу>` означает, что версия программы из резервной копии будет установлена в указанную директорию.

   > При указании имени директории для установки программы используйте строчные буквы латинского алфавита, цифры и нижнее подчеркивание.

   Если требуется автоматически запустить Kaspersky MLAD после отката программы, выполните команду с ключом `--autostart`.

Сценарий восстановления Kaspersky MLAD из резервной копии

При необходимости, например, в случае неисправности сервера, на котором установлен Kaspersky MLAD, вы можете восстановить программу из резервной копии Kaspersky MLAD с помощью команды `restore` утилиты mladctl.

Сценарий восстановления программы из ее резервной копии состоит из следующих этапов:

1. **Перенос резервной копии программы на сервер Kaspersky MLAD**

   Скопируйте директорию с резервной копией программы на сервер, на котором выполняется восстановления программы.

2. **Восстановление Kaspersky MLAD**

   Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

   Для восстановления программы из резервной копии выполните команду `restore` утилиты mladctl:

   `mladctl restore`

   Если требуется, вы можете выполнить команду со следующими ключами:

   - `--autostart` – автоматически запускает Kaspersky MLAD после восстановления программы.
   - `-b <полный путь к резервной копии программы>` – выполняет восстановление программы из указанной резервной копии. Если при выполнении команды вы не использовали этот ключ, вы можете выбрать директорию с резервной копией программы во время восстановления программы.

- `-f <полный путь к директории, в которую требуется установить программу>` – устанавливает программу из резервной копии в указанную директорию. Если при выполнении команды вы не использовали этот ключ, вы можете выбрать существующую пустую директорию для установки программы во время восстановления программы.

  > Директория, выбранная для установки Kaspersky MLAD должна быть пустой или отсутствовать (директория будет автоматически создана в процессе установки программы).
  > При указании имени директории для установки программы используйте строчные буквы латинского алфавита, цифры и нижнее подчеркивание.

Следуйте указаниям утилиты.

Добавление информации о предыдущей установленной версии программы

Перед обновлением программы, версия которой меньше 6.0.0-001, на версию 6.0.0-001 и выше необходимо добавить информацию о такой сборке программы в конфигурационный файл утилиты mladctl.

Чтобы добавить информацию о предыдущей установленной версии программы:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.
2. Выполните команду:

   `mladctl add -f <полный путь к директории, в которой установлена программа>`

   где `-f <полный путь к директории, в которой установлена программа>` означает, что в конфигурационный файл утилиты будет добавлена информация о программе, установленной в указанной директории.

Очистка программы

При необходимости вы можете удалить параметры и данные из программы, сбросив программу до состояния только что установленной.

Очистка программы выполняется с помощью команды `clean` утилиты mladctl.

> В результате очистки Kaspersky MLAD будут потеряны все данные Kaspersky MLAD, полученные, загруженные и обработанные с момента установки программы, а также все созданные активы, ML-модели и пресеты и заданные параметры программы. Если эти данные и параметры вам еще раз понадобятся в будущем, сделайте резервную копию Kaspersky MLAD или убедитесь в ее наличии. Вы можете выполнить резервное копирование при обновлении программы или с помощью команды `backup` утилиты mladctl.

Чтобы очистить программу:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

2. Выполните команду:

   `sudo mladctl clean`

   Если требуется, вы можете выполнить команду с ключом `-f <полный путь к директории, в которой установлена программа>`. Если при выполнении команды вы не использовали этот ключ, вы можете выбрать директорию во время очистки программы.

3. Следуйте указаниям утилиты.

Чтобы очистить программу в неинтерактивном режиме:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

2. Выполните команду:

   `sudo mladctl clean -q -f <полный путь к директории, в которой установлена программа>`

   где:

   `-q` означает, что очистка программы будет выполнена в неинтерактивном режиме.

   `-f <полный путь к директории, в которой установлена программа>` означает, что будет выполнена очистка программы, установленной в указанной директории.

Подготовка к работе

Перед началом работы с Kaspersky MLAD требуется убедиться, что выполнены следующие действия:

1. Описания тегов принимаемой телеметрии и активов иерархической структуры подготовлены для импорта в Kaspersky MLAD в виде файла формата XLSX. Файл создается квалифицированным техническим специалистом Заказчика, специалистом "Лаборатории Касперского" или сертифицированным интегратором.

2. При необходимости подготовлен набор пресетов, необходимый для контроля поступления данных и оценки работоспособности Kaspersky MLAD. Описания пресетов подготовлены в виде файла в формате JSON. Файл создается квалифицированным техническим специалистом Заказчика, специалистом "Лаборатории Касперского" или сертифицированным интегратором. Пресеты также могут быть созданы пользователем в веб-интерфейсе программы.

3. Источник данных телеметрии включен и настроен на отправку данных в Kaspersky MLAD. Для источника данных подготовлен файл в формате JSON с описанием тегов источника. Файл создается квалифицированным техническим специалистом Заказчика, специалистом "Лаборатории Касперского" или сертифицированным интегратором.

4. Сеть передачи данных подготовлена для доставки данных телеметрии от источника данных к серверу Kaspersky MLAD, сетевое оборудование надлежащим образом настроено, передача данных разрешена.

5. Подготовлены конфигурационные параметры и/или файлы того коннектора или источников данных, которые будут использованы в Kaspersky MLAD для приема данных телеметрии или событий от внешних систем. Коннектор или источники данных должны быть настроены и включены после запуска Kaspersky MLAD.

6. Если ML-модели предоставляются в рамках *Услуги построения модели и внедрения Kaspersky MLAD*, ML-модели созданы и обучены на исторических данных телеметрии специалистом "Лаборатории Касперского" или сертифицированным интегратором. ML-модели подготовлены для импорта в Kaspersky MLAD в виде файлов формата TAR. Системному администратору Kaspersky MLAD переданы коды для активации ML-моделей. Коды для активации ML-моделей хранятся в надежном хранилище.

Запуск, остановка и перезапуск Kaspersky MLAD

Чтобы запустить программу:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

2. Выполните команду:

   ```
   mladctl start
   ```

   Если требуется, вы можете выполнить команду с ключом `-f <полный путь к директории, в которой установлена программа>`. Если при выполнении команды вы не использовали этот ключ, вы можете выбрать директорию со сборкой программы во время запуска программы.

3. Следуйте указаниям утилиты.

Kaspersky MLAD будет запущен.

Чтобы остановить программу:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

2. Выполните команду:

   ```
   mladctl stop
   ```

   Если требуется, вы можете выполнить команду с ключом `-f <полный путь к директории, в которой установлена программа>`. Если при выполнении команды вы не использовали этот ключ, вы можете выбрать директорию со сборкой программы во время остановки программы.

3. Следуйте указаниям утилиты.

Kaspersky MLAD будет остановлен.

При остановке программа запоминает статусы служб. При запуске программы работа служб будет восстановлена с прежними статусами.

Чтобы перезапустить программу:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

2. Выполните команду:

   `sudo mladctl restart -f <полный путь к директории, в которой установлена программа>`

   где `-f <полный путь к директории, в которой установлена программа>` означает, что будет перезапущена программа, установленная в указанной директории.

Обновление сертификатов Kaspersky MLAD

В Kaspersky MLAD используются следующие сертификаты:

- сертификаты для подключения к Kaspersky MLAD через веб-интерфейс;
- сертификаты для подключения коннекторов и служб.

Необходимо обновлять сертификаты в следующих случаях:

- текущие сертификаты скомпрометированы;
- закончился срок действия сертификатов;
- требуется выполнить обновление сертификатов в соответствии с требованиями информационной безопасности на предприятии.

Обновление сертификата для подключения к Kaspersky MLAD через веб-интерфейс

По умолчанию для подключения к веб-интерфейсу Kaspersky MLAD использует самоподписанный сертификат, который автоматически генерируется на этапе установки программы. При использовании самоподписанного сертификата для подключения к веб-интерфейсу Kaspersky MLAD браузер будет отображать предупреждение о том, что сертификат безопасности или устанавливаемое соединение не является доверенным.

Если требуется использовать доверенные сертификаты для подключения к веб-интерфейсу Kaspersky MLAD, вы можете заменить самоподписанный сертификат сертификатом, полученным от аккредитованного центра сертификации, или пользовательским сертификатом, соответствующим стандартам безопасности вашей организации.

Kaspersky MLAD использует директорию <директория с установленной программой>/ssl/nginx/ для хранения сертификатов, обеспечивающих подключение к веб-интерфейсу.

Обновление сертификата для подключения к Kaspersky MLAD через веб-интерфейс выполняет квалифицированный технический специалист Заказчика, сотрудник "Лаборатории Касперского" или сертифицированный интегратор.

Чтобы обновить сертификаты для подключения к Kaspersky MLAD через веб-интерфейс:

1. Получите доверенный сертификат и ключ к этому сертификату для подключения к веб-интерфейсу Kaspersky MLAD.

   Сертификат требуется получить для IP-адреса и доменного имени сервера, на котором установлен Kaspersky MLAD.

2. Перейдите в директорию, в которой находятся доверенный сертификат и ключ к этому сертификату.

3. В командной строке выполните следующие команды:

   ```
   sudo chown root:root <новый сертификат>.crt <ключ к новому сертификату>.key
   sudo chmod 640 <новый сертификат>.crt <ключ к новому сертификату>.key
   sudo cp <новый сертификат>.crt <директория с установленной программой>/ssl/nginx/mlad_nginx.crt
   sudo cp <ключ к новому сертификату>.key <директория с установленной программой>/ssl/nginx/mlad_nginx.key
   ```

   Новый сертификат и его ключ будут сохранены в директории <директория с установленной программой>/ssl/nginx/ в виде файлов mlad_nginx.crt и mlad_nginx.key соответственно.

4. Перейдите в директорию, в которой установлена программа, и перезапустите Kaspersky MLAD.

После перезапуска Kaspersky MLAD будет использовать новый сертификат для подключения к веб-интерфейсу.

Обновление сертификата для подключения коннекторов и служб

В Kaspersky MLAD вы можете использовать защищенное соединение для коннекторов AMQP Connector, CEF Connector, HTTP Connector, MQTT Connector и WebSocket Connector, а также служб Data Source Manager и Mail Notifier. Вы можете обновлять сертификаты для подключения службы Data Source Manager к нескольким источникам данных по защищенному соединению в разделе **Источники данных** в основном меню. Для подключения остальных коннекторов и службы Mail Notifier по защищенному соединению обновление сертификатов производится в разделе **Системные параметры**.

Для подключения коннекторов AMQP Connector, CEF Connector, HTTP Connector, MQTT Connector и WebSocket Connector, а также служб Data Source Manager и Mail Notifier по защищенному соединению рекомендуется использовать сертификаты, созданные по стандарту X.509, с длиной ключа к сертификату не менее 4 096 бит.

Сертификат для подключения коннектора KICS Connector содержится в файле свертки, который вы можете обновить в Kaspersky Industrial CyberSecurity for Networks. Обновленный файл свертки вы можете загрузить в Kaspersky MLAD при настройке коннектора KICS Connector. Подробную информацию о создании файла свертки вы можете получить в *справке Kaspersky Industrial CyberSecurity for Networks*.

Kaspersky Machine Learning for Anomaly Detection совместим с Kaspersky Industrial CyberSecurity for Networks версии 4.0 и выше.

Первый запуск Kaspersky MLAD

В этом разделе приводится последовательность действий, которые требуется выполнить системному администратору при первом запуске Kaspersky MLAD, чтобы настроить работу с программой.

Сценарий первого запуска Kaspersky MLAD состоит из следующих этапов:

1. **Изменение параметров конфигурационных файлов**

   При необходимости до запуска Kaspersky MLAD измените параметры конфигурационных файлов .env и config.env. Если при установке программы был использован ключ `--autostart`, перезапустите программу.

   > Изменение параметров конфигурационных файлов выполняет только квалифицированный технический специалист Заказчика, сотрудник "Лаборатории Касперского" или сертифицированный интегратор.

2. **Запуск Kaspersky MLAD**

   Если при установке программы не был использован ключ `--autostart`, запустите Kaspersky MLAD. При запуске программы автоматически запускаются следующие службы, необходимые для работы Kaspersky MLAD:

   - API Server;
   - Web Server;
   - Message Broker;
   - Keeper;
   - Time Series Database;
   - Database;
   - Logger;
   - Docker API Server;
   - Migrations;
   - Push Server.

3. **Подключение к веб-интерфейсу Kaspersky MLAD**

   Откройте веб-интерфейс программы в поддерживаемом браузере и введите адрес электронной почты и пароль первого пользователя Kaspersky MLAD с ролью системного администратора, указанные при установке программы. Измените пароль для своей учетной записи. Для безопасного подключения к веб-интерфейсу Kaspersky MLAD рекомендуется установить доверенный сертификат.

   В разделе **Системные параметры** в меню администратора укажите имя объекта мониторинга.

4. **Загрузка конфигурации тегов и активов иерархической структуры в Kaspersky MLAD**

   Для дальнейшей работы загрузите конфигурацию тегов и активов в Kaspersky MLAD. Конфигурация тегов и активов описывается в файле в формате XLSX. Пример описания конфигурации тегов и активов см. в Приложении.

5. **Настройка коннекторов и источников данных**

   Для работы с данными настройте коннекторы, используемые на вашем объекте мониторинга. Вы можете настроить следующие коннекторы:

   - KICS Connector;
   - CEF Connector;
   - HTTP Connector;
   - MQTT Connector;
   - AMQP Connector;
   - WebSocket Connector.

   Для получения данных по протоколу OPC UA создайте одну или несколько карточек источников данных OPC UA.

6. **Настройка служб**

   В разделе **Системные параметры** в меню администратора настройте службы, которые требуется использовать для вашего объекта мониторинга. В разделе **Службы** проверьте статусы служб и при необходимости запустите их. Например, для получения данных должно быть выполнено подключение к источникам данных или запущены необходимые коннекторы, а для правильного обнаружения аномалий должна быть запущена служба *Anomaly Detector*.

7. **Подключение к коннекторам и источникам данных**

   Запустите коннекторы и подключитесь к источникам данных, используемым для вашего объекта мониторинга. Перейдите в раздел **Информационная панель** и убедитесь, что данные поступают в Kaspersky MLAD в онлайн-режиме.

8. **Создание учетных записей для пользователей**

   Создайте учетные записи для пользователей программы и назначьте им необходимые роли. Создайте подписки на уведомления об инцидентах для пользователей.

Kaspersky Machine Learning for Anomaly Detection подготовлен к работе, данные поступают и обрабатываются программой.

Пользователи могут приступать к работе с Kaspersky MLAD, используя веб-интерфейс.

Удаление программы

Удаление Kaspersky MLAD выполняет квалифицированный технический специалист Заказчика, сотрудник "Лаборатории Касперского" или сертифицированный интегратор.

В результате удаления Kaspersky MLAD будут потеряны все данные Kaspersky MLAD, полученные, загруженные и обработанные с момента установки программы, а также все созданные активы, ML-модели и пресеты и заданные параметры программы. Рекомендуется проверить наличие резервной копии Kaspersky MLAD. Вы можете выполнить резервное копирование при обновлении программы или с помощью команды `backup` утилиты mladctl.

Чтобы удалить Kaspersky MLAD:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

2. Выполните команду:

   `mladctl uninstall`

   Если требуется, вы можете выполнить команду со следующими ключами:

   - `--delete-backup` – удаляет резервные копии программы, хранящиеся в директории, в которой установлена программа.
   - `--self` – удаляет утилиту mladctl.
   - `-f <полный путь к директории, в которой установлена программа>` – удаляет программу, установленную в указанной директории. Если при выполнении команды вы не использовали этот ключ, вы можете выбрать директорию программы во время удаления программы.

3. Следуйте указаниям утилиты.

   При подтверждении удаления установленных сертификатов утилита удалит директорию, в которой хранятся резервные копии.

Программа Kaspersky MLAD будет удалена.

Чтобы удалить Kaspersky MLAD в неинтерактивном режиме:

1. Выполните вход в систему с учетными данными пользователя с root-правами, от имени которого вы хотите запустить утилиту mladctl.

2. Выполните команду:

   `mladctl uninstall -q -f <полный путь к директории, в которой установлена программа>`

   где:

   `-q` означает, что программа будет удалена в неинтерактивном режиме.

   `-f <полный путь к директории, в которой установлена программа>` означает, что будет удалена программа, установленная в указанной директории.

   Если требуется, вы можете выполнить команду со следующими ключами:

   - `--delete-backup` – удаляет резервные копии программы.
   - `--self` – удаляет утилиту mladctl.

Программа Kaspersky MLAD будет удалена.

Веб-интерфейс Kaspersky MLAD

Работа с Kaspersky MLAD осуществляется через веб-интерфейс. В этом разделе приведено описание основных элементов веб-интерфейса Kaspersky MLAD.

Главное окно веб-интерфейса программы содержит следующие элементы:

- меню в левой части окна веб-интерфейса программы;
- рабочую область в центральной части окна веб-интерфейса программы.

Разделы основного меню и меню администратора доступны пользователям с правами доступа к соответствующим функциям программы. Доступ к функциям программы определяется списком прав, заданных для роли пользователя.

В нижней части основного меню и меню администратора доступно меню пользователя, предоставляющее возможность выбирать язык веб-интерфейса, изменять пароль своей учетной записи, выходить из учетной записи, переходить на страницу системы ведения журналов для просмотра журналов программы, а также переключаться между меню. Переключение между основным меню и меню администратора осуществляется нажатием на одну из следующих кнопок:

- – для перехода в меню администратора.
- – для перехода в основное меню.

При необходимости вы можете свернуть или развернуть меню нажатием на << или >> соответственно в левом верхнем углу страницы.

Основное меню

В таблице ниже описаны разделы основного меню Kaspersky MLAD.

Разделы основного меню

Раздел	Описание
Информационная панель	Открывает раздел, который содержит информацию о последних зарегистрированных инцидентах, службах программы и их статусах.
Мониторинг	Открывает раздел, в котором отображаются данные, поступающие в систему в реальном времени. Вы также можете настроить параметры отображения поступающих данных на графических областях.
История	Открывает раздел, который содержит полную историю поступивших в систему данных и результаты их анализа ML-моделями. Вы также можете настроить параметры отображения исторических данных на графических областях.
Временной срез	Открывает раздел, который содержит информацию о значениях технологических параметров, полученных от датчиков в один и тот же момент времени. Вы также можете настроить параметры отображения данных на графике.
Процессор событий	Открывает раздел, в котором вы можете просматривать информацию о полученных из внешних систем событиях и выявленных среди них паттернах, а также управлять мониторами для отслеживания определенных событий, паттернов или значений параметров событий.
Инциденты	Открывает раздел, который содержит журнал зарегистрированных инцидентов. В рамках анализа инцидентов вы можете добавить приоритет, статус, причину, экспертные рекомендации и комментарии к инциденту или группе инцидентов.
Модели	Открывает раздел, в котором вы можете управлять используемыми в системе разметками, ML-моделями, элементами ML-моделей и шаблонами ML-моделей. Управление разметками, ML-моделями, элементами ML-моделей и шаблонами ML-моделей доступно системным администраторам и пользователям с правами из группы прав Управление ML-моделями.

Раздел	Описание
Пресеты	Открывает раздел, в котором вы можете управлять пресетами и графическими областями в их составе.
Службы	Открывает раздел, в котором вы можете просматривать информацию о службах и их статусах, а также запускать, останавливать и перезапускать службы. Управление статусами служб доступно системным администраторам и пользователям с правом **Управление статусами служб программы** из группы прав Работа со службами программы.
Источники данных	Открывает раздел, в котором вы можете управлять источниками данных. Управление источниками данных доступно системным администраторам.

Меню администратора

В таблице ниже описаны разделы меню администратора Kaspersky MLAD.

Разделы меню администратора

Раздел	Описание
Лицензирование	Открывает раздел, в котором вы можете управлять лицензионными ключами.
Пользователи	Открывает раздел, в котором вы можете управлять учетными записями пользователей.
Роли	Открывает раздел, в котором вы можете управлять ролями пользователей.
Права	Открывает раздел, который содержит информацию о правах пользователей.
Уведомления	Открывает раздел, в котором вы можете управлять подписками на уведомления и получателями уведомлений. Управление уведомлениями доступно системным администраторам и пользователям с правами из группы прав Управление уведомлениями.
Системные параметры	Открывает раздел, в котором вы можете управлять параметрами Kaspersky MLAD.
Активы	Открывает раздел, в котором вы можете управлять активами и тегами. Управление активами и тегами доступно системным администраторам и пользователям с правами из группы прав Управление активами и тегами.

Меню пользователя

В таблице ниже описаны элементы меню пользователя Kaspersky MLAD.

Элементы меню пользователя

Элемент меню	Описание
	Позволяет выбрать язык локализации для веб-интерфейса Kaspersky MLAD. Доступны английский и русский языки.
	Открывает справку Kaspersky MLAD в новой вкладке браузера.
	Открывает окно с краткой информацией о программе.
	Осуществляет переход в систему ведения журналов (Grafana ™) в новой вкладке браузера. Этот раздел доступен системным администраторам и пользователям с правом Работа с журналами программы.
	Осуществляет переход в меню администратора из основного меню. В меню администратора вы можете управлять лицензионными ключами, параметрами Kaspersky MLAD, ролями и учетными данными пользователей, а также управлять подписками на уведомления и получателями уведомлений, активами и тегами. Меню администратора доступно только системным администраторам.
	Осуществляет переход в основное меню из меню администратора. В основном меню вы можете управлять ML-моделями их элементами, разметками и шаблонами ML-моделей, управлять статусами служб, а также просматривать исторические данные и данные, поступающие в реальном времени, просматривать зарегистрированные инциденты, события и паттерны.
	Позволяет изменить пароль учетной записи текущего пользователя и осуществить выход из учетной записи.

Подключение к Kaspersky MLAD и завершение пользовательской сессии

Для подключения к веб-интерфейсу Kaspersky MLAD нужно использовать поддерживаемый браузер.

Если авторизованный пользователь использует программу меньше, чем указано в параметре **Период неактивности пользователя (мин)**, то Kaspersky MLAD автоматически завершает сессию подключения для этого пользователя. Для продолжения работы в программе потребуется повторная авторизация пользователя. Пользовательская сессия считается активной в следующих случаях:

- Пользователь взаимодействует с элементами интерфейса программы (например, нажимает на кнопки, переходит в разделы меню программы).
- Пользователь вводит значения параметров с помощью клавиатуры.

При выполнении любого из вышеперечисленных действий продлевает сессию пользователя на время, заданное в параметре **Период неактивности пользователя (мин)**.

Пользователь может досрочно завершить свою пользовательскую сессию, выйдя из своей учетной записи.

При необходимости системный администратор может отозвать токены аутентификации для учетной записи пользователя. При отзыве токенов для пользователя будет завершена сессия работы в программе одновременно на всех устройствах, на которых он был авторизован.

Веб-адрес, адрес электронной почты и пароль для подключения к программе требуется запросить у системного администратора Kaspersky MLAD.

Подключение к веб-интерфейсу

Чтобы подключиться к Kaspersky MLAD через браузер:

1. На компьютере откройте поддерживаемый браузер.
2. В адресной строке браузера введите веб-адрес сервера Kaspersky MLAD, полученный от системного администратора Kaspersky MLAD.
3. На открывшейся странице ввода учетных данных введите адрес электронной почты и пароль пользователя.

   При первом подключении к веб-интерфейсу в качестве системного администратора используйте указанные при установке программы адрес электронной почты и пароль первого пользователя с ролью системного администратора.
4. Нажмите на кнопку **Войти** или на клавишу **ENTER**.

В окне браузера отобразится раздел **Информационная панель**.

При первом подключении пользователя к Kaspersky MLAD в браузере откроется **окно изменения пароля**. Если пропуск смены пароля разрешен в параметрах безопасности, вы можете пропустить изменение пароля нажатием на кнопку **Пропустить** и изменить его позже. При истечении срока действия пароля, заданного при настройке параметров безопасности, в браузере также откроется окно изменения пароля.

- **Новый пароль** – введите новый пароль для учетной записи пользователя

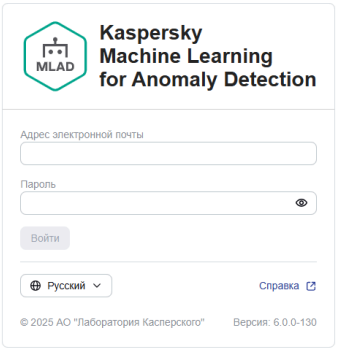
  Новый пароль должен удовлетворять следующим требованиям:

  - Не совпадает с предыдущими паролями. Количество ранее использованных паролей, с которыми новый пароль не должен совпадать, задается администратором при настройке параметров безопасности.
  - Содержит минимальное количество символов, заданное администратором при настройке параметров безопасности.
  - Содержит буквы латинского алфавита, цифры и/или специальные символы в соответствии с политикой паролей, заданной администратором при настройке параметров безопасности.

- **Подтверждение пароля** – введите повторно пароль для учетной записи пользователя.

Если вы закрыли окно браузера без завершения сессии подключения, сессия останется действующей до истечения времени, заданного администратором в параметре **Период неактивности пользователя (мин)** при настройке параметров безопасности. В течение этого времени программа предоставляет доступ к веб-интерфейсу Kaspersky MLAD без запроса учетных данных пользователя, если для подключения используются те же компьютер, браузер и учетная запись операционной системы. В случае неактивного использования программы дольше, чем указано в параметре **Период неактивности пользователя (мин)**, Kaspersky MLAD завершает пользовательскую сессию.

В случае многократной неудачной авторизации Kaspersky MLAD заблокирует вашу учетную запись при достижении числа неудачных попыток авторизации на определенный период. Количество неудачных попыток авторизации и период блокировки учетной записи задаются при настройке параметров безопасности Kaspersky MLAD.



Завершение сессии подключения к Kaspersky MLAD

После окончания работы с Kaspersky MLAD в браузере требуется завершить сессию подключения к программе.

Чтобы завершить сессию подключения к программе,

в окне браузера в нижнем левом углу страницы веб-интерфейса Kaspersky MLAD нажмите на кнопку и выберите пункт **Выход из Kaspersky MLAD**.

После завершения сессии подключения к программе в окне браузера отобразится страница ввода учетных данных.

Изменение пароля учетной записи

Рекомендуется изменять пароль в следующих случаях:

- выполнено первое подключение к Kaspersky MLAD после создания учетной записи в программе;
- текущий пароль скомпрометирован;
- истекает срок действия пароля в соответствии с требованиями информационной безопасности на предприятии.

Чтобы изменить пароль своей учетной записи:

1. В нижнем левом углу страницы веб-интерфейса Kaspersky MLAD нажмите на кнопку и выберите пункт **Изменить пароль**.

   В браузере откроется окно **Изменение пароля**.

2. В поле **Текущий пароль** введите ваш текущий пароль.

3. В полях **Новый пароль** и **Подтверждение пароля** введите новый пароль.

   Новый пароль должен удовлетворять следующим требованиям:

   - Не совпадает с предыдущими паролями. Количество ранее использованных паролей, с которыми новый пароль не должен совпадать, задается при настройке параметров безопасности.
   - Содержит минимальное количество символов, заданное при настройке параметров безопасности.
   - Содержит буквы латинского алфавита, цифры и/или специальные символы в соответствии с политикой паролей, заданной при настройке параметров безопасности.

4. Нажмите на кнопку **Изменить**.

Выбор языка веб-интерфейса Kaspersky MLAD

В Kaspersky MLAD доступны английский и русский языки для веб-интерфейса программы. Вы можете изменить язык веб-интерфейса до и после подключения к программе.

Чтобы изменить язык веб-интерфейса до подключения к программе,

в левом нижнем углу страницы ввода учетных данных выберите нужный язык: русский или английский.

Чтобы изменить язык веб-интерфейса после подключения к программе:

1. В левом нижнем углу страницы веб-интерфейса Kaspersky MLAD нажмите на кнопку ⊕.
2. Выберите нужный язык: русский или английский.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky MLAD.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Во время установки или обновления Kaspersky MLAD.
- Прочитав документ license_ru.txt. Этот документ включен в комплект поставки программы.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки или обновления программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку или обновление программы и не должны использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование программы, предоставляемое вам на основании Лицензионного соглашения.

Список доступных функций и срок использования программы зависят от лицензии, по которой используется программа.

Предусмотрены следующие типы лицензий:

- *Базовая* – бесплатная лицензия.

  Этот тип лицензии не ограничен по времени и количеству поддерживаемых тегов. Вы можете использовать базовые функции программы до добавления лицензионного ключа или после истечения срока действия пробной или коммерческой лицензии. Если после добавления лицензионного ключа для лицензии, по которой ограничено количество поддерживаемых тегов, количество тегов в программе превышает количество поддерживаемых тегов, вам нужно снизить количество тегов в программе до разрешенного количества.

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с программой.

  Этот тип лицензии ограничен по времени. Вы можете приобрести эту лицензию с ограничением по количеству поддерживаемых тегов в соответствии с количеством тегов на вашем объекте мониторинга.

  По истечении срока действия пробной лицензии останутся доступными только базовые функции программы. Для продолжения работы Kaspersky MLAD вам нужно приобрести коммерческую лицензию.

  Пробная лицензия имеет небольшой срок действия. Вы можете использовать программу по пробной лицензии только в течение одного срока пробного использования.

  Если после истечения срока действия пробной лицензии вы добавили лицензионный ключ для действующей коммерческой лицензии, по которой недоступен конструктор моделей, то ML-модели, шаблоны и элементы ML-моделей, созданные вручную во время пробного использования программы, станут недоступны для изменения, копирования и удаления. При добавлении лицензионного ключа для действующей коммерческой лицензии с конструктором моделей вы можете продолжить управлять ML-моделями, шаблонами и элементами ML-моделей, созданными вручную во время действия пробной лицензии.

- *Коммерческая* – платная лицензия.

  Этот тип лицензии ограничен по времени.

  Для активации функциональности программы вам нужно добавить лицензионный ключ для действующей коммерческой лицензии. В Kaspersky MLAD предусмотрены следующие виды коммерческой лицензии:

  - Коммерческая лицензия без конструктора моделей и процессора событий.

    Если вам нужны все функции программы, кроме работы с ML-моделями, созданными вручную, копирования и удаления элементов ML-моделей, работы с шаблонами ML-моделей, а также работы с процессором событий требуется приобрести коммерческую лицензию без конструктора моделей и процессора событий. Вы можете приобрести эту лицензию с ограничением по количеству поддерживаемых тегов в соответствии с количеством тегов на вашем объекте мониторинга.

  - Коммерческая лицензия с конструктором моделей.

    Если при работе с Kaspersky MLAD вам нужны функции работы с ML-моделями, созданными вручную, копирования и удаления элементов ML-моделей, работы с шаблонами ML-моделей, требуется приобрести коммерческую лицензию с конструктором моделей. Вы можете приобрести эту лицензию с ограничением по количеству поддерживаемых тегов в соответствии с количеством тегов на вашем объекте мониторинга.

  - Коммерческая лицензия с процессором событий.

    Если при работе с Kaspersky MLAD вам нужны функции работы с процессором событий, требуется приобрести коммерческую лицензию с процессором событий.

  - Коммерческая лицензия с полной функциональностью.

    Если вам нужны все функции программы, требуется приобрести коммерческую лицензию с конструктором моделей и процессором событий. Вы можете приобрести эту лицензию с ограничением по количеству поддерживаемых тегов в соответствии с количеством тегов на вашем объекте мониторинга.

По истечении срока действия коммерческой лицензии останутся доступными только базовые функции программы. Для продолжения работы Kaspersky MLAD вам нужно продлить срок действия коммерческой лицензии.

Рекомендуется продлевать срок действия лицензии не позднее даты ее окончания, чтобы обеспечить непрерывную работу Kaspersky MLAD.

Услуги технической поддержки предоставляются при наличии действующего *Договора об оказании технической поддержки*. Объем предоставляемых услуг технической поддержки определяется действующим *Договором об оказании технической поддержки*.

О лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- идентификатор лицензии или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, тегов, по которым программа может получать данные телеметрии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- информация о том, предоставляется ли лицензия в первый раз или повторно.

О лицензионном ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в программу, применив *файл лицензионного ключа*. Лицензионный ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы с программой требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть активным и резервным.

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В программе не может быть больше одного активного лицензионного ключа.

Резервный лицензионный ключ – лицензионный ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Резервный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом, или в случае удаления активного лицензионного ключа. Резервный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве резервного лицензионного ключа.

О файле лицензионного ключа

Файл лицензионного ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего программу.

Вы получаете файл лицензионного ключа после приобретения Kaspersky MLAD или после заказа пробной версии Kaspersky MLAD. Способ получения файла лицензионного ключа определяется дистрибьютором "Лаборатории Касперского", у которого вы приобрели программу (например, файл лицензионного ключа может быть отправлен по указанному вами адресу электронной почты).

Вы также можете добавить в программу лицензионный ключ, полученный при приобретении Kaspersky MLAD предыдущей версии. Лицензионный ключ можно добавить в программу до даты окончания его срока годности.

Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно утерян, вы можете его восстановить. Для восстановления файла ключа вам нужно обратиться к продавцу лицензии.

Доступная функциональность Kaspersky MLAD в зависимости от лицензии

В таблице ниже приведен набор доступных функций Kaspersky MLAD в зависимости от выбранной лицензии.

Функции	Базовая лицензия	Коммерческая лицензия без конструктора моделей и процессора событий	Коммерческая лицензия с конструктором моделей	Коммерческая лицензия с процессором событий	Пробная лицензия или коммерческая лицензия с полной функциональностью
Базовые функции	✓	✓	✓	✓	✓

Функции	Базовая лицензия	Коммерческая лицензия без конструктора моделей и процессора событий	Коммерческая лицензия с конструктором моделей	Коммерческая лицензия с процессором событий	Пробная лицензия или коммерческая лицензия с полной функциональностью
Доступны следующие функции: • Установка, удаление, обновление, резервное копирование программы и откат программы к предыдущей версии. При использовании программы по базовой лицензии новые сборки для обновления не предоставляются. • Подключение к веб-интерфейсу и завершение сессии подключения. • Выбор языка локализации веб-интерфейса. • Просмотр справки Kaspersky MLAD. • Просмотр информации о версии программы. • Просмотр журналов Kaspersky MLAD. • Изменение собственного пароля. • Управление учетными записями пользователей. • Управление ролями. • Управление подписками на уведомления об инцидентах, дополнительными контактами и группами контактов. • Настройка параметров Kaspersky MLAD.					

Функции	Базовая лицензия	Коммерческая лицензия без конструктора моделей и процессора событий	Коммерческая лицензия с конструктором моделей	Коммерческая лицензия с процессором событий	Пробная лицензия или коммерческая лицензия с полной функциональностью
• Управление активами и тегами. • Управление источниками данных. • Просмотр данных в разделах **Мониторинг**, **История** и **Временной срез**, за исключением выбора элемента ML-модели. • Управление пресетами. • Просмотр статусов служб. • Управление статусами служб, за исключением служб Anomaly Detector, Trainer, Similar Anomaly, Event Processor, Stream Processor.					
Выбор элемента ML-модели в разделах **Мониторинг**, **История** и **Временной срез**	—	✓	✓	✓	✓
Работа с процессором событий	—	—	—	✓	✓
Работа с инцидентами и группами инцидентов	—	✓	✓	✓	✓
Работа с разметками	—	✓	✓	✓	✓
Работа с импортированными ML-моделями	—	✓	✓	✓	✓
Работа с ML-моделями, созданными вручную	—	—	✓	—	✓
Копирование ML-модели	—	✓	✓	✓	✓
Копирование элемента ML-модели	—	—	✓	—	✓
Удаление ML-модели	—	✓	✓	✓	✓
Удаление элемента ML-модели	—	—	✓	—	✓
Работа с шаблонами ML-моделей	—	—	✓	—	✓
Обучение предиктивных элементов и элементов на основе эллиптического конверта	—	✓	✓	✓	✓
Просмотр результатов обучения ML-модели	—	✓	✓	✓	✓
Подготовка ML-модели к публикации	—	✓	✓	✓	✓
Публикация ML-модели	—	✓	✓	✓	✓
Запуск и остановка инференса ML-модели	—	✓	✓	✓	✓

Функции	Базовая лицензия	Коммерческая лицензия без конструктора моделей и процессора событий	Коммерческая лицензия с конструктором моделей	Коммерческая лицензия с процессором событий	Пробная лицензия или коммерческая лицензия с полной функциональностью
Управление статусами служб Anomaly Detector, Trainer, Similar Anomaly, Stream Processor	—	✓	✓	✓	✓
Управление статусом службы Event Processor	—	—	—	✓	✓

Добавление лицензионного ключа

Вы можете добавить лицензионный ключ в Kaspersky MLAD при подключении к программе через веб-интерфейс.

Добавлять лицензионный ключ может только системный администратор.

Чтобы добавить лицензионный ключ:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Лицензирование**.

3. Нажмите на кнопку **Добавить лицензионный ключ**.

   Кнопка недоступна, если активный и резервный лицензионные ключи уже добавлены в программу. Если требуется, вы можете удалить лицензионный ключ.

   Справа отобразится панель **Добавление лицензионного ключа**.

4. Выберите файл лицензионного ключа в формате KEY.

   После выбора файла лицензионного ключа в панели **Добавление лицензионного ключа** отобразится информация о добавленном ключе.

   Если в программе отсутствовали лицензионные ключи и срок годности добавляемого лицензионного ключа уже начался, он автоматически будет добавлен в программу в качестве активного. Если срок годности добавляемого лицензионного ключа еще не начался и срок его годности не пересекается со сроком годности текущего активного лицензионного ключа, он будет добавлен в программу в качестве резервного.

5. Если в программу был ранее добавлен лицензионный ключ, при необходимости выполните одно из следующих действий:

   - Если требуется загрузить ключ в качестве активного и в программе уже есть активный лицензионный ключ, в блоке параметров **Статус лицензионного ключа** выберите **Активный лицензионный ключ**.

     Предыдущий активный лицензионный ключ будет заменен и удален из программы.

   - Если требуется загрузить ключ в качестве активного и срок его годности пересекается со сроком годности ранее загруженного резервного ключа, в блоке параметров **Статус лицензионного ключа** выберите **Активный лицензионный ключ** и в блоке параметров **Применить резервный ключ** выберите один из следующих вариантов применения резервного ключа:

     - **По окончании срока годности активного ключа**. Резервный лицензионный ключ станет активным после окончания срока годности активного лицензионного ключа.

     - **В момент начала срока годности резервного ключа**. Резервный ключ станет активным в момент начала срока его годности. Предыдущий активный лицензионный ключ будет удален из программы. Вы можете использовать удаленный лицензионный ключ на другом объекте мониторинга до окончания срока годности этого ключа.

   - Если требуется загрузить ключ в качестве резервного и срок его годности пересекается со сроком годности ранее загруженного активного ключа, в блоке параметров **Статус лицензионного ключа** выберите **Резервный лицензионный ключ** и в блоке параметров **Применить резервный ключ** выберите один из следующих вариантов применения резервного ключа:

     - **По окончании срока годности активного ключа**. Резервный лицензионный ключ станет активным после окончания срока годности текущего активного лицензионного ключа.

     - **В момент начала срока годности резервного ключа**. Резервный ключ станет активным в момент начала срока его годности. Предыдущий активный лицензионный ключ будет удален из программы.

       Невозможно добавить лицензионный ключ в качестве резервного, если срок его годности заканчивается раньше текущего активного лицензионного ключа.

6. Нажмите на кнопку **Добавить**.

Лицензионный ключ будет загружен в программу.

Просмотр информации о добавленном лицензионном ключе

При подключении к Kaspersky MLAD вы можете просматривать информацию о добавленном лицензионном ключе. За 30 дней до окончания срока годности лицензионного ключа в веб-интерфейсе программы отображается уведомление с информацией о количестве дней, оставшемся до окончания срока годности ключа.

Чтобы просмотреть информацию о лицензионном ключе:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Лицензирование**.

Для добавленного лицензионного ключа отображается следующая информация:

- Информация о количестве дней до окончания срока его годности.
- **Название программы** – информация о программе, которая будет активирована после добавления лицензионного ключа.
- **Статус лицензионного ключа** – информация о статусе ключа. Предусмотрены следующие статусы ключа:
  - **Активный лицензионный ключ** – лицензионный ключ используется в текущий момент для работы программы.
  - **Резервный лицензионный ключ** – лицензионный ключ, не используемый в текущий момент.
  - **Срок годности истек** – срок годности лицензионного ключа истек.
- **Номер лицензии** – номер заказа.
- **Ключ** – уникальная буквенно-цифровая последовательность.
- **Наименование компании** – наименование компании, для которой была приобретена лицензия.
- **Дата активации** – дата первого добавления лицензионного ключа в программу.
- **Ключ действителен до** – дата окончания срока годности лицензионного ключа.
- **Функциональность** – информация о количестве доступных тегов, а также возможности использовать ML-модели, конструктор моделей и/или процессор событий.

Удаление лицензионного ключа

При подключении к программе через веб-интерфейс вы можете удалить добавленный лицензионный ключ из программы (например, если требуется заменить этот лицензионный ключ на другой). После удаления лицензионного ключа вам будут доступны только базовые функции программы.

После удаления лицензионного ключа вы продолжите получать данные по тегам с помощью источников данных и коннекторов, а также сможете просмотреть данные по тегам в разделах **Мониторинг** и **История**. В свою очередь ML-модели перестанут обрабатывать данные по тегам, а также формировать инциденты и артефакты. Просмотр сформированных ранее артефактов станет недоступным. Вы также не сможете использовать созданные и импортированные ML-модели.

Недоступная функциональность снова активируется при следующем добавлении лицензионного ключа для коммерческой лицензии.

Перед удалением активного лицензионного ключа рекомендуется добавить в программу резервный лицензионный ключ. При удалении активного лицензионного ключа ранее добавленный резервный лицензионный ключ станет активным. Срок действия лицензии будет продлен в соответствии со сроком годности добавленного лицензионного ключа.

Если вы удалили лицензионный ключ до окончания срока его годности, вы можете повторно добавить его в программу с сохранением исходной даты окончания срока действия лицензии.

Удалять лицензионный ключ может только системный администратор.

Чтобы удалить лицензионный ключ:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Лицензирование**.

3. В правом верхнем углу карточки нужного лицензионного ключа нажмите на кнопку .

   Откроется окно с запросом подтверждения.

4. Подтвердите удаление лицензионного ключа.

Лицензионный ключ будет удален из программы.

Обработка и хранение данных в Kaspersky MLAD

Этот раздел содержит информацию о предоставлении данных и о директориях для хранения данных.

О предоставлении данных

Программа не передает пользовательские данные в "Лабораторию Касперского". Пользовательские данные обрабатываются на компьютерах, на которых установлена программа.

Данные, передаваемые во внешние системы

Данные передаются во внешние системы по защищенному каналу связи.

Если настроена отправка уведомлений о регистрации инцидентов по почте, программа передает следующие данные на SMTP-сервер:

- идентификатор инцидента;
- имя элемента ML-модели, который зарегистрировал инцидент;
- статус зарегистрированного инцидента;
- причину зарегистрированного инцидента;
- имя актива, к которому относится тег или ML-модель, элемент которой зарегистрировал инцидент;
- приоритет инцидента;
- уровень критичности актива;
- экспертные рекомендации к зарегистрированному инциденту;
- дату и время начала инцидента;
- имя ML-модели, элемент которой зарегистрировал инцидент;
- имя топ-тега;
- описание топ-тега;
- значение топ-тега в момент регистрации инцидента и его единицу измерения;
- ссылку для перехода в раздел **История** в момент начала инцидента;
- имя детектора, зарегистрировавшего инцидент;

- значение артефакта элемента ML-модели в момент регистрации инцидента;
- значение порога блокировки, превышенное в момент регистрации инцидента.

Если настроена отправка уведомлений о регистрации инцидентов через коннекторы MQTT Connector, AMQP Connector, WebSocket Connector и/или KICS Connector, программа передает следующие данные на MQTT-брокер, AMQP-брокер, WebSocket-сервер и/или в Kaspersky Industrial CyberSecurity for Networks:

- идентификатор инцидента;
- дату и время начала инцидента;
- дату и время завершения инцидента;
- имя и уникальный идентификатор (UUID) ML-модели, зарегистрировавшей инцидент;
- уникальный идентификатор (UUID) элемента ML-модели;
- идентификатор и описание топ-тега;
- имя детектора, зарегистрировавшего инцидент;
- ссылку для перехода в раздел **История** в момент начала инцидента;
- значение артефакта элемента ML-модели в момент регистрации инцидента (при наличии);
- значение порога блокировки, превышенное в момент регистрации инцидента (при наличии);
- значение топ-тега в момент регистрации инцидента;
- статус инцидента;
- комментарий к инциденту (при наличии);
- идентификатор группы инцидентов (при наличии);
- имя группы инцидента (при наличии);
- экспертные рекомендации (при наличии);
- идентификаторы релевантных тегов;
- причину инцидента (при наличии).

Если настроена отправка уведомлений о регистрации инцидентов через коннектор CEF Connector, программа передает следующие данные в SIEM-систему:

- имя поставщика программы;
- название программы;
- версию Kaspersky MLAD;
- идентификатор подписи программы;
- дату и время начала инцидента;

- дату и время завершения инцидента;
- имя детектора, зарегистрировавшего инцидент;
- имя ML-модели, зарегистрировавшей инцидент;
- ссылку для перехода в раздел **История** в момент начала инцидента;
- описание топ-тега;
- комментарий к инциденту (при наличии);
- имя группы инцидента (при наличии);
- значение топ-тега в момент регистрации инцидента;
- идентификатор группы инцидентов (при наличии);
- идентификатор инцидента;
- идентификатор топ-тега.

Если настроена отправка зарегистрированных событий через коннектор CEF Connector, программа передает следующие данные в SIEM-систему:

- имя поставщика программы;
- название программы;
- версию Kaspersky MLAD;
- идентификатор подписи программы;
- имя монитора, который зарегистрировал событие;
- идентификатор монитора;
- дату и время регистрации события;
- количество активаций на скользящем окне;
- тип элемента, который вызвал активацию монитора;
- имя головы внимания (при наличии);
- имя дочерней головы внимания (при наличии);
- скользящее окно монитора, за время которого ведется учет количества активаций;
- порог активаций, при достижении которого монитор отправляет оповещение во внешнюю систему;
- информацию, является ли обнаруженный элемент новым для программы;
- содержимое элемента, вызвавшего последнюю активацию монитора;
- идентификатор элемента, который вызвал активацию монитора.

Если настроена отправка журналов событий информационной безопасности, программа передает следующие данные на syslog-сервер:

- имя поставщика программы;
- название программы;
- версию Kaspersky MLAD;
- идентификатор подписи программы;
- идентификатор события ИБ;
- дату и время события ИБ;
- тип события ИБ;
- уточнение типа события ИБ;
- уровень важности события ИБ;
- имя пользователя, действия которого привели к записи события ИБ;
- IP-адрес компьютера, с которого пользователем были произведены действия, записанные в журналы событий ИБ;
- результат события ИБ;
- краткое содержание события ИБ;
- подробное описание события ИБ.

Данные, обрабатываемые локально на сервере Kaspersky MLAD

Для выполнения своих основных функций программа может принимать, хранить и обрабатывать следующую информацию:

- Информацию о полных резервных копиях программы, если выполнялось резервное копирование или обновление программы. Информация о полных резервных копиях программы хранится на сервере Kaspersky MLAD до их удаления пользователем.
- Информацию о резервных копиях томов (volumes) Docker, которые создаются во время удаления программы. Информация о резервных копиях томов Docker хранится на сервере Kaspersky MLAD до их удаления пользователем.
- Файлы с текстом Лицензионного соглашения текущей установленной версии программы.
- Файл legal_notices.txt с информацией о стороннем коде.
- Сертификаты для подключения к программе через веб-интерфейс.
- Сертификаты и ключи к сертификатам для шифрования соединения коннекторов и служб Kaspersky MLAD с внешними системами.

- Публичные ключи для проверки цифровой подписи дистрибутива. Публичные ключи хранятся на сервере Kaspersky MLAD до их удаления пользователем.

- Данные об учетных записях пользователей: идентификатор учетной записи, фамилию, имя, отчество, адрес электронной почты, состояние учетной записи (активна или заблокирована), пароль.

  В качестве фамилии, имени и отчества пользователя могут быть указаны значения, не идентифицирующие пользователя как физическое лицо (например, цех и должность). Информация, указанная в полях **Фамилия**, **Имя** и **Отчество** пользователей при создании учетных записей, хранится в открытом виде и программой не обрабатывается.

  Адреса электронной почты, указанные при создании учетных записей, используются при подключении пользователей к веб-интерфейсу программы. Адреса электронной почты пользователей указываются в журналах событий информационной безопасности. Адреса электронной почты используются для отправки уведомлений о зарегистрированных инцидентах.

  Адреса электронной почты пользователей хранятся в открытом виде.

  Kaspersky MLAD не хранит пароли пользователей в открытом виде. Для хранения паролей используется алгоритм расчета хеш-суммы scrypt. Kaspersky MLAD добавляет соль к паролю для предотвращения его декодирования. Пароли пользователей не записываются в журналы программы.

  Данные об учетных записях пользователей вводит системный администратор в меню администратора.

- Данные о ролях и назначенных для этих ролей прав: идентификатор роли, название роли, состояние роли (активна или неактивна), список назначенных прав, дату и время создания роли, дату и время изменения роли.

  Данные о ролях вводит системный администратор в меню администратора.

- Данные о подписках на уведомления: идентификатор подписки, название подписки, адреса электронной почты пользователей или дополнительных контактов для отправки уведомлений, имя, идентификатор и описание группы контактов, пользователей, которые входят в группу контактов, имя и описание дополнительного контакта, типы инцидентов, активы, модели и теги, по которым отправляются уведомления, состояние уведомления (активно или неактивно), информацию, включена ли отправка уведомлений об учетных инцидентах, язык уведомления.

  Данные о подписках, дополнительных контактах и групп контактов вводит системный администратор в меню администратора или пользователь с правами из группы прав **Управление уведомлениями**.

- Информацию о загруженных в Kaspersky MLAD лицензионных ключах.

- Данные об источниках данных: идентификатор, имя и описание карточки источника данных, состояние соединения с источником данных, тип источника данных, информация о тегах, поступающих от источника данных: теги источника данных, тип имени тега, используемое для преобразования в идентификатор тега в источнике данных, регулярное выражение, применяемое к имени тега для его преобразования в идентификатор тега, шаблон, по которому формируется идентификатор тега источника данных, тип преобразования; параметры для подключения и загрузки данных по протоколу OPC UA: адрес подключения, время ожидания подключения к серверу OPC UA, конфигурационный файл коннектора, информацию, требуется ли масштабировать полученные значения тегов, политику безопасности соединения, режим безопасности сообщений, имя пользователя и пароль для подключения к серверу, сертификат клиента, закрытый ключ клиента, пароль для закрытого ключа клиента, корневой сертификат OPC UA-сервера.

- Данные о параметрах Kaspersky MLAD:
  - Основные параметры программы: имя объекта мониторинга, URL- и IP-адреса для формирования ссылки на инциденты в уведомлениях об инцидентах, интервал получения данных из службы Message Broker, интервал получения статистических данных об инцидентах из базы данных, часовой пояс объекта мониторинга.
  - Параметры безопасности программы: количество попыток авторизации, период блокировки пользователя, период неактивности пользователя, информацию, является ли смена пароля при первом подключении обязательной, количество паролей пользователя, хранящихся в истории, срок действия пароля, минимальную длину пароля, информацию, требуется ли использование в пароле прописных, строчных букв латинского алфавита, цифр и/или специальных символов, объем и время хранения журналов событий информационной безопасности.
  - Параметры службы Anomaly Detector: информацию, требуется ли использовать детекторы Limit Detector, Forecaster и/или Rule Detector, информацию, требуется ли пропускать разрывы в данных, максимальное количество запрашиваемых записей из службы Message Broker, количество сообщений, отправляемых в одном блоке в службу Message Broker.
  - Параметры службы Keeper: информацию, требуется ли сохранять значения всех тегов, время ожидания получения значений тегов, инцидентов и метрик.
  - Параметры службы Mail Notifier: адрес электронной почты отправителя уведомлений, адрес и порт SMTP-сервера, имя пользователя и пароль для подключения к SMTP-серверу, информацию, требуется ли использовать TLS-соединение, сертификат и ключ к сертификату SMTP-сервера.
  - Параметры службы Similar Anomaly: минимальное и максимальное количество инцидентов для группы, максимальное расстояние между схожими инцидентами.
  - Параметры службы Stream Processor: период равноинтервальной сетки, конфигурационный файл с параметрами службы Stream Processor.

    В конфигурационном файле службы Stream Processor хранятся идентификаторы тегов, которые обрабатываются службой, и значения параметров обработки тегов.

    > Значения параметров обработки тегов задаются специалистами "Лаборатории Касперского" индивидуально для каждого объекта мониторинга.

  - Параметры службы Trainer: максимальное количество одновременно обучаемых элементов.
  - Параметры коннектора HTTP Connector: размер записываемого блока, максимальный размер загружаемого файла, информацию, требуется ли использовать TLS-соединение и рекомендуемые параметры TLS-соединения, сертификат и ключ к сертификату HTTPS-сервера, корневой сертификат для проверки подписи сертификата клиента, информацию, требуется ли масштабировать полученные значения тегов, информацию, требуется ли игнорировать регистр в именах тегов.
  - Параметры коннектора MQTT Connector: информацию, требуется ли использовать TLS-соединение и рекомендуемые параметры TLS-соединения, адрес и порт MQTT-брокера, имя пользователя и пароль для подключения к MQTT-брокеру, корневой сертификат для проверки подписи сертификата клиента, сертификат клиента и ключ к сертификату клиента, список подписок MQTT для получения тегов, топик MQTT для публикации сообщений, формат обработки поступающих данных, конфигурационный файл коннектора, информацию, требуется ли масштабировать полученные значения тегов.

    В конфигурационном файле коннектора MQTT Connector хранятся идентификаторы, имена, описания, типы и единицы измерения тегов.

- Параметры коннектора AMQP Connector: информацию, требуется ли использовать TLS-соединение и рекомендуемые параметры TLS-соединения, адрес и порт AMQP-брокера, имя пользователя и пароль для подключения к AMQP-брокеру, корневой сертификат для проверки подписи сертификата клиента, сертификат клиента и ключ к сертификату клиента, виртуальный узел AMQP, имена точек обмена AMQP для получения значений тегов и для публикации сообщений, список подписок и очередь для получения значений тегов, топик AMQP для публикации сообщений, формат обработки поступающих данных, конфигурационный файл коннектора, информацию, требуется ли масштабировать полученные значения тегов.

  В конфигурационном файле коннектора AMQP Connector хранятся идентификаторы, имена, описания, типы и единицы измерения тегов.

- Параметры коннектора KICS Connector: файл свертки для коннектора KICS Connector, пароль для коннектора KICS Connector, информацию, требуется ли отправлять сообщения в Kaspersky Industrial CyberSecurity for Networks, частоту семплирования тегов, информацию, требуется ли масштабировать полученные значения тегов.

- Параметры коннектора CEF Connector: информацию, требуется ли получать события для службы Event Processor, информацию, требуется ли отправлять зарегистрированные инциденты и/или события в SIEM-систему, IP-адрес и порт для отправки событий и инцидентов в SIEM-системы, информацию, требуется ли отправлять журналы событий ИБ на syslog-сервер, транспортный протокол для отправки событий ИБ на syslog-сервер, адрес и порт syslog-сервер для отправки событий ИБ, информацию, требуется ли использовать защищенное TLS-соединение и рекомендуемые параметры TLS-соединения, сертификат и ключ к сертификату сервера, корневой сертификат для проверки подписи сертификата клиента, сертификат и ключ к сертификату клиента, корневой сертификат для проверки подписи сертификата сервера.

- Параметры коннектора WebSocket Connector: URL-адрес WebSocket-сервера, корневой сертификат для проверки подписи сертификата сервера, сертификат и ключ к сертификату клиента, формат обработки поступающих данных, конфигурационный файл коннектора, информацию, требуется ли масштабировать полученные значения тегов, информацию, требуется ли отправлять инциденты, информацию, требуется ли использовать рекомендуемые параметры TLS-соединения.

- Параметры службы Event Processor: конфигурационный файл службы, информацию, требуется ли обрабатывать инциденты как события, максимальное количество слоев сети, коэффициент, определяющий допустимую дисперсию длительности паттерна, интервал получения событий эпизода, размера эпизода, способ сохранения состояния службы Event Processor, периодичность создания резервных копий компонента, резервную копию состояния службы Event Processor, режим отправки оповещений при активации монитора в режиме сна, периодичность и продолжительность режима сна, интервал истории событий для обработки в режиме сна, порог вероятности эксфильтрации, файл с весами модели для выявления эксфильтрации, смещение и размер буфера.

- Параметры приоритетов инцидентов: идентификатор приоритета инцидента, названия приоритета инцидента на русском и английском языке, цвет, оценка и код приоритета инцидента.

- Параметры статуса инцидентов: идентификатор статуса инцидента, названия статуса инцидента на русском и английском языке, порядковый номер сортировки, информацию, требуется ли отображать зарегистрированные инциденты с этим статусом.

- Параметры причины инцидентов: идентификатор причины инцидента, название причины инцидента, порядковый номер сортировки.

- Параметры службы ведения журналов: уровни ведения журналов служб и коннекторов программы.

- Параметры временных интервалов для графиков в разделах **Мониторинг**, **История** и **Временной срез**: идентификатор временного интервала, названия временного интервала на русском и английском языке, порядковый номер сортировки, идентификатор пользователя, который создал временной

интервал, идентификатор пользователя, который последним изменил временной интервал, значение временного интервала.

- Параметры отображения пунктов основного меню и меню администратора: информацию, требуется ли отображать пункты основного меню и меню администратора в веб-интерфейсе программы.

Параметры Kaspersky MLAD задает системный администратор в меню администратора.

- Данные об активах и тегах: имя актива, идентификатор актива, идентификатор родительского актива, к которому относится актив, описание актива, уровень критичности актива, имя типа актива, идентификатор типа актива, имена и значения специальных параметров типа актива, описание типа актива, идентификатор и имя актива, к которому относится тег, идентификатор и имя тега, альтернативное имя тега, описание тега, единицу измерения тега, верхние и нижние пороги блокировки, сигнализации и достоверности измерений, комментарий к тегу, координаты расположения датчика объекта мониторинга в пространстве по осям абсцисс, ординат и аппликат, имя устройства, от которого поступают теги из внешней системы, параметры смещения и множителя, с помощью которых выполняется перерасчет полученных от источников данных и коннекторов значений тегов.

  Данные об активах и тегах вводит системный администратор в меню администратора.

- Данные о пресетах: имя пресета, идентификатор пресета, идентификатор и имя актива, к которому относится пресет, имена и идентификаторы тегов, входящих в пресет, название и описание графической области, режим масштабирования оси, верхнюю и нижнюю границы отображения значений тегов, контрольные линии, информацию о тегах, входящих в состав графической области, информацию, требуется ли настроить выражение для раздела **Временной срез**, подписи осей абсцисс и ординат, название выражения для расчета значений тегов, выражения для расчета значений тегов, цвет графика для пресета в разделе **Временной срез**.

  Данные может ввести любой пользователь в разделе **Пресеты**.

- Информацию о количестве поступивших в секунду наблюдений по тегам и событий. Данные рассчитывает программа на основании данных, полученных от внешних систем.

- Информацию о значениях тегов и событий, поступивших в систему. Данные поступают от внешних систем, для которых пользователь настроил получение данных.

- Информацию о сформированных артефактах. Данные рассчитывает программа на основании данных, полученных от внешних систем.

- Информацию о статусах служб программы: имя и текущий статус службы. Программа отображает статус службы, полученный из соответствующих компонентов.

- Данные о зарегистрированных инцидентах и группах инцидентов: идентификатор инцидента, дату и время начала инцидента, приоритет инцидента, уровень критичности актива, имя и идентификатор топ-тега, причину инцидента, имя детектора, зарегистрировавшего инцидент, имя группы инцидентов, статус инцидента, имя ML-модели, элемент ML-модели, значение артефакта элемента ML-модели, пороговое значение, значение топ-тега, пороги блокировки, описание и единицу измерения тега, тип инцидента, дату и время формирования наблюдения, время, на которое формирование наблюдения отстает от поступления этого наблюдения в программе или опережает его, экспертные рекомендации к инциденту и к группе, комментарий к инциденту, имя и идентификатор группы инцидентов, количество инцидентов в группе, дату и время создания группы инцидентов, статус зарегистрированных инцидентов в группе, идентификаторы тегов группы, порог блокировки, который был достигнут при регистрации инцидента.

  Программа формирует эти данные в результате анализа полученных данных и на основании параметров, заданных пользователем.

- Параметры отображения графиков в разделах **Мониторинг** и **История**: высоту графиков, пресет для перехода в раздел **История** (только при настройке параметров отображения графика в разделе **Мониторинг**), информацию, требуется ли отображать график наблюдений в выбранном цвете, цвет графиков наблюдений, информацию, требуется ли отображать график прогнозов в выбранном цвете, цвет графиков прогнозов, информацию, требуется ли отображать на графиках имена и описания тегов, прогнозируемое значение тега и/или индивидуальную ошибку тега, информацию, требуется ли отображать индикаторы для всех инцидентов на графиках, информацию, требуется ли отображать на графиках пороги блокировки и/или контрольные линии, элемент ML-модели, используемый для формирования прогнозируемых значений, пресеты, временные интервалы, дату и время для отображения графиков.

  Данные может ввести любой пользователь в разделах **Мониторинг** и **История**.

- Параметры отображения графиков в разделе **Временной срез**: высоту графиков, элемент ML-модели, используемый для формирования прогнозируемых значений, пресеты, временные интервалы, дату и время для отображения графиков.

  Данные может ввести любой пользователь в разделе **Временной срез**.

- Параметры обработки и отображения данных для процессора событий: идентификатор, имя и состояние головы внимания, информацию, включено ли распознавание паттернов, параметры предмета внимания (индивидуальны для каждого объекта мониторинга), информацию, требуется ли обобщать параметры условий, параметры условий головы внимания (индивидуальны для каждого объекта мониторинга).

  Если в параметрах службы Event Processor включен переключатель **Обрабатывать инциденты как события**, то программа хранит и обрабатывает следующие данные:

  - имя детектора;
  - имя используемой ML-модели;
  - имя и идентификатор топ-тега;
  - имя группы инцидентов, в которую входит зарегистрированный инцидент;
  - значение топ-тега;
  - идентификатор инцидента.

  Данные для процессора событий может ввести любой пользователь в разделе **Процессор событий**.

- Данные о мониторинге событий и паттернов в процессоре событий: имя и идентификатор монитора, статус отправки оповещений об активациях монитора, состояние монитора, количество зарегистрированных активаций на скользящем окне, дату и время последней активации, размер списка активаций, тип подписки, слои, на которых отслеживаются паттерны, скользящее окно, порог активации, голову внимания, параметр предмета внимания, информацию, отслеживает ли монитор события или паттерны при обобщенном предмете внимания, тип активации, имена параметров события, за значениями которых наблюдает монитор, типы фильтров, типы значений, которые отслеживает монитор, значения параметров событий, которые отслеживает монитор, идентификатор значения параметра события, события или паттерна, обнаружение которого привело к активации монитора, дату и время обнаружения события в потоке событий, временной интервал между текущим событием и предыдущим событием в потоке событий на скользящем окне, количество повторений события в потоке событий на скользящем окне, количество параметров события, для которых поступили значения от объекта мониторинга, дату и время последнего обнаружения события в потоке событий на скользящем окне, параметр предмета внимания и его значение, вызвавшее активацию монитора, дату и время активации монитора, параметры события, поступившего от объекта мониторинга, количество событий, входящих в состав паттерна, который вызвал активацию монитора, общее количество повторений паттерна в потоке событий, дату и время DNS-запроса, IP-адрес хоста, домен первого уровня в DNS-запросе, содержание DNS-запроса, длина строки DNS-запроса без домена, значение энтропии, рассчитанное для строки DNS-запроса без домена, вероятность того, что DNS-запрос содержит признаки эксфильтрации данных, час активности в формате UTC, количество событий, которые были обнаружены в необычные для них часы активности, признак, указывающий, является ли час активности необычным для поступивших событий, последнее событие, обнаруженное в необычный час активности, идентификатор обобщенного события, идентификатор обобщенного паттерна, количество активаций монитора обобщенным событием или паттерном, количество событий в составе обобщенного паттерна, количество значений параметра предмета внимания, обнаружение которых вызвало активацию монитора, временной интервал между первым и последним событием в обнаруженном обобщенном паттерне, обнаруженное обобщенное событие, обнаруженный обобщенный паттерн, значения параметров предмета внимания, обнаружение которых вызвало активацию монитора.

  Программа формирует данные в результате анализа полученных данных и параметров, заданных пользователем в разделе **Процессор событий**.

- Данные о регистрации паттернов в процессоре событий: идентификатор паттерна, дату и время последнего обнаружения паттерна на интервале, количество обнаружений паттерна в потоке событий объекта мониторинга за заданный период, количество событий в составе паттерна, дату и время последнего обнаружения паттерна в потоке событий или в режиме сна, дату и время начала и окончания периода загрузки паттернов, тип паттерна, голову внимания, значения параметров события, по которым регистрируются паттерны, параметры шаблона, по которым регистрируются паттерны (индивидуальны для каждого объекта мониторинга), идентификатор вложенного паттерна, дату и время окончания вложенного паттерна в последовательности паттернов, количество обнаружений вложенного паттерна, количество событий в составе вложенного паттерна, временной интервал между вложенным паттерном и паттерном, выявленным в последовательности паттернов на текущем слое до вложенного паттерна, дату и время последнего обнаружения вложенного паттерна в последовательности паттернов на текущем слое, идентификаторы событий, входящих в состав паттерна, дату и время обнаружения события в структуре паттерна, временной интервал между выбранным событием и предыдущим событием, количество повторений события в структуре выбранного паттерна, количество параметров события, для которых поступили значения от объекта мониторинга, дату и время последнего обнаружения события в потоке событий.

  Программа формирует данные в результате анализа данных и параметров, заданных пользователем в разделе **Процессор событий**.

- Информация о ML-моделях и их параметрах: идентификатор (ID) и уникальный идентификатор (UUID) ML-модели, имя, описание, статус и состояние ML-модели, имя пользователя, который последним изменил ML-модель, дату и время последнего изменения ML-модели, имя пользователя, который создал ML-модель, дату и время создания или загрузки ML-модели, имена и идентификаторы входящих в нее элементов, интервал времени и разметки для проведения инференса, оценка исторического инференса.

  Данные вводит и/или загружает системный администратор или пользователь с правами **Управление ML-моделями** в разделе **Модели**.

- Информацию об элементах ML-моделей и их параметрах:

  - Общие параметры для всех типов элементов ML-моделей: идентификатор, имя и описание элемента ML-модели, статус и состояние элемента ML-модели, интервал времени, при достижении которого регистрируется повторный инцидент, интервал времени, в течение которого не регистрируются повторные инциденты, интервал наблюдения за аномалией, доля длительности аномалии в интервале, причину и статус инцидента, приоритет инцидента, уровень критичности актива, цвет точек-индикаторов для инцидентов, экспертные рекомендации.

  - Основные параметры предиктивных элементов ML-моделей: архитектуру элемента, шаг сетки в секундах, имена и идентификаторы входных и выходных тегов, порог регистрации инцидентов, степенной показатель суммарной ошибки прогноза, коэффициент сглаживания суммарной ошибки прогноза, количество шагов входного окна для входных значений, количество шагов, на которое смещается начало выходного окна относительно начала входного окна, количество шагов выходного окна.

  - Параметры нейросетевого элемента с Dense-архитектурой: множители для вычисления количества нейронов на слоях, функции активации на слоях, коэффициент регуляризации для предотвращения переобучения элемента ML-модели.

  - Параметры нейросетевого элемента с RNN-архитектурой: количество GRU-нейронов на слоях, количество распределенных по времени нейронов на слоях декодирующего блока, информацию, требуется ли восстанавливать данные, принимаемые на вход сети, коэффициент регуляризации для предотвращения переобучения элемента ML-модели.

  - Параметры нейросетевого элемента с CNN-архитектурой: размер фильтров на слоях, количество фильтров на слоях, коэффициент регуляризации для предотвращения переобучения элемента ML-модели, размер окна выборки максимума, количество нейронов на слоях декодирующего блока, информацию, требуется ли восстанавливать данные, принимаемые на вход сети.

  - Параметры нейросетевого элемента с TCN-архитектурой: коэффициент регуляризации для предотвращения переобучения элемента ML-модели, размер фильтров, количество слоев в остаточном блоке, количество фильтров на слоях, расширения на слоях, тип слоя перед выходным, функцию активации.

  - Параметры нейросетевого элемента с Transformer-архитектурой: коэффициент регуляризации в кодирующем блоке, количество голов внимания, количество кодирующих блоков, множители для вычисления количества нейронов на слоях декодирующего блока.

  - Параметры обучения предиктивного элемента: интервал времени для обучения, имена и идентификаторы разметок для обучения, информацию, требуется ли зафиксировать порог регистрации инцидентов, максимальную продолжительность обучения, соотношение обучающей и валидационной выборок, максимальное количество эпох для обучения, количество эпох, в течение которых должны отсутствовать валидационные потери при ранней остановке обучение, разрешение графиков для отображения результатов обучения, размер пакета данных для обучения, количество блоков, режим инференса, режим обучения, режим автоматического разделения данных на блоки, используемый объем памяти для обучения, информацию, требуется ли инициализировать веса модели значениями из результатов предыдущего обучения и/или перемешивать данные, значение для инициализации генератора псевдослучайных чисел, коэффициент скорости обучения, алгоритм оптимизации обучения, алгоритм оптимизации потерь.

  - Информацию о результатах обучения предиктивного элемента: очередь обучения (идентификаторы и имена элементов ML-модели, которые ожидают очереди на обучение), статус обучения, имена и идентификаторы обучающихся элементов, количество блоков, на которые разбиты данные для обучения, имя пользователя, который запустил обучения элемента, продолжительность обучения, дату и время начала и окончания обучения, продолжительность интервалов времени данных в обучающей

выборке, количество узлов РИВС, входящий в обучающую выборку, ошибки обучения и валидации, прогноз обученной ML-модели на обучающей выборке.

- Параметры элементов на основе диагностических правил: информацию, требуется ли интерпретировать невозможность оценки условия как выполнение правила, параметры фильтрации по времени: тип интервала, годы, дни, дни недели и интервал времени, в течение которого требуется проверять входные данные в соответствии с заданным правилом; информация о вычислимых тегах: имя вычислимого тега, тип и имена тегов, значения которых использованы для расчета вычислимого тега, выражение для расчета вычислимого тега, состояние проверки выражения для расчета вычислимого тега; параметры условия на поведение тегов: тип и имя тега, для которого добавлено условие, поведение тега, условие выполнения правила, количество шагов РИВС, пороговое значение тега, минимальное количество срабатываний правила для регистрации инцидента, значение уклона тренда, интервал времени между соседними оценками тренда, значение порога изменений, направление изменения значений тега, значение тега, максимальное отклонение тега от указанного значения, направление изменения разброса значения тега, информацию, используется ли в правиле пауза и параметры паузы: минимальный и максимальный интервалы ожидания, используемые групповой и логический операторы.

- Параметры элементов на основе эллиптического конверта: порог регистрации инцидентов, шаг сетки в секундах, имена и идентификаторы входных тегов, которые необходимо включить в ML-модель.

- Параметры обучения элемента на основе эллиптического конверта: интервал времени для обучения, имена и идентификаторы разметок для обучения, информацию, требуется ли зафиксировать порог регистрации инцидентов, долю выборки для оценки среднего и ковариации, долю выбросов в выборке, значение для инициализации генератора псевдослучайных чисел, разрешение графиков для отображения результатов обучения, информацию, предполагается ли, что значения тегов центрированы.

- Информацию о результатах обучения элемента на основе эллиптического конверта: очередь обучения (идентификаторы и имена элементов ML-модели, которые ожидают очереди на обучение), статус обучения, имена и идентификаторы обучающихся элементов, имя пользователя, который запустил обучения элемента, продолжительность обучения, дату и время начала и окончания обучения, продолжительность интервалов времени данных в обучающей выборке, количество узлов РИВС, входящий в обучающую выборку, степень отклонения тегов, значения тегов, распределение значений тегов и корреляция тегов.

Данные вводит и/или загружает системный администратор или пользователь с правами **Управление ML-моделями** в разделе **Модели**.

- Информацию о разметках: идентификатор, имя и описание разметки, информация о связанных с разметкой ML-моделях и элементах ML-моделей, интервал, с которым рассчитываются данные на РИВС, цвет разметки, способ появления разметки в программе, информацию, используется ли разметка в качестве основного индикатора инференса, параметры фильтрации по времени: тип интервала, годы, дни, дни недели и интервал времени, в течение которого требуется проверять входные данные в соответствии с заданными условиями разметки; информация о вычислимых тегах: имя вычислимого тега, тип и имена тегов, значения которых использованы для расчета вычислимого тега, выражение для расчета вычислимого тега, состояние проверки выражения для расчета вычислимого тега; параметры условия на поведение тегов: тип и имя тега, для которого добавлено условие, поведение тега, условие выполнения правила, количество шагов РИВС, пороговое значение тега, минимальное количество срабатываний правила для регистрации инцидента, значение уклона тренда, интервал времени между соседними оценками тренда, значение порога изменений, направление изменения значений тега, значение тега, максимальное отклонение тега от указанного значения, направление изменения разброса значения тега, информацию, используется ли в правиле пауза и параметры паузы: минимальный и максимальный интервалы ожидания, используемые групповой и логический операторы.

  Данные вводит и/или загружает системный администратор или пользователь с правами **Управление ML-моделями** в разделе **Модели**.

- Журналы событий информационной безопасности: идентификатор событий ИБ, дату и время события ИБ, тип события ИБ, уточнение типа события ИБ, уровень важности события ИБ, адрес электронной почты пользователя, действия которого привели к записи события ИБ, IP-адрес компьютера, с которого пользователем были произведены действия, записанные в журналы событий ИБ, результат события ИБ, краткое содержание события ИБ, подробное описание события ИБ.

  IP-адреса компьютеров, с которых было выполнено подключение к веб-интерфейсу программы, указываются в журналах событий информационной безопасности.

  Данные формируются Kaspersky MLAD автоматически.

  Kaspersky MLAD хранит журналы событий ИБ в течении времени, заданном в параметре **Время хранения журналов событий информационной безопасности (сут)** при настройке параметров безопасности. Программа удаляет ранние записи журналов событий ИБ при превышении объема для хранения события ИБ, заданного в параметре **Объем журналов событий информационной безопасности (МБ)**.

- Журналы контейнеров Kaspersky MLAD: дату и время события, уровень важности события, имя контейнера, для которого зарегистрировано событие, описание события.

  Данные формируются Kaspersky MLAD автоматически.

  Kaspersky MLAD хранит журналы контейнеров в течение двух дней.

Система ведения журналов (Grafana) не передает пользовательские данные в "Лабораторию Касперского" или на сторонние серверы. Вы можете ознакомиться с порядком хранения и обработки данных в системе ведения журналов в руководстве пользователя системы ведения журналов Grafana.

Данные, обрабатываемые на компьютерах пользователей

При работе с веб-интерфейсом Kaspersky MLAD в файлах cookie браузера пользователя хранятся следующие данные:

- Индивидуальные токены JSON Web Token для поддержки пользовательской сессии подключения к веб-интерфейсу программы. Индивидуальный токен хранится в файлах cookie браузера пользователя в течение периода неактивности пользователя, заданного при настройке параметров безопасности.

- Идентификатор запущенной сессии Grafana, если пользователь переходил к просмотру журналов программы. Идентификатор сессии Grafana хранится в файлах cookie браузера пользователя в течение 30 дней.

В браузере пользователя хранятся данные, которые используются для отображения веб-интерфейса: последний использованный язык локализации веб-интерфейса программы, последний использованный вариант отображения основного меню (скрытое или развернутое отображение), последние использованные значения временного интервала, пресета, даты и времени, элементы ML-моделей и параметры отображения графиков в разделах **Мониторинг**, **История** и **Временной срез**, последние использованные параметры нумерации страниц, последние заданные фильтры для отображения данных в разделе **Процессор событий**, последние использованные значения статуса и причины инцидентов в разделе **Инциденты**, информация о динамических пресетах по инцидентам, информация о текущей установленной версии Kaspersky MLAD. Эти данные хранятся в браузере бессрочно. Вы можете самостоятельно удалить эти данные из локального хранилища браузера.

При экспорте инцидентов программа сохраняет на компьютер пользователя файл формата XLSX со следующими данными:

- именем объекта мониторинга;

- периодом, за который были выгружены инциденты;

- идентификаторами зарегистрированных инцидентов;
- датами и временем зарегистрированных инцидентов;
- приоритетами инцидентов;
- статусами зарегистрированных инцидентов;
- именами групп, в которые входят зарегистрированные инциденты;
- именами и идентификаторами топ-тегов, оказавших наибольшее влияние на регистрацию инцидентов;
- значениями топ-тегов;
- единицами измерения топ-тегов;
- описаниями топ-тегов;
- именами ML-моделей, зарегистрировавших инциденты;
- именами детекторов, зарегистрировавших инциденты.

При экспорте журналов событий информационной безопасности из системы ведения журналов Grafana программа сохраняет на компьютер пользователя файл формата CSV со следующими данными:

- идентификаторами событий ИБ;
- датами и временем событий ИБ;
- типами событий ИБ;
- уточнениями типов событий ИБ;
- уровнями важности событий ИБ;
- именами пользователей, действия которых привели к записи событий ИБ;
- IP-адресами компьютеров, с которых пользователями были произведены действия, записанные в журналы событий ИБ;
- результатами событий ИБ;
- краткими содержаниями событий ИБ;
- подробными описаниями событий ИБ.

При экспорте журналов контейнеров из системы ведения журналов Grafana программа сохраняет на компьютер пользователя файл формата CSV со следующими данными:

- датами и временем событий;
- уровнями важности событий;
- именем контейнера, для которого зарегистрированы события;
- описаниями событий.

При экспорте конфигурации активов и тегов программа сохраняет на компьютер пользователя файл формата XLSX со следующими данными:

- идентификатором типа актива;
- уникальным именем типа актива;
- именами специальных параметров для типа актива (при наличии);
- описанием типа актива (при наличии);
- идентификатором актива;
- именем актива;
- уникальным именем актива в рамках его родительского актива;
- описанием актива (при наличии);
- именем родительского актива, к которому относится актив (при наличии);
- идентификатором родительского актива (при наличии);
- именами специальных параметров актива (при наличии);
- значениями специальных параметров актива (при наличии);
- уровнем критичности актива;
- идентификатором тега;
- уникальным именем тега;
- уникальным альтернативным именем тега (при наличии);
- описанием тега;
- именем родительского актива, к которому относится тег (при наличии);
- идентификатором родительского актива;
- типом тега (при наличии);
- единицей измерения тега;
- нижним и верхним порогами блокировки (при наличии);
- нижним и верхним порогами сигнализации (при наличии);
- нижним и верхним порогами достоверности измерений (при наличии);
- комментарием к тегу;
- координатами расположения датчика объекта мониторинга по осям абсцисс, ординат и аппликат (при наличии);

- значением смещения, которое необходимо добавить к значению тега, полученному от источника данных или коннектора;
- значением множителя, на которое необходимо умножить значение тега, полученное от источника данных или коннектора.

При экспорте пресетов программа сохраняет на компьютер пользователя файл формата JSON со следующими данными:

- именем пресета;
- идентификатором пресета;
- порядковым номером отображения пресета в разделе **Пресеты**;
- списком идентификаторов тегов, входящих в состав пресета;
- идентификатором актива, к которому относится пресет;
- информацией, требуется ли отображать пресет в разделе **Временной срез**;

- параметрами графической области в составе пресета:
  - названием графической области;
  - описанием графической области;
  - порядковым номером отображения графической области в пресета в разделах **Мониторинг**, **История** и **Пресеты**;
  - верхней и нижней границами отображения значений тегов в графической области;
  - параметрами контрольных линий:
    - идентификатором контрольной линии;
    - контрольным значением;
    - цветом контрольной линии.
  - режимом масштабирования оси;
  - способом масштабирования графика в режиме единой оси;
  - списком идентификаторов тегов, входящих в состав графической области;
  - идентификатором графической области;
  - идентификатором пресета, к которому относится графическая область.
- при использовании пресета для отображения данных в разделе **Временной срез** программа сохраняет следующие данные:
  - подпись по оси абсцисс на графике в разделе **Временной срез**;
  - название выражения, по которому рассчитываются значения тегов;
  - подпись по оси ординат на графике в разделе **Временной срез**;
  - выражение, по которому рассчитываются значения тегов;
  - цвет графика для пресета в разделе **Временной срез**.

При экспорте файла с весами модели для выявления эксфильтрации программа сохраняет на компьютер пользователя веса модели, которую процессор событий использует для выявления признаком эксфильтрации данных в DNS-запросах.

При экспорте конфигурационного файла источника данных OPC UA программа сохраняет на компьютер пользователя файл формата JSON со следующими данными:

- Список тегов в источнике данных. Для каждого тега хранятся следующие параметры:
  - Имя тега в <PRODUCT_NAM_NOM>.
  - Идентификатор узла, по которому доступен тег в источнике данных.
  - Путь к тегу в источнике данных.
  - Преобразование текстовых значений конкретного тега в числовые (текстовое значение тега в источнике данных и соответствующее числовое значение).
- Преобразование текстовых значений всех тегов в числовые (текстовое значение тега в источнике данных и соответствующее числовое значение).
- Кодек Python, используемый для декодирования текстовых значений тегов.

При экспорте параметров Kaspersky MLAD программа сохраняет на компьютер пользователя конфигурационные файлы со следующими данными:

- Файл с параметрами статусов инцидентов, содержащий следующие данные:
  - идентификатор статуса инцидента;
  - название статуса инцидента на русском языке;
  - название статуса инцидента на английском языке;
  - порядковый номер статуса инцидента для сортировки;
  - информацию, требуется ли отображать зарегистрированные инциденты с этим статусом.
- Файл с параметрами причин инцидентов, содержащий следующие данные:
  - идентификатор причины инцидента;
  - название причины инцидента;
  - порядковый номер причины инцидента для сортировки.

- Файл с параметрами временных интервалов отображения данных на графиках **Мониторинг**, **История** и **Временной срез**, содержащий следующие данные:
  - идентификатор временного интервала;
  - название временного интервала на русском языке;
  - название временного интервала на английском языке;
  - порядковый номер временного интервала для сортировки;
  - идентификатор пользователя, который создал временный интервал;
  - идентификатор пользователя, который последним изменил временной интервал;
  - значение временного интервала в миллисекундах.
- Параметры служб и коннекторов Kaspersky MLAD:
  - идентификаторы параметров;
  - имена параметров в базе данных Kaspersky MLAD;
  - типы введенных значений;
  - введенные или выбранные значения;
  - имя блока параметров, к которому относится текущий параметр;
  - порядковый номер отображения параметра в текущем разделе;
  - требования к значению параметра.
- Конфигурационный файл службы Stream Processor, содержащий следующие данные:
  - идентификаторы тегов, которые обрабатываются службой Stream Processor;
  - значения параметров обработки тегов.

    Значения параметров обработки тегов задаются специалистами "Лаборатории Касперского" индивидуально для каждого объекта мониторинга.
- Конфигурационные файлы коннекторов MQTT Connector, AMQP Connector и WebSocket Connector, содержащие следующие данные:
  - идентификаторы тегов, полученные с помощью коннектора MQTT Connector, AMQP Connector или WebSocket Connector;
  - единицу измерения временной метки тегов;
  - тип получаемых данных;
  - формат шаблона для декодирования типа получаемых данных.

- Конфигурационный файл службы Event Processor, содержащий следующие данные:
  - правила соответствия параметров событий, полученных коннектором CEF Connector, с именами параметров событий для обработки в службе Event Processor;
  - список обрабатываемых параметров событий;
  - время и масштаб времени для обработки событий;
  - интервал времени, за который Kaspersky MLAD восстанавливает эпизоды после перезапуска службы Event Processor;
  - частоту (в минутах) синхронизации информации об активациях мониторов в таблицу базы данных службы Event Processor;
  - порядок и взаимосвязь параметров событий для их отображения на графе отношений в разделе **История событий**.
- Файл свертки для коннектора KICS Connector, содержащий следующие данные:
  - В зашифрованном виде открытый ключ сертификата сервера Kaspersky Industrial CyberSecurity for Networks, сертификат, выданный сервером Kaspersky Industrial CyberSecurity for Networks для коннектора KICS Connector (с закрытым ключом).

    Содержимое файла зашифровано с помощью пароля, который был указан при добавлении коннектора KICS Connector или при создании нового файла свертки для этого коннектора.
  - Конфигурационные данные для коннектора KICS Connector: имя пользователя, под которым Kaspersky MLAD будет подключаться к серверу Kaspersky Industrial CyberSecurity for Networks, идентификатор коннектора KICS Connector, адрес сервера Kaspersky Industrial CyberSecurity for Networks для подключения.

Директории для хранения данных программы

Kaspersky MLAD использует для хранения данных следующие директории и их поддиректории:

- Директории программы (по умолчанию /opt/kaspersky/mlad):
  - . – корневая директория программы. Используется для хранения конфигурационного файла .env, журналов установки и обновления Kaspersky MLAD, подписи дистрибутива, утилиты mladctl для проверки целостности дистрибутива, установки, обновления, резервного копирования, восстановления, запуска, остановки, очистки и удаления программы. Также в корне директории программы хранятся примечания к текущему выпуску Kaspersky MLAD (Release Notes).
  - ./configs – директория для хранения конфигурационных файлов Kaspersky MLAD. Директория содержит следующие поддиректории:
    - /environment – директория для хранения конфигурационного файла config.env, а также конфигурационных файлов служб Database и Time Series Database.
    - ./logger – директория для хранения конфигурационных файлов службы Logger.
  - ./data – директория для хранения данных, которые загружаются с использованием коннектора HTTP Connector.
  - ./legal – директория для хранения текста Лицензионного соглашения, метки о дате его принятия пользователем, а также файла legal_notices.txt, в котором содержится информация о стороннем коде.
  - ./ssl – директория для хранения скрипта генерации самоподписанного сертификата, обеспечивающего HTTPS-соединение с браузером пользователя Kaspersky MLAD.
  - ./ssl/tokens – директория для хранения ключа JWT (JSON Web Token).
  - ./ssl/nginx – директория для хранения сертификатов, обеспечивающих HTTPS-соединение с браузером пользователя Kaspersky MLAD.
  - ./ssl/public_cert – директория для хранения публичных ключей для проверки цифровой подписи дистрибутива.
  - ./mlad_backup-<номер версии>-<номер сборки> – директория для хранения резервных копий Kaspersky MLAD по умолчанию. Резервная копия Kaspersky MLAD может быть создана с помощью команды backup утилиты mladctl или в процессе обновления программы с помощью команды upgrade. При выполнении резервного копирования программы вы можете указать другую директорию для хранения резервной копии. Содержимое повторяет структуру корневой директории, в которую установлен Kaspersky MLAD, а также содержит следующие поддиректории:
    - ./containers_backup – директория для хранения архива с резервной копией контейнеров служб Kaspersky MLAD.
    - ./volumes_backup – директория для хранения архива с резервной копией томов (volumes) Docker.
  - ./volumes_backup_<дата удаления> – директория для хранения резервных копий томов (volumes) Docker, которые создаются во время удаления Kaspersky MLAD.
- Директория /var/lib/docker/volumes/:

- ./<имя директории программы>_postgres-volume – директория для хранения файлов базы данных Postgres.
- ./<имя директории программы>_influxdb-volume – директория для хранения файлов службы Time Series Database.
- ./<имя директории программы>_logger-volume – директория для хранения файлов подсистемы ведения журналов.
- ./<имя директории программы>_webstatic-volume – директория для хранения статических данных веб-интерфейса программы.

- /etc/hosts – служебный файл, описывающий соответствие IP-адресов и имен хостов внешних серверов.

Доступ ко всем директориям, кроме корневой директории, директорий configs и /var/lib/docker/volumes/ и файла /etc/hosts, есть у пользователей с root-правами и пользователя, от имени которого выполнялась установка программы. Доступ к корневой директории, директориям configs и /var/lib/docker/volumes/ и файлу /etc/hosts есть только у пользователей с root-правами.

Удаление или изменение любого файла Kaspersky MLAD может привести к нарушению работоспособности программы.

Задачи системного администратора

Этот раздел содержит описание задач системного администратора, выполняемых в меню администратора программы.

Управление учетными записями пользователей

Для того чтобы обеспечить безопасную работу пользователей с Kaspersky MLAD, вам нужно создать учетную запись для каждого пользователя.

Управление учетными записями пользователей Kaspersky MLAD доступно системным администраторам.

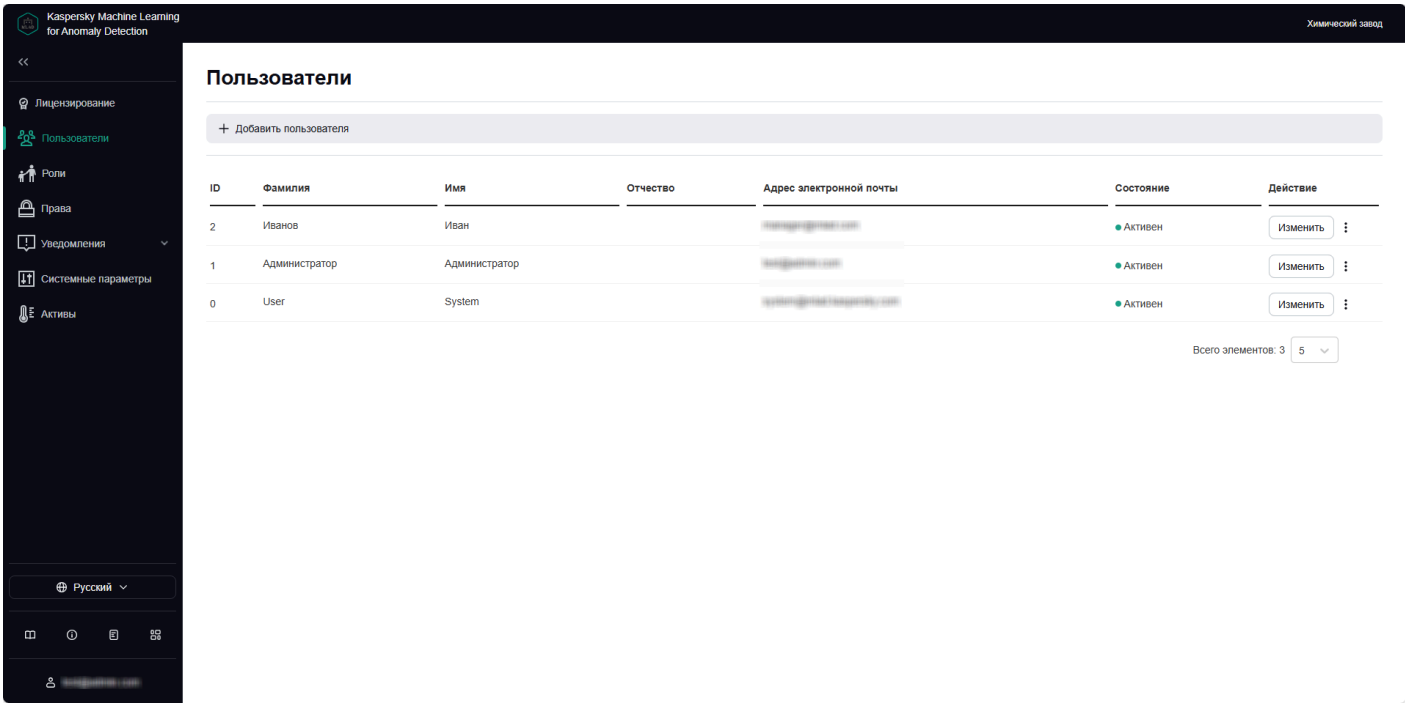
Все созданные учетные записи пользователей и **информация о них** отображаются в таблице раздела **Пользователи** в меню администратора.

- **ID** – идентификатор пользователя.
- **Фамилия** – фамилия пользователя.
- **Имя** – имя пользователя.
- **Отчество** – отчество пользователя.
- **Адрес электронной почты** – адрес электронной почты пользователя.
- **Состояние** – параметр, описывающий состояние блокировки учетной записи пользователя. Если пользователь заблокирован, в столбце **Состояние** отображается красная точка со значением **Не активен**. Заблокированный пользователь не может авторизоваться в Kaspersky MLAD и использовать программу. Если пользователь разблокирован, в столбце **Состояние** отображается зеленая точка со значением **Активен**.
- **Действие** – кнопка, позволяющая изменять учетную запись пользователя.

При установке программы создается специальная системная учетная запись `User System`, которая не предназначена для использования персоналом при работе с Kaspersky MLAD. Подключение к веб-интерфейсу программы с помощью этой учетной записи невозможно. Для уточнения возможности изменения ее параметров рекомендуется проконсультироваться со специалистом "Лаборатории Касперского" или сертифицированным интегратором.

При необходимости вы можете изменять учетные записи пользователей. Kaspersky MLAD не позволяет удалять учетные записи пользователей. Если вы хотите запретить доступ к веб-интерфейсу Kaspersky MLAD для определенной учетной записи, рекомендуется заблокировать ее. Позже вы можете разблокировать эту учетную запись, если потребуется. Вы также можете разблокировать учетную запись, заблокированную при достижении пользователем количества неудачных попыток авторизации до истечения периода блокировки. Вы можете указать количество неудачных попыток авторизации и период блокировки учетной записи при настройке параметров безопасности Kaspersky MLAD.

Рядом с каждой учетной записью находится вертикальное меню ⋮, позволяющее отзывать токены аутентификации или просматривать список прав для определенной учетной записи пользователя.



Раздел **Пользователи**

Создание учетной записи пользователя

Управление учетными записями пользователей Kaspersky MLAD доступно системным администраторам.

Чтобы создать учетную запись пользователя:

1. В нижнем левом углу страницы нажмите на кнопку ⚙.

   Вы перейдете в меню администратора.

2. Выберите раздел **Пользователи**.

3. Нажмите на кнопку **Добавить пользователя**.

   Справа отобразится панель **Добавление пользователя**.

4. В поле **Фамилия** введите фамилию пользователя.

5. В поле **Имя** введите имя пользователя.

6. Если требуется, в поле **Отчество** введите отчество пользователя.

7. В поле **Адрес электронной почты** укажите адрес электронной почты пользователя.

   Подключение пользователя к Kaspersky MLAD будет осуществляться по заданному адресу электронной почты.

8. В поле **Пароль** введите пароль для учетной записи пользователя.

   Пароль должен удовлетворять следующим требованиям:

   - Содержит минимальное количество символов, заданное в параметре **Минимальная длина пароля**.
   - Содержит буквы латинского алфавита, цифры и/или специальные символы в соответствии с политикой паролей, заданной при настройке параметров безопасности.

9. В поле **Подтверждение пароля** подтвердите пароль для учетной записи пользователя.

10. Нажмите на кнопку **Сохранить**.

    Информация о новом пользователе отобразится в таблице. Если требуется, вы можете изменить учетные записи пользователей или отозвать их токены аутентификации

При создании учетной записи вы не можете присвоить роль пользователю. Вы можете присвоить пользователю роль только при изменении учетной записи.

Изменение учетной записи пользователя

Управление учетными записями пользователей Kaspersky MLAD доступно системным администраторам.

При изменении учетной записи пользователя вы можете присвоить пользователю нужную роль. Вы также можете заблокировать или разблокировать учетную запись пользователя.

При блокировке пользователя Kaspersky MLAD автоматически отзывает токены аутентификации у учетной записи и завершает пользовательскую сессию. Заблокированный пользователь не может авторизоваться в Kaspersky MLAD и использовать программу.

При изменении пароля для какой-либо учетной записи Kaspersky MLAD также автоматически отзывает токены аутентификации и завершает пользовательскую сессию пользователя, для которого был изменен пароль. Пользователь, для которого был изменен пароль, может подключиться к веб-интерфейсу, используя новый пароль.

Чтобы изменить учетную запись пользователя:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Пользователи**.

3. В строке той учетной записи, которую вы хотите изменить, нажмите на кнопку **Изменить**.

   Справа отобразится панель **Изменение пользователя**.

4. Если требуется, введите новую фамилию, имя и/или отчество пользователя.

5. В поле **Роли** присвойте роль для учетной записи пользователя, установив соответствующий флажок.

6. Если требуется, укажите новый адрес электронной почты пользователя.

7. Если требуется изменить пароль, в полях **Пароль** и **Подтверждение пароля** введите новый пароль.

   Новый пароль должен удовлетворять следующим требованиям:

   - Не совпадает с предыдущими паролями. Количество ранее использованных паролей, с которыми новый пароль не должен совпадать, задается значением параметра **Количество паролей пользователя, хранящихся в истории**.
   - Содержит минимальное количество символов, заданное в параметре **Минимальная длина пароля**.
   - Содержит буквы латинского алфавита, цифры и/или специальные символы в соответствии с политикой паролей, заданной при настройке параметров безопасности.

8. Если требуется заблокировать или разблокировать учетную запись пользователя, выполните одно из следующих действий:

   - Если требуется разблокировать учетную запись пользователя, установите переключатель **Состояние** в положение **Активен**.
   - Если требуется заблокировать учетную запись пользователя, установите переключатель **Состояние** в положение **Не активен**.

   Kaspersky MLAD не позволяет удалять учетные записи пользователей. Если вы хотите запретить доступ к Kaspersky MLAD для определенной учетной записи, рекомендуется заблокировать ее.

9. Нажмите на кнопку **Сохранить**.

Измененная информация о пользователе отобразится в таблице.

Отзыв токенов аутентификации для учетной записи пользователя

Управление учетными записями пользователей Kaspersky MLAD доступно системным администраторам.

После подключения пользователя к веб-интерфейсу внутри Kaspersky MLAD создается индивидуальный токен, позволяющий сохранять авторизацию пользователя в программе между сессиями подключения к веб-интерфейсу программы, в том числе связанными с перезапуском браузера. Если пользователь авторизовался на нескольких устройствах, для каждой пользовательской сессии создается свой токен.

При необходимости в любой момент вы можете отозвать токены аутентификации для учетной записи пользователя. В результате для пользователя, чьи токены аутентификации вы отозвали, будет завершена сессия подключения к программе одновременно на всех устройствах, на которых он был авторизован. Отзыв токенов аутентификации может быть полезен в случае, если требуется принудительно завершить сессии подключения к программе для определенного пользователя. После отзыва токенов пользователь может снова авторизоваться и продолжить использовать Kaspersky MLAD.

Чтобы отозвать токены аутентификации для учетной записи пользователя:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Пользователи**.

3. Рядом с учетной записью, для которой требуется отозвать токены аутентификации, откройте вертикальное меню и выберите пункт **Отозвать токены**.

4. В открывшемся окне подтвердите отзыв токенов аутентификации.

Токены аутентификации для учетной записи пользователя будет отозваны, пользовательская сессия будет завершена.

Просмотр прав доступа для учетной записи пользователя

Управление учетными записями пользователей Kaspersky MLAD доступно системным администраторам.

В разделе **Пользователи** вы можете просмотреть список прав для определенной учетной записи пользователя.

Чтобы просмотреть права доступа для учетной записи пользователя:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Пользователи**.

3. Рядом с учетной записью, для которой требуется просмотреть список прав доступа, откройте вертикальное меню и выберите пункт **Список прав**.

На странице откроется окно с информацией о роли и правах доступа выбранной учетной записи.

Управление ролями

В Kaspersky MLAD вы можете разграничивать доступ пользователей к функциям программы в зависимости от задач пользователей, используя типовые роли.

Управление ролями доступно системным администраторам.

Роль – это набор прав доступа к функциям программы, который вы можете назначить пользователю.

Для доступа к функциям программы могут использоваться учетные записи со следующими ролями:

- Роль системного администратора – создается автоматически при установке программы. Роль системного администратора автоматически присваивается первому пользователю, созданному во время установки Kaspersky MLAD. Пользователь с ролью системного администратора имеет доступ ко всем функциям программы. Роль системного администратора не может быть изменена или удалена.

- Пользовательская роль – создается вручную в разделе **Роли**. Доступ к функциям программы зависит от списка прав, предоставленных для пользовательской роли. Количество пользовательских ролей не ограничено.

В разделе **Роли** отображается таблица с **информацией о всех созданных ролях**.

- **ID** – идентификатор роли пользователя.
- **Роль** – название роли пользователя.
- **Состояние** – параметр, описывающий состояние роли. Если роль используется, в столбце **Состояние** отображается зеленая точка со значением **Активна**. Если роль не используется, в столбце **Состояние** отображается красная точка со значением **Не активна**. Если роль не активна, то функции программы, связанные с правами роли, недоступны пользователю, которому назначена эта роль.
- **Права** – кнопка, позволяющая просмотреть список прав роли пользователя в Kaspersky MLAD.
- **Создана** – дата и время создания роли пользователя.
- **Обновлена** – дата и время обновления роли пользователя.

Создание роли

Управление ролями доступно системным администраторам.

Вы можете создавать пользовательские роли и выбирать для них права доступа к функциям программы. После создания активной роли она станет доступной для назначения пользователям программы.

Чтобы создать роль:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Роли**.

3. Нажмите на кнопку **Создать**.

   Справа отобразится панель **Создание роли**.

4. В поле **Название роли** укажите нужное название роли.

   Вы можете ввести не более 30 символов.

5. Если требуется, в поле **Описание роли** укажите описание роли.

6. Для предоставления прав доступа роли выполните следующие действия:

   a. Нажмите на кнопку **Выбрать права**.

      Справа отобразится панель **Предоставление прав для роли**.

   b. В списке прав выберите права доступа к функциям программы, которые вы хотите предоставить роли.

      При выборе пункта **Права на все действия** роли будут доступны все функции системного администратора.

   c. Нажмите на кнопку **Сохранить**.

7. Выполните одно из следующих действий:

   - Если требуется использовать роль для пользователей программы, установите переключатель **Состояние** в положение **Активна**.
   - Если требуется выключить использование роли для пользователей программы, установить переключатель **Состояние** в положение **Не активна**.

     Если роль не активна, то функции программы, связанные с правами роли, недоступны пользователю, которому назначена эта роль.

8. Нажмите на кнопку **Сохранить**.

Изменение роли

Управление ролями доступно системным администраторам.

Чтобы изменить роль:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Роли**.

3. Установите флажок рядом с ролью, которую вы хотите изменить.

4. Нажмите на кнопку **Изменить**.

   Справа отобразится панель **Изменение роли**.

5. Измените параметры роли. Описание параметров см. в инструкции по созданию роли.

6. Нажмите на кнопку **Сохранить**.

Удаление роли

Управление ролями доступно системным администраторам.

При удалении пользовательской роли, которая назначена пользователям Kaspersky MLAD, у пользователей будут отозваны права доступа к функциям программы, связанные с этой ролью.

Вы не можете удалить роль системного администратора.

Чтобы удалить роль:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Роли**.

3. Установите флажки рядом с названиями ролей, которые вы хотите удалить.

4. Нажмите на кнопку **Удалить**.

5. В открывшемся окне подтвердите удаление ролей.

Просмотр прав доступа для роли

Управление ролями доступно системным администраторам.

В разделе **Роли** вы можете просмотреть список прав доступа к функциям программы для пользователей с определенной ролью.

Чтобы просмотреть права доступа для роли:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Роли**.

3. Нажмите на кнопку **Список прав** рядом с ролью, для которой требуется просмотреть список прав.

   На странице откроется окно с информацией о правах доступа к функциям программы для выбранной роли.

Управление уведомлениями

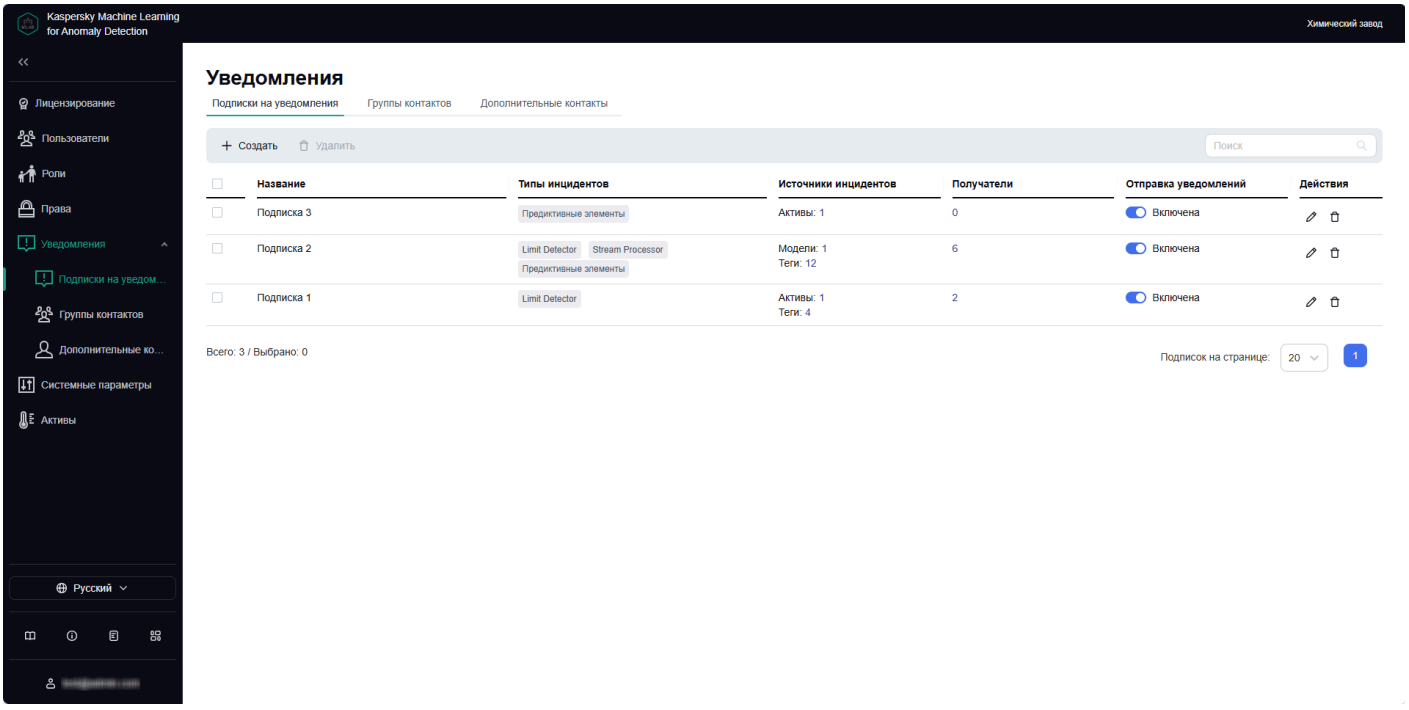
В разделе **Уведомления** на вкладке **Подписки на уведомления** вы можете создавать подписки на уведомления. Уведомления могут быть отправлены на адреса электронной почты пользователей программы или дополнительных контактов. На вкладке **Дополнительные контакты** вы можете задать дополнительные контакты. В качестве дополнительных контактов вы можете указать сотрудников вашей организации, для которых не созданы учетные записи в Kaspersky MLAD.

Управление уведомлениями доступно системным администраторам и пользователям с правами из группы прав **Управление уведомлениями**.

При необходимости вы можете объединить пользователей программы и дополнительные контакты в группу контактов и при создании подписки на уведомления указать созданную группу в качестве получателя уведомлений. При возникновении инцидента Kaspersky MLAD отправит уведомление об инциденте на все адреса электронной почты получателей, входящих в группу. Вы можете создать группу контактов на вкладке **Группы контактов**.

При необходимости вы можете изменять и удалять подписки на уведомления об инцидентах, дополнительные контакты и группы контактов.

Для отправки уведомлений предварительно требуется настроить и запустить службу Mail Notifier.



Раздел **Уведомления**

Управление подписками на уведомления

В Kaspersky MLAD вы можете создавать подписки на уведомления для отправки информации о зарегистрированных программой инцидентах на адреса электронной почты пользователей программы, дополнительных контактов и/или групп контактов.

Управление уведомлениями доступно системным администраторам и пользователям с правами из группы прав **Управление уведомлениями**.

Все созданные подписки и **информация о них** отображаются на вкладке **Подписки на уведомления** раздела **Уведомления** в меню администратора. Если требуется, вы можете изменить количество отображаемых подписок с помощью раскрывающегося списка в правом нижнем углу страницы. Для поиска подписок по имени вы можете использовать поле **Поиск** в правом верхнем углу страницы.

- **Название** – название подписки на уведомления об инцидентах.
- **Типы инцидентов** – типы инцидентов, уведомления о которых получает пользователь. Вы можете получать уведомления о следующих типах инцидентах:
  - **Предиктивные элементы** – инциденты, зарегистрированные предиктивными элементами ML-моделей.
  - **Диагностические правила** – инциденты, зарегистрированные диагностическими правилами ML-моделей.
  - **Эллиптические конверты** – инциденты, зарегистрированные эллиптическими конвертами ML-моделей.
  - **Limit Detector** – инциденты, зарегистрированные при достижении тегом верхнего или нижнего порога блокировки.
  - **Stream Processor** – инциденты, зарегистрированные при обнаружении потери данных или наблюдений, поступивших в Kaspersky MLAD слишком рано или поздно.
- **Источники инцидентов** – число ML-моделей, активов и/или тегов, по инцидентам которых Kaspersky MLAD отправляет уведомления. При нажатии на число справа отображается панель с вкладками **Модели**, **Активы** и/или **Теги**. На каждой вкладке отобразится дерево активов с информацией об объектах, выбранных при создании подписки на уведомления. Для поиска ML-моделей, активов и/или тегов по имени используйте поле **Поиск**.
- **Получатели** – количество пользователей программы и дополнительных контактов, которым Kaspersky MLAD отправляет уведомления об инцидентах. При нажатии на количество справа отобразится панель с информацией о контактах, которые получают уведомления об инцидентах. При необходимости вы можете найти определенные контакты среди получателей уведомлений с помощью поля **Поиск**.
- **Отправка уведомлений** – переключатель, позволяющий включить или выключить отправку уведомлений.
- **Действия** – кнопки, позволяющие изменить или удалить подписку на уведомления об инцидентах.

Kaspersky MLAD позволяет временно выключить отправку уведомлений об инцидентах вместо удаления их конфигураций. Вы можете включить отправку уведомления в любое время. Для управления состоянием подписки на уведомления включите или выключите переключатель в столбце **Отправка уведомлений** для нужной подписки.

Создание подписки на уведомления

Управление уведомлениями доступно системным администраторам и пользователям с правами из группы прав **Управление уведомлениями**.

Вы можете создавать подписки на уведомления об инцидентах, зарегистрированных при обработке данных телеметрии и/или в результате работы ML-модели. В подписке необходимо указать как минимум одного адресата (пользователя программы или дополнительного контакта), которому Kaspersky MLAD будет отправлять уведомления по подписке. Kaspersky MLAD отправляет адресату уведомления по каждому инциденту, зарегистрированному для активов, тегов и/или ML-моделей, выбранных в подписке.

Чтобы создать подписку на уведомления об инцидентах:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Уведомления** и откройте вкладку **Подписки на уведомления**.

3. На открывшейся странице нажмите на кнопку **Создать**.

   Справа отобразится панель **Создание подписки на уведомления**.

4. В поле **Название** введите название подписки.

5. В поле **Язык уведомления** выберите язык, на котором будут приходить уведомления об инцидентах.

   По умолчанию для уведомлений об инцидентах используется текущий язык локализации веб-интерфейса Kaspersky MLAD. Доступны английский и русский языки.

6. Если требуется, выключите переключатель **Отправка уведомлений**.

   При выключенном переключателе Kaspersky MLAD не будет отправлять уведомления об инцидентах. По умолчанию переключатель включен.

7. В блоке параметров **Контакты** выберите как минимум одного адресата уведомлений:

   a. В раскрывающемся списке **Группы контактов** выберите группы контактов, которым требуется отправлять уведомления об инцидентах.

      Если требуется отменить выбор группы, нажмите на кнопку ✕ рядом с соответствующей группой. Если требуется отменить выбор всех групп, нажмите на кнопку ✕ в правой части раскрывающегося списка.

   b. В раскрывающемся списке **Пользователи** выберите пользователей программы, которым требуется отправлять уведомления.

      Если требуется отменить выбор пользователя, нажмите на кнопку ✕ рядом с соответствующим пользователем. Если требуется отменить выбор всех пользователей, нажмите на кнопку ✕ в правой части раскрывающегося списка.

   c. В раскрывающемся списке **Дополнительные контакты** выберите дополнительные адреса электронной почты, на которые требуется отправлять уведомления об инцидентах.

      Если требуется отменить выбор дополнительного контакта, нажмите на кнопку ✕ рядом с соответствующим контактом. Если требуется отменить выбор всех дополнительных контактов, нажмите на кнопку ✕ в правой части раскрывающегося списка.

Информация о выбранных адресатах отобразится в таблице **Выбранные контакты**. Для поиска определенных адресатов в таблице введите поисковый запрос в поле **Поиск**.

8. В блоке параметров **Инциденты** выполните следующие действия:

a. В раскрывающемся списке **Типы инцидентов** выберите один или несколько элементов:

- **Предиктивные элементы**, если вы хотите настроить подписку на уведомления об инцидентах, зарегистрированных предиктивными элементами ML-моделей.
- **Диагностические правила**, если вы хотите настроить подписку на уведомления об инцидентах, зарегистрированных диагностическими правилами ML-моделей.
- **Эллиптические конверты**, если вы хотите настроить подписку на уведомления об инцидентах, зарегистрированных эллиптическими конвертами ML-моделей.
- **Limit Detector**, если вы хотите настроить подписку на уведомления о достижении тегом верхнего или нижнего порога блокировки.
- **Stream Processor**, если вы хотите настроить подписку на уведомления о прекращении или прерывании входного потока данных определенного тега, об обнаружении наблюдений, поступивших слишком рано или поздно.

b. Нажмите на кнопку **Выбрать источники инцидентов**.

Справа отобразится панель **Выбор источников инцидентов**. В зависимости от выбранных типов инцидентов в панели отобразятся вкладки **Активы**, **Модели** и/или **Теги**. На каждой вкладке отобразится дерево активов для выбора ML-моделей, активов и/или тегов, по инцидентам которых необходимо отправлять уведомления. С помощью кнопок ⊞ и ⊟, расположенных слева от имен активов вы можете отображать и скрывать части дерева активов.

c. В открывшейся панели выполните следующие действия:

a. Если необходимо отправлять уведомления об инцидентах, зарегистрированных для любых тегов и/или элементов ML-моделей, входящих в состав определенных активов, в дереве активов на вкладке **Активы** выберите нужные активы. Для поиска определенных активов по имени вы можете использовать поле **Поиск** в правом верхнем углу вкладки.

Если после создания подписки в выбранный актив добавятся новые ML-модели, теги и/или активы с ML-моделями и тегами, Kaspersky MLAD также будет отправлять по ним уведомления. Если вы переместите теги в другой актив, для которого отсутствует подписка, Kaspersky MLAD перестанет отправлять уведомления об инцидентах перемещенных тегов.

Для просмотра выбранных активов вы можете включить переключатель **Только выбранные активы**.

b. Если вы выбрали **Предиктивные элементы**, **Диагностические правила** и/или **Эллиптические конверты** в раскрывающемся списке **Типы инцидентов**, в дереве активов на вкладке **Модели** выберите ML-модели, по инцидентам элементов которых необходимо отправлять уведомления. Для поиска определенных ML-моделей по имени вы можете использовать поле **Поиск** в правом верхнем углу вкладки.

Уведомления будут приходить только по выбранным ML-моделям. Если после создания подписки в активы, к которым относятся выбранные ML-модели, добавятся новые ML-модели, уведомления по их инцидентам отправляться не будут.

Для просмотра выбранных ML-моделей вы можете включить переключатель **Только выбранные модели**.

c. Если вы выбрали **Limit Detector** и/или **Stream Processor** в раскрывающемся списке **Типы инцидентов**, в дереве активов на вкладке **Теги** выберите теги, по инцидентам которых необходимо отправлять уведомления. Для поиска определенных тегов по имени вы можете использовать поле **Поиск** в правом верхнем углу вкладки.

Уведомления будут приходить только по выбранным тегам. Если после создания подписки в активы, к которым относятся выбранные теги, добавятся новые теги, уведомления по их инцидентам отправляться не будут. Если вы переместите выбранные теги в другой актив, Kaspersky MLAD продолжит отправлять уведомления об их инцидентах.

Для просмотра выбранных тегов вы можете включить переключатель **Только выбранные теги**.

d. Нажмите на кнопку **Сохранить**.

d. Если требуется получать уведомления по всем зарегистрированным инцидентам (в том числе от неопубликованных ML-моделей), выключите переключатель **Отправлять уведомления только об учетных инцидентах**.

По умолчанию, переключатель включен. При включенном переключателе уведомления отправляются по инцидентам выбранных ML-моделей и ML-моделей, входящих в состав выбранных активов, только если ML-моделям присвоен статус **Опубликована**.

9. Нажмите на кнопку **Сохранить**.

Информация о новой подписке на уведомления отобразится в таблице. Если требуется, вы можете изменить или удалить подписку.

Для каждого инцидента, зарегистрированного по выбранным ML-моделям и/или тегам, будет отправляться отдельное уведомление на указанные адреса электронной почты.

Изменение подписки на уведомления

Управление уведомлениями доступно системным администраторам и пользователям с правами из группы прав **Управление уведомлениями**.

Чтобы изменить подписку на уведомления об инцидентах:

1. В нижнем левом углу страницы нажмите на кнопку .

Вы перейдете в меню администратора.

2. Выберите раздел **Уведомления** и откройте вкладку **Подписки на уведомления**.

3. Нажмите на кнопку в столбце **Действия** рядом с подпиской на уведомления, которую вы хотите изменить.

4. Если требуется, измените параметры подписки на уведомления. Описание параметров см. в инструкции по созданию подписки на уведомления.

5. Нажмите на кнопку **Сохранить** для сохранения изменений.

Для каждого инцидента, зарегистрированного по выбранным ML-моделям и/или тегам, будет отправляться отдельное уведомление на указанные адреса электронной почты.

Измененная информация о подписке на уведомления отобразится в таблице. Если требуется, вы можете удалить подписку или отключить отправку уведомлений по подписке, выключив переключатель **Отправка уведомлений** для нужной подписки в таблице уведомлений.

Удаление подписки на уведомления

Управление уведомлениями доступно системным администраторам и пользователям с правами из группы прав **Управление уведомлениями**.

Чтобы удалить подписку на уведомления об инцидентах:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Уведомления** и откройте вкладку **Подписки на уведомления**.

3. Выполните одно из следующих действий:

   - Если требуется удалить определенную подписку на уведомления, нажмите на кнопку в столбце **Действия** рядом с нужной подпиской.

   - Если требуется удалить несколько подписок на уведомления, установите флажки рядом с нужными подписками и нажмите на кнопку **Удалить**.

4. В открывшемся окне подтвердите удаление подписок.

Информация о подписках будет удалена из таблицы.

Kaspersky MLAD позволяет временно выключить отправку уведомлений вместо удаления подписок. Информация о подписках на уведомления отображается на вкладке **Подписки на уведомления**. Вы можете включить отправку уведомлений в любое время. Включить или выключить отправку уведомлений вы можете с помощью переключателя в столбце **Отправка уведомлений** таблицы подписок или при изменении соответствующей подписки.

Работа с группами контактов

Группа контактов – это набор адресов электронной почты, используемый Kaspersky MLAD для одновременной отправки уведомлений об инцидентах. Вы можете включить в группу контактов как пользователей программы, так и дополнительные контакты.

Управление группами контактов доступно системным администраторам и пользователям с правами из группы прав **Управление уведомлениями**.

Созданные группы контактов и **информация о них** отображается на вкладке **Группы контактов** раздела **Уведомления**. Если требуется, вы можете изменить количество отображаемых групп контактов с помощью раскрывающегося списка в правом нижнем углу страницы.

- **Имя группы** – имя группы контактов.
- **Описание** – описание группы контактов.
- **Контакты** – число пользователей программы и дополнительных контактов, включенных в группу контактов. При нажатии на число справа отобразится панель с информацией о контактах, которые входят в группу.
- **Действия** – кнопки, позволяющие изменить или удалить группу контактов.

Поиск и фильтрация групп контактов

Поиск и фильтрация групп контактов доступны системным администраторам и пользователям с правами из группы прав **Управление уведомлениями**.

Поиск выполняется по именам групп контактов.

Чтобы найти нужные группы контактов,

на вкладке **Группы контактов** раздела **Уведомления** введите поисковый запрос в поле **Поиск**. Поиск выполняется по мере ввода символов в строку поиска.

Если требуется сбросить поисковый запрос, нажмите на кнопку в строке поиска.

Вы также можете выполнять фильтрацию групп контактов. Фильтрация применяется к группам, найденным в соответствии с поисковым запросом. Если поисковый запрос не задан, фильтрация применяется ко всем созданным группам контактов.

Чтобы отфильтровать группы контактов:

1. В разделе **Уведомления** откройте вкладку **Группы контактов** и нажмите на кнопку , расположенную справа от поля **Поиск**.

   Справа отобразятся параметры фильтрации.

2. В раскрывающемся списке **Пользователи** выберите одного или несколько пользователей, которые должны входить в группу контактов.

3. В раскрывающемся списке **Дополнительные контакты** выберите один или несколько дополнительных контактов, которые должны входить в группу контактов.

4. Если требуется сбросить параметры фильтрации, выполните одно из следующих действий:

   - Для сброса конкретного контакта нажмите на кнопку рядом с нужным контактом.
   - Для сброса всех выбранных контактов для конкретного параметра фильтрации нажмите на кнопку рядом с нужным параметром.

5. Нажмите на кнопку **Применить**.

Если применены какие-либо параметры фильтрации, справа от поля **Поиск** отображается кнопка .

Создание группы контактов

Управление группами контактов доступно системным администраторам и пользователям с правами из группы прав **Управление уведомлениями**.

Вы можете создать группу контактов и добавить в нее пользователей программы и дополнительные контакты. После создания группы вы можете указать ее в параметрах подписки на уведомления об инцидентах для одновременной отправки уведомления на несколько адресов электронной почты.

Чтобы создать группу контактов:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Уведомления** и откройте вкладку **Группы контактов**.

3. На открывшейся странице нажмите на кнопку **Создать**.

   Справа отобразится панель **Создание группы контактов**.

4. В поле **Имя группы** укажите имя группы контактов.

5. Если требуется, в поле **Описание** укажите описание группы контактов.

6. Если требуется, в блоке параметров **Контакты** выполните следующие действия:

   a. В раскрывающемся списке **Пользователи** выберите одного или несколько пользователей для добавления в группу контактов.

   Если требуется исключить пользователя из группы, нажмите на кнопку × рядом с соответствующим пользователем. Если требуется исключить из группы всех пользователей, нажмите на кнопку × в правой части раскрывающегося списка.

   b. В раскрывающемся списке **Дополнительные контакты** выберите один или несколько дополнительных контактов для добавления в группу контактов.

   Если требуется исключить дополнительный контакт из группы, нажмите на кнопку × рядом с соответствующим контактом. Если требуется исключить из группы все дополнительные контакты, нажмите на кнопку × в правой части раскрывающегося списка.

   Информация о выбранных контактах отобразится в таблице **Выбранные контакты**. Для поиска определенных контактов в таблице введите поисковый запрос в поле **Поиск**.

   Если требуется исключить из группы выбранные контакты, нажмите на кнопку рядом с соответствующим контактом или установите флажки напротив нужных контактов и нажмите на кнопку **Удалить**.

7. Нажмите на кнопку **Сохранить**.

Информация о новой группе контактов отобразится в таблице. Если требуется, вы можете изменить или удалить группу контактов.

Изменение группы контактов

Управление группами контактов доступно системным администраторам и пользователям с правами из группы прав **Управление уведомлениями**.

Чтобы изменить группу контактов:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Уведомления** и откройте вкладку **Группы контактов**.

3. Нажмите на кнопку в столбце **Действия** рядом с группой контактов, которую вы хотите изменить.

4. Если требуется, измените параметры группы контактов. Описание параметров см. в инструкции по созданию группы контактов.

5. Нажмите на кнопку **Сохранить**.

   Измененная информация о группе контактов отобразится в таблице. Если требуется, вы можете удалить группу контактов.

Удаление группы контактов

Управление группами контактов доступно системным администраторам и пользователям с правами из группы прав **Управление уведомлениями**.

При необходимости вы можете удалить группу контактов. При удалении группы контактов Kaspersky MLAD автоматически исключает из нее пользователей и дополнительные контакты в ее составе. При этом пользователи и дополнительные контакты из программы не удаляются.

После удаления группы контактов Kaspersky MLAD перестанет отправлять уведомления об инцидентах на адреса электронной почты пользователей и дополнительных контактов, ранее входящих в состав удаленной группы контактов.

Чтобы удалить группу контактов:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Уведомления** и откройте вкладку **Группы контактов**.

3. Выполните одно из следующих действий:

   - Если требуется удалить определенную группу контактов, нажмите на кнопку в столбце **Действия** рядом с нужной группой.
   - Если требуется удалить несколько групп контактов, установите флажки рядом с нужными группами и нажмите на кнопку **Удалить**.

4. В открывшемся окне подтвердите удаление групп.

Группа контактов будет удалена из таблицы.

Работа с дополнительными контактами

При необходимости вы можете отправлять уведомления об инцидентах на произвольные адреса электронной почты, не связанные с учетными записями пользователей программы. Для этого в Kaspersky MLAD предусмотрена возможность создавать дополнительные контакты на вкладке **Дополнительные контакты** раздела **Уведомления**. Созданные дополнительные контакты и **информация о них** отображаются в виде таблицы.

- **Имя контакта** – имя дополнительного контакта.
- **Адрес электронной почты** – адрес электронной почты дополнительного контакта, на который будут приходить уведомления об инцидентах.
- **Описание** – описание дополнительного контакта.
- **Действия** – кнопки, позволяющие изменить или удалить дополнительный контакт.

Управление дополнительными контактами доступно системным администраторам и пользователям с правами из группы прав **Управление уведомлениями**.

После создания дополнительного контакта вы можете добавить его в группу контактов и/или в подписку для отправки уведомления об инцидентах на несколько адресов электронной почты. Если требуется, вы можете изменить количество отображаемых контактов с помощью раскрывающегося списка в правом нижнем углу страницы. Для поиска дополнительных контактов введите поисковый запрос в поле **Поиск** в правом верхнем углу страницы.

Создание дополнительного контакта

Управление дополнительными контактами доступно системным администраторам и пользователям с правами из группы прав **Управление уведомлениями**.

Вы можете создавать дополнительные контакты для отправки уведомлений на адреса электронной почты, не относящиеся к пользователям программы.

Чтобы создать дополнительный контакт:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Уведомления** и откройте вкладку **Дополнительные контакты**.

3. На открывшейся странице нажмите на кнопку **Создать**.

   Справа отобразится панель **Создание дополнительного контакта**.

4. В поле **Имя контакта** введите укажите имя дополнительного контакта.

5. В поле **Адрес электронной почты** укажите адрес электронной почты дополнительного контакта.

6. Если требуется, в поле **Описание** укажите описание дополнительного контакта.

7. Нажмите на кнопку **Сохранить**.

   Информация о новом дополнительном контакте отобразится в таблице. Если требуется, вы можете изменить дополнительный контакт или удалить его.

Вы можете добавить созданный дополнительный контакт в группу контактов и/или в подписку для отправки уведомления об инцидентах на несколько адресов электронной почты.

Изменение дополнительного контакта

Управление дополнительными контактами доступно системным администраторам и пользователям с правами из группы прав **Управление уведомлениями**.

Чтобы изменить дополнительный контакт:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Уведомления** и откройте вкладку **Дополнительные контакты**.

3. Нажмите на кнопку в столбце **Действия** рядом с дополнительным контактом, который вы хотите изменить.

4. Если требуется, измените параметры дополнительного контакта. Описание параметров см. в инструкции по созданию дополнительного контакта.

5. Нажмите на кнопку **Сохранить**.

   Измененная информация о дополнительном контакте отобразится в таблице. Если требуется, вы можете удалить дополнительный контакт.

Удаление дополнительного контакта

Управление дополнительными контактами доступно системным администраторам и пользователям с правами из группы прав **Управление уведомлениями**.

При необходимости вы можете удалить дополнительный контакт. При удалении дополнительного контакта Kaspersky MLAD автоматически исключает его из групп контактов, в которые он был добавлен. Kaspersky MLAD также перестанет отправлять уведомления об инцидентах на адрес электронной почты удаленного дополнительного контакта.

Чтобы удалить дополнительный контакт:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Уведомления** и откройте вкладку **Дополнительные контакты**.

3. Выполните одно из следующих действий:

   - Если требуется удалить определенный дополнительный контакт, нажмите на кнопку в столбце **Действия** рядом с нужным контактом.

   - Если требуется удалить несколько дополнительных контактов, установите флажки рядом с нужными контактами и нажмите на кнопку **Удалить**.

4. В открывшемся окне подтвердите удаление контактов.

Информация о дополнительных контактах будет удалена из таблицы.

Настройка параметров Kaspersky MLAD

Этот раздел содержит инструкции по настройке параметров служб и коннекторов Kaspersky MLAD, а также по настройке параметров безопасности, уровней ведения журналов служб программы, параметров отображения меню программы и по управлению приоритетами, типовыми статусами и причинами инцидентов.

Настройка основных параметров Kaspersky MLAD

Kaspersky MLAD позволяет указать имя объекта мониторинга, URL-адрес и IP-адрес для формирования ссылок на инциденты в уведомлениях, а также периодичность получения новых данных от объекта мониторинга. Имя объекта мониторинга отображается в правом верхнем углу каждого раздела веб-интерфейса Kaspersky MLAD.

Работы по настройке основных параметров Kaspersky MLAD могут выполнять системные администраторы.

Чтобы настроить основные параметры Kaspersky MLAD:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **Основные**.

   Справа отобразится список параметров.

3. В поле **Имя объекта мониторинга** укажите имя объекта мониторинга.

4. В поле **URL-адрес для уведомлений об инцидентах** укажите URL-адрес для формирования ссылок на инциденты в уведомлениях об инцидентах, отправляемых по электронной почте.

   Если задан параметр **IP-адрес для уведомлений об инцидентах**, то для формирования ссылок используется заданный IP-адрес.

5. В поле **IP-адрес для уведомлений об инцидентах** укажите IP-адрес для формирования ссылок на инциденты в уведомлениях об инцидентах, отправляемых по электронной почте.

6. В поле **Интервал получения данных из службы Message Broker (мс)** укажите интервал обновления данных телеметрии в веб-интерфейсе программы.

   Чем больше указанное значение параметра, тем реже происходит обновление данных. По умолчанию этот параметр имеет значение `500`.

7. В поле **Интервал получения статистических данных об инцидентах из базы данных (мс)** укажите интервал обновления в веб-интерфейсе программы данных о зарегистрированных программой инцидентах.

   По умолчанию этот параметр имеет значение `5000`.

8. В раскрывающемся списке **Часовой пояс объекта мониторинга** выберите нужный часовой пояс компьютера, на котором установлен Kaspersky MLAD.

   Данные на графиках в разделах программы отображаются в выбранном часовом поясе.

9. Нажмите на кнопку **Сохранить**.

Настройка параметров безопасности Kaspersky MLAD

Kaspersky MLAD позволяет указать условия временной блокировки учетных записей пользователей, период неактивности пользователя в соответствии с политикой безопасности на предприятии, а также параметры хранения журналов событий информационной безопасности (далее также "события ИБ") в базе данных Kaspersky MLAD. Запись журналов событий информационной безопасности в базу данных ведется автоматически. Если требуется, вы можете указать параметры внешней системы, в которую требуется отправлять журналы событий ИБ.

Работы по настройке параметров безопасности Kaspersky MLAD могут выполнять системные администраторы.

Чтобы настроить основные параметры Kaspersky MLAD:

1. В нижнем левом углу страницы нажмите на кнопку ⚙.

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **Безопасность**.

   Справа отобразится список параметров.

3. В блоке параметров **Параметры авторизации** выполните следующие действия:

   a. В поле **Количество попыток авторизации** укажите количество неудачных попыток авторизации, при достижении которого Kaspersky MLAD временно заблокирует учетную запись пользователя.

      По умолчанию этот параметр имеет значение `3`.

   b. В поле **Период блокировки пользователя (сек.)** укажите время в секундах, в течение которого учетная запись пользователя будет заблокирована после достижения заданного количества неудачных попыток авторизации.

      По умолчанию этот параметр имеет значение `120`.

   c. В поле **Период неактивности пользователя (мин)** укажите допустимую продолжительность неактивной пользовательской сессии в минутах.

      При достижении заданного периода Kaspersky MLAD автоматически завершает сессию неактивного пользователя. По умолчанию этот параметр имеет значение `1440`.

   d. Если требуется запретить пользователям пропускать смену пароля при первом подключении к веб-интерфейсу программы, включите переключатель **Требовать обязательную смену пароля при первом подключении**.

      По умолчанию этот переключатель выключен.

4. В блоке параметров **Политика паролей** выполните следующие действия:

   a. В поле **Количество паролей пользователя, хранящихся в истории** укажите количество последних паролей пользователя, которые хранятся в программе.

      Вы можете указать значение начиная с `1`. По умолчанию этот параметр имеет значение `5`.

      При изменении пароля пользователя новый пароль не должен соответствовать паролям, хранящимся в Kaspersky MLAD. Программа хранит пароли в зашифрованном виде.

   b. В поле **Срок действия пароля (сут)** укажите количество дней, в течение которых пользователь может использовать свой пароль для подключения к программе без его изменения.

      По умолчанию этот параметр имеет значение `180`.

   c. В поле **Минимальная длина пароля** укажите минимальное количество символов, которое должны содержать пароли пользователей.

      Вы можете указать значение в диапазоне от `8` до `128`. По умолчанию этот параметр имеет значение `8`.

   d. Если в соответствии с политикой безопасности пароли пользователей должны содержать прописные буквы латинского алфавита, включите переключатель **Требовать использование прописных букв латинского алфавита (A-Z)**.

      По умолчанию этот переключатель включен.

   e. Если в соответствии с политикой безопасности пароли пользователей должны содержать строчные буквы латинского алфавита, включите переключатель **Требовать использование строчных букв латинского алфавита (a-z)**.

      По умолчанию этот переключатель включен.

   f. Если в соответствии с политикой безопасности пароли пользователей должны содержать цифры, включите переключатель **Требовать использование цифр (0-9)**.

      По умолчанию этот переключатель включен.

   g. Если в соответствии с политикой безопасности пароли пользователей должны содержать специальные символы, включите переключатель **Требовать использование специальных символов (_!@#$%^&*)**.

      По умолчанию этот переключатель включен.

5. В блоке параметров **Параметры хранения журналов событий информационной безопасности** выполните следующие действия:

   a. В поле **Объем журналов событий информационной безопасности (МБ)** задайте ограничение занимаемого объема в мегабайтах для хранения журналов событий ИБ в базе данных.

      При незаполненном поле или при значении 0 Kaspersky MLAD хранит все журналы событий ИБ в течение срока, заданного в параметре **Время хранения журналов событий информационной безопасности (сут)**. По умолчанию для этого параметра значение не установлено.

      При превышении заданного объема журналов событий ИБ в базе данных Kaspersky MLAD удаляет наиболее ранние записи.

   b. В поле **Время хранения журналов событий информационной безопасности (сут)** укажите количество дней для хранения журналов событий ИБ в базе данных.

      По умолчанию этот параметр имеет значение `100`.

6. Нажмите на кнопку **Сохранить**.

Настройка службы Anomaly Detector

Вы можете настроить процесс обнаружения аномалий с учетом особенностей вашего объекта мониторинга, включив или выключив обнаружение аномалий определенного типа в параметрах службы Anomaly Detector.

Работы по настройке службы Anomaly Detector могут выполнять системные администраторы.

Чтобы настроить параметры службы Anomaly Detector:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **Anomaly Detector**.

   Справа отобразится список параметров.

3. С помощью переключателя **Использовать детектор Limit Detector** включите или выключите использование детектора Limit Detector.

   Детектор Limit Detector регистрирует инциденты при обнаружении превышений верхнего или нижнего порогов блокировки, заданных для тега.

4. С помощью переключателя **Использовать детектор Forecaster** включите или выключите обнаружение аномалий предиктивными элементами ML-модели.

   Предиктивные элементы ML-модели регистрируют инциденты при обнаружении расхождений между наблюдаемыми и прогнозируемыми значениями тегов.

5. С помощью переключателя **Использовать детектор Rule Detector** включите или выключите обнаружение аномалий элементами ML-модели на основе диагностических правил.

   Диагностические правила регистрируют инциденты при достижении значения, полученного в результате выполнения диагностического правила, установленного порога.

6. С помощью переключателя **Пропускать разрывы в данных** включите или выключите функцию пропуска разрывов в поступающем потоке данных.

   Если переключатель включен, при инференсе ML-модели ее элементы не формируют артефакты, когда по тегам элемента ML-модели не поступают данные в течение времени, большего чем период РИВС, заданный в параметре **Шаг сетки (сек.)** этого элемента.

7. В поле **Максимальное количество запрашиваемых записей из службы Message Broker** введите количество записей, которое требуется запрашивать от службы Message Broker для последующей обработки в Anomaly Detector.

   Чем больше заданное значение, тем реже служба Anomaly Detector запрашивает записи у службы Message Broker. Значение зависит от количества данных телеметрии, которые поступают в Kaspersky MLAD в реальном времени.

8. В поле **Количество сообщений, отправляемых в одном блоке в службу Message Broker** введите количество инцидентов, которое требуется отправлять в службу Message Broker за один раз.

9. Нажмите на кнопку **Сохранить**.

Настройка службы Keeper

Kaspersky MLAD использует службу Keeper для маршрутизации данных телеметрии, которые подлежат сохранению в базе данных. Вы можете настроить параметры, определяющие скорость получения данных от коннекторов и внешних источников данных, а также объем данных, подлежащих сохранению в базе Kaspersky MLAD.

Работы по настройке параметров маршрутизации данных Kaspersky MLAD могут выполнять системные администраторы.

Чтобы настроить параметры службы Keeper:

1. В нижнем левом углу страницы нажмите на кнопку ⚙.

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **Keeper**.

   Справа отобразится список параметров.

3. Выполните одно из следующих действий:

   - Если требуется сохранять в базе данных значения как известных, так и неизвестных программе тегов, поступающих от внешних источников, включите переключатель **Сохранять значения всех тегов**.
   - Если требуется сохранять значения только известных программе тегов, выключите переключатель **Сохранять значения всех тегов**.

4. В поле **Время ожидания получения значений тегов (мс)** введите максимальное время ожидания в миллисекундах для получения значений тегов.

   Чем больше заданное значение, тем реже служба Keeper получает значения тегов и записывает их в базу данных. Рекомендуется указать значение, соответствующее частоте получения данных телеметрии от объекта мониторинга.

5. В поле **Время ожидания получения инцидентов (мс)** введите максимальное время ожидания в миллисекундах для получения инцидентов.

   Чем больше заданное значение, тем реже служба Keeper получает сведения об инцидентах и записывает их в базу данных. Рекомендуется указать значение, соответствующее частоте регистрации инцидентов.

6. В поле **Время ожидания получения метрик (мс)** введите максимальное время ожидания в миллисекундах для получения метрик.

   Чем больше заданное значение, тем реже служба Keeper получает метрики (количество полученных наблюдений по тегам, количество событий и количество сформированных артефактов) и записывает их в базу данных. Рекомендуется указать значение, соответствующее частоте получения метрик от коннектора CEF Connector.

7. Нажмите на кнопку **Сохранить**.

Настройка службы Mail Notifier

Kaspersky MLAD использует службу Mail Notifier для уведомления пользователей о регистрации программой инцидентов.

Работы по настройке службы Mail Notifier могут выполнять системные администраторы.

Настройка службы Mail Notifier не является обязательной и необходима, если вы хотите получать по электронной почте уведомления об инцидентов. Предварительно в сети объекта мониторинга требуется настроить SMTP-сервер.

Чтобы настроить службу Mail Notifier:

1. В нижнем левом углу страницы нажмите на кнопку ⚙.

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **Mail Notifier**.

   Справа отобразится список параметров.

3. В поле **Адрес электронной почты отправителя уведомлений** укажите адрес электронной почты, с которой будут приходить уведомления об инцидентах.

4. В поле **Адрес SMTP-сервера** укажите IP-адрес SMTP-сервера.

5. В поле **Порт SMTP-сервера** укажите порт SMTP-сервера.

6. Если SMTP-сервер использует аутентификацию клиента, в полях **Имя пользователя для SMTP-сервера** и **Пароль для SMTP-сервера** укажите имя пользователя и пароль для подключения к SMTP-серверу.

7. С помощью переключателя **Использовать TLS-соединение** включите или выключите использование защищенного TLS-соединения.

   По умолчанию использование защищенного TLS-соединения выключено.

   Во избежание компрометации отправляемых данных рекомендуется включить использование защищенного TLS-соединения. Рекомендуется использовать защищенное TLS-соединение по протоколу TLS-1.2 или TLS-1.3 с использованием набора шифров из списка рекомендованных.

8. Если вы используете защищенное TLS-соединение, выполните следующие действия:

   a. Загрузите сертификат SMTP-сервера с помощью кнопки **Обзор** под параметром **Сертификат SMTP-сервера**.

   b. Загрузите закрытый ключ к файлу сертификата SMTP-сервера с помощью кнопки **Обзор** под параметром **Закрытый ключ к сертификату SMTP-сервера**.

   > Рекомендуется использовать сертификат с длиной ключа к сертификату 4 096 бит при использовании алгоритма RSA или 256 бит при использовании алгоритма ECDH.
   > Загрузка сертификатов и закрытого ключа к сертификату возможна только в виде файла в формате DER или PEM.

   Если требуется удалить файл сертификата или ключ к сертификату, нажмите на кнопку в соответствующем поле. Если требуется сохранить файл сертификата или ключ к сертификату на компьютере, нажмите на кнопку в соответствующем поле.

9. Нажмите на кнопку **Сохранить**.

Настройка службы Similar Anomaly

Kaspersky MLAD использует службу Similar Anomaly для выявления схожих инцидентов и объединения их в группы. В группах вы можете просматривать похожие инциденты, которые были зарегистрированы в разное время.

> Работы по настройке службы Similar Anomaly могут выполнять системные администраторы.

Чтобы настроить параметры службы Similar Anomaly:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **Similar Anomaly**.

   Справа отобразится список параметров службы.

3. В поле **Минимальное количество инцидентов для группы** введите минимальное количество похожих инцидентов для формирования группы.

4. В поле **Максимальное количество инцидентов для группы** введите максимальное количество инцидентов, которое может входить в одну группу.

   Чем больше указанное значение, тем большее количество инцидентов может быть отнесено программой к одной группе.

5. В поле **Максимальное расстояние между схожими инцидентами** введите максимальное расстояние, на которое могут отставать друг от друга схожие инциденты.

   Вы можете указать значение в диапазоне от `0` до `1`.

6. Нажмите на кнопку **Сохранить**.

Настройка службы Stream Processor

Служба Stream Processor собирает данные телеметрии, поступающие от объекта мониторинга в произвольные моменты реального времени (входной поток), и приводит их к РИВС (выходной поток). На основе накопленных данных служба Stream Processor определяет значения тегов в выходном потоке данных. После преобразования данных в выходной поток служба Stream Processor передает данные на обработку в ML-модель.

При преобразовании поступающих данных телеметрии служба Stream Processor учитывает возможные потери данных (например, в случае временного отключения сети объекта мониторинга) и обрабатывает наблюдения, поступившие в Kaspersky MLAD слишком рано или поздно. В таких случаях служба Stream Processor формирует инциденты и/или передает значения тегов по умолчанию в выходной поток данных.

Служба Stream Processor также может вычислять производные теги на основе поступающих данных телеметрии (например, для вычисления скользящего среднего или среднего значения группы тегов).

Конфигурационный файл службы Stream Processor для загрузки поставляется специалистами "Лаборатории Касперского" или сертифицированным интегратором.

Работы по настройке службы Stream Processor могут выполнять системные администраторы.

Чтобы настроить параметры службы Stream Processor:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **Stream Processor**.

3. В поле **Период равноинтервальной сетки (сек.)** укажите период в секундах, с которым служба Stream Processor будет обрабатывать поступающие данные телеметрии.

4. С помощью кнопки **Обзор** под параметром **Конфигурационный файл** добавьте файл, который содержит параметры конфигурации для службы Stream Processor.

   Если требуется удалить файл конфигурации для службы Stream Processor, нажмите на кнопку . Если требуется сохранить файл конфигурации на компьютере, нажмите на кнопку .

5. Нажмите на кнопку **Сохранить**.

Настройка службы Trainer

Kaspersky MLAD использует службу Trainer для обучения элементов ML-моделей. Вы можете настроить параметр, определяющий количество элементов ML-моделей, которое служба Trainer может обучать одновременно.

Работы по настройке службы Trainer могут выполнять системные администраторы.

Чтобы настроить службу Trainer:

1. В нижнем левом углу страницы нажмите на кнопку ⚙.

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **Trainer**.

   Справа отобразится список параметров.

3. В поле **Максимальное количество одновременно обучаемых элементов** введите количество элементов, которое служба Trainer может обучать одновременно.

   > Чем больше объем обрабатываемых данных и сложность элементов ML-моделей для обучения, тем больше аппаратных ресурсов задействует служба Trainer. Для максимальной производительности службы рекомендуется ввести значение, не превышающее количество ядер сервера, на котором установлена программа.

4. Нажмите на кнопку **Сохранить**.

Настройка коннектора HTTP Connector

Kaspersky MLAD использует коннектор HTTP Connector для получения данных из CSV-файлов путем загрузки данных методом `POST`. Вы можете загружать данные через порт 4999 по протоколу HTTP или HTTPS, указав нужный протокол в запросе.

В Kaspersky MLAD загрузка файлов сертификатов и файла ключа возможна только в формате DER или PEM. Если требуется, вы можете изменить формат файлов сертификатов и ключа к сертификату, используя утилиту OpenSSL. Например, для изменения формата файла сертификата с P12 на PEM в консоли выполните команду:

```
openssl pkcs12 -in <имя сертификата>.p12 -clcerts -nokeys -out <имя сертификата>.pem
```

> Работы по настройке коннектора HTTP Connector могут выполнять системные администраторы.

Чтобы настроить работу коннектора HTTP Connector:

1. В нижнем левом углу страницы нажмите на кнопку ⚙.

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **HTTP Connector**.

   Справа отобразится список параметров.

3. В поле **Размер записываемого блока (количество тегов)** укажите количество значений тегов, которое единовременно записывается в службу Message Broker.

   Указанное значение влияет на количество итераций для записи значений тегов из CSV-файла в службу Message Broker в зависимости от общего количества наблюдений по тегам, полученным с помощью коннектора HTTP Connector.

4. В поле **Максимальный размер загружаемого файла (МБ)** укажите максимальный размер файла в мегабайтах, передаваемого в коннектор HTTP Connector.

   При попытке загрузить CSV-файл большего размера файл не будет передан в коннектор HTTP Connector.

5. С помощью переключателя **Использовать TLS-соединение** включите или выключите использование защищенного TLS-соединения.

   По умолчанию использование защищенного TLS-соединения включено.

   > Во избежание компрометации получаемых и/или отправляемых данных рекомендуется оставить включенным использование защищенного TLS-соединения.

6. Если вы используете защищенное TLS-соединение, с помощью переключателя **Использовать рекомендуемые параметры TLS-соединения** включите или выключите использование рекомендуемых параметров TLS-соединения.

   По умолчанию использование рекомендуемых параметров TLS-соединения включено.

   При включенном переключателе используется защищенное TLS-соединение по протоколу TLS-1.2 или TLS-1.3 с использованием набора шифров из списка рекомендованных.

7. Если вы используете защищенное TLS-соединение, выполните следующие действия:

   a. Добавьте сертификат HTTPS-сервера и ключ к сертификату с помощью кнопки **Обзор** под параметрами **Сертификат HTTPS-сервера** и **Закрытый ключ к сертификату HTTPS-сервера**.

      > Рекомендуется использовать сертификат с длиной ключа к сертификату 4 096 бит при использовании алгоритма RSA или 256 бит при использовании алгоритма ECDH.

   b. Если вы используете сертификаты клиента, то добавьте корневой сертификат для проверки подписи сертификата клиента с помощью кнопки **Обзор** под параметром **Сертификат CA для проверки подписи сертификата клиента**.

   > Загрузка сертификатов и ключа к сертификату возможна только в виде файла в формате DER или PEM.

   Если требуется удалить файл сертификата или ключ к сертификату, нажмите на кнопку в соответствующем поле. Если требуется сохранить файл сертификата или ключ к сертификату на компьютере, нажмите на кнопку в соответствующем поле.

8. С помощью переключателя **Масштабировать полученные значения тегов** включите или выключите конвертацию значений тегов с учетом параметров **Смещение** и **Множитель**, заданных при создании тега.

   По умолчанию конвертация полученных значений тегов выключена.

9. С помощью переключателя **Игнорировать регистр в именах тегов** включите или выключите учет регистра при соотнесении имен тегов, добавленных в программу, с именами тегов, по которым в программу поступают данные из CSV-файлов.

10. Нажмите на кнопку **Сохранить**.

Kaspersky MLAD будет получать данные из CSV-файлов с помощью коннектора HTTP Connector.

Пример отправки CSV-файла в коннектор HTTP Connector через curl по протоколу HTTP методом `POST` на порт 4999 сервера Kaspersky MLAD:

```
curl -F "file=@<имя файла>.csv" -X POST "http://<IP-адрес или доменное имя сервера Kaspersky MLAD>:4999/upload"
```

Коннектор HTTP Connector принимает CSV-файлы со следующими полями:

```
timestamp;tag_name;value
```

где:

- `timestamp` – временная метка в формате %Y-%m-%dT%H:%M:%S.
- `tag_name` – имя тега.
- `value` – значение тега.

  Если значение тега содержит дробную часть, используйте точку при отделении целой и дробной частей.

Настройка коннектора MQTT Connector

Kaspersky MLAD использует коннектор MQTT Connector для получения данных и отправки сообщений о регистрации инцидентов по протоколу MQTT (Message Queuing Telemetry Transport).

Конфигурационный файл коннектора поставляется специалистами "Лаборатории Касперского" или сертифицированным интегратором.

Работы по настройке коннектора MQTT Connector могут выполнять системные администраторы.

Чтобы настроить работу коннектора MQTT Connector:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **MQTT Connector**.

   Справа отобразится список параметров.

3. С помощью переключателя **Использовать TLS-соединение** включите или выключите использование защищенного TLS-соединения.

   По умолчанию использование защищенного TLS-соединения включено.

   Во избежание компрометации получаемых и/или отправляемых данных рекомендуется оставить использование защищенного TLS-соединения включенным.

4. Если вы используете защищенное TLS-соединение, с помощью переключателя **Использовать рекомендуемые параметры TLS-соединения** включите или выключите использование рекомендуемых параметров TLS-соединения.

   По умолчанию использование рекомендуемых параметров TLS-соединения включено.

   При включенном переключателе используется защищенное TLS-соединение по протоколу TLS-1.2 или TLS-1.3 с использованием набора шифров из списка рекомендованных.

5. В поле **MQTT-брокер (адрес:порт)** укажите имя хоста и порт внешнего MQTT-брокера, с которым будет взаимодействовать коннектор MQTT Connector.

   По умолчанию этот параметр имеет значение `mqtt_broker:1883`.

6. Если MQTT-брокер использует аутентификацию клиента, в полях **Имя пользователя для MQTT-соединения** и **Пароль для MQTT-соединения** укажите имя пользователя и пароль для подключения к MQTT-брокеру.

7. Если вы используете защищенное TLS-соединение и собственный удостоверяющий центр для выпуска сертификатов, добавьте корневой сертификат для проверки подписи сертификата MQTT-брокера с помощью кнопки **Обзор** под параметром **Сертификат CA для проверки подписи сертификата сервера**.

   Если требуется удалить файл сертификата, нажмите на кнопку . Если требуется сохранить файл сертификата на компьютере, нажмите на кнопку .

8. Если вы используете защищенное TLS-соединение и на MQTT-брокере включена аутентификация клиента, выполните следующие действия:

   a. Добавьте сертификат клиента с помощью кнопки **Обзор** под параметром **Сертификат клиента**.

   b. Добавьте закрытый ключ к сертификату клиента с помощью кнопки **Обзор** под параметром **Закрытый ключ к сертификату клиента**.

   > Рекомендуется использовать сертификат с длиной ключа к сертификату 4 096 бит при использовании алгоритма RSA или 256 бит при использовании алгоритма ECDH.
   > Загрузка сертификатов и закрытого ключа к сертификату возможна только в виде файла в формате DER или PEM.

   Если требуется удалить файл сертификата или ключ к сертификату, нажмите на кнопку в соответствующем поле. Если требуется сохранить файл сертификата или ключ к сертификату на компьютере, нажмите на кнопку в соответствующем поле.

9. В поле **Список подписок MQTT для получения тегов** введите имя списка подписок MQTT, от которых коннектор MQTT Connector будет получать значения тегов.

   По умолчанию этот параметр имеет значение `tags`.

10. В поле **Топик MQTT для публикации сообщений** укажите имя топика, в котором коннектор MQTT Connector будет публиковать сообщения о регистрации инцидента.

    Если значение этого параметра не установлено, то отправка сообщений не производится.

    По умолчанию для этого параметра значение не установлено.

11. В раскрывающемся списке **Формат данных** выберите формат, в котором будут поступать данные от внешних систем, а также в котором будут отправляться сообщения об инцидентах.

    Для выбора доступны следующие варианты: `JSONBatch`, `Topic`, `SmartHome`, `Kaspersky IoT Secure Gateway`.

    По умолчанию этот параметр имеет значение `JSONBatch`.

    Если вы затрудняетесь с выбором формата данных, обратитесь к специалистам "Лаборатории Касперского" или сертифицированному интегратору.

    Если вам не подходит ни один из форматов данных и сообщений об инцидентах, вы можете обратиться к специалистам "Лаборатории Касперского" для добавления нужного формата.

12. Если вы выбрали формат данных `Topic`, то добавьте конфигурационный файл, содержащий параметры коннектора для этого формата данных, с помощью кнопки **Обзор** под параметром **Конфигурационный файл коннектора**.

    Если требуется удалить файл сертификата, нажмите на кнопку . Если требуется сохранить файл сертификата на компьютере, нажмите на кнопку .

13. С помощью переключателя **Масштабировать полученные значения тегов** включите или выключите конвертацию значений тегов с учетом параметров **Смещение** и **Множитель**, заданных при создании тега.

    По умолчанию конвертация полученных значений тегов выключена.

14. Нажмите на кнопку **Сохранить**.

Kaspersky MLAD будет получать данные и отправлять сообщения о регистрации инцидентов по протоколу MQTT.

Настройка коннектора AMQP Connector

Kaspersky MLAD использует коннектор AMQP Connector для получения данных и отправки сообщений о регистрации инцидентов по протоколу AMQP (Advanced Message Queuing Protocol).

Конфигурационный файл коннектора поставляется специалистами "Лаборатории Касперского" или сертифицированным интегратором.

Работы по настройке коннектора AMQP Connector могут выполнять системные администраторы.

Чтобы настроить работу коннектора AMQP Connector:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **AMQP Connector**.

   Справа отобразится список параметров.

3. С помощью переключателя **Использовать TLS-соединение** включите или выключите использование защищенного TLS-соединения.

   По умолчанию использование защищенного TLS-соединения включено.

   > Во избежание компрометации получаемых и/или отправляемых данных рекомендуется оставить использование защищенного TLS-соединения включенным.

4. Если вы используете защищенное TLS-соединение, с помощью переключателя **Использовать рекомендуемые параметры TLS-соединения** включите или выключите использование рекомендуемых параметров TLS-соединения.

   По умолчанию использование рекомендуемых параметров TLS-соединения включено.

   При включенном переключателе используется защищенное TLS-соединение по протоколу TLS-1.2 или TLS-1.3 с использованием набора шифров из списка рекомендованных.

5. В поле **AMQP-брокер (адрес:порт)** укажите имя хоста и порт внешнего AMQP-брокера, с которым будет взаимодействовать коннектор AMQP Connector.

   По умолчанию этот параметр имеет значение `rabbitmq:5672`.

6. Если AMQP-брокер использует аутентификацию клиента, в полях **Имя пользователя для AMQP-соединения** и **Пароль для AMQP-соединения** укажите имя пользователя и пароль для подключения к AMQP-брокеру.

7. Если вы используете защищенное TLS-соединение и собственный удостоверяющий центр для выпуска сертификатов, добавьте корневой сертификат для проверки подписи сертификата AMQP-брокера с помощью кнопки **Обзор** под параметром **Сертификат CA для проверки подписи сертификата сервера**.

   > Загрузка сертификата возможна только в виде файла в формате DER или PEM.

   Если требуется удалить файл сертификата, нажмите на кнопку . Если требуется сохранить файл сертификата на компьютере, нажмите на кнопку .

8. Если вы используете защищенное TLS-соединение и на AMQP-брокере включена аутентификация клиента, выполните следующие действия:

   a. Добавьте сертификат клиента с помощью кнопки **Обзор** под параметром **Сертификат клиента**.

   b. Добавьте закрытый ключ к сертификату клиента с помощью кнопки **Обзор** под параметром **Закрытый ключ к сертификату клиента**.

   > Рекомендуется использовать сертификат с длиной ключа к сертификату 4 096 бит при использовании алгоритма RSA или 256 бит при использовании алгоритма ECDH.
   > Загрузка сертификата и закрытого ключа к сертификату возможна только в виде файла в формате DER или PEM.

   Если требуется удалить файл сертификата или ключ к сертификату, нажмите на кнопку в соответствующем поле. Если требуется сохранить файл сертификата или ключ к сертификату на компьютере, нажмите на кнопку в соответствующем поле.

9. В поле **Виртуальный узел AMQP** укажите виртуальный узел для установки соединения между коннектором AMQP Connector и внешним AMQP-брокером.

   По умолчанию этот параметр имеет значение `/`.

10. В поле **Имя точки обмена (exchange) AMQP для получения значений тегов** укажите имя точки обмена для получения значений тегов от внешнего AMQP-брокера.

    Если значение для этого параметра не установлено, то получение значений тегов через коннектор AMQP Connector не происходит.

    По умолчанию для этого параметра значение не установлено.

11. В поле **Список подписок AMQP для получения значений тегов** укажите имя списка подписок, от которых коннектор AMQP Connector будет получать значения тегов.

    По умолчанию этот параметр имеет значение `#`.

12. Если требуется, в поле **Очередь AMQP для получения значений тегов** укажите имя очереди для коннектора AMQP Connector.

13. В поле **Имя точки обмена (exchange) AMQP для публикации сообщений** укажите имя точки обмена для отправки сообщений о регистрации инцидентов.

    Если значение для этого параметра не установлено, то отправка сообщений не происходит. Вы можете указать то же имя, которое указали в пункте 10 этой инструкции.

    По умолчанию для этого параметра значение не установлено.

14. В поле **Топик AMQP для публикации сообщений** укажите имя топика, в котором коннектор AMQP Connector будет публиковать сообщения о регистрации инцидента.

    По умолчанию этот параметр имеет значение `alert`.

15. В раскрывающемся списке **Формат данных** выберите формат, в котором будут поступать данные от внешних систем, а также в котором будут отправляться сообщения об инцидентах.

    Для выбора доступны следующие варианты: `JSONBatch`, `Topic`, `SmartHome`, `Kaspersky IoT Secure Gateway`.

    По умолчанию этот параметр имеет значение `JSONBatch`.

    > Если вы затрудняетесь с выбором формата данных, обратитесь к специалистам "Лаборатории Касперского" или сертифицированному интегратору.

    > Если вам не подходит ни один из форматов данных и сообщений об инцидентах, вы можете обратиться к специалистам "Лаборатории Касперского" для добавления нужного формата.

16. Если вы выбрали формат данных `Topic`, то добавьте конфигурационный файл, содержащий параметры коннектора для этого формата данных, с помощью кнопки **Обзор** под параметром **Конфигурационный файл коннектора**.

    Если требуется удалить конфигурационный файл, нажмите на кнопку . Если требуется сохранить загруженный конфигурационный файл на компьютере, нажмите на кнопку .

17. С помощью переключателя **Масштабировать полученные значения тегов** включите или выключите конвертацию значений тегов с учетом параметров **Смещение** и **Множитель**, заданных при создании тега.

    По умолчанию конвертация полученных значений тегов выключена.

18. Нажмите на кнопку **Сохранить**.

Kaspersky MLAD будет получать данные и отправлять сообщения о регистрации инцидентов по протоколу AMQP.

Настройка коннектора KICS Connector

Kaspersky MLAD использует коннектор KICS Connector для получения данных от Kaspersky Industrial CyberSecurity for Networks версии 4.0 и выше и отправки обратно сообщений о регистрации инцидентов.

Предварительно в Kaspersky Industrial CyberSecurity for Networks требуется создать и добавить коннектор для интеграции с Kaspersky MLAD. Подробную информацию о создании и добавлении коннектора вы можете получить в разделе *Добавление коннектора* в *справке Kaspersky Industrial CyberSecurity for Networks*.

Работы по интеграции с Kaspersky Industrial CyberSecurity for Networks версии 4.0 и выше могут выполнять системные администраторы.

Чтобы настроить коннектор KICS Connector:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **KICS Connector**.

   Справа отобразится список параметров.

3. С помощью кнопки **Обзор** под параметром **Файл свертки для коннектора KICS Connector (zip)** добавьте файл, содержащий параметры настройки взаимодействия Kaspersky MLAD и Kaspersky Industrial CyberSecurity for Networks.

   Подробную информацию о создании файла свертки вы можете получить в *справке Kaspersky Industrial CyberSecurity for Networks*. Созданный файл свертки требуется сохранить на компьютере, на котором установлен Kaspersky MLAD.

   Если требуется удалить файл свертки, в поле **Файл свертки для коннектора KICS Connector (zip)** нажмите на кнопку . Если требуется сохранить файл свертки на компьютере, нажмите на кнопку .

4. В поле **Пароль для коннектора KICS Connector** введите пароль, который вы указали при добавлении коннектора в Kaspersky Industrial CyberSecurity for Networks.

5. С помощью переключателя **Отправлять сообщения в Kaspersky Industrial CyberSecurity for Networks** включите или выключите отправку сообщений о регистрации инцидентов в Kaspersky Industrial CyberSecurity for Networks.

6. В поле **Частота семплирования значений тегов (Гц)** укажите частоту в герцах, с которой требуется получать значения тегов из Kaspersky Industrial CyberSecurity for Networks.

   Укажите в этом поле значение `0`, если не требуется использовать семплирование.

7. С помощью переключателя **Масштабировать полученные значения тегов** включите или выключите конвертацию значений тегов с учетом параметров **Смещение** и **Множитель**, заданных при создании тега.

   По умолчанию конвертация полученных значений тегов выключена.

8. Нажмите на кнопку **Сохранить**.

Kaspersky MLAD будет получать данные из Kaspersky Industrial CyberSecurity for Networks и отправлять обратно сообщения о регистрации инцидентов.

Настройка коннектора CEF Connector

Kaspersky MLAD использует коннектор CEF Connector для получения данных от внешних источников событий (промышленного интернета вещей, сетевых устройств и приложений) и отправки во внешнюю систему сообщений о регистрации инцидентов.

Вы также можете использовать коннектор CEF Connector для отправки журналов событий информационной безопасности Kaspersky MLAD во внешнюю систему. Запись журналов событий ИБ в базу данных Kaspersky MLAD ведется автоматически.

Для получения событий от внешних источников с помощью коннектора CEF Connector требуется настроить службу Event Processor.
Перед настройкой параметров коннектора CEF Connector в веб-интерфейсе Kaspersky MLAD для получения событий в файле .env требуется указать IP-адрес и номер порта, по которому будет осуществляться подключение внешнего источника событий к коннектору CEF Connector. Изменение параметров конфигурационного файла выполняет только квалифицированный технический специалист Заказчика, сотрудник "Лаборатории Касперского" или сертифицированный интегратор.

Работы по настройке коннектора CEF Connector могут выполнять системные администраторы.

Чтобы настроить коннектор CEF Connector:

1. В нижнем левом углу страницы нажмите на кнопку ⚙.

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **CEF Connector**.

   Справа отобразится список параметров.

3. С помощью переключателя **Получать события для службы Event Processor** включите или выключите использование коннектора CEF Connector для получения событий из внешней системы.

4. С помощью переключателя **Отправлять зарегистрированные инциденты в SIEM-систему** включите или выключите отправку во внешнюю систему сообщений об инцидентах, зарегистрированных программой.

5. С помощью переключателя **Отправлять зарегистрированные события в SIEM-систему** включите или выключите отправку во внешнюю систему сообщений о событиях, зарегистрированных службой Event Processor.

6. В поле **IP-адрес для отправки событий и инцидентов в SIEM-систему** укажите IP-адрес для подключения внешней системы к коннектору CEF Connector и отправки событий, обработанных службой Event Processor, и инцидентов.

7. В поле **Порт для отправки событий и инцидентов в SIEM-систему** укажите номер порта для подключения внешней системы к коннектору CEF Connector и отправки событий, обработанных службой Event Processor, и инцидентов.

8. Если требуется отправлять журналы событий ИБ Kaspersky MLAD во внешнюю систему, включите переключатель **Отправлять журналы событий информационной безопасности на syslog-сервер** и выполните следующие действия:

   a. В раскрывающемся списке **Транспортный протокол для отправки событий информационной безопасности на syslog-сервер** выберите протокол, который требуется использовать для отправки журналов событий ИБ.

      Kaspersky MLAD поддерживает протоколы TCP и UDP для отправки журналов событий ИБ во внешнюю систему.

   b. В поле **Адрес syslog-сервера для отправки событий информационной безопасности** укажите IP-адрес или имя хоста внешней системы, в которую требуется отправлять журналы событий ИБ.

   c. В поле **Порт syslog-сервера для отправки событий информационной безопасности** укажите номер порта внешней системы, в которую требуется отправлять журналы событий ИБ.

9. С помощью переключателя **Использовать TLS-соединение** включите или выключите использование защищенного TLS-соединения при использовании Kaspersky MLAD в качестве клиента.

   По умолчанию использование защищенного TLS-соединения включено.

   > Во избежание компрометации получаемых и/или отправляемых данных рекомендуется оставить включенным использование защищенного TLS-соединения.

10. Если вы включили использование защищенного TLS-соединения, с помощью переключателя **Использовать рекомендуемые параметры TLS-соединения** включите или выключите использование рекомендуемых параметров TLS-соединения.

    При включенном переключателе используется защищенное TLS-соединение по протоколу TLS-1.2 или TLS-1.3 с использованием набора шифров из списка рекомендованных.

11. Если требуется использовать защищенное TLS-соединение для серверной части коннектора CEF Connector, выполните следующие действия:

    a. Добавьте сертификат сервера и ключ к сертификату с помощью кнопки **Обзор** под параметрами **Сертификат сервера** и **Закрытый ключ к сертификату сервера**.

    > Рекомендуется использовать сертификат с длиной ключа к сертификату не менее 4 096 бит при использовании алгоритма RSA или 256 бит при использовании алгоритма ECDH.

    b. Если используются сертификаты клиента, добавьте корневой сертификат для проверки подписи сертификата клиента с помощью кнопки **Обзор** под параметром **Сертификат CA для проверки подписи сертификата клиента**.

    > Загрузка сертификатов и ключа к сертификату возможна только в виде файла в формате DER или PEM.

    Если требуется удалить файл сертификата или ключ к сертификату, нажмите на кнопку в соответствующем поле. Если требуется сохранить файл сертификата или ключ к сертификату на компьютере, нажмите на кнопку в соответствующем поле.

12. Если требуется использовать защищенное TLS-соединение для клиентской части коннектора CEF Connector, при необходимости выполните следующие действия:

    a. Добавьте сертификат клиента и ключ к сертификату с помощью кнопки **Обзор** под параметрами **Сертификат клиента** и **Закрытый ключ к сертификату клиента**.

    > Рекомендуется использовать сертификат с длиной ключа к сертификату не менее 4 096 бит при использовании алгоритма RSA или 256 бит при использовании алгоритма ECDH.

    b. Если используются сертификаты сервера, добавьте корневой сертификат для проверки подписи сертификата сервера с помощью кнопки **Обзор** под параметром **Сертификат CA для проверки подписи сертификата сервера**.

    > Загрузка сертификатов и ключа к сертификату возможна только в виде файла в формате DER или PEM.

    Если требуется удалить файл сертификата или ключ к сертификату, нажмите на кнопку в соответствующем поле. Если требуется сохранить файл сертификата или ключ к сертификату на компьютере, нажмите на кнопку в соответствующем поле.

13. Нажмите на кнопку **Сохранить**.

Настройка коннектора WebSocket Connector

Kaspersky MLAD использует коннектор WebSocket Connector для получения данных и отправки сообщений о регистрации инцидентов по протоколу WebSocket.

Конфигурационный файл коннектора поставляется специалистами "Лаборатории Касперского" или сертифицированным интегратором.

Работы по настройке коннектора WebSocket Connector могут выполнять системные администраторы. Описанная в этом разделе инструкция приведена для ознакомительных целей.

Чтобы настроить коннектор WebSocket Connector:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **WebSocket Connector**.

   Справа отобразится список параметров.

3. В поле **URL-адрес WebSocket-сервера** укажите веб-адрес WebSocket-сервера, с которым будет взаимодействовать коннектор WebSocket Connector.

   Укажите веб-адрес в формате `WebSocket -протокол://адрес:порт/`.

4. Если требуется использовать защищенное соединение и вы используете собственный удостоверяющий центр для выпуска сертификатов, добавьте корневой сертификат для проверки подписи сертификата WebSocket-сервера с помощью кнопки **Обзор** под параметром **Сертификат CA для проверки подписи сертификата сервера**.

   Если требуется удалить файл сертификата, нажмите на кнопку . Если требуется сохранить файл сертификата на компьютере, нажмите на кнопку .

5. Если требуется использовать защищенное соединение и на WebSocket-сервере включена аутентификация клиента, выполните следующие действия:

   a. Добавьте сертификат клиентского приложения WebSocket с помощью кнопки **Обзор** под параметром **Сертификат клиента**.

   b. Добавьте закрытый ключ к сертификату клиентского приложения WebSocket с помощью кнопки **Обзор** под параметром **Закрытый ключ к сертификату клиента**.

   Рекомендуется использовать сертификат с длиной ключа к сертификату 4 096 бит при использовании алгоритма RSA или 256 бит при использовании алгоритма ECDH.

   Если требуется удалить файл сертификата или ключ к сертификату, нажмите на кнопку в соответствующем поле. Если требуется сохранить файл сертификата или ключ к сертификату на компьютере, нажмите на кнопку в соответствующем поле.

6. В раскрывающемся списке **Формат данных** выберите формат, в котором будут поступать данные от внешних систем, а также в котором будут отправляться сообщения об инцидентах.

   Для выбора доступны следующие варианты: `JSONBatch`, `Topic`, `SmartHome`, `Kaspersky IoT Secure Gateway`.

   По умолчанию этот параметр имеет значение `JSONBatch`.

   > Если вы затрудняетесь с выбором формата данных, обратитесь к специалистам "Лаборатории Касперского" или сертифицированному интегратору.

   > Если вам не подходит ни один из форматов данных и сообщений об инцидентах, вы можете обратиться к специалистам "Лаборатории Касперского" для добавления нужного формата.

7. Если вы выбрали формат данных `Topic`, то добавьте конфигурационный файл, содержащий параметры коннектора для этого формата данных, с помощью кнопки **Обзор** под параметром **Конфигурационный файл коннектора**.

   Если требуется удалить конфигурационный файл, нажмите на кнопку . Если требуется сохранить загруженный конфигурационный файл на компьютере, нажмите на кнопку .

8. С помощью переключателя **Масштабировать полученные значения тегов** включите или выключите конвертацию значений тегов с учетом параметров **Смещение** и **Множитель**, заданных при создании тега.

   По умолчанию конвертация полученных значений тегов выключена.

9. С помощью переключателя **Отправлять инциденты** включите или выключите отправку сообщений о зарегистрированных в Kaspersky MLAD инцидентах на WebSocket-сервер.

10. Если вы используете защищенное TLS-соединение, с помощью переключателя **Использовать рекомендуемые параметры TLS-соединения** включите или выключите использование рекомендуемых параметров TLS-соединения.

    По умолчанию использование рекомендуемых параметров TLS-соединения включено.

    При включенном переключателе используется защищенное TLS-соединение по протоколу TLS-1.2 или TLS-1.3 с использованием набора шифров из списка рекомендованных.

11. Нажмите на кнопку **Сохранить**.

Kaspersky MLAD будет получать данные и отправлять сообщения о регистрации инцидентов по протоколу WebSocket.

Настройка службы Event Processor

Kaspersky MLAD использует службу Event Processor для выявления паттернов и аномальных последовательностей событий и паттернов.

В случае перезапуска Kaspersky MLAD повторно задавать параметры службы Event Processor не нужно. Kaspersky MLAD восстанавливает состояние службы Event Processor из базы данных или файла в битовом формате. При значительном объеме обработанных событий и зарегистрированных паттернов процесс восстановления может занимать несколько минут. До момента восстановления состояния службы Event Processor в разделе **Процессор событий** не будут выполняться запросы и обновляться данные, а также в это время не будут обрабатываться данные, поступающие от коннектора CEF Connector. Эти данные временно сохраняются в очереди сообщений системы и обрабатываются после восстановления состояния службы Event Processor.

Для работы службы Event Processor может потребоваться большой объем оперативной памяти на сервере, на котором установлен Kaspersky MLAD. Объем используемой оперативной памяти зависит от интенсивности потока событий и объема обрабатываемой истории событий. Также на объем используемой оперативной памяти влияет правильность настройки параметров службы Event Processor.

Работы по настройке службы Event Processor могут выполнять системные администраторы.

Чтобы настроить параметры службы Event Processor:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **Event Processor**.

   Справа отобразится список параметров службы.

3. В блоке **Основной режим** выполните следующие действия:

a. С помощью кнопки **Обзор** под параметром **Конфигурационный файл процессора событий** добавьте файл, который содержит параметры конфигурации для службы Event Processor.

Файл конфигурации создается квалифицированным техническим специалистом Заказчика, сотрудником "Лаборатории Касперского" или сертифицированным интегратором.

Если требуется удалить файл конфигурации для службы Event Processor, нажмите на кнопку . Если требуется сохранить файл конфигурации на компьютере, нажмите на кнопку .

Изменение файла конфигурации службы Event Processor приводит к полной потере данных службы.

b. Если требуется обрабатывать инциденты, зарегистрированные службой Anomaly Detector, включите переключатель **Обрабатывать инциденты как события**.

c. В поле **Максимальное количество слоев сети** укажите количество слоев нейросемантической сети, которое будет использоваться.

По умолчанию количество слоев сети для событийных данных, имеющих в основе определенную структуру, составляет десять слоев. В большинстве случаев нейросемантической сети в основе процессора событий достаточно десяти слоев для иерархического представления данных. Для выявления протяженных по времени паттернов периодических процессов может потребоваться увеличение значения параметра **Максимальное количество слоев сети**.

d. В поле **Коэффициент, определяющий допустимую дисперсию длительности паттерна** укажите коэффициент, с помощью которого будет определяться допустимая дисперсия интервалов между элементами в одном паттерне.

Если фактическая величина дисперсии меньше либо равна указанной, то выявленные последовательности событий будут относиться к одному паттерну.

e. В поле **Интервал получения событий эпизода (сек.)** укажите интервал времени в секундах, за который служба Event Processor формирует эпизод из поступающих на обработку событий.

Если скорость получения событий составляет около 1000 событий в секунду, то рекомендуется указывать такое значение периода получения новых событий, чтобы за указанный период поступало количество событий, близкое к значению, которое указано в поле **Размер эпизода (количество событий)**. Если скорость получения событий гораздо ниже, то период получения новых событий следует выставлять, исходя из баланса операционной актуальности обработки событий.

f. В поле **Размер эпизода (количество событий)** укажите максимальное количество событий в эпизоде для последующей обработки службой Event Processor.

Если скорость получения событий составляет около 1000 событий в секунду, то в этом поле рекомендуется указывать значение равное `4096`.

g. В раскрывающемся списке **Способ сохранения состояния службы Event Processor** выберите один из следующих способов сохранения состояния службы Event Processor:

- **Таблица базы данных** – Kaspersky MLAD сохраняет результат обработки каждого эпизода в таблице базы данных. Рекомендуется использовать этот способ сохранения состояния службы.
- **Файл в битовом формате** – Kaspersky MLAD сохраняет состояние службы Event Processor с частотой, заданной в поле **Периодичность создания резервных копий компонента**. Программа сохраняет состояние службы в файле, указанном в поле **Файл, содержащий резервную копию состояния компонента**. Рекомендуется использовать этот способ сохранения состояния службы для отладки.

Сохранение состояния службы Event Processor в файл в битовом формате рекомендуется использовать для отладки и настройки параметров программы сотрудниками "Лаборатории Касперского" в процессе выполнения работ по внедрению Kaspersky MLAD.

По умолчанию служба Event Processor сохраняет результаты обработки потока событий в таблице базы данных.

Изменение способа сохранения состояния службы Event Processor приводит к полной потере данных службы.

h. Если вы выбрали способ хранения состояния службы Event Processor в файле в битовом формате, в поле **Периодичность создания резервных копий компонента** укажите период (в днях, часах и минутах), через который будет выполняться резервное копирование службы Event Processor.

i. Если вы выбрали способ хранения состояния службы Event Processor в файле в битовом формате, добавьте файл, который содержит резервную копию службы Event Processor. с помощью кнопки **Обзор** под параметром **Файл, содержащий резервную копию состояния компонента**.

   Файл будет использован, если понадобится восстановить состояние службы Event Processor. Восстановление состояния службы Event Processor выполняют специалисты "Лаборатории Касперского" в рамках расширенной технической поддержки.

   Если требуется удалить файл, содержащий резервную копию службы Event Processor, нажмите на кнопку . Если требуется сохранить файл, содержащий резервную копию службы, на компьютере, нажмите на кнопку .

4. В блоке **Режим сна** выполните следующие действия:

   a. В поле **Отправка оповещений при активации монитора в режиме сна** выберите одно из следующих значений:

      - **Отправлять оповещения об активации монитора любым паттерном** – Kaspersky MLAD отправляет оповещения об активации монитора при выявлении в режиме сна паттернов в соответствии с заданными критериями мониторинга. В разделе **Процессор событий** на вкладке **Мониторинг** обновится количество активаций монитора.

      - **Не отправлять оповещения об активациях монитора** – Kaspersky MLAD не отправляет оповещений об активации монитора в режиме сна.

      - **Отправлять оповещения об активации монитора новым паттерном** – Kaspersky MLAD отправляет оповещения об активации монитора при выявлении в режиме сна новых паттернов в соответствии с заданными критериями мониторинга. В разделе **Процессор событий** на вкладке **Мониторинг** обновится количество активаций монитора.

      - **Отправлять оповещения об активации монитора ранее зарегистрированным паттерном** – Kaspersky MLAD отправляет оповещения об активации монитора при выявлении в режиме сна стабильных паттернов в соответствии с заданными критериями мониторинга. В разделе **Процессор событий** на вкладке **Мониторинг** обновится количество активаций монитора.

   b. В поле **Периодичность режима сна** укажите, как часто (в днях) и в какое время (в формате UTC) служба Event Processor будет переходить в режим сна для повторной обработки событий.

      В качестве времени начала режима сна рекомендуется указать время, когда поток событий наименее интенсивен.

      Если заданное время сна не наступило в текущий день, процессор событий перейдет в режим сна в этот же день. Если время сна уже наступило в текущий день, служба Event Processor перейдет в режим сна в указанное время через заданное количество дней.

   c. В поле **Продолжительность режима сна (ЧЧ:ММ)** укажите интервал времени (в часах и минутах), в течении которого служба Event Processor будет обрабатывать события в режиме сна.

   d. В поле **Интервал истории событий для обработки в режиме сна** укажите интервал времени (в днях, часах и минутах), за который требуется передать проанализированные события на повторную обработку службой Event Processor в режиме сна.

5. В блоке **Эксфильтрация данных по DNS** выполните следующие действия:

   a. В поле **Порог вероятности эксфильтрации** укажите пороговое значение, при достижении которого ML-модель процессора событий считает, что DNS-запрос, поступивший в виде события, содержит признаки эксфильтрации данных.

      По умолчанию этот параметр имеет значение `0.5`.

   b. С помощью кнопки **Обзор** под параметром **Веса модели для выявления эксфильтрации** добавьте файл с весами ML-модели, которую процессор событий использует для выявления признаков эксфильтрации данных в DNS-запросах.

      > Файл с весами ML-модели для выявления признаков эксфильтрации данных в DNS-запросах создается сотрудником "Лаборатории Касперского" или сертифицированным интегратором.

      Если требуется удалить файл, содержащий веса ML-модели для выявления эксфильтрации, нажмите на кнопку . Если требуется сохранить файл на компьютере, нажмите на кнопку .

   c. В поле **Смещение** укажите значение смещения ML-модели для выявления признаков эксфильтрации данных в DNS-запросах.

      По умолчанию этот параметр имеет значение `-12.4`.

   d. В поле **Размер буфера** укажите количество событий, содержащие DNS-запросы, которые требуется передать на обучение.

      По умолчанию этот параметр имеет значение `100`.

6. Нажмите на кнопку **Сохранить**.

Настройка приоритетов, статусов и причин инцидентов

Kaspersky MLAD позволяет указать приоритеты и причины для инцидентов, а также статусы для инцидентов и групп инцидентов.

Приоритет инцидента представляет собой отметку о степени важности зарегистрированного инцидента. По умолчанию при установке Kaspersky MLAD доступны следующие приоритеты инцидентов: **Очень низкий**, **Низкий**, **Средний**, **Высокий**, **Очень высокий**. Приоритет присваивается инциденту автоматически в соответствии с приоритетом, заданным в параметрах элемента ML-модели, зарегистрировавшего этот инцидент. Если в параметрах элемента ML-модели приоритет инцидента не задан, инцидентам присваивается приоритет, соответствующий уровню критичности актива, к которому относится элемент ML-модели, зарегистрировавший инцидент. Иначе инциденту присваивается приоритет **Средний**. При необходимости вы можете изменить названия приоритетов и цвета, используемые для отображения приоритетов при просмотре инцидентов.

Статус инцидента и группы инцидентов представляет собой отметку о статусе анализа инцидента, проводимого экспертом. По умолчанию при установке Kaspersky MLAD доступны следующие статусы инцидентов и групп инцидентов: **Исследуется**, **Ожидается решение**, **Инструкции даны**, **Проблема закрыта**, **Причина неизвестна**, **Игнорировать** и **Ложное срабатывание**. Для статусов **Проблема закрыта** и **Игнорировать** по умолчанию снят флажок **Уведомлять об инциденте**. Если при регистрации инцидентам автоматически присваивается один из этих статусов, то уведомления об этих инцидентах не будут отправлены по электронной почте, а точки-индикаторы инцидентов не будут отображены в разделах **Мониторинг** и **История**. Статус инцидента может быть присвоен автоматически в одном из следующих случаев:

- Если инцидент был автоматически отнесен к группе, для которой установлен статус.
- Если инцидент зарегистрирован элементом ML-модели, в параметрах которого задан статус инцидента по умолчанию.

Причина инцидента представляет собой отметку о причине возникновения инцидента, которую добавляет эксперт по результатам анализа инцидента.

Вы можете добавлять причины и статусы инцидентов. Созданные причины и статусы инцидентов станут доступными для выбора в разделе **Инциденты**. Если требуется, вы можете изменить или удалить статусы и причины инцидентов.

Работы по настройке приоритетов, причин и статусов инцидентов могут выполнять системные администраторы.

Чтобы изменить приоритеты инцидентов:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **Инциденты**.
3. В блоке **Приоритеты инцидентов** выберите один или несколько приоритетов инцидентов и нажмите на кнопку **Изменить**.
4. Если требуется, измените названия приоритетов и цвета, используемые для отображения приоритетов в таблице инцидентов.
5. Нажмите на кнопку **Сохранить**.

Чтобы добавить статус инцидентов:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **Инциденты**.
3. В блоке **Статусы инцидентов** нажмите на кнопку **Создать**.

   Справа отобразится панель **Создание элемента**.

4. В поле **Значение, русский язык** укажите название статуса инцидента на русском языке.
5. В поле **Значение, английский язык** укажите название статуса инцидента на английском языке.

6. В поле **Сортировка** укажите порядковый номер, с которым статус инцидента будет отсортирован в раскрывающемся списке **Статус инцидента** в разделе **Инциденты**.

   Статусы инцидентов будут отсортированы по их названиям, если порядковые номера статусов инцидентов совпадают.

7. Если требуется отправлять уведомления о регистрации инцидентов с добавляемым статусом и отображать его индикатор в блоке ошибки прогноза для разделов **Мониторинг** и **История**, установите флажок **Уведомлять об инциденте**.

   Если вы снимите флажок, то уведомления об этих инцидентах, которым автоматически присваивается этот статус, не будут отправлены по электронной почте, а точки-индикаторы инцидентов не будут отображены в разделах **Мониторинг** и **История**.

8. Нажмите на кнопку **Сохранить**.

Чтобы добавить причину инцидентов:

1. В меню администратора выберите раздел **Системные параметры** → **Инциденты**.

2. В блоке **Причины инцидентов** нажмите на кнопку **Создать**.

   Справа отобразится панель **Создание элемента**.

3. В поле **Причина инцидента** укажите название причины инцидента.

4. В поле **Сортировка** укажите порядковый номер, с которым причина инцидента будет отсортирована в раскрывающемся списке **Причина инцидента** в разделе **Инциденты**.

   Причины инцидентов будут отсортированы по их названиям, если порядковые номера причин инцидентов совпадают.

5. Нажмите на кнопку **Сохранить**.

Чтобы изменить статусы или причины инцидентов:

1. В меню администратора выберите раздел **Системные параметры** → **Инциденты**.

2. Для изменения параметров инцидентов, выполните одно из следующих действий:

   - Если требуется изменить статусы инцидентов и групп инцидентов, в блоке параметров **Статусы инцидентов** выберите один или несколько статусов инцидентов и нажмите на кнопку **Изменить**.

   - Если требуется изменить причины инцидентов, в блоке параметров **Причины инцидентов** выберите одну или несколько причин инцидентов нажмите на кнопку **Изменить**.

3. Внесите необходимые изменения.

4. Нажмите на кнопку **Сохранить**.

Чтобы удалить статусы или причины инцидентов:

1. В меню администратора выберите раздел **Системные параметры** → **Инциденты**.
2. Для удаления параметров инцидентов, выполните одно из следующих действий:
   - Если требуется удалить статусы инцидентов и групп инцидентов, в блоке параметров **Статусы инцидентов** выберите один или несколько статусов инцидентов и нажмите на кнопку **Удалить**.
   - Если требуется удалить причины инцидентов, в блоке параметров **Причины инцидентов** выберите одну или несколько причин инцидентов и нажмите на кнопку **Удалить**.
3. В открывшемся окне подтвердите удаление.

Kaspersky MLAD удалит информацию о статусах или причинах инцидентов из соответствующих таблиц, а также из информации об инцидентах и группах инцидентов в разделе **Инциденты**, для которых были выбраны эти причины или статусы инцидентов.

Настройка ведения журналов служб Kaspersky MLAD

Вы можете настроить уровни ведения журналов служб Kaspersky MLAD для записи определенной информации о состоянии программы и ее отображения в системе ведения журналов (Grafana). Соответствие служб Kaspersky MLAD и имен образов и контейнеров Docker, см. в Приложении.

Работы по настройке ведения журналов служб Kaspersky MLAD могут выполнять системные администраторы.

Чтобы настроить уровни ведения журналов служб Kaspersky MLAD:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.
2. Выберите раздел **Системные параметры** → **Ведение журналов**.

   Справа отобразится список служб Kaspersky MLAD.

3. Если требуется, в раскрывающемся списке рядом с именем необходимой службы измените уровень ведения журналов службы.

   В Kaspersky MLAD доступны следующие уровни ведения журналов:

   - **Отладка** – ведение журналов всей информации в программе;
   - **Инфо** – ведение журналов общей информации о работе программы;
   - **Общие** – ведение журналов важной информации о работе программы;
   - **Важные** – ведение журналов ошибок, возникших в работе программы, и событий, которые могут привести к ошибкам в работе программы;
   - **Ошибка** – ведение журналов ошибок, возникших в работе программы;
   - **Критические** – ведение журналов критических ошибок, возникших в работе программы.

   По умолчанию для большинства служб используется уровень ведения журналов **Общие**. Для службы API Server по умолчанию используется уровень ведения журналов **Инфо**.

4. Нажмите на кнопку **Сохранить**.

Настройка временных интервалов отображения данных

Kaspersky MLAD позволяет указать временной интервал (масштаб) отображения данных на графиках в разделах **Мониторинг**, **История** и **Временной срез**. По умолчанию при установке Kaspersky MLAD доступны следующие временные интервалы:

- 1, 5, 10, 15 и 30 минут;
- 1, 3, 6 и 12 часов;
- 1, 2, 15 и 30 дней;
- 3 и 6 месяцев;
- 1, 2 и 3 года.

Вы можете добавлять временные интервалы отображения данных на графиках. Созданные временные интервалы станут доступными для выбора в разделах **Мониторинг**, **История** и **Временной срез**. Если требуется, вы также можете изменить или удалить временные интервалы.

Работы по настройке временных интервалов отображения данных на графиках могут выполнять системные администраторы.

Чтобы добавить временной интервал отображения данных:

1. В нижнем левом углу страницы нажмите на кнопку ⚙.

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **Графики**.

3. В блоке параметров **Временные интервалы** нажмите на кнопку **Создать**.

   Справа отобразится панель **Создание элемента**.

4. В поле **Временной интервал (сек.)** укажите временной интервал в секундах, за который вы хотите отображать данные на графиках.

   При вводе временного интервала Kaspersky MLAD автоматически разбивает значение временного интервала по единицам измерения времени (годы, месяцы, недели, дни, часы, минуты, секунды) в полях **Значение, русский язык** и **Значение, английский язык**.

5. Если требуется, в поле **Значение, русский язык** измените название временного интервала на русском языке.

6. Если требуется, в поле **Значение, английский язык** измените название временного интервала на английском языке.

7. В поле **Сортировка** укажите порядковый номер, с которым временной интервал будет отсортирован в раскрывающихся списках в разделах **Мониторинг**, **История** и **Временной срез**.

8. Нажмите на кнопку **Сохранить**.

Чтобы изменить временные интервалы отображения данных:

1. В меню администратора выберите раздел **Системные параметры → Графики**.

2. В блоке параметров **Временные интервалы** выберите один или несколько временных интервалов и нажмите на кнопку **Изменить**.

3. Внесите необходимые изменения.

4. Нажмите на кнопку **Сохранить**.

Чтобы удалить временные интервалы отображения данных:

1. В меню администратора выберите раздел **Системные параметры → Графики**.

2. В блоке параметров **Временные интервалы** выберите один или несколько временных интервалов и нажмите на кнопку **Удалить**.

3. В открывшемся окне подтвердите удаление.

Информация о временных интервалах будет удалена из таблицы.

Настройка уровней критичности активов

Kaspersky MLAD позволяет указать уровни критичности для активов.

Уровень критичности актива представляет собой отметку о степени влияния отказа единицы оборудования на ход производственного процесса объекта мониторинга. По умолчанию при установке Kaspersky MLAD доступны следующие уровни критичности активов: **Очень низкий**, **Низкий**, **Средний**, **Высокий**, **Очень высокий**.

Уровень критичности актива автоматически присваивается инциденту в качестве приоритета, если в параметрах элемента ML-модели, зарегистрировавшего инцидент, не задан приоритет. Уровень критичности актива также отображается при просмотре технических характеристик инцидентов. При необходимости вы можете изменить названия уровней критичности и цвета, используемые для их отображения.

Работы по настройке уровней критичности активов могут выполнять системные администраторы и пользователи с правом **Настройка уровней критичности активов** из группы прав **Управление активами и тегами**.

Чтобы изменить уровни критичности активов:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **Активы**.

3. В блоке **Уровни критичности активов** выберите один или несколько уровней критичности активов и нажмите на кнопку **Изменить**.

4. Если требуется, измените названия уровней критичности и цвета, используемые для отображения уровней критичности в разделе **Инциденты**.

5. Нажмите на кнопку **Сохранить**.

Настройка отображения пунктов меню Kaspersky MLAD

Работы по настройке отображения пунктов меню Kaspersky MLAD могут выполнять системные администраторы.

Чтобы настроить отображение пунктов меню Kaspersky MLAD:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. На открывшейся странице в меню слева выберите раздел **Системные параметры** → **Меню**.

   Справа отобразится список параметров.

3. В блоке параметров **Доступность пунктов основного меню** с помощью переключателя включите или выключите отображение раздела в основном меню.

4. В блоке параметров **Доступность пунктов меню администратора** с помощью переключателя включите или выключите отображение раздела в меню администратора.

5. Нажмите на кнопку **Сохранить**.

Экспорт и импорт параметров Kaspersky MLAD

Kaspersky MLAD позволяет выполнять экспорт и импорт конфигурационных файлов, которые содержат параметры служб и коннекторов программы, а также параметры безопасности, уровней ведения журналов служб программы, параметры отображения меню программы, параметры приоритетов, типовых статусов и причин инцидентов и параметры уровней критичности активов, настраиваемые через веб-интерфейс. Это может сократить время настройки Kaspersky MLAD при повторном развертывании программы.

При экспорте параметров Kaspersky MLAD не сохраняет в архивный файл пароли, указанные в разделе **Системные параметры**, а также файлы сертификатов и ключей к файлам сертификатов, загруженных в этом разделе.

Экспорт и импорт файла конфигурации служб Kaspersky MLAD доступен системным администраторам.

Чтобы экспортировать файлы конфигурации из Kaspersky MLAD:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры**.

3. Нажмите на кнопку **Экспорт**, которая расположена в верхней части открывшейся страницы.

   Файлы конфигурации Kaspersky MLAD будут сохранены в виде архива mlad-settings.tar.gz на локальном компьютере.

Чтобы загрузить файлы конфигурации в Kaspersky MLAD:

1. В меню администратора выберите раздел **Системные параметры**.

2. Нажмите на кнопку **Импорт**, которая расположена в верхней части открывшейся страницы.

3. В открывшемся окне выберите архивный файл, содержащий необходимую конфигурацию параметров Kaspersky MLAD.

   Файлы конфигурации Kaspersky MLAD будут загружены в программу.

Управление активами и тегами

Управление активами и тегами доступно системным администраторам и пользователям с правами из группы прав **Управление активами и тегами**.

Активы и теги являются первичными элементами иерархической структуры объекта мониторинга. Иерархическая структура отображается в виде дерева активов.

В виде тегов в Kaspersky MLAD передаются показания датчиков, команды и состояния объекта мониторинга. На основании полученных значений тегов вы можете выполнять обучение и инференс ML-моделей.

В разделе **Активы** в меню администратора вы можете просматривать созданные или загруженные в Kaspersky MLAD активы и теги. Дерево активов отображается в левой части экрана. Активы в дереве активов отображаются со значком. С помощью кнопок › и ⌄ слева от имен активов вы можете отображать и скрывать состав активов. Если вы выбрали актив или тег для просмотра и затем свернули дерево, вы можете вновь развернуть структуру дерева до уровня выбранного элемента с помощью кнопки ⊗ слева от названия выбранного актива или тега.

Вы можете создавать активы и теги, а также изменять параметры тегов, например пороги блокировки тегов. Вы также можете добавить активы и теги объекта мониторинга путем их импорта из файла в формате XLSX. При необходимости вы можете удалить теги или активы целиком и экспортировать их в файл в формате XLSX.

Kaspersky MLAD получает данные телеметрии по тегам от устройств объекта мониторинга с помощью коннекторов и источников данных. Поступающие в программу значения для тегов, заданных в дереве активов, а также идентификаторы этих тегов хранятся в службе Time Series Database.

Если вы используете процессор событий и настроили монитор **Эксфильтрация данных по DNS**, то при активации этого монитора в иерархической структуре объекта мониторинга будет создан актив **DNS Exfiltration**. Программа автоматически наполняет этот актив тегами, содержащими информацию о DNS-запросах, которые привели к активации монитора.

Об иерархической структуре объекта мониторинга

Иерархическая структура объекта мониторинга (далее также *иерархическая структура*) – это способ представления объекта мониторинга в виде дерева активов, конечные узлы которого являются тегами, а промежуточные – активами.

Активы могут представлять различные элементы организационной структуры предприятия (цеха, производства, заводы) или технические системы (агрегаты, установки). Схема организации активов, их типы и число определяются Заказчиком и зависят от структуры конкретного объекта мониторинга. Каждый актив имеет только один вышестоящий элемент. Этим элементом может быть другой актив (родительский актив) или головной элемент иерархической структуры (*Root*), соответствующий объекту мониторинга в целом.

Теги и активы представляют собой первичные элементы иерархической структуры. Вы можете выполнить импорт и экспорт дерева активов в виде файла в формате XLSX, а также создавать активы и теги и управлять ими в разделе **Активы**.

Помимо первичных элементов в процессе или в результате работы Kaspersky MLAD в иерархическую структуру могут быть добавлены следующие функциональные элементы:

- Разметки;
- ML-модели;
- Шаблоны ML-моделей;
- Пресеты.

О тегах и способах получения наблюдений по тегам

Основными объектами наблюдения в Kaspersky MLAD являются теги. *Тег* – именованный параметр технологического процесса, например, измеряемый параметр (температура или давление) или состояние (включено, выключено или номер режима). В виде тегов могут передаваться измерения физических параметров, а также уставки, команды или состояния систем регулирования. Значения тегов передаются и принимаются устройствами по определенным протоколам. Значения тегов отображаются на графиках в разделах **История** и **Мониторинг**, а также используются для обнаружения инцидентов.

Kaspersky MLAD поддерживает несколько способов получения данных телеметрии (тегов). В зависимости от характеристик объекта мониторинга и возможностей передачи тегов вы можете выбрать один или несколько из следующих способов получения значений тегов в режиме реального времени:

- С помощью службы **Data Source Manager**, если на объекте мониторинга есть возможность передавать теги от АСУ ТП по протоколу OPC UA в онлайн-режиме.
- С помощью коннекторов Kaspersky Industrial CyberSecurity for Networks, который анализирует зеркалированный трафик и передает теги в Kaspersky MLAD в онлайн-режиме. Kaspersky MLAD передает обратно информацию об обнаруженных инцидентах.
- С помощью коннектора **MQTT Connector**, если на объекте мониторинга есть возможность передавать теги по протоколу MQTT и принимать сообщения о регистрации инцидентов в онлайн-режиме.
- С помощью коннектора **AMQP Connector**, если на объекте мониторинга есть возможность передавать теги по протоколу AMQP и принимать сообщения о регистрации инцидентов в онлайн-режиме.
- С помощью коннектора **WebSocket Connector**, если на объекте мониторинга есть возможность передавать теги по протоколу WebSocket и принимать сообщения о регистрации инцидентов в онлайн-режиме.
- С помощью коннектора **CEF Connector**, если на объекте мониторинга есть возможность передавать теги с помощью технологии CEF и принимать сообщения о регистрации инцидентов в онлайн-режиме.
- Если вышеперечисленные способы передачи тегов недоступны, с помощью коннектора **HTTP Connector** можно настроить периодическую выгрузку тегов в виде CSV-файлов по протоколу HTTP или HTTPS (например, один раз в час или один раз в минуту), написав скрипт выгрузки тегов.

Вы также можете загружать значения тегов из файлов формата CSV с помощью коннектора **HTTP Connector**.

Поиск и фильтрация объектов в разделе Активы

Поиск и фильтрация в разделе **Активы** доступны системным администраторам и пользователям с правом **Просмотр активов и тегов** из группы прав **Управление активами и тегами**.

В разделе **Активы** в дереве активов вы можете выполнять поиск и фильтрацию следующих объектов:

- активов;
- тегов.

Поиск выполняется по именам объектов.

Чтобы найти нужные объекты в дереве активов,

в разделе **Активы** введите поисковый запрос в поле **Поиск**. Поиск выполняется по мере ввода символов в строку поиска.

Если найдены объекты, удовлетворяющие поисковому запросу, в дереве активов отобразятся найденные объекты, а также разделы дерева активов, в составе которых были найдены эти объекты.

Если требуется сбросить поисковый запрос, нажмите на кнопку в строке поиска.

Вы также можете выполнять фильтрацию объектов в дереве активов. Фильтрация применяется к объектам, найденным в соответствии с поисковым запросом. Если поисковый запрос не задан, фильтрация применяется ко всем объектам в дереве активов.

Чтобы отфильтровать объекты в дереве активов:

1. В разделе **Активы** нажмите на кнопку , расположенную над деревом активов.

   Справа отобразятся параметры фильтрации.

2. В раскрывающемся списке **Тип раздела** выберите один или несколько типов разделов дерева активов.

   Вы можете выбрать следующие типы разделов: **Активы** и **Теги**.

3. Если требуется сбросить параметры фильтрации, выполните одно из следующих действий:

   - Для сброса конкретного параметра фильтрации нажмите на кнопку рядом с нужным параметром.
   - Для сброса всех параметров фильтрации нажмите на кнопку **Очистить фильтры** в правом верхнем углу страницы.

4. Если требуется скрыть отображение параметров фильтрации, нажмите на кнопку рядом с полем **Поиск**.

Фильтрация объектов выполняется по мере выбора параметров фильтрации. Если найдены объекты, удовлетворяющие параметрам фильтрации, в дереве отобразятся найденные объекты, а также разделы дерева активов, в составе которых были найдены эти объекты.

Если к дереву активов применены какие-либо параметры фильтрации, над деревом активов отображается кнопка .

Создание актива

Создание активов доступно системным администраторами пользователям с правом **Создание активов и тегов** из группы прав **Управление активами и тегами**.

В Kaspersky MLAD вы можете создавать активы и распределять теги по активам наиболее удобным для вас способом. Например, вы можете создавать активы в соответствии с производственной структурой объекта мониторинга вплоть до единиц оборудования, от которых поступают данные телеметрии.

Чтобы создать новый актив:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Активы** и нажмите на кнопку +.

3. В открывшейся панели в раскрывающемся списке **Тип элемента** выберите значение **Актив**.

4. В раскрывающемся списке **Актив** выберите раздел дерева активов, в составе которого требуется создать актив.

5. В поле **Имя** укажите имя актива.

   Имена активов должны быть уникальными в рамках одного раздела дерева активов.

   > При вводе имени актива не допускается перенос части имени на новую строку и использование обратной косой черты (\).

6. Если требуется, в поле **Описание** укажите описание актива.

7. Если требуется, в раскрывающемся списке **Уровень критичности** выберите уровень критичности.

8. В раскрывающемся списке **Тип актива** выберите тип актива.

   Если вы загрузили конфигурацию активов и тегов в Kaspersky MLAD вы можете выбрать один из типов активов, заданных в файле конфигурации. Типы активов указываются на вкладке **directory_types** конфигурационного файла. Если вы не загружали конфигурацию активов и тегов, выберите тип **Системный актив**.

9. Если вы выбрали один из типов активов, заданных в импортированном файле конфигурации, при необходимости укажите значения для специальных параметров активов.

   Имена специальных параметров указываются на вкладке **directory_types** конфигурационного файла.

10. Нажмите на кнопку **Сохранить**.

    Актив будет создан. Если требуется, вы можете изменить расположение актива в дереве.

Вы также можете создавать вложенные активы с помощью дерева активов. Для этого рядом с именем того раздела, в который требуется добавить актив, откройте вертикальное меню ... и выберите пункт **Добавить актив**.

Изменение параметров актива

> Изменение параметров актива доступно системным администраторам и пользователям с правом **Изменение активов и тегов** из группы прав **Управление активами и тегами**.

Вы можете изменять параметры созданных ранее активов.

Чтобы изменить параметры актива в дереве активов:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Активы**.

3. В дереве активов выберите актив, который требуется изменить.

   Справа отобразится список параметров с заданными значениями.

4. В правом верхнем углу страницы нажмите на кнопку **Изменить**.

5. Если требуется, измените следующие параметры:

   - Имя актива.
   - Раздел дерева активов, к которому вы хотите отнести актив.

     Подразделы актива и их теги будут перемещены в новый актив.
   - Уровень критичности.
   - Тип актива.
   - Описание актива.
   - Значения для специальных параметров актива.

6. Нажмите на кнопку **Сохранить**.

Актив будет изменен. Если требуется, вы можете изменить расположение актива в дереве.

Создание тега

Создание тегов доступно системным администраторами пользователям с правом **Создание активов и тегов** из группы прав **Управление активами и тегами**.

Чтобы создать новый тег:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Активы** и выполните одно из следующих действий:

   - Нажмите на кнопку +, в раскрывающемся списке **Тип элемента** выберите **Тег** и в раскрывающемся списке **Актив** выберите раздел дерева активов, к которому вы хотите отнести создаваемый тег.

     Активы в дереве активов требуется предварительно загрузить или создать вручную.
   - В дереве активов рядом с разделом, в который требуется добавить тег, откройте вертикальное меню ••• и выберите пункт **Добавить тег**.

3. В поле **Имя** укажите уникальное имя тега.

> При вводе имени тега не допускается перенос части имени на новую строку и использование обратной косой черты (\).

4. Если требуется, выполните следующие действия:

   a. В поле **Описание** укажите описание тега.

   b. В поле **Альтернативное имя** укажите альтернативное имя тега.

      Альтернативное имя может использоваться для подключения к источнику данных (например, к серверу OPC UA), если тег в источнике данных называется не так как в активах.

      > При вводе альтернативного имени тега не допускается перенос части имени на новую строку и использование обратной косой черты (\).

   c. В поле **ID** укажите уникальный числовой идентификатор тега.

      Рекомендуется заполнять это поле, только если у вас есть особая причина назначить тегу конкретный числовой идентификатор. В ином случае оставьте поле пустым и идентификатор будет назначен автоматически.

      Вы можете указать значение в диапазоне от 1 до 1 000 000.

   d. В поле **Единица измерения** укажите единицу измерения для тега (например, % или мПа).

   e. В блоке **Пороги блокировки** в полях **Нижний** и **Верхний** укажите нижний и верхний пороги предельно допустимых значений тега.

      Эти параметры требуются для работы детектора Limit Detector. В момент, когда значение тега достигает верхнего или нижнего порога блокировки, детектор Limit Detector регистрирует инцидент.

      Если включена функция **Всегда показывать пороги блокировки**, вертикальный масштаб графика будет зафиксирован пороговыми линиями, выводимыми по нижней и верхней границам графической области, к которой относится тег, при условии, что значения тега находятся в заданном диапазоне. Если значения тега выйдут за заданные пороги, то вертикальный масштаб будет автоматически изменен для отображения запредельных значений тега.

   f. В блоке **Пороги сигнализации** в полях **Нижний** и **Верхний** укажите нижний и верхний пороги значений тега, при достижении которых оператору следует обратить внимание на поведение тегов.

   g. В блоке **Пороги достоверности измерений** в полях **Нижний** и **Верхний** укажите нижний и верхний пороги физически возможных значений тега, в том числе с учетом ограничений измерительного оборудования.

   h. В блоке параметров **Конвертация значений** в полях **Смещение** и **Множитель** укажите значение, которое необходимо добавить к значению тега, и значение, на которое необходимо умножить значение тега, полученное с помощью коннекторов или источников данных.

      Программа конвертирует значения тега по формуле `a * x + b`, где:

      - `a` – значение множителя, заданного в поле **Множитель**;
      - `x` – полученное значение тега;
      - `b` – значение смещения, заданного в поле **Смещение**.

      Конвертация производится при включенном переключателе **Масштабировать полученные значения тегов** в параметрах коннекторов и источников данных. Конвертация значений возможна для тегов, полученных с помощью коннекторов MQTT Connector, AMQP Connector, WebSocket Connector и KICS Connector, а также с помощью источников данных OPC UA.

Конвертацию значений необходимо применять при получении значений тега в единице измерения, отличной от указанной в поле **Единица измерения**.

i. Если значения тега поступают в программу с помощью коннектора KICS Connector, в поле **Устройство внешней системы** укажите имя устройства, созданного во внешней системе, для которого требуется получать теги.

j. В полях **X**, **Y**, **Z** укажите координаты расположения датчика объекта мониторинга в пространстве.

Вы можете использовать произвольную точку в качестве начала координат.

Вы можете использовать координаты датчиков для расчета значения тегов при создании пресета и их отображения на графике в разделе **Временной срез**.

k. В поле **Комментарий** введите краткий комментарий к тегу.

5. Нажмите на кнопку **Сохранить**.

Новый тег отобразится в группе **Теги** дерева активов. Группа **Теги** создается автоматически и отображается в составе выбранного раздела дерева активов. Если требуется, вы можете изменить расположение тегов в дереве.

Изменение тега

Изменение тегов доступно системным администраторам и пользователям с правом **Изменение активов и тегов** из группы прав **Управление активами и тегами**.

Вы можете изменять созданные ранее теги.

Чтобы изменить тег:

1. В нижнем левом углу страницы нажмите на кнопку ⚙.

   Вы перейдете в меню администратора.

2. Выберите раздел **Активы**.

3. В дереве активов выберите тег, который требуется изменить.

   Вы можете отображать или скрывать данные дерева активов с помощью кнопок › и ⌄ слева от имен активов.

   Справа отобразится список параметров с заданными значениями. В правом верхнем углу страницы над параметрами тега отобразится количество ML-моделей, которые используют выбранный тег.

4. В правом верхнем углу страницы нажмите на кнопку **Изменить**.

5. Если требуется, измените параметры тега. Описание параметров см. в инструкции по созданию тега.

   При использовании коннектора KICS Connector Kaspersky MLAD периодически проверяет сведения о тегах, полученных от Kaspersky Industrial CyberSecurity for Networks. Если имя тега и/или информация об устройстве тега были изменены вручную, программа автоматически обновит имя тега и/или сведения об устройстве в соответствии с именем тега и именем устройства в Kaspersky Industrial CyberSecurity for Networks после следующей проверки.

6. Нажмите на кнопку **Сохранить**.

Если требуется, вы можете изменить расположение тегов в дереве.

Вы также можете перейти к изменению тега, нажав на вертикальное меню ••• рядом с нужным тегом и выбрав пункт **Изменить тег**.

Перемещение активов и тегов

Перемещение активов и тегов доступно системным администраторам и пользователям с правом **Изменение активов и тегов** из группы прав **Управление активами и тегами**.

Вы можете перемещать активы и/или теги в дереве активов. Все активы и теги, входящие в состав выбранного актива, будут перемещены.

Чтобы переместить актив и/или тег:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Активы**.

3. В дереве активов установите флажки рядом с именами активов и/или тегов, которые требуется переместить.

4. Над деревом активов нажмите на кнопку .

5. В открывшейся панели в раскрывающемся списке **Актив** выберите актив, в который вы хотите перенести выбранные активы и/или теги.

6. Нажмите на кнопку **Сохранить**.

В разделе **Активы** отобразится измененное дерево активов.

Удаление актива или тега

Удаление доступно системным администраторам и пользователям с правом **Удаление активов и тегов** из группы прав **Управление активами и тегами**.

Вы можете удалить теги, если они не используются в ML-моделях или разметках. Вы можете удалить активы, в которых нет ML-моделей, разметок или тегов, используемых в ML-моделях.

Удаление тега в программе не приводит к удалению тега на объекте мониторинга.

Перед удалением тега необходимо удалить его из файла конфигурации коннектора или источника данных, через который поступали данные по этому тегу.

Чтобы удалить тег:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Активы**.

3. Выполните одно из следующих действий:

   - В дереве активов выберите нужный тег и нажмите на кнопку **Удалить** в правом верхнем углу страницы.
   - В вертикальном меню **...** справа от нужного тега выберите пункт **Удалить тег**.

4. В открывшемся окне подтвердите удаление тега.

Чтобы удалить актив:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Активы**.

3. Выполните одно из следующих действий:

   - В дереве активов выберите нужный актив и нажмите на кнопку **Удалить** в правом верхнем углу страницы.
   - В вертикальном меню **...** справа от нужного актива выберите пункт **Удалить актив**.

4. В открывшемся окне подтвердите удаление актива.

Чтобы удалить один или несколько активов и/или тегов:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Активы**.

3. В дереве активов установите флажки рядом с именами активов и/или тегов.

   Если требуется удалить один или несколько тегов из актива, разверните соответствующий раздел дерева активов, нажав на кнопку › , и выберите нужные теги.

4. Нажмите на кнопку , расположенную над деревом активов.

5. В открывшемся окне подтвердите удаление активов и/или тегов.

Если выбранные теги не используются ML-моделями и разметками и/или в выбранных активах нет ML-моделей, разметок или тегов, используемых в ML-моделях, в открывшемся окне отображается значок . Выбранные активы и/или теги будут удалены из Kaspersky MLAD безвозвратно.

Если выбранные теги используются ML-моделями и разметками и/или в выбранных активах есть ML-модели, разметки или теги, используемые в ML-моделях, в открывшемся окне отображается значок . В таком случае вы не можете удалить выбранные активы и/или теги. Для удаления тегов требуется предварительно убрать их из разметок, входных и/или выходных тегов элементов ML-модели, созданной вручную, или удалить элементы ML-моделей, в которых они используются. Для удаления активов требуется предварительно удалить ML-модели, которые относятся к нужным активам.

Проверка текущей структуры тегов

Проверка структуры тегов доступна системным администраторам и пользователям с правом **Просмотр активов и тегов** из группы прав **Управление активами и тегами**.

Kaspersky MLAD получает данные телеметрии от устройств объекта мониторинга с помощью коннекторов и источников данных и сохраняет идентификаторы тегов и значения по тегам, заданным в дереве активов, в службе Time Series Database. При включенной функции сохранения значений всех тегов в службе Time Series Database также хранятся идентификаторы и значения неизвестных тегов (отсутствующих в дереве активов).

Kaspersky MLAD позволяет сравнить текущую структуру тегов, которая отображается в дереве активов и используется для объекта мониторинга, со структурой тегов, сохраненной для этого объекта мониторинга в службе Time Series Database. Kaspersky MLAD выявляет теги, которые были получены от внешних устройств, но отсутствуют в текущей структуре тегов и не используются для объекта мониторинга. Если требуется, вы можете добавить эти теги в текущую структуру тегов.

Если Kaspersky MLAD обнаруживает неизвестные теги, полученные от внешних устройств через коннектор KICS Connector, эти теги будут автоматически созданы в разделе **kics** дерева активов. Программа автоматически присвоит тегам идентификаторы и заполнит следующие сведения, полученные от Kaspersky Industrial CyberSecurity for Networks:

- идентификаторы тегов;
- имена тегов;
- описания тегов;
- единицы измерения тегов;
- имена устройств, для которых получены теги.

Kaspersky MLAD совместим с Kaspersky Industrial CyberSecurity for Networks версии 4.0 и выше.

Чтобы сравнить текущую структуру тегов со структурой в службе Time Series Database:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Активы** и нажмите на кнопку .

   Текущая структура тегов, используемая для объекта мониторинга, сравнивается со структурой тегов, которая хранится в службе Time Series Database. Сообщение о результате выполненного сравнения отобразится в верхней части страницы.

   В случае выявления отсутствующих тегов Kaspersky MLAD отобразит список этих тегов с именами в формате **Tag <идентификатор тега>**.

3. Если требуется добавить отсутствующие теги, выполните следующие действия:

   a. В поле **Актив** для каждого обнаруженного тега выберите актив, к которому вы хотите отнести тег.

   b. Нажмите на кнопку **Добавить**.

   Kaspersky MLAD добавит теги в дерево активов. Для этих тегов будут указаны только их идентификаторы, имена в формате **Tag <идентификатор тега>** и активы, к которым вы отнесли теги. Если требуется, вы можете изменить добавленные теги.

Загрузка конфигурации активов и тегов в систему

Конфигурация активов и тегов создается в процессе выполнения работ по внедрению Kaspersky MLAD и построению ML-модели. Конфигурация активов и тегов предоставляется в виде файла в формате XLSX.

Загрузка конфигурации активов и тегов доступна системным администраторам и пользователям с правом **Импорт активов и тегов** из группы прав **Управление активами и тегами**.

Чтобы загрузить конфигурацию активов и тегов в Kaspersky MLAD:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Активы** и нажмите на кнопку .

   Справа откроется панель **Импорт иерархической структуры**.

3. В поле **Импорт файла** добавьте файл в формате XLSX, содержащий необходимую конфигурацию активов и тегов иерархической структуры.

   Если требуется выбрать другой файл конфигурации активов и тегов, нажмите на кнопку и выберите новый файл.

4. В раскрывающемся списке **Актив** выберите раздел дерева активов, в который требуется загрузить конфигурацию активов и тегов из файла.

   Если загружаемый файл конфигурации содержит активы самого верхнего уровня, то выберите головной элемент иерархической структуры **Root**.

5. В раскрывающемся списке **Режим импорта** выберите одно из следующих значений:

   - **Добавить и обновить**. Kaspersky MLAD добавит новые активы и теги из файла конфигурации и обновит информацию о ранее созданных и/или импортированных активах и тегах в составе выбранного раздела.

   - **Только обновить**. Kaspersky MLAD обновит информацию о ранее созданных и/или импортированных активах и тегах в составе выбранного раздела.

     Если в файле конфигурации описаны новые активы и/или теги, они не будут добавлены в иерархическую структуру.

   - **Перезаписать**. Kaspersky MLAD удалит ранее созданные и/или импортированные активы и теги из выбранного раздела и создаст новые активы и теги из файла конфигурации.

6. Если требуется рассматривать все активы и теги из файла конфигурации в качестве новых вхождений, включите переключатель **Рассматривать все элементы как новые**.

   Вы можете использовать этот переключатель для загрузки вложенных активов, повторяющихся в разных разделах дерева активов. Для этого загрузите конфигурацию вложенных активов в режиме импорта **Добавить и обновить** несколько раз и при каждой загрузке укажите разные родительские активы. При этом загрузить теги с именами, совпадающими с именами ранее созданных и/или загруженных тегов, невозможно.

7. Если требуется учитывать регистр в основных и альтернативных именах тегов из файла конфигурации, установите переключатель **Проверка уникальности имен тегов** в положение **Учитывать регистр**.

   По умолчанию регистр в именах тегов не учитывается.

8. Для интерпретации числовых значений в файле конфигурации в параметре **Типы разделителей** выберите один из следующих вариантов:

   - **Разделитель разрядов - пробел, разделитель дробной части - запятая**, если в числовых значениях разряды разделены пробелами, а дробные части отделены запятыми от целых частей.

   - **Разделитель разрядов - запятая, разделитель дробной части - точка**, если в числовых значениях разряды разделены запятыми, а дробные части отделены точками от целых частей.

   В поле **Образец** отображается формат, по которому программа считывает числовые значения из файла конфигурации в соответствии с выбранным вариантом.

9. Нажмите на кнопку **Сохранить**.

Конфигурация активов и тегов будет загружена в Kaspersky MLAD. Активы и теги отобразятся в виде дерева активов.

Сохранение конфигурации активов и тегов в файл

Сохранение конфигурации активов и тегов доступно системным администраторам и пользователям с правом **Экспорт активов и тегов** из группы прав **Управление активами и тегами**.

Вы можете сохранить структуру тегов и активов в файл в формате XLSX для дальнейшего использования. Например, в сохраненном файле вы можете изменить параметры текущих активов и/или тегов или добавить в иерархическую структуру новые активы и/или теги, после чего загрузить обновленный файл конфигурации в программу повторно.

Чтобы сохранить конфигурацию активов и тегов в файл в формате XLSX:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Активы** и нажмите на кнопку .

Конфигурация активов и тегов будет сохранена в файл mlad_structure.xlsx (см. пример в Приложении).

Работа с основным меню

Этот раздел содержит описание пользовательских задач, выполняемых в основном меню программы.

Доступ к функциям программы в основном меню зависит от роли, назначенной учетной записи пользователя. Пользователям с ролью системного администратора доступны все функции программы.

Сценарий: работа с Kaspersky MLAD

В этом разделе описаны действия пользователя при работе в основном меню Kaspersky MLAD.

Сценарий работы с программой состоит из следующих этапов:

1. **Создание пресетов для мониторинга участков защищаемого объекта**

   Для быстрого доступа к необходимым данным загрузите конфигурацию пресетов в Kaspersky MLAD. Конфигурация пресетов создается специалистом "Лаборатории Касперского" или сертифицированным интегратором. Конфигурация пресетов описывается в файле в формате JSON. Пример описания конфигурации пресетов см. в Приложении.

   Вы также можете создать пресеты, которые включают в себя теги, соответствующие агрегатам установки, в веб-интерфейсе программы. Если требуется, вы можете изменить уже существующие пресеты.

2. **Подготовка ML-моделей**

   Для анализа телеметрии объекта мониторинга и выявления аномалий необходимо подготовить ML-модели. Добавьте в Kaspersky MLAD ML-модели и разметки. Обучите элементы ML-модели и проверьте результаты обучения. При необходимости скорректируйте параметры обучения и обучите нужные элементы заново. Запустите инференс ML-модели для регистрации инцидентов. При необходимости опубликуйте ML-модель для регистрации учетных инцидентов.

3. **Просмотр исторических данных**

   Перейдите в раздел **История**. Выберите элемент ML-модели и пресет и укажите дату и интервал времени для просмотра исторических данных технологических параметров и результатов их обработки ML-моделями – сформированных артефактов и/или зарегистрированных инцидентов. При просмотре исторических данных вы можете использовать навигацию.

4. **Мониторинг в онлайн-режиме**

   Для просмотра поступающих значений технологических параметров и результатов их обработки ML-моделями в онлайн-режиме, перейдите в раздел **Мониторинг**. Выберите элемент ML-модели и пресет и интервал времени для отображения поступающих данных.

5. **Просмотр данных в разделе Временной срез**

   Для просмотра значений технологических параметров, полученных от датчиков объекта мониторинга в один и тот же момент времени, перейдите в раздел **Временной срез**. Выберите элемент ML-модели и пресет и укажите дату и интервал времени для просмотра данных. При просмотре данных вы можете использовать навигацию.

6. **Работа с инцидентами**

   Перейдите в раздел **Инциденты** и просмотрите информацию о зарегистрированных инцидентах. Проанализируйте инциденты и добавьте экспертные рекомендации или комментарии, в которых вы можете указать, являются ли зарегистрированные инциденты аномалиями.

Если вы подписаны на уведомления об инцидентах, при возникновении аномальной ситуации вы получите сообщение по электронной почте. В сообщении указываются дата и время начала инцидента, а также ссылка, по которой вы можете перейти в раздел **История**.

7. **Работа с событиями и паттернами**

   Для работы с событиями и паттернами настройте параметры конфигурации внимания и отображение параметров событий. Для отслеживания определенных событий, паттернов или значений параметров событий перейдите в раздел **Процессор событий** и создайте мониторы. Просмотрите события и паттерны, выявленные процессором событий.

Просмотр сводных данных в разделе Информационная панель

В разделе **Информационная панель** представлена сводная информация о количестве событий и наблюдений по тегам, поступающих в Kaspersky MLAD, зарегистрированных инцидентах и о статусе служб.

Информация на странице разбита на следующие блоки:

- **Поступающие данные** – график, на котором отображается количество поступающих в Kaspersky MLAD событий и наблюдений по тегам. Вы можете включить или выключить отображение на графике поступающих событий и наблюдений по тегам, нажав на соответствующую легенду подписи данных, которая расположена под графиком. Левая шкала графика отображает диапазон количества наблюдений по тегам, поступающих в секунду. Правая шкала графика отображает диапазон количества событий, поступающих в секунду.

- **Последние инциденты** – таблица, содержащая **информацию о последних зарегистрированных**

инцидентах.

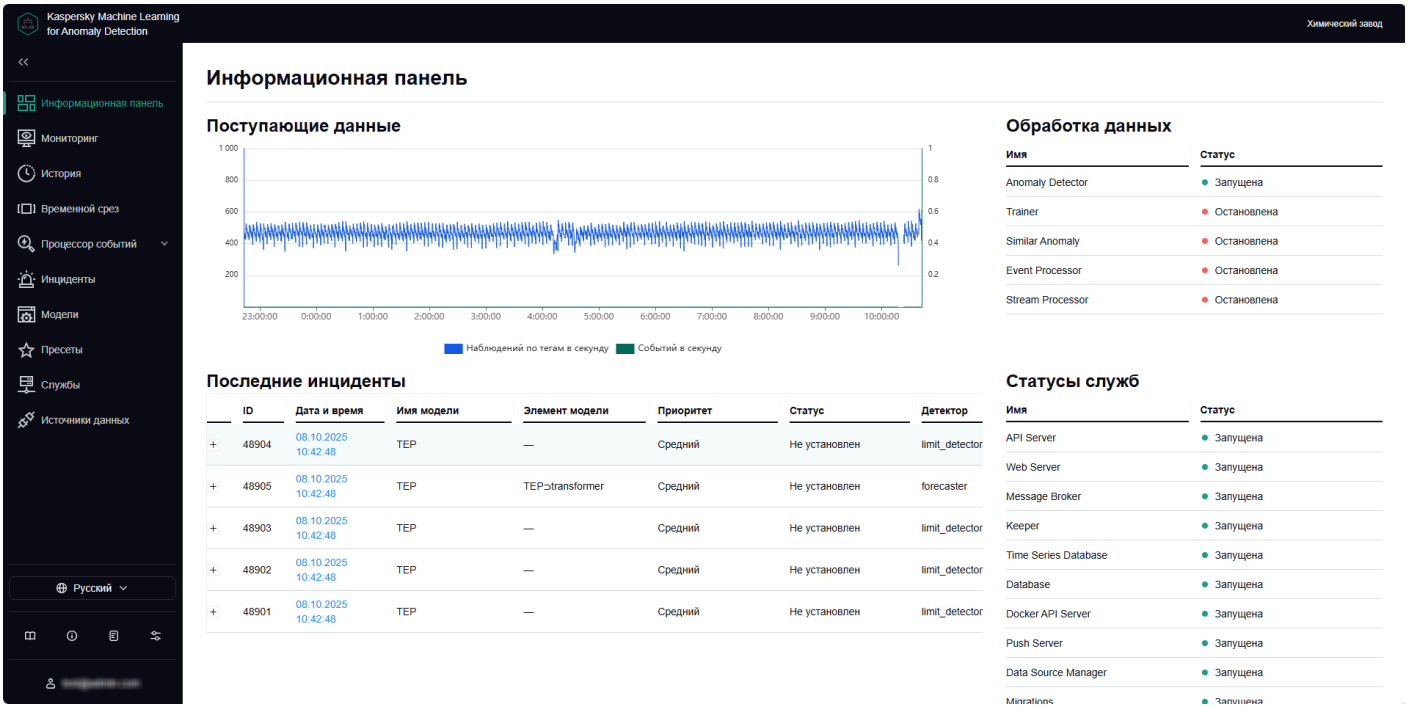
- **ID** – идентификатор зарегистрированного инцидента.
- **Дата и время** – дата и время начала инцидента по часам объекта мониторинга, отображенное в часовом поясе компьютера.
- **Имя модели** – имя ML-модели, элемент которой зарегистрировал инцидент.
- **Элемент модели** – имя элемента ML-модели, который зарегистрировал инцидент. Имена элементов отображаются в формате `<имя ML-модели> ⊃ <имя элемента>`.
- **Приоритет** – приоритет зарегистрированного инцидента.
- **Статус** – статус зарегистрированного инцидента, указанный экспертом по результатам анализа инцидента или присвоенный автоматически в соответствии со статусом инцидента, заданным для элемента ML-модели, зарегистрировавшего инцидент.
- **Детектор** – тип зарегистрированного инцидента.

При нажатии на кнопку + около инцидента в таблице инцидентов раскрывается окно с техническими характеристиками выбранного инцидента:

- **Инцидент** – блок, содержащий информацию об инциденте:
  - **Уровень критичности** – степень влияния отказа единицы оборудования, для которого зарегистрирован инцидент, на ход производственного процесса объекта мониторинга.
  - **Имя актива** – имя актива, содержащего тег или элемент ML-модели, для которых зарегистрирован инцидент.
  - **Имя модели** – имя ML-модели, элемент которой зарегистрировал инцидент.
  - **Элемент модели** – имя элемента ML-модели, который зарегистрировал инцидент.
  - **Детектор** – тип зарегистрированного инцидента.
  - **Значение артефакта элемента ML-модели** – значение отклонения поведения объекта мониторинга от нормального на момент регистрации инцидента. Отсутствует, если инцидент зарегистрирован детектором Limit Detector или службой Stream Processor.
  - **Пороговое значение** – пороговое значение для регистрации инцидента элементом ML-модели. Если инцидент зарегистрирован детектором Limit Detector, для этого параметра указывается значение верхнего или нижнего порога блокировки, которое было достигнуто тегом.
- **Топ-тег** – блок, содержащий информацию о теге, который оказал наибольшее влияние на регистрацию инцидента, если такой тег известен:
  - **Имя топ-тега (ID топ-тега)** – имя и идентификатор тега, оказавшего наибольшее влияние на регистрацию инцидента.
  - **Значение топ-тега** – зарегистрированное в момент инцидента значение топ-тега.
  - **Пороги блокировки** – предельно допустимые значения топ-тега. Пределы блокировки требуются для правильной работы детектора Limit Detector. В момент, когда значение тега достигает верхнего или нижнего порога блокировки, детектор Limit Detector регистрирует инцидент.
  - **Описание** – описание топ-тега.
  - **Единица измерения** – единица измерения значений топ-тега.

- **Обработка данных** – таблица, в которой отображается статусы служб, используемых для обработки событий и наблюдений по тегам, поступающим в Kaspersky MLAD, обучения и инференса ML-моделей, а также регистрации инцидентов.
- **Статусы служб** – таблица, в которой для каждой службы отображается ее статус.

Из раздела **Информационная панель** вы можете перейти в раздел **История**, нажав на дату и время начала инцидента в таблице **Последние инциденты**. В разделе **История** отображается подробная информация о зарегистрированных Kaspersky MLAD инцидентах.



Раздел **Информационная панель**

Просмотр поступающих данных в разделе Мониторинг

В разделе **Мониторинг** вы можете просматривать поступающие в реальном времени значения тегов, входящих в пресет и их прогнозируемые значения.

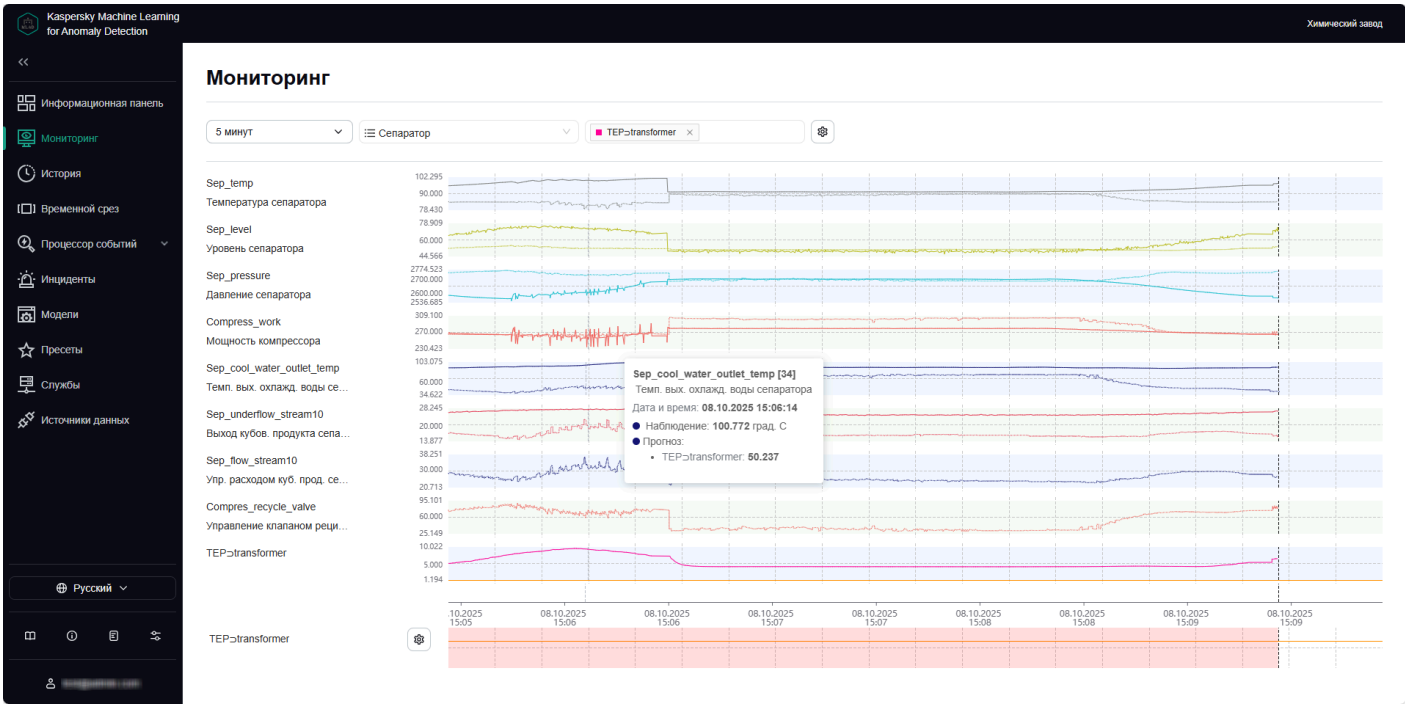
Центральная часть раздела **Мониторинг** представляет собой совокупность горизонтальных сегментов, предназначенных для отображения графиков. Каждый такой сегмент называется *графической областью*. Первыми отображаются графические области для выбранного пресета. В одной графической области пресета может отображаться график одного тега или графики нескольких тегов, наложенные друг на друга. Состав тегов, данные которых отображаются в графической области, вы можете определить при создании пресета. На графиках отображаются значения тегов пресета, поступающих в Kaspersky MLAD от объекта мониторинга. При выборе элементов ML-моделей на графиках единичных графических областей вы можете дополнительно к графикам тегов отобразить связанные с этими тегами артефакты выбранных элементов ML-моделей.

Если при настройке отображения графиков для высоты графиков было выбрано значение 190 px или более, то слева от каждой графической области появится ползунок, с помощью которого вы можете изменять масштаб отображения графиков. Для этого с помощью ползунка измените диапазон значений, который требуется отображать в графической области. Выбранный диапазон применяется к графической области независимо от диапазонов для других графических областей пресета. Для просмотра частей графической области, которые выходят в за пределы выбранного диапазона, зажмите ползунок и перетащите его вверх или вниз.

После графических областей пресета отображаются графические области для каждого выбранного элемента ML-модели. В таких графических областях отображаются графики артефактов элементов ML-моделей. Значение артефакта элемента ML-модели зависит от аналитических алгоритмов, используемых элементом, и отображается в виде цветной линии. Цвет этой линии соответствует цвету, выбранному для параметра **Цвет точек-индикаторов инцидентов** при создании соответствующего элемента. На графиках также отображается оранжевая линия, которая соответствует порогу, при превышении которого элемент ML-модели регистрирует инцидент.

В нижней части раздела расположена дополнительная графическая область, содержащая график артефакта элемента ML-модели, выбранного в панели **Параметры отображения графика артефакта элемента ML-модели**. Красная линия на графике соответствует значению артефакта элемента ML-модели, а оранжевая линия соответствует порогу, при превышении которого Kaspersky MLAD регистрирует инцидент. Область графика, в которой значение артефакта элемента ML-модели превышает заданный порог, окрашивается в красный цвет. В нижней части окна отображаются цветные точки-индикаторы, соответствующие зарегистрированным инцидентам.

В зависимости от выбранного масштаба времени и плотности инцидентов одна точка-индикатор может соответствовать одному или нескольким близко расположенным инцидентам, зарегистрированных одним или несколькими элементами ML-моделей. В этом случае при наведении курсора на точку-индикатор отображаются границы интервала времени, которому соответствует точка-индикатор. Инциденты находятся внутри указанного интервала. Для точек-индикаторов, которые соответствуют инцидентам, зарегистрированным одним элементом ML-модели, цвет задается при создании этого элемента. Для точек-индикаторов, которые соответствуют группе инцидентов, зарегистрированных разными элементами, зарезервирован фиолетовый цвет. Для точек-индикаторов, которые соответствуют инцидентам, зарегистрированным детектором Limit Detector, зарезервирован красный цвет.



Раздел **Мониторинг**

Выбор элементов ML-моделей в разделе Мониторинг

В разделе **Мониторинг** вы можете просматривать поступающие в реальном времени значения тегов, входящих в пресет, артефакты, сформированные выбранными элементами ML-моделей, а также информацию о количестве зарегистрированных инцидентов.

Если для объекта мониторинга используются разные ML-модели для обработки данных, Kaspersky MLAD позволяет выбрать несколько элементов ML-моделей для отображения результатов их инференса. Для детектора Limit Detector элемент ML-модели не создается. Точки-индикаторы инцидентов, зарегистрированных с помощью этого детектора, отображаются, если включено использование детектора Limit Detector и включен режим отображения индикаторов для всех инцидентов.

Функциональность доступна после добавления лицензионного ключа.

Чтобы просмотреть результаты инференса элементов ML-модели:

1. В основном меню выберите раздел **Мониторинг**.

2. На открывшейся странице в раскрывающемся списке **Элемент модели** выберите один или несколько элементов ML-модели.

   Имена элементов отображаются в формате `< имя ML-модели > ⊃ < имя элемента >`.

   Программа автоматически сформирует динамический пресет для выбранного элемента ML-модели. Если выбрано более одного элемента, Kaspersky MLAD сформирует динамические пресеты для каждого выбранного элемента

   При выборе пресета на графических областях отобразятся значения тегов, поступающих в Kaspersky MLAD за выбранный интервал времени. Если вы настроили отображение графиков, то на графиках единичных графических областей также отобразятся артефакты, связанные с тегами таких областей и сформированные элементами ML-моделей, в составе которых используются эти теги.

   Ниже графиков тегов выбранного пресета отобразятся графики артефактов выбранных элементов ML-моделей. Значения, отображаемые на графиках, зависят от аналитических алгоритмов, используемых элементами для выявления аномалий.

   Если требуется скрыть отображение артефактов какого-либо выбранного ранее элемента ML-модели, нажмите на значок ✕ рядом с этим элементом.

3. Если требуется отображать график артефакта одного из уже выбранных элементов дополнительно в нижней фиксированной графической области, выполните следующие действия:

   a. Нажмите на кнопку ⚙ под графиками тегов в левой части страницы.

      Справа отобразится панель **Параметры отображения графика артефакта элемента ML-модели**.

   b. В раскрывающемся списке **Элемент модели** выберите элемент ML-модели. Вы можете выбрать только один элемент ML-модели из списка.

   c. Нажмите на кнопку **Закрыть**.

   На графике артефакта элемента ML-модели отобразится значение артефакта этого элемента в виде красной линии. Область графика, в которой значение артефакта превышает заданный порог (оранжевая линия), окрашивается в красный цвет.

В нижней части графика отобразятся точки-индикаторы инцидентов, зарегистрированных выбранными элементами ML-модели. Если включен режим отображения индикаторов для всех инцидентов, то отобразятся точки-индикаторы инцидентов, зарегистрированных всеми ML-моделями, а также детектором Limit Detector.

Просмотр данных для определенного пресета в разделе Мониторинг

Если был выбран элемент ML-модели, то программа автоматически сформирует динамический пресет по этому элементу, который вы можете выбрать для отображения графиков тегов, участвующих в элементе. Сформированные динамические пресеты отображаются в группе **Динамические пресеты** дерева активов в раскрывающемся списке **Пресет**. На графических областях отобразятся поступающие данные по тегам сформированного динамического пресета.

При необходимости вы можете выбрать любой другой пресет для просмотра поступающих данных.

Чтобы просмотреть поступающие данные для определенного пресета в режиме реального времени:

1. В основном меню выберите раздел **Мониторинг**.
2. На открывшейся странице в раскрывающемся списке **Пресет** выберите необходимый пресет.

   На странице отобразятся графики для тегов, которые входят в выбранный пресет, в соответствии с параметрами графической области, заданными при создании этого пресета.

   Теги динамических пресетов отображаются только в единичных графических областях. Настройка отображения динамических пресетов невозможна.

Если требуется, вы можете изменить временной интервал отображения данных или настроить отображение графиков. Также вы можете изменить состав отображаемых тегов, изменив пресет.

Выбор интервала времени в разделе Мониторинг

Kaspersky MLAD позволяет выбирать временной интервал (масштаб) отображения поступающих данных.

Чтобы выбрать временной интервал:

1. В основном меню выберите раздел **Мониторинг**.
2. На открывшейся странице в раскрывающемся списке выберите нужный интервал времени. По умолчанию для выбора доступны следующие значения:

   - 1, 5, 10, 15 и 30 минут;
   - 1, 3, 6 и 12 часов;
   - 1, 2, 15 и 30 дней;
   - 3 и 6 месяцев;
   - 1, 2 и 3 года.

   Если требуется, системный администратор может создать, изменить или удалить временные интервалы.

На графиках выбранного пресета отобразятся значения тегов и результаты инференса выбранных элементов ML-моделей за выбранный интервал времени.

Настройка параметров отображения графиков в разделе Мониторинг

Kaspersky MLAD позволяет настроить параметры отображения графических областей пресетов в разделе **Мониторинг**.

Чтобы настроить параметры отображения графических областей пресетов:

1. В основном меню выберите раздел **Мониторинг**.
2. На открывшейся странице нажмите на кнопку  в верхней части экрана.

   Справа отобразится панель **Параметры отображения графиков**.
3. В раскрывающемся списке **Высота графиков** выберите одно из следующих значений: 55 px, 110 px, 145 px, 190 px, 390 px, 570 px.

   По умолчанию параметр **Высота графиков** имеет значение 55 px. При значении 190 px и более слева от графических областей появятся ползунки, с помощью которых вы можете изменять масштаб отображения графиков.
4. В раскрывающемся списке **Для перехода в раздел История использовать** выберите пресет, графики которого по умолчанию будут отображаться при переходе в раздел **История**.
5. Если требуется, включите переключатель **Отображать графики наблюдений в выбранном цвете** и в поле **Цвет графиков наблюдений** выберите цвет.
6. Если требуется, включите переключатель **Отображать графики прогнозов в выбранном цвете** и в поле **Цвет графиков прогнозов** выберите цвет.
7. С помощью переключателя **Имя и описание тега** включите или выключите отображение имен и описаний тегов слева от графиков.
8. С помощью переключателя **Прогнозируемое значение тега** включите или выключите отображение прогнозируемых значений выходных тегов предиктивных элементов, если соответствующие элементы выбраны для отображения.

   Эллиптические конверты и диагностические правила не формируют прогноза значений тегов.
9. С помощью переключателя **Индивидуальная ошибка тега** включите или выключите отображение индивидуальных ошибок прогноза значений выходных тегов предиктивных элементов, если соответствующие элементы выбраны для отображения.
10. С помощью переключателя **Отображать индикаторы для всех инцидентов** включите или выключите отображение точек-индикаторов инцидентов, зарегистрированных всеми ML-моделями, а не только выбранными для отображения, а также детектором Limit Detector.

    Если этот переключатель выключен, то будут отображаться только точки-индикаторы для инцидентов, которые были зарегистрированы выбранными элементами ML-модели.

11. Если требуется отображать установленные технические пределы для тегов на графиках, выполните следующие действия:

    a. Включите переключатель **Пороги блокировки**.

    b. Если требуется всегда отображать установленные технические пределы, включите переключатель **Всегда показывать пороги блокировки**.

    Если этот переключатель выключен, то технические пределы будут отображаться, только если значение какого-либо тега приблизилось к соответствующему пределу в отображаемой на экране области графика.

12. Если требуется отображать контрольные линии для графических областей, включите переключатель **Контрольные линии**.

13. Нажмите на кнопку **Закрыть** для возвращения к просмотру графиков в разделе **Мониторинг**.

    Заданные параметры отображения графических областей пресетов в разделе **Мониторинг** будут применены.

Просмотр данных в разделе История

В разделе **История** доступна история поступивших данных, результат их обработки Kaspersky MLAD с формированием артефактов ML-модели и информацией о зарегистрированных инцидентах.

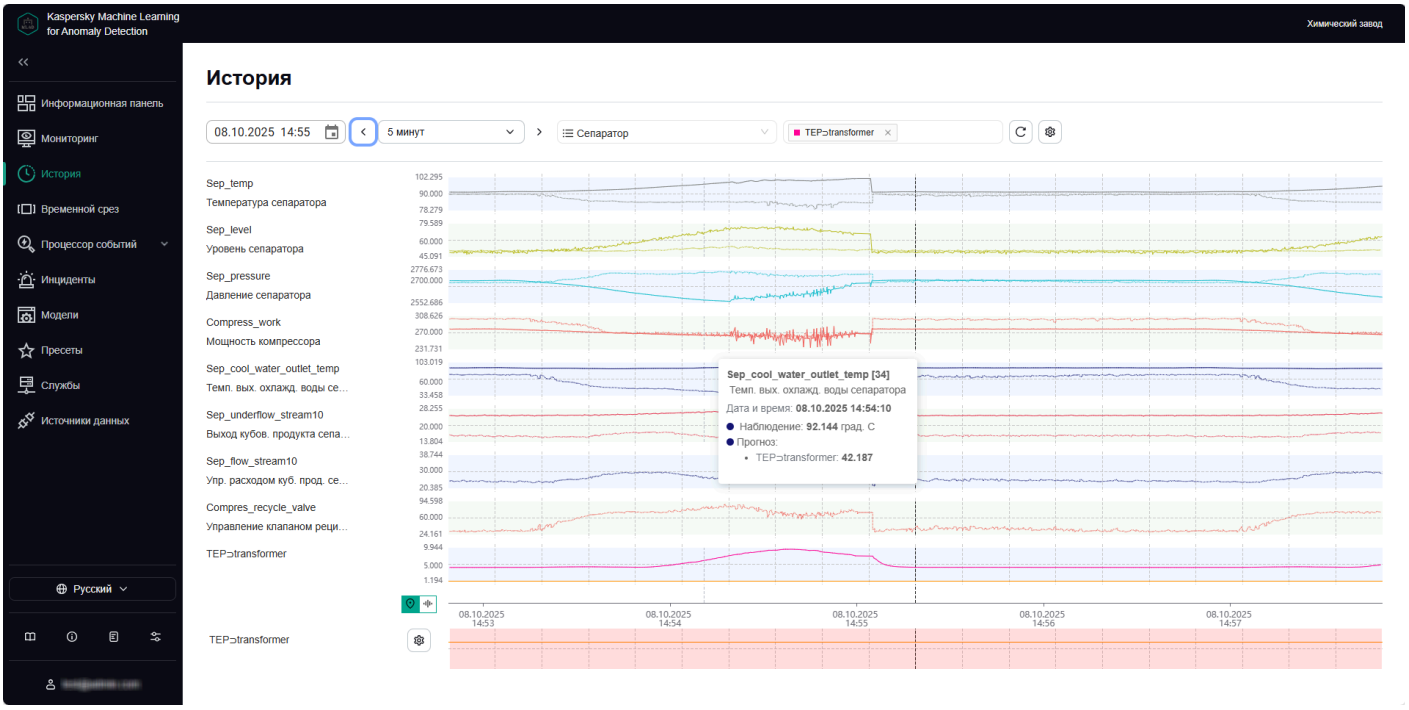
Центральная часть раздела **История** представляет собой совокупность горизонтальных сегментов, предназначенных для отображения графиков. Каждый такой сегмент называется *графической областью*. Первыми отображаются графические области для выбранного пресета. В одной графической области пресета может отображаться график одного тега или графики нескольких тегов, наложенные друг на друга. Состав тегов, данные которых отображаются в графической области, вы можете определить при создании пресета. На графиках отображаются значения тегов пресета, поступивших в Kaspersky MLAD от объекта мониторинга за выбранный интервал времени. При выборе элементов ML-моделей на графиках единичных графических областей вы можете дополнительно к графикам тегов отобразить связанные с этими тегами артефакты выбранных элементов ML-моделей.

Если при настройке отображения графиков для высоты графиков было выбрано значение 190 px или более, то слева от каждой графической области появится ползунок, с помощью которого вы можете изменять масштаб отображения графиков. Для этого с помощью ползунка измените диапазон значений, который требуется отображать в графической области. Выбранный диапазон применяется к графической области независимо от диапазонов для других графических областей пресета. Для просмотра частей графической области, которые выходят в за пределы выбранного диапазона, зажмите ползунок и перетащите его вверх или вниз.

После графических областей пресета отображаются графические области для каждого выбранного элемента ML-модели. В таких графических областях отображаются графики артефактов элементов ML-модели. Значение артефакта элемента ML-модели зависит от аналитических алгоритмов, используемых элементом, и отображается в виде цветной линии. Цвет этой линии соответствует цвету, выбранному для параметра **Цвет точек-индикаторов инцидентов** при создании соответствующего элемента. На графиках также отображается оранжевая линия, которая соответствует порогу, при превышении которого элемент ML-модели регистрирует инцидент.

В нижней части раздела расположена дополнительная графическая область, содержащая график артефакта элемента ML-модели, выбранного в панели **Параметры отображения графика артефакта элемента ML-модели**. Красная линия на графике соответствует значению артефакта элемента ML-модели, а оранжевая линия соответствует порогу, при превышении которого Kaspersky MLAD регистрирует инцидент. Область графика, в которой значение артефакта элемента ML-модели превышает заданный порог, окрашивается в красный цвет. В нижней части окна отображаются цветные точки-индикаторы, соответствующие зарегистрированным инцидентам.

В зависимости от выбранного масштаба времени и плотности инцидентов одна точка-индикатор может соответствовать одному или нескольким близко расположенным инцидентам, зарегистрированным одним или несколькими элементами ML-моделей. В этом случае при наведении курсора на точку-индикатор отображаются границы интервала времени, которому соответствует точка-индикатор. Инциденты находятся внутри указанного интервала. Для точек-индикаторов, которые соответствуют инцидентам, зарегистрированным одним элементом ML-модели, цвет задается при создании этого элемента. Для точек-индикаторов, которые соответствуют группе инцидентов, зарегистрированных разными элементами, зарезервирован фиолетовый цвет. Для точек-индикаторов, которые соответствуют инцидентам, зарегистрированным детектором Limit Detector, зарезервирован красный цвет.



Раздел **История**

Выбор элементов ML-модели в разделе История

В разделе **История** доступна история поступивших данных, результат их обработки Kaspersky MLAD с формированием артефактов выбранными элементами ML-моделями и регистрацией инцидентов.

Если для объекта мониторинга используются разные ML-модели для обработки данных, Kaspersky MLAD позволяет выбрать несколько элементов ML-моделей для отображения результатов их инференса. Для детектора Limit Detector элемент ML-модели не создается. Точки-индикаторы инцидентов, зарегистрированных с помощью этого детектора, отображаются, если включено использование детектора Limit Detector и включен режим отображения индикаторов для всех инцидентов.

Функциональность доступна после добавления лицензионного ключа.

Чтобы просмотреть результаты инференса элементов ML-модели:

1. В основном меню выберите раздел **История**.

2. На открывшейся странице в раскрывающемся списке **Элемент модели** выберите один или несколько элементов ML-модели.

   Имена элементов отображаются в формате `< имя ML-модели > ⊃ < имя элемента >`.

   Программа автоматически сформирует динамический пресет для выбранного элемента ML-модели. Если выбрано более одного элемента, Kaspersky MLAD сформирует динамические пресеты для каждого выбранного элемента

   При выборе пресета на графических областях отобразятся значения тегов, поступивших в Kaspersky MLAD за выбранный интервал времени. Если вы настроили отображение графиков, то на графиках единичных графических областей также отобразятся артефакты, связанные с тегами таких областей и сформированные элементами ML-моделей, в составе которых используются эти теги.

   Ниже графиков тегов выбранного пресета отобразятся графики артефактов выбранных элементов ML-моделей. Значения, отображаемые на графиках, зависят от аналитических алгоритмов, используемых элементами для выявления аномалий.

   Если требуется скрыть отображение артефактов какого-либо выбранного ранее элемента ML-модели, нажмите на значок ✕ рядом с этим элементом.

3. Если требуется отображать график артефакта одного из уже выбранных элементов дополнительно в нижней фиксированной графической области, выполните следующие действия:

   a. Нажмите на кнопку ⚙ под графиками тегов в левой части страницы.

      Справа отобразится панель **Параметры отображения графика артефакта элемента ML-модели**.

   b. В раскрывающемся списке **Элемент модели** выберите элемент ML-модели. Вы можете выбрать только один элемент ML-модели из списка.

   c. Нажмите на кнопку **Закрыть**.

   На графике артефакта элемента ML-модели отобразится значение артефакта выбранного элемента в виде красной линии. Область графика, в которой значение артефакта превышает заданный порог (оранжевая линия), окрашивается в красный цвет.

В нижней части графика отобразятся точки-индикаторы инцидентов, зарегистрированных выбранными элементами ML-модели. Если включен режим отображения индикаторов для всех инцидентов, то отобразятся точки-индикаторы инцидентов, зарегистрированных всеми ML-моделями, а также детектором Limit Detector.

Просмотр исторических данных для определенного пресета

Если был выбран элемент ML-модели, то программа автоматически сформирует динамический пресет по этому элементу, который вы можете выбрать для отображения графиков тегов, участвующих в элементе. Сформированные пресеты отображаются в группе **Динамические пресеты** дерева активов в раскрывающемся списке **Пресет**. На графических областях отобразятся исторические данные по тегам сформированного динамического пресета.

При необходимости вы можете выбрать любой другой пресет для просмотра исторических данных.

Если вы хотите просмотреть исторические данные тегов из динамического пресета по инциденту, в разделе **Инциденты** вам нужно нажать на дату регистрации нужного инцидента.

Чтобы просмотреть исторические данные для определенного пресета:

1. В основном меню выберите раздел **История**.
2. На открывшейся странице в раскрывающемся списке **Пресет** выберите необходимый пресет.

   На странице отобразятся графики для тегов, которые входят в выбранный пресет, в соответствии с параметрами графических областей, заданными при создании этого пресета.

   Теги динамических пресетов отображаются только в единичных графических областях. Настройка отображения динамических пресетов невозможна.

Вы можете просматривать всю историю данных, используя навигацию по времени. Если необходимо, вы можете изменить дату и интервал времени или выбрать элементы ML-моделей для просмотра результатов их работы. Также вы можете изменить состав отображаемых тегов, изменив пресет.

Выбор даты и интервала времени в разделе История

Kaspersky MLAD позволяет выбрать дату, а также фиксированный интервал времени (масштаб) отображения исторических данных или произвольный интервал времени, например, когда был зафиксирован инцидент.

Чтобы выбрать дату для отображения исторических данных:

1. В основном меню выберите раздел **История**.
2. Нажмите на кнопку и в открывшемся окне выберите дату и время, для которых требуется отображать исторические данные на графиках.
3. Нажмите на кнопку **Применить**.

   На графиках вертикальная синяя линия будет указывать на выбранную дату и время (центр графика).
4. Если требуется выбрать другие дату и время (точку) на графике, нажмите на кнопку слева от оси времени, и выберите нужную точку.

   Выбранная точка станет новым центром графика. Вертикальная синяя пунктирная линия будет указывать на выбранные дату и время.

Чтобы выбрать интервал времени для отображения исторических данных:

1. В основном меню выберите раздел **История**.
2. На открывшейся странице выполните одно из следующих действий:

   - Если требуется отображать данные за фиксированный интервал времени, в раскрывающемся списке выберите необходимый интервал времени. По умолчанию доступны следующие временные интервалы:

     - 1, 5, 10, 15 и 30 минут;
     - 1, 3, 6 и 12 часов;
     - 1, 2, 15 и 30 дней;
     - 3 и 6 месяцев;
     - 1, 2 и 3 года.

     При необходимости системный администратор может создать, изменить или удалить временные интервалы.

   - Если требуется отображать данные за произвольный интервал времени, нажмите на кнопку , которая расположена слева от оси времени, выберите на оси времени нужный интервал и нажмите на . Если требуется еще раз изменить масштаб, повторите это действие.

На графиках выбранного пресета отобразятся значения тегов и результаты инференса выбранных элементов ML-моделей за выбранный интервал времени.

Навигация по времени в разделе История

Kaspersky MLAD предоставляет возможность навигации по времени для удобного просмотра исторических данных.

Чтобы использовать навигацию по времени при просмотре данных:

1. В основном меню выберите раздел **История**.
2. На открывшейся странице выберите интервал времени, за который требуется просмотреть данные.
3. С помощью кнопок ‹ и ›, расположенных в верхней части страницы, перемещайтесь по оси времени влево или вправо.

Сдвиг по оси времени на графике просмотра исторических данных будет происходить на выбранный интервал времени.



Навигация по времени

На графиках вертикальная синяя пунктирная линия указывает на середину выбранного временного интервала и совпадает с выбранными датой и временем. Если выбран интервал **1 день**, то на графике отображаются исторические данные за 12 часов до и после выбранных даты и времени относительно пунктирной линии. Если требуется, вы можете изменить временной интервал.

Настройка параметров отображения графиков в разделе История

Kaspersky MLAD позволяет настроить параметры отображения графических областей пресетов в разделе **История**.

Чтобы настроить параметры отображения графических областей:

1. В основном меню выберите раздел **История**.
2. На открывшейся странице нажмите на кнопку  в верхней части экрана.

   Справа отобразится панель **Параметры отображения графиков**.
3. В раскрывающемся списке **Высота графиков** выберите одно из следующих значений: 55 px, 110 px, 145 px, 190 px, 380 px, 570 px.

   По умолчанию параметр **Высота графиков** имеет значение 55 px. При значении 190 px и более слева от графических областей появятся ползунки, с помощью которых вы можете изменять масштаб отображения графиков.
4. Если требуется, включите переключатель **Отображать графики наблюдений в выбранном цвете** и в поле **Цвет графиков наблюдений** выберите цвет.
5. Если требуется, включите переключатель **Отображать графики прогнозов в выбранном цвете** и в поле **Цвет графиков прогнозов** выберите цвет.
6. С помощью переключателя **Имя и описание тега** включите или выключите отображение имен и описаний тегов слева от графиков.
7. С помощью переключателя **Прогнозируемое значение тега** включите или выключите отображение прогнозируемых значений выходных тегов предиктивных элементов, если соответствующие элементы выбраны для отображения.

   Эллиптические конверты и диагностические правила не формируют прогноза значений тегов.
8. С помощью переключателя **Индивидуальная ошибка тега** включите или выключите отображение индивидуальных ошибок прогноза значений выходных тегов предиктивных элементов, если соответствующие элементы выбраны для отображения.
9. С помощью переключателя **Отображать индикаторы для всех инцидентов** включите или выключите отображение точек-индикаторов инцидентов, зарегистрированных всеми ML-моделями, а не только выбранными для отображения, а также детектором Limit Detector.

   Если этот переключатель выключен, то будут отображаться только точки-индикаторы для инцидентов, которые были зарегистрированы выбранными элементами ML-модели.

10. Если требуется отображать установленные технические пределы для тегов на графиках, выполните следующие действия:

    a. Включите переключатель **Пороги блокировки**.

    b. Если требуется всегда отображать установленные технические пределы, включите переключатель **Всегда показывать пороги блокировки**.

    Если этот переключатель выключен, то технические пределы будут отображаться, только если значение какого-либо тега приблизилось к соответствующему пределу в отображаемой на экране области графика.

11. Если требуется отображать контрольные линии для графических областей, включите переключатель **Контрольные линии**.

12. Нажмите на кнопку **Закрыть** для возвращения к просмотру графиков в разделе **История**.

Заданные параметры отображения графических областей пресетов в разделе **История** будут применены.

Просмотр данных в разделе Временной срез

В разделе **Временной срез** вы можете просматривать значения технологических параметров, полученные от датчиков объекта мониторинга в один и тот же момент времени. Датчики должны быть однотипными (иметь одинаковую размерность) и расположены в пространстве линейно, например, датчики давления в трубе нефтепровода.

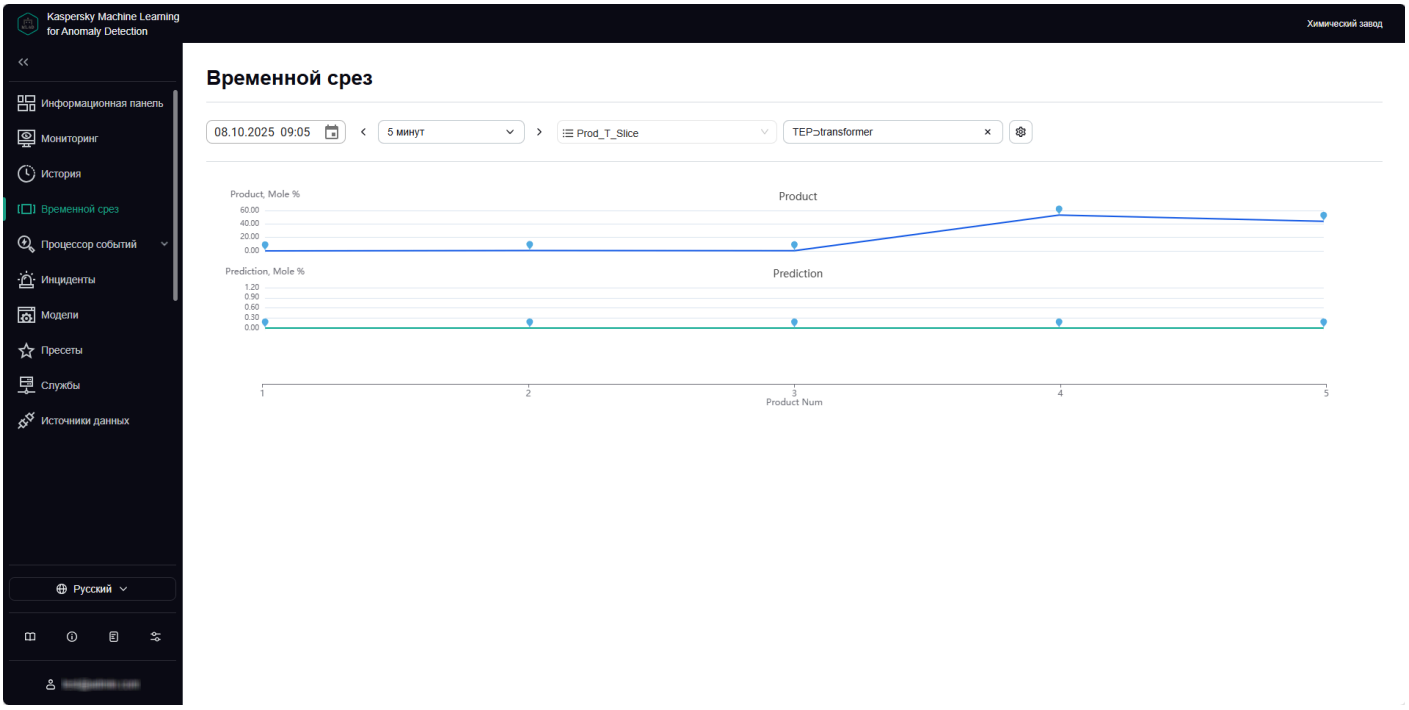
Данные представлены в виде графиков, которые позволяют увидеть, был ли зафиксирован инцидент в выбранный момент времени и где находится вероятный источник инцидента.

В нижней части страницы расположен блок, отображающий индивидуальные ошибки тегов. Данные представлены в виде столбчатой диаграммы. Величина ошибки для каждого тега отображается при наведении курсора мыши на столбец. Справа от графиков тегов пресета расположен график ошибки прогноза.

В разделе **Временной срез** в раскрывающемся списке вы можете выбрать пресет, дату и время получения данных. В список входят специальные пресеты, которые можно создать в разделе **Пресеты**. В специальном пресете должны присутствовать только однотипные теги, у которых указаны координаты по оси абсцисс. Вы можете дополнительно указать динамически вычисляемые для каждого тега выражения, основанные на реальных и прогнозируемых значениях тегов, индивидуальных ошибках прогноза, а также значениях координат тегов и задаваемых в выражениях константах.

Также вы можете настроить отображение графиков, выбрать интервал времени для просмотра данных, а также выбрать определенный элемент ML-модели, чтобы просмотреть индивидуальные ошибки тегов пресета, полученные в результате обработки данных выбранным элементом ML-модели.

Результаты обработки данных возможно просмотреть только для предиктивных элементов ML-модели.



Раздел **Временной срез**

Выбор определенного элемента ML-модели в разделе Временной срез

Если для объекта мониторинга используется ML-модель, которая имеет несколько элементов для обработки и прогнозирования данных, Kaspersky MLAD позволяет выбрать определенный элемент ML-модели для отображения в разделе **Временной срез** индивидуальных ошибок тегов, полученных в результате работы этого элемента.

Функциональность доступна после добавления лицензионного ключа.

Результаты обработки данных возможно просмотреть только для предиктивных элементов ML-модели.

Чтобы просмотреть индивидуальные ошибки тега, полученные в результате обработки данных определенным элементом ML-модели:

1. В основном меню выберите раздел **Временной срез**.
2. На открывшейся странице в раскрывающемся списке **Элемент модели** выберите нужный элемент ML-модели.

   Имена элементов отображаются в формате `<имя ML-модели> ⊃ <имя элемента>`.

В нижней части раздела отобразятся индивидуальные ошибки тегов, полученные в результате обработки данных выбранным элементом ML-модели.

Просмотр данных для определенного пресета в разделе Временной срез

Чтобы просмотреть данные для определенного пресета:

1. В основном меню выберите раздел **Временной срез**.
2. На открывшейся странице в раскрывающемся списке **Пресет** выберите необходимый пресет.

   На странице отобразятся графики для тегов, которые входят в выбранный пресет.

Если требуется, вы можете изменить временной интервал отображения данных, настроить отображение графика или выбрать элемент ML-модели. Также вы можете изменить состав отображаемых тегов, изменив пресет.

Выбор даты и интервала времени в разделе Временной срез

Kaspersky MLAD позволяет выбрать дату и временной интервал (масштаб) отображения поступающих данных.

Чтобы выбрать дату для отображения поступающих данных:

1. В основном меню выберите раздел **Временной срез**.
2. Нажмите на кнопку и в открывшемся окне выберите дату и время, для которых требуется отображать данные.
3. Нажмите на кнопку **Применить**.

   На графиках отобразятся значения тегов для выбранных даты и времени.

Чтобы выбрать интервал времени для отображения поступающих данных:

1. В основном меню выберите раздел **Временной срез**.
2. На открывшейся странице в раскрывающемся списке в верхней части страницы выберите необходимый интервал времени. По умолчанию доступны следующие временные интервалы:
   - 1, 5, 10, 15 и 30 минут;
   - 1, 3, 6 и 12 часов;
   - 1, 2, 15 и 30 дней;
   - 3 и 6 месяцев;
   - 1, 2 и 3 года.

   Если требуется, системный администратор может создать, изменить или удалить временные интервалы.

На странице отобразятся графики заданного пресета для выбранного интервала времени.

Навигация по времени в разделе Временной срез

Kaspersky MLAD предоставляет возможность навигации по времени для удобного просмотра данных.

Чтобы использовать навигацию по времени при просмотре данных:

1. В основном меню выберите раздел **Временной срез**.
2. На открывшейся странице выберите интервал времени, за который требуется просмотреть данные.
3. С помощью кнопок ‹ и ›, расположенных в верхней части страницы, перемещайтесь по оси времени влево или вправо.

Сдвиг по оси времени на графике просмотра данных будет происходить на выбранный интервал времени.



Навигация по времени

Настройка параметров отображения графиков в разделе Временной срез

Kaspersky MLAD позволяет настроить параметры отображения графиков пресетов в разделе **Временной срез**.

Чтобы настроить параметры отображения графиков пресетов:

1. В основном меню выберите раздел **Временной срез**.
2. На открывшейся странице нажмите на кнопку , которая расположена в верхней части экрана.

   Справа отобразится панель **Параметры отображения графиков**.
3. В раскрывающемся списке **Высота графиков** выберите одно из следующих значений: 55 px, 110 px, 145 px, 190 px, 380 px, 570 px.

   По умолчанию параметр **Высота графиков** имеет значение 55 px. При значении 190 px и более слева от графических областей появятся ползунки, с помощью которых вы можете изменять масштаб отображения графиков.
4. Нажмите на кнопку **Закрыть** для возвращения к просмотру графиков.

Заданные параметры отображения графиков будут применены.

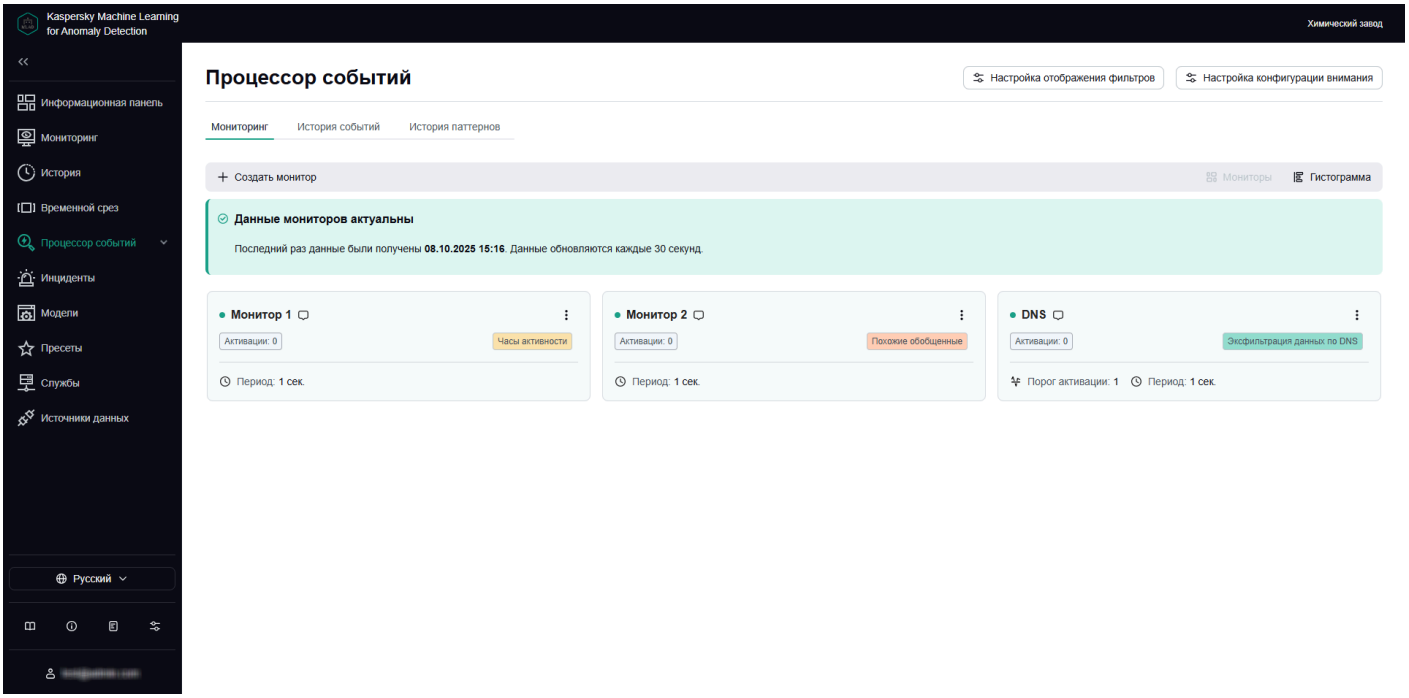
Работа с процессором событий

В разделе **Процессор событий** представлены данные о событиях, а также структуре паттернов, выявленных с помощью службы Event Processor в потоке событий, которые поступают от внешних источников и от службы Anomaly Detector.

В разделе **Процессор событий** вы можете просматривать историю полученных событий и историю регистрации новых и/или устойчиво повторяющихся паттернов. Вы также можете настроить отображение параметров событий и параметры регистрации паттернов. На вкладке **Мониторинг** вы можете осуществлять мониторинг определенных событий, паттернов или значений параметров событий, поступающих в процессор событий в потоке данных от объектов мониторинга. С помощью мониторов вы также можете отслеживать обобщенные события и паттерны, необычные часы активности для поступивших событий, а также признаки эксфильтрации данных в DNS-запросах.

Функциональность доступна после добавления лицензионного ключа для коммерческой лицензии с процессором событий.
Предварительно требуется настроить службу Event Processor.

В случае перезапуска Kaspersky MLAD восстанавливает состояние службы Event Processor и приостанавливает обработку данных, поступающих от коннектора CEF Connector. Эти данные временно сохраняются во внутренней очереди брокера сообщений программы. До восстановления службы Event Processor на вкладках раздела **Процессор событий** будет отображаться уведомление о том, что служба Event Processor остановлена. При значительном объеме обработанных событий и зарегистрированных паттернов процесс восстановления службы может занимать несколько минут.



Раздел **Процессор событий**

О процессоре событий

Процессор событий в составе Kaspersky MLAD предназначен для выявления в потоке событий, поступающих от объектов мониторинга, закономерностей в виде повторяющихся событий и паттернов, а также для выявления новых событий и паттернов. Новые события и паттерны могут указывать на аномалию в работе объекта мониторинга.

Вы также можете сфокусировать внимание процессора события на общее поведение объекта мониторинга. Процессор событий будет регистрировать обобщенные события и паттерны, в составе которых будут отсутствовать обобщенные параметры событий.

Процессор событий может отслеживать часы активности по времени поступивших событий. События, обнаруженные в необычное для них время, могут также указывать на аномалию в работе объекта мониторинга.

Процессор событий также может выявлять признаки эксфильтрации данных в DNS-запросах, сведения о которых поступают в Kaspersky MLAD в виде событий.

О событиях

Служба Event Processor обрабатывает данные, поступающие от объектов мониторинга и от службы Anomaly Detector, в виде событий. *Событие* – это набор значений из заранее заданного перечня параметров, описывающих то, что произошло на объекте мониторинга. Набор параметров событий зависит от объекта мониторинга и задается в конфигурационном файле для службы Event Processor. Каждому событию присваивается идентификатор, по которому идентифицируются параметры этого события и их значения. В совокупности с метками времени событий идентификаторы определяют историю событий.

Процессор событий предназначен для работы только с категориальными значениями параметров событий. Значения параметров событий преобразуются к строковому типу. Для работы с численными значениями данных телеметрии при обработке потока событий Kaspersky MLAD использует службу Anomaly Detector. Системный администратор может включить обработку инцидентов от службы Anomaly Detector в качестве событий при настройке параметров службы Event Processor.

Событие представляет собой явление, обособленное от других событий, и при этом могут существовать интервалы времени, в течение которых никаких событий не происходило. На регистрацию события могут повлиять такие факторы, как действия персонала, изменение режима работы устройства на предприятии или выполнение специалистом команд на АСУ ТП.

Примеры ситуаций, которые могут привести к регистрации событий в Kaspersky MLAD

Примеры событий приведены для разных объектов мониторинга.

- *Вход сотрудника*.
  - Время события: 10.11.21 09:03;
  - Параметры события:
    - Источник: СКУД;
    - Сотрудник: Иванов;
    - Пост: дверь машзала, внешняя сторона;
    - Результат: Проход.
- *Запуск установки*.
  - Время события: 10.11.21 09:09;
  - Параметры события:
    - Источник: АРМ оператора;
    - Пользователь: Иванов;
    - Оборудование: Установка №1;
    - Команда: Поджиг включен;
    - Ток: 44 А;
    - Продолжительность: 10 сек.
- *Выход на режим*.
  - Время события: 10.11.21 09:24;
  - Параметры события:
    - Источник: АСУ ТП;
    - Оборудование: Установка №1;
    - Номинальный режим: True.

Событие регистрируется службой Event Processor один раз. При поступлении потока событий процессор событий распознает ранее выявленные события. В случае обнаружения событий, которые не соответствуют ранее выявленным, процессор событий регистрирует новые события.

Вы можете просматривать полученные события в виде графа или таблицы. Для просмотра событий требуется загрузить их в разделе **Процессор событий** → **История событий**. Параметры событий, указанные в конфигурационном файле для службы Event Processor, могут встречаться не во всех событиях, поступающих от объекта мониторинга. Таким образом, при просмотре полученных событий часть параметров может отсутствовать.

О паттернах

В потоке событий, поступающих от объекта мониторинга, процессор событий выявляет закономерности в виде иерархии стабильных (устойчиво повторяющихся) паттернов. Такие закономерности могут быть представлены *простыми паттернами* (последовательностью событий) или *составными паттернами* (последовательностью паттернов). В свою очередь паттерны, образующие составной паттерн, называются вложенными.

Последовательность событий или паттернов считается повторяющейся, если составляющие ее элементы следуют в одном и том же порядке, при этом интервалы времени между аналогичными элементами в разных последовательностях отличаются друг от друга не более чем на некоторый максимально допустимый диапазон. Допустимый диапазон интервалов между элементами паттерна рассчитывается с учетом значения параметра **Коэффициент, определяющий допустимую дисперсию длительности паттерна**. Паттерны обусловлены сложившимися на предприятии практиками, регламентами или техническими особенностями производственного процесса.

Процессор событий представляет выявленные закономерности как послойную иерархию вложенных элементов (структуру паттерна) до уровня событий. События являются элементами первого слоя, простые паттерны – элементами второго слоя, составные паттерны – элементами третьего слоя и выше. Значения параметров события являются элементами нулевого слоя.

Паттерн регистрируется службой Event Processor один раз и включает в себя идентификаторы вложенных элементов этого паттерна и интервалы времени между ними. При поступлении потока событий процессор событий распознает ранее выявленные паттерны. В случае обнаружения паттернов, которые не соответствуют ранее выявленным закономерностям, процессор событий регистрирует новые паттерны.

К новым паттернам будут относиться последовательности событий или паттернов как с нарушением порядка или состава вложенных паттернов (например, включение агрегата до того, как оператор появился на рабочем месте), так и со значительным изменением интервалов между событиями или вложенными паттернами при сохранении их последовательности (например, включение агрегата через слишком короткий или, наоборот, слишком длинный интервал времени после появления оператора на рабочем месте). Таким образом, процессор событий регистрирует паттерны с новой структурой.

Новые паттерны могут указывать на аномалию в работе объекта мониторинга. Вы можете просмотреть структуру нового паттерна для изучения ее отклонений от структуры ранее выявленных закономерностей.

Если вновь выявленная последовательность событий или паттернов начинает устойчиво повторяться, такая последовательность превращается в стабильный паттерн.

При необходимости служба Event Processor может регистрировать паттерны, в которых не являются важными значения одного или нескольких параметров событий (например, имя сотрудника, который включил агрегат). Такие паттерны называются *обобщенными*. Для регистрации обобщенных паттернов необходимо при настройке параметров конфигурации внимания задать **Обобщенное внимание** в качестве типа внимания. Вы также можете указать **Обобщенный параметр** в качестве типа условия при настройке параметров условий к предмету внимания. Параметры предмета и условий внимания, заданные в качестве обобщенных, не будут отображаться при просмотре структуры обобщенных паттернов на вкладке **История паттернов**.

О механизме внимания

Поток событий, поступающих от объекта мониторинга, как правило, содержит множество несвязанных между собой событий. Служба Event Processor поддерживает механизм внимания, который позволяет выявлять паттерны на определенном подмножестве событий из всего потока.

Внимание – это специальная конфигурация процессора событий, которую требуется настроить для отслеживания событий и паттернов по отдельным подмножествам истории событий, а также для выявления событий, поступивших в необычное для них время, и общности в поведении объекта мониторинга.

Основой конфигурации внимания служат головы внимания, которые задают значение параметра предмета внимания и значения параметров условий к предмету внимания. Предмет внимания соответствует основному параметру события, по которому процессор событий будет регистрировать события и паттерны, а условия соответствуют дополнительным критериям регистрации событий и паттернов для других параметров событий. Голова внимания обрабатывает из всего потока входных событий только те события, которые удовлетворяют обозначенному предмету внимания и условиям. Процессор событий может обрабатывать поток событий для нескольких голов внимания одновременно.

Процессор событий может регистрировать обобщенные события и паттерны для отслеживания общего поведения по разным значениям параметра предмета внимания. Для этого при настройке параметров предмета внимания необходимо задать **Обобщенное внимание** в качестве типа внимания. Вы также можете указать **Обобщенный параметр** в качестве типа условия при настройке параметров условий к предмету внимания. Параметры предмета и условий внимания, заданные в качестве обобщенных, не будут отображаться при просмотре обобщенных событий или паттернов, но будут влиять на правила выделения этих обобщенных событий и паттернов из потока.

Вы можете настроить параметры конфигурации внимания в разделе **Процессор событий**.

О режимах работы процессора событий

В Kaspersky MLAD предусмотрены следующие режимы работы службы Event Processor:

- **Основной режим**. В основном режиме работы процессор событий обрабатывает входящий поток событий в виде эпизодов. *Эпизод* – это последовательность событий из всего потока, ограниченная по времени и/или количеству событий. Эпизод считается сформированным при выполнении одного из следующих условий:

  - Время накопления эпизода достигло предела, заданного в параметре **Интервал получения событий эпизода (сек.)** службы Event Processor.

  - Количество накопленных событий достигло предела, заданного в параметре **Размер эпизода (количество событий)** службы Event Processor.

  По полученному в потоке событий эпизоду служба Event Processor выявляет новые и/или повторяющиеся (стабильные) события и паттерны по каждой из заданных голов внимания. Вы можете создавать головы внимания и управлять ими в разделе **Процессор событий**.

  При поступлении события, временная метка которого относится к ранее обработанному эпизоду, служба Event Processor не пересматривает структуру паттернов, выявленных при обработке этого эпизода. Служба Event Processor учитывает события, поступившие в Kaspersky MLAD с временной задержкой, при выявлении паттернов во время повторной обработки истории событий в режиме сна.

- **Режим сна**. Для улучшения качества выявленных паттернов и их структуры процессор событий может переходить в режим сна в соответствии с заданным расписанием. Обработка потока событий в онлайн-режиме приостанавливается, при этом Kaspersky MLAD накапливает поступающие события во внутреннем ограниченном буфере сервера для последующей обработки после перехода из режима сна в основной режим работы.

  В режиме сна процессор событий повторно анализирует последовательности событий, обработанные ранее в основном режиме работы. Для выявления более сложных структур паттернов в режиме сна процессор событий обрабатывает последовательности событий за более длительные интервалы времени, чем время накопления эпизода в основном режиме.

  В параметрах службы Event Processor вы можете настроить расписание режима сна (например, на время, когда поток событий наименее интенсивен), а также интервал времени, за который требуется передать события, проанализированные в основном режиме работы, на повторную обработку.

О мониторах

Монитор – источник извещений о выявлении процессором событий паттернов, событий или значений параметров событий в соответствии с заданными критериями мониторинга. Критерии мониторинга определяют голову внимания, дополнительные фильтры на значения параметров событий, а также скользящий временной интервал и количество последовательных активаций монитора на скользящем временном интервале.

Вы можете создавать мониторы для оповещения о выявлении следующих вхождений в потоке событий:

- **Значения параметров событий**. Вы можете создать монитор для оповещения о выявлении новых или ранее встречавшихся значений определенного параметра события. Например, если вы хотите отслеживать новых пользователей на объекте мониторинга, то при создании монитора вам нужно выбрать тип подписки **Значения параметров** и настроить его на выявление новых значений по параметру **Пользователь**.

- **События**. Вы можете создать монитор для оповещения о выявлении новых или ранее встречавшихся событий. Вы также можете сфокусировать внимание процессора событий на определенном параметре событий. Например, если вы хотите отслеживать новые действия конкретного пользователя на объекте мониторинга, то при создании монитора вам нужно выбрать тип подписки **События** и в параметре события **Пользователь** указать имя пользователя, действия которого вы хотите отслеживать.

- **Эксфильтрация данных по DNS**. Вы можете создать монитор для оповещения о выявлении признаков эксфильтрации данных в DNS-запросах. Для этого при создании монитора вам нужно выбрать тип подписки **Эксфильтрация данных по DNS** и уточнить как минимум два условия активации монитора в блоке **Фильтры**, где для первого условия фильтрации необходимо выбрать параметр события, по которому идентифицируется хост, отправивший DNS-запрос, а для второго условия фильтрации необходимо выбрать параметр события, соответствующий DNS-запросу.

- **Часы активности**. Вы можете создать монитор для оповещения о выявлении событий в необычное для них время активности. Например, если вы хотите отслеживать необычную активность в действиях конкретных пользователей, то при создании монитора вам нужно выбрать тип подписки **Часы активности** и голову внимания с вниманием на параметре **Пользователь**. Предварительно необходимо создать голову внимания с вниманием на параметре **Пользователь** и указать для этого параметра имена пользователей, часы активности которых необходимо отслеживать.

- **Паттерны**. Вы можете создать монитор для оповещения о выявлении новых или ранее встречавшихся паттернов. Например, если вы хотите отслеживать закономерности в действиях конкретного пользователя на объекте мониторинга, то при создании монитора вам нужно выбрать тип подписки **Паттерны**, сфокусировать внимание процессора событий на параметре **Пользователь** и указать в этом параметре имя пользователя, закономерности в действиях которого вы хотите отслеживать.

- **События головы внимания**. Вы можете создать монитор для оповещения о выявлении событий в фокусе внимания процессора событий. Например, если вы хотите отслеживать действия более узкого круга пользователей в фокусе внимания, то при создании монитора вам нужно выбрать тип подписки **События головы внимания**, выбрать голову внимания с вниманием на параметре **Пользователь** и уточнить круг пользователей для этого параметра в блоке **Фильтры**.

- **Похожие обобщенные события или паттерны**. Вы можете создать монитор для оповещения о выявлении похожих обобщенных событий или паттернов. Если вы хотите отслеживать общие закономерности в действиях различных пользователей на объекте мониторинга, то при создании монитора вам нужно выбрать тип подписки **Похожие обобщенные**, выбрать голову с обобщенным вниманием на параметре **Пользователь**, а также выбрать вариант **Подписка на паттерны** для параметра **Подписка на события или паттерны**.

- **Уникальные обобщенные события или паттерны**. Вы можете создать монитор для оповещения о выявлении уникальных обобщенных событий или паттернов. Например, если вы хотите отслеживать новые общие закономерности в действиях любого пользователя, то при создании монитора вам нужно выбрать тип подписки **Уникальные обобщенные**, выбрать голову с обобщенным вниманием на параметре **Пользователь** и условиями на дополнительные параметры, соответствующим ожиданиям в поведении разных пользователей, и выбрать вариант **Подписка на паттерны** для параметра **Подписка на события или паттерны**. Вам также нужно указать в параметре **Скользящее окно (сек.)** интервал времени, в течение которого процессор событий будет ожидать похожий обобщенный паттерн по другим пользователям. Если процессор событий не обнаружит такой паттерн, монитор отправит оповещение об активации.

Фильтры в составе критериев мониторинга могут задаваться нечетко. Например, вы можете создать монитор для отслеживания ситуаций, при которых какой-либо пользователь (отслеживание по всем значениям параметра **Пользователь**) ходил к серверу бухгалтерии (значение параметра **Сервер**) более десяти раз (значение поля **Порог активации**) за последние пять минут (значение скользящего временного интервала).

При обнаружении в потоке поступающих данных событий, паттернов и значений параметров событий, соответствующих критериям мониторинга, процессор событий активирует монитор. Kaspersky MLAD отображает информацию о количестве активаций монитора при его просмотре, а также отправляет во внешнюю систему оповещения об активации мониторов при достижении заданного порога на скользящем окне с помощью коннектора CEF Connector.

Созданные пользователем мониторы отображаются в разделе **Процессор событий** на вкладке **Мониторинг**.

Настройка отображения параметров событий

Перед обработкой событий службой Event Processor требуется настроить отображение параметров событий.

> Функциональность доступна после добавления лицензионного ключа для коммерческой лицензии с процессором событий.

Чтобы настроить отображение параметров событий:

1. В основном меню выберите раздел **Процессор событий** → **Мониторинг**.
2. На открывшейся странице нажмите на кнопку **Настройка отображения фильтров**.

   Справа отобразится панель **Настройка отображения фильтров параметров событий**.

3. Для настройки отображения фильтров параметров событий в блоке **Фильтры** на вкладках **История событий** и **История паттернов** установите флажки рядом с именами нужных параметров событий.

   По умолчанию в панели отображаются **параметры событий от службы Anomaly Detector**. Для отображения пользовательских параметров событий требуется загрузить конфигурационный файл службы Event Processor. По умолчанию выбраны все доступные параметры событий.

   Если включена функция **Обрабатывать инциденты как события**, то в процессор событий поступают события со следующими параметрами:

   - **incident_detection_system** – тип зарегистрированного инцидента.
   - **incident_model_name** – имя используемой ML-модели.
   - **incident_tag_name** – имя тега, поведение которого привело к регистрации инцидента.
   - **incident_group_name** – имя группы инцидентов, в которую входит зарегистрированный инцидент.
   - **incident_triggered_tag_value** – значение тега, поведение которого привело к регистрации инцидента.
   - **incident_id** – идентификатор зарегистрированного инцидента.
   - **incident_tag_id** – идентификатор тега, поведение которого привело к регистрации инцидента.

   При необходимости вы можете изменить порядок отображения параметров событий в блоке **Фильтры**. Для этого нужно перетащить параметр события в нужное место в панели **Настройка отображения фильтров параметров событий**, удерживая за точки слева (⠿) от имени нужного параметра события.

4. Нажмите на кнопку **Сохранить**.

Настройка параметров конфигурации внимания

Перед обработкой событий службой Event Processor требуется настроить параметры конфигурации внимания.

Основой конфигурации внимания служат головы внимания, которые задают значение параметра предмета внимания и значения параметров условий к предмету внимания. Предмет внимания соответствует основному параметру события, по которому процессор событий будет регистрировать события и паттерны, а условия соответствуют критериям регистрации событий и паттернов для других параметров событий. Голова внимания обрабатывает из всего потока входных событий только те события, которые удовлетворяют обозначенному предмету внимания и условиям.

Процессор событий может регистрировать обобщенные события и паттерны для отслеживания общего поведения по разным значениям параметра предмета внимания. Для этого при настройке параметров предмета внимания необходимо задать **Обобщенное внимание** в качестве типа внимания. Вы также можете указать **Обобщенный параметр** в качестве типа условия при настройке параметров условий к предмету внимания. Параметры предмета и условий внимания, заданные в качестве обобщенных, не будут отображаться в зарегистрированных событиях и паттернах, но будут влиять на правила выделения этих обобщенных событий и паттернов из потока.

Все созданные головы внимания и **информация о них** отображается в панели **Головы внимания**. Для просмотра информации о головах внимания в панели **Головы внимания** необходимо нажать на кнопку **Настройка конфигурации внимания**.

- **Имя** – имя головы внимания.
- **Параметр предмета внимания** – имя параметра события, выбранного в качестве предмета внимания.
- **Тип внимания** – тип внимания, в соответствии с которым процессор событий регистрирует события и паттерны.
- **Состояние** – признак, указывающий, используется ли эта голова внимания.
- **Действия** – кнопки, позволяющие изменить или удалить головы внимания.

Добавление головы внимания

Вы можете создать несколько голов внимания и использовать разные головы внимания для разных мониторов одновременно.

Функциональность доступна после добавления лицензионного ключа для коммерческой лицензии с процессором событий.

Большое количество голов внимания может привести к снижению производительности процессора событий и замедлению работы основных служб Kaspersky MLAD (прием данных, обнаружение аномалий, работа веб-интерфейса). Для уточнения количества голов внимания рекомендуется проконсультироваться со специалистом "Лаборатории Касперского" или сертифицированным интегратором.

Чтобы добавить голову внимания:

1. В основном меню выберите раздел **Процессор событий → Мониторинг**.
2. На открывшейся странице нажмите на кнопку **Настройка конфигурации внимания**.

   Справа отобразится панель **Головы внимания**.
3. Для добавления головы внимания нажмите на кнопку **Добавить голову внимания**.

   Справа отобразится панель **Добавление головы внимания**.
4. В поле **Имя** введите имя головы внимания.
5. Для использования головы внимания при обработке потока событий установите переключатель **Состояние** в положение **Активна**.
6. Для автоматического выявления паттернов в соответствии с параметрами головы внимания установите переключатель **Распознавание паттернов** в положение **Включено**.

   При включенном переключателе служба Event Processor хранит выявленные паттерны в памяти программы. Если голова внимания не будет использована для выявления паттернов монитором или просмотра истории паттернов, рекомендуется установить переключатель **Распознавание паттернов** в положение **Выключено**.

7. В блоке параметров **Предмет внимания** выполните следующие действия:

   a. В раскрывающемся списке **Параметр события** выберите основной параметр события, по которому требуется регистрировать события и паттерны.

   b. В раскрывающемся списке **Тип внимания** выберите одно из следующих значений:

   - **Внимание**. При регистрации событий и паттернов внимание процессора событий будет направлено на выбранный параметр события с учетом выбранного значения.

   - **Обобщенное внимание**. При регистрации событий и паттернов процессор событий обобщит выбранные значения по выбранному параметру события.

     При выборе этого типа внимания процессор событий будет регистрировать обобщенные паттерны, при просмотре которых не будет отображаться выбранный параметр события с выбранным значением. Процессор событий будет отслеживать каждое заданное значение параметра события отдельно.

   c. Выполните одно из следующих действий:

   - Если требуется включить во внимание все значения параметра события или обобщить их во внимании, в раскрывающемся списке **Тип значения** выберите **Все значения**.

     При выборе варианта **Все значения** процессор событий будет отслеживать события и паттерны по каждому конкретному значения параметра события отдельно. Для обеспечения стабильной производительности процессора событий рекомендуется указать конкретные значения предмета события.

   - Если требуется включить во внимание конкретные значения параметра события или обобщить эти значения во внимании, в раскрывающемся списке **Тип значения** выберите **Определенные значения** и введите нужное значение в поле **Значение**. Начните вводить нужное значение, чтобы все подходящие значения параметров отобразились в списке.

     Если вы выбрали **Обобщенное внимание** в качестве типа внимания, выберите не менее двух значений параметра события.

   - Если требуется включить во внимание значения параметра события по шаблону или обобщить их во внимании, в раскрывающемся списке **Тип значения** выберите **Регулярное выражение** и введите шаблон значения с помощью регулярного выражения в поле **Значение**.

     В регулярных выражениях используется формат, поддерживаемый на языке программирования Python. Подробнее о популярных специальных символах регулярных выражений см. в Приложении.

8. Если требуется обобщить остальные параметры событий, установите переключатель **Обобщение параметров условий** в положение **Включено**.

   Если в качестве типа внимания было выбрано обобщенное внимание, то при включенном переключателе процессор событий обобщит остальные параметры событий по всем их значениям. В таком случае процессор событий не зарегистрирует ни одного события или паттерна. Для того, чтобы процессор событий сформировал события или паттерны необходимо задать в блоке параметров **Условия** хотя бы один параметр события без обобщения по его значениям.

9. Если требуется уточнить критерии регистрации паттернов по дополнительным параметрам событий, в блоке параметров **Условия** выполните следующие действия:

   a. Нажмите на кнопку **Добавить условие**.

   b. В раскрывающемся списке **Параметр события** выберите дополнительный параметр события, по которому требуется уточнить выборку данных для регистрации событий и паттернов.

   c. В раскрывающемся списке **Тип условия** выберите одно из следующих значений:

   - **Параметр**. При регистрации событий и паттернов процессор событий будет учитывать значения выбранного параметра события с учетом выборки данных, полученных для основного параметра события.

   - **Обобщенный параметр**. При регистрации событий и паттернов внимание процессора событий обобщит значения выбранного параметра с учетом выборки данных, полученных для основного параметра события.

     При выборе этого типа условия процессор событий будет регистрировать паттерны, при просмотре которых не будет отображаться выбранный параметр события с выбранным значением.

     Это значение доступно, если для предмета внимания выбран тип **Обобщенное внимание**.

   d. Выполните одно из следующих действий:

   - Если требуется включить во внимание новые значения параметра события или обобщить их во внимании, в раскрывающемся списке **Тип значения** выберите **Новые значения**.

     Элемент **Новые значения** доступен в следующих случаях:

     - В качестве типа условия выбран тип **Параметр**.

     - В качестве типа внимания выбран тип **Внимание**, переключатель **Обобщение параметров условий** выключен, а в качестве типа условия выбран тип **Обобщенный параметр**.

   - Если требуется включить во внимание все значения параметра события или обобщить их во внимании, в раскрывающемся списке **Тип значения** выберите **Все значения**.

     Элемент **Все значения** доступен в следующих случаях:

     - Переключатель **Обобщение параметров условий** включен, а в качестве типа условия выбран тип **Параметр**.

     - Переключатель **Обобщение параметров условий** выключен, а в качестве типа условия выбран тип **Обобщенный параметр**.

   - Если требуется включить во внимание конкретные значения параметра события или обобщить эти значения во внимании, в раскрывающемся списке **Тип значения** выберите **Определенные значения** и введите нужное значение в поле **Значение**. Начните вводить нужное значение, чтобы все подходящие значения параметров отобразились в списке.

   - Если требуется включить во внимание значения параметра события по шаблону или обобщить их во внимании, в раскрывающемся списке **Тип значения** выберите **Регулярное выражение** и введите шаблон значения с помощью регулярного выражения в поле **Значение**.

     В регулярных выражениях используется формат, поддерживаемый на языке программирования Python. Подробнее о популярных специальных символах регулярных выражений см. в Приложении.

Вы можете задать более одного условия по дополнительным параметрам событий. При необходимости вы можете удалить ранее добавленное условие нажатием на кнопку напротив строки с нужным условием.

Заданные условия будут дополнительно применены к выборке данных, полученных для основного параметра события, заданного в блоке параметров **Предмет внимания**. Например, если был выбран тип **Обобщенное внимание**, то при включенном переключателе **Обобщение параметров условий** процессор событий будет регистрировать паттерны, в составе которых будут отображаться только те параметры событий, которые были заданы в блоке параметров **Условия**, с учетом их выбранных значений. Если переключатель выключен, то процессор событий будет регистрировать паттерны, в составе которых не будут отображаться обобщенный параметр, заданный в блоке параметров **Предмет внимания**. При этом будут учитываться значения параметров событий, заданные в блоке параметров **Условия**.

10. Нажмите на кнопку **Сохранить**.

Информация о новой голове внимания отобразится в таблице в панели **Головы внимания**. Если требуется, вы можете изменить имя головы внимания, а также включить или выключить использование головы внимания при обработке событий.

Изменение головы внимания

При необходимости вы можете включить или выключить использование головы внимания при обработке потока событий.

Изменение параметров предмета и условий внимания недоступно. Если требуется, вы можете удалить головы внимания или создать новые.

Функциональность доступна после добавления лицензионного ключа для коммерческой лицензии с процессором событий.

Чтобы изменить голову внимания:

1. В основном меню выберите раздел **Процессор событий** → **Мониторинг**.
2. На открывшейся странице нажмите на кнопку **Настройка конфигурации внимания**.

   Справа отобразится панель **Головы внимания**.
3. Нажмите на кнопку рядом с головой внимания, параметры которой требуется изменить.
4. Если требуется, измените имя головы внимания.
5. Если требуется включить или выключить использование головы внимания при обработке потока событий, выполните одно из следующих действий:

   - Если требуется использовать голову внимания при обработке потока событий, установите переключатель **Состояние** в положение **Активна**.
   - Если требуется выключить использование головы внимания при обработке потока событий, установите переключатель **Состояние** в положение **Не активна**.

6. Если требуется включить или выключить выявление паттернов головой внимания, выполните одно из следующих действий:

   - Если требуется выявлять паттерны с помощью головы внимания, установите переключатель **Распознавание паттернов** в положение **Включено**.
   - Если требуется выключить выявление паттернов с помощью головы внимания, установите переключатель **Распознавание паттернов** в положение **Выключено**.

   При включенном переключателе служба Event Processor хранит выявленные паттерны в памяти программы. Если голова внимания не будет использована для выявления паттернов монитором или просмотра истории паттернов, рекомендуется выключить переключатель **Распознавание паттернов**.

7. Нажмите на кнопку **Сохранить**.

Удаление головы внимания

Функциональность доступна после добавления лицензионного ключа для коммерческой лицензии с процессором событий.

Чтобы удалить голову внимания:

1. В основном меню выберите раздел **Процессор событий → Мониторинг**.
2. На открывшейся странице нажмите на кнопку **Настройка конфигурации внимания**.

   Справа отобразится панель **Головы внимания**.
3. Нажмите на кнопку рядом с головой внимания, которую требуется удалить.
4. В открывшемся окне подтвердите удаление головы внимания.

Информация о голове внимания будет удалена из таблицы в панели **Головы внимания**. Паттерны, обнаруженные в соответствии с этой головой внимания, также будут удалены из Kaspersky MLAD.

Работа с мониторами

Функциональность доступна после добавления лицензионного ключа для коммерческой лицензии с процессором событий.

В разделе **Процессор событий → Мониторинг** вы можете управлять мониторами для отслеживания определенных событий, паттернов или значений параметров событий. С помощью мониторов вы также можете отслеживать обобщенные события или паттерны, а также события, поступившие в необычное для них время. Вы можете просматривать краткую статистику количества зарегистрированных активаций по каждому созданному монитору в виде гистограммы.

Работа с мониторами осуществляется на вкладке **Мониторы**, расположенной в правом верхнем углу раздела.

На вкладке отображаются все созданные в программе мониторы со следующей краткой информацией:

- Имя монитора.
- Значок статуса отправки оповещений об активациях монитора. Предусмотрены следующие значки:
  - – отображается, если отправка оповещений об активациях монитора включена.
  - – отображается, если отправка оповещений об активациях монитора выключена.
- Количество активаций монитора на скользящем окне.
- Тип подписки монитора. Для каждого монитора могут отображаться следующие значения:
  - **Значения параметров**. Монитор отслеживает появление определенных значений параметров событий.
  - **События**. Монитор отслеживает появление определенных событий.
  - **Эксфильтрация данных по DNS**. Монитор отслеживает признаки эксфильтрации данных в DNS-запросах. При активации монитора Kaspersky MLAD автоматически создает актив **DNS Exfiltration** и наполняет его тегами с именами в формате `<IP-адрес хоста, отправившего DNS-запрос>_<домен первого уровня в DNS-запросе>`. В качестве значений тегов указываются значения вероятностей, с которыми соответствующие DNS-запросы содержат признаки эксфильтрации.
  - **Часы активности**. Монитор отслеживает появление событий в необычное для них время.
  - **Паттерны**. Монитор отслеживает появление закономерностей в поведении объекта мониторинга.
  - **События головы внимания**. Монитор отслеживает появление событий в соответствии с параметрами конфигурации внимания.
  - **Уникальные обобщенные**. Монитор отслеживает появление уникальных обобщенных событий или паттернов.
  - **Похожие обобщенные**. Монитор отслеживает появление похожих обобщенных событий или паттернов.
- **Порог активации** – количество активаций монитора на скользящем окне, при достижении которого программа отправляет оповещение об активации монитора во внешнюю систему.
- **Период** – скользящее окно, за время которого ведется учет количества активаций монитора.

При необходимости вы можете просмотреть **подробную информацию о каждом мониторе**. Для этого нажмите на карточку нужного монитора.

- **Имя** – имя просматриваемого монитора.
- **Состояние** – параметр, определяющий состояние монитора. Возможные состояния: **Активен** или **Не активен**.
- **Отправка оповещений** – параметр, определяющий включена ли отправка оповещений об активациях монитора.
- **ID монитора** – идентификатор просматриваемого монитора.
- **Количество активаций** – количество зарегистрированных активаций монитора на скользящем окне.
- **Дата и время последней активации** – дата и время, когда монитор в последний раз был активирован.
- **Размер списка активаций** – параметр, величина которого определяет количество последних активаций монитора, отображаемых в таблице **Список активаций**.
- **Тип подписки** – параметр, определяющий что отслеживает просматриваемый монитор.
- **Отслеживание паттернов на слоях** – номера слоев, на которых отслеживаются паттерны. Этот параметр отображается только при активации монитора паттерном.
- **Скользящее окно** – параметр, определяющий интервал времени от текущего момента времени назад по временной последовательности, в течение которого ведется учет количества активаций. Окно сдвигается синхронно течению времени по временным меткам в событиях.
- **Порог активации** – количество активаций, которое должен зарегистрировать монитор на скользящем окне, прежде чем отправить во внешнюю систему оповещение об активации монитора с помощью коннектора CEF Connector.
- **Голова внимания** – голова внимания, на которой сфокусировано внимание процессора событий. Этот параметр отображается только для типов подписки **События головы внимания**, **Паттерны**, **Уникальные обобщенные**, **Похожие обобщенные** и **Часы активности**.
- **Параметр предмета внимания** – параметр предмета внимания, на котором сфокусировано внимание процессора событий. Этот параметр отображается только для типов подписки **События головы внимания**, **Паттерны**, **Уникальные обобщенные**, **Похожие обобщенные** и **Часы активности**.
- **Подписка на события** – параметр, определяющий, отслеживает ли монитор обобщенные события. Этот параметр отображается только для типов подписки **Уникальные обобщенные** и **Похожие обобщенные**.
- **Подписка на паттерны** – параметр, определяющий, отслеживает ли монитор обобщенные паттерны. Этот параметр отображается только для типов подписки **Уникальные обобщенные** и **Похожие обобщенные**.
- **Тип активации** – параметр, определяющий, отслеживает ли монитор только новые или новые и ранее выявленные значения параметров событий, события и паттерны. Этот параметр отображается только для типов подписки **Значения параметров**, **События**, **Паттерны**, **События головы внимания** и **Эксфильтрация данных по DNS**.
- **Фильтры** – таблица, содержащая информацию о фильтрах, используемых в мониторах с типом подписки для типов подписки **Значения параметров**, **События**, **Паттерны**, **События головы**

внимания или **Эксфильтрация данных по DNS**. Для каждого элемента отображаются следующие данные:

- **Имя параметра** – имя параметра события, за значениями которого наблюдает просматриваемый монитор.
  Для каждого объекта мониторинга поступающие события и их параметры индивидуальны. Имена параметров событий определяются в конфигурационном файле для службы Event Processor. Работы по созданию и загрузке файла конфигурации выполняет квалифицированный технический специалист Заказчика, сотрудник "Лаборатории Касперского" или сертифицированный интегратор на этапе настройки службы Event Processor.

- **Тип фильтра** – параметр, определяющий тип фильтра для параметров событий, по которым текущий монитор отслеживает значения параметров событий, события и паттерны. Для мониторов с подпиской на события справа от типа фильтра отображается значок ⚠, если появление значений параметров событий отслеживается отдельно с помощью дочерних мониторов (переключатель для параметра события установлен в положение **Отслеживать по каждому значению**).

- **Тип значения** – параметр, определяющий какие типы значений отслеживает просматриваемый монитор: значения по шаблону, определенные, новые (если переключатель **Тип активации** установлен в положение **Отслеживать только новые элементы**) или все значения.

- **Значения** – значения параметра события, за которыми наблюдает просматриваемый монитор.

- **Список активаций** – таблица, содержащая информацию о последних активациях монитора:

  - **ID значения параметра** – идентификатор значения параметра события, обнаружение которого вызвало активацию монитора. Этот параметр отображается только для типа подписки **Значения параметров**.

  - **ID события** – идентификатор события, обнаружение которого вызвало активацию монитора. Этот параметр отображается только для типов подписки **События**, **События головы внимания**, **Часы активности** и **Эксфильтрация данных по DNS**, а также **Уникальные обобщенные** и **Похожие обобщенные** с подпиской на события.

  - **ID паттерна** – идентификатор паттерна, обнаружение которого привело к активации монитора. Этот параметр отображается только для типов подписки **Паттерны**, а также **Уникальные обобщенные** и **Похожие обобщенные** с подпиской на паттерны.

  - **Системные параметры** – блок системных параметров, который содержит следующую информацию:

    - **Дата и время события** – дата и время обнаружения события в потоке событий.

    - **Интервал от предыдущего элемента** – временной интервал между текущим событием и предыдущим событием в потоке событий на скользящем окне. Kaspersky MLAD отображает временные интервалы между событиями при первом обнаружении паттерна, в состав которого входят события. При повторном обнаружении паттерна процессор событий учитывает указанный администратором коэффициент допустимой дисперсии интервалов между этими событиями.

    - **Общее количество активаций** – количество повторений события в потоке событий на скользящем окне.

    - **Количество параметров** – количество параметров события, для которых поступили значения от объекта мониторинга.

- **Последняя активация** – дата и время последнего обнаружения события в потоке событий на скользящем окне.

Этот блок параметров отображается только типов подписки **Значения параметров**, **События**, **События головы внимания**, **Часы активности** и **Эксфильтрация данных по DNS**, а также **Уникальные обобщенные** и **Похожие обобщенные** с подпиской на события.

- **Предмет внимания** – параметр предмета внимания и его значение, обнаружение которого вызвало активацию монитора. Этот параметр отображается только для типов подписки **Паттерны**, а также **Уникальные обобщенные** и **Похожие обобщенные** с подпиской на паттерны.

- **Дата и время активации** – дата и время активации монитора. Этот параметр отображается только для типов подписки **Паттерны**, а также **Уникальные обобщенные** и **Похожие обобщенные** с подпиской на паттерны.

- **Параметр события** – значение параметра события, поступившего от объекта мониторинга. Этот параметр отображается только для типа подписки **Значения параметров**.

- **Параметры события** – значения параметров события, поступивших от объекта мониторинга. Этот параметр отображается только для типов подписки **События**, **События головы внимания**, **Часы активности** и **Эксфильтрация данных по DNS**, а также **Уникальные обобщенные** и **Похожие обобщенные** с подпиской на события.

- **Количество событий** – количество событий, входящих в состав паттерна, который вызвал активацию монитора. Этот параметр отображается только для типов подписки **Паттерны**, а также **Уникальные обобщенные** и **Похожие обобщенные** с подпиской на паттерны.

- **Общее количество активаций** – количество повторений паттерна в потоке событий на скользящем окне. Этот параметр отображается только для типов подписки **Паттерны**, а также **Уникальные обобщенные** и **Похожие обобщенные** с подпиской на паттерны.

- **Эксфильтрация данных по DNS** – таблица, содержащая информацию о DNS-запросах, содержащих признаки эксфильтрации:

  - **Дата и время** – дата и время DNS-запроса.

  - **Хост** – IP-адрес хоста, отправившего DNS-запрос.

  - **Домен первого уровня** – домен первого уровня в DNS-запросе.

  - **DNS-запрос** – содержание DNS-запроса.

  - **Длина** – длина строки DNS-запроса без домена.

  - **Энтропия** – значение энтропии, рассчитанное для строки DNS-запроса без домена. Процессор событий учитывает значение энтропии при принятии решения, содержит ли DNS-запрос признаки эксфильтрации данных.

  - **Вероятность** – вероятность того, что DNS-запрос содержит признаки эксфильтрации данных.

  Эта таблица отображается только для мониторов с типом подписки **Эксфильтрация данных по DNS**.

- **Статистика по часам активности** – таблица, содержащая информацию об обнаружении событий в необычные для них часы активности:

- **Час активности (UTC)** – час активности в формате UTC.
- **Количество событий** – количество событий, которые были обнаружены в необычные для них часы активности.
- **Необычная активность** – признак, указывающий, является ли час активности необычным для поступивших событий.
- **Последнее событие в необычное время активности** – последнее событие, обнаруженное в необычный час активности.

Эта таблица отображается только для мониторов с типом подписки **Часы активности**.

- **Статистика по обобщенным событиям** – таблица, содержащая информацию об обобщенных событиях:
  - **ID события** – идентификатор обобщенного события.
  - **Количество активаций** – количество зарегистрированных активаций монитора на скользящем окне.
  - **Количество предметов внимания** – количество значений параметра предмета внимания, обнаружение которых вызвало активацию монитора.
  - **Событие** – обнаруженное обобщенное событие.
  - **Предметы внимания** – значения параметра предмета внимания, обнаружение которых вызвало активацию монитора.

  Эта таблица отображается только при активации монитора похожими обобщенными событиями.
- **Статистика по обобщенным паттернам** – таблица, содержащая информацию об обобщенных паттернах:
  - **ID паттерна** – идентификатор обобщенного паттерна.
  - **Количество активаций** – количество зарегистрированных активаций монитора на скользящем окне.
  - **Количество событий** – количество событий в составе обобщенного паттерна.
  - **Количество предметов внимания** – количество значений параметра предмета внимания, обнаружение которых вызвало активацию монитора.
  - **Длительность паттерна** – временной интервал между первым и последним событием в обнаруженном паттерне. При повторном обнаружении паттерна процессор событий учитывает указанный администратором коэффициент допустимой дисперсии интервалов между событиями паттерна.
  - **Паттерн** – обнаруженный обобщенный паттерн.
  - **Предметы внимания** – значения параметра предмета внимания, обнаружение которых вызвало активацию монитора.

  Эта таблица отображается только при активации монитора похожими обобщенными паттернами.

Просмотр гистограммы с краткой статистикой количества активаций осуществляется на вкладке **Гистограмма**, расположенной в правом верхнем углу раздела.

Создание монитора

Процессор событий формирует паттерны только по определенным направлениям, которые необходимо предварительно задать в конфигурации внимания. Перед работой с мониторами также необходимо настроить отображение параметров событий.

> Функциональность доступна после добавления лицензионного ключа для коммерческой лицензии с процессором событий.
> Предварительно требуется настроить службу Event Processor.

Чтобы создать монитор:

1. В основном меню выберите раздел **Процессор событий → Мониторинг**.
2. Нажмите на кнопку **Создать монитор**.

   Справа отобразится панель **Создание монитора**.
3. В поле **Имя** укажите имя монитора.
4. Если требуется выключить монитор, установите переключатель **Состояние** в положение **Не активен**.

   По умолчанию монитор включен.
5. Если требуется выключить отправку оповещений об активациях монитора во внешнюю систему через коннектор CEF Connector, установите переключатель **Отправка оповещений** в положение **Выключена**.

   По умолчанию отправка оповещений об активациях монитора включена.
6. В поле **Скользящее окно (сек.)** укажите интервал в секундах от текущего момента времени назад по временной последовательности, за который монитор будет обрабатывать поступившие значения параметров, события или паттерны.
7. В поле **Размер списка активаций** укажите количество активаций монитора, которое требуется отображать при просмотре информации о мониторе.

8. В блоке параметров **Тип подписки** выберите один из следующих вариантов:

- Если требуется отслеживать появление определенных событий, выберите **События**.
- Если требуется отслеживать появление определенных значений параметров событий, выберите **Значения параметров**.
- Если требуется отслеживать признаки эксфильтрации данных в DNS-запросах, выберите **Эксфильтрация данных по DNS**.

  Для работы этого монитора требуется предварительно файл с весами ML-модели, которую процессор событий использует для выявления признаков эксфильтрации данных в DNS-запросах, при настройке службы Event Processor.
- Если требуется отслеживать поступление событий в необычное для них время, выберите **Часы активности**.
- Если требуется отслеживать появление закономерностей в поведении объекта мониторинга, выберите **Паттерны**.
- Если требуется отслеживать появление событий в фокусе внимания, выберите **События головы внимания**.
- Если требуется отслеживать уникальные обобщенные события или паттерны, выберите **Уникальные обобщенные**.
- Если требуется отслеживать похожие обобщенные события или паттерны, выберите **Похожие обобщенные**.

9. В блоке параметров **Параметры активации** выполните следующие действия:

a. В поле **Порог активации** укажите количество активаций монитора на скользящем окне, после достижения которого монитор отправит оповещение во внешнюю систему.

Параметр отображается, если в блоке параметров **Тип подписки** был выбран вариант **Эксфильтрация данных по DNS**, **Значения параметров**, **События**, **Паттерны** или **События головы внимания**.

b. Если требуется отслеживать новые события, паттерны или значения параметров событий, установите переключатель **Тип активации** в положение **Отслеживать только новые элементы**.

Параметр отображается, если в блоке параметров **Тип подписки** был выбран вариант **Эксфильтрация данных по DNS**, **Значения параметров**, **События**, **Паттерны** или **События головы внимания**.

c. В раскрывающемся списке **Подписка на слои паттернов** выберите слои, на которых требуется отслеживать паттерны.

Если слои не выбраны, процессор событий отслеживает паттерны на всех уровнях вложенности.

Параметр отображается, если в блоке параметров **Тип подписки** был выбран вариант **Паттерны**.

d. В раскрывающемся списке **Голова внимания** выберите голову внимания для фокусировки внимания монитора на нужные направления развития поведения объекта мониторинга.

Параметр отображается, если в блоке параметров **Тип подписки** был выбран вариант **Часы активности**, **Паттерны**, **События головы внимания**, **Уникальные обобщенные** или **Похожие обобщенные**.

e. В поле **Подписка на события или паттерны** выберите один из следующих вариантов:

- Если требуется отслеживать обобщенные события, выберите **Подписка на события**.
- Если требуется отслеживать обобщенные паттерны, выберите **Подписка на паттерны**.

Параметр отображается, если в блоке параметров **Тип подписки** был выбран вариант **Уникальные обобщенные** или **Похожие обобщенные**.

10. В блоке параметров **Фильтры** выполните следующие действия для уточнения условий активации монитора:

    a. Если требуется задать условия для типов подписки **Паттерны** и **События головы внимания**, нажмите на кнопку **Добавить фильтр**.

    Для типов подписки **События** и **Значения параметров** необходимо задать хотя бы одно условие активации монитора, поэтому при выборе одного из этих типов подписки в блоке **Фильтры** уже отображается строка с одним условием.

    b. Выполните одно из следующих действий:

    - Если требуется отслеживать события по всем заданным значениям в рамках одного монитора, установите переключатель в положение **Отслеживать по всем значениям одновременно**.

    - Если требуется создать дочерние мониторы на каждое заданное значение параметра события, выбранного в раскрывающемся списке **Параметр события**, и отслеживать их появление отдельно, установите переключатель в положение **Отслеживать по каждому значению**.

    Переключатель отображается, если в блоке параметров **Тип подписки** был выбран вариант **События**.

    c. В раскрывающемся списке **Параметр события** выберите параметр события, по которому требуется уточнить условия активации монитора.

    d. В раскрывающемся списке **Тип фильтра** выберите одно из следующих значений:

    - **Внимание**, если требуется сфокусировать внимание процессора событий на выбранном параметре события.

      Это значение доступно для выбора, если для монитора выбрана голова внимания.

    - **Обобщенное внимание**, если на выбранном параметре требуется сфокусировать обобщенное внимание процессора событий.

      Это значение доступно для выбора, если для монитора выбрана голова внимания с обобщенным вниманием.

    - **Параметр**, если требуется активировать монитор при отслеживании конкретных значений параметра события.

    - **Обобщенный параметр**, если требуется активировать монитор при отслеживании обобщенных значений параметра события.

      Это значение доступно для выбора, если для монитора выбрана голова внимания с обобщением параметров условий.

    При уточнении условий активации монитора по параметрам события, заданных для выбранной головы внимания в качестве предмета внимания или условий к нему, этим параметрам события автоматически присваивается типы фильтров, заданные в выбранной голове внимания. Фильтрация значений параметров события будет выполняться относительно значений, отслеживаемых головой внимания.

    e. Выполните одно из следующих действий:

    - Если требуется включить во внимание все значения параметра события или обобщить их во внимании, в раскрывающемся списке **Тип значения** выберите **Все значения**.

    - Если требуется включить во внимание конкретное значение параметра события или обобщить это значение во внимании, в раскрывающемся списке **Тип значения** выберите **Определенные значения**

и введите нужное значение в поле **Значение**. Начните вводить нужное значение, чтобы все подходящие значения параметров отобразились в списке.

- Если требуется включить во внимание значения параметра события по шаблону или обобщить их во внимании, в раскрывающемся списке **Тип значения** выберите **Регулярное выражение** и введите шаблон значения с помощью регулярного выражения в поле **Значение**.

  В регулярных выражениях используется формат, поддерживаемый на языке программирования Python. Подробнее о популярных специальных символах регулярных выражений см. в Приложении.

- Если требуется включить во внимание новые значения параметра события или обобщить их во внимании, в раскрывающемся списке **Тип значения** выберите **Новые значения**.

  Этот тип значения доступен, если переключатель **Тип активации** установлен в положении **Отслеживать только новые элементы**.

Если требуется, вы можете задать более одного условия активации монитора. При необходимости вы можете удалить ранее добавленное условие нажатием на кнопку 🗑 напротив строки с нужным условием.

> Если в блоке параметров **Тип подписки** был выбран вариант **Эксфильтрация данных по DNS**, то в блоке **Фильтры** необходимо задать условия активации монитора как минимум по двум параметрам. Для первого условия фильтрации необходимо выбрать параметр события, по которому идентифицируется хост, отправивший DNS-запрос. Для второго условия фильтрации необходимо выбрать параметр события, соответствующий DNS-запросу.

11. Нажмите на кнопку **Сохранить**.

Новый монитор будет создан и отобразится на вкладке **Мониторинг**.

Изменение монитора

При необходимости вы можете включить или выключить использование монитора.

> Функциональность доступна после добавления лицензионного ключа для коммерческой лицензии с процессором событий.

Чтобы изменить монитор:

1. В основном меню выберите раздел **Процессор событий** → **Мониторинг**.
2. В вертикальном меню ⋮ нужной карточки монитора выберите пункт **Изменить**.
3. Если требуется, укажите новое имя монитора.
4. Если требуется изменить состояние монитора, выполните одно из следующих действий:
   - Если требуется использовать монитор, установите переключатель **Состояние** в положение **Активен**.
   - Если требуется выключить монитор, установите переключатель **Состояние** в положение **Не активен**.

5. Если требуется включить или выключить отправку оповещений об активациях монитора, выполните одно из следующих действий:

   - Если требуется включить отправку оповещений об активациях монитора, установите переключатель **Отправка оповещений** в положение **Включена**.
   - Если требуется выключить отправку оповещений об активациях монитора, установите переключатель **Отправка оповещений** в положение **Выключена**.

6. Нажмите на кнопку **Сохранить**.

Удаление монитора

Функциональность доступна после добавления лицензионного ключа для коммерческой лицензии с процессором событий.

Чтобы удалить монитор:

1. В основном меню выберите раздел **Процессор событий** → **Мониторинг**.
2. В вертикальном меню ⋮ нужной карточки монитора выберите пункт **Удалить**.
3. Подтвердите удаление монитора.

   Монитор будет удален.

Просмотр истории событий

Kaspersky MLAD позволяет просматривать события и, которые поступили от внешних источников событий. Для просмотра событий требуется загрузить их в разделе **Процессор событий** → **История событий**. При загрузке истории процессор событий также отобразит обобщенные события, соответствующие заданным критериям фильтрации.

Перед просмотром событий необходимо настроить параметры отображения событий и конфигурацию внимания.

Функциональность доступна после добавления лицензионного ключа для коммерческой лицензии с процессором событий.

Вы можете просматривать **информацию о выявленных событиях** в виде таблицы.

- **ID события** – идентификатор выявленного события.
- **Системные параметры** – параметр, содержащий следующую информацию о событии:
  - **Последнее обнаружение в интервале** – дата и время последнего обнаружения события в потоке событий за заданный период.
  - **Количество обнаружений в интервале** – количество обнаружений события в потоке событий за заданный период.
  - **Общее количество активаций** – количество повторений события в потоке событий на скользящем окне.
  - **Последняя активация** – дата и время последнего обнаружения события в потоке событий.
  - **Количество параметров** – количество параметров события, для которых поступили значения от объекта мониторинга.
- **Параметры события** – значения параметров события, поступивших от объекта мониторинга.

Kaspersky MLAD также отображает поступившие события в виде графа отношений параметров событий. Вершины графа соответствуют значениям параметров событий, а дуги между вершинами графа соответствуют связям между значениями параметров поступивших событий. Вы можете навести курсор мыши на граф события и просмотреть информацию о параметрах событий и их значениях. Вы также можете навести курсор мыши на дугу графа события и просмотреть информацию о количестве связей между значениями параметров событий. Граф отношений параметров событий отображается на вкладке **Граф**.

Для каждого объекта мониторинга поступающие события и их параметры индивидуальны. Список параметров событий определяется в конфигурационном файле для службы Event Processor. Работы по созданию и загрузке файла конфигурации выполняет системный администратор на этапе настройки службы Event Processor.

Чтобы загрузить данные для просмотра поступивших событий:

1. В основном меню выберите раздел **Процессор событий** → **История событий**.

2. В блоке параметров **Фильтры** выполните следующие действия:

   a. Выберите даты и время начала и окончания периода, за который вы хотите загрузить и просмотреть события, нажав на кнопку .

   b. Если требуется просмотреть конкретные события, в раскрывающемся списке **ID события** выберите один или несколько идентификаторов событий, которые требуется просмотреть. Начните вводить идентификатор, чтобы все подходящие события отобразились в списке.

   Идентификаторы событий вы можете заранее просмотреть, например, в таблице **Список активаций** при просмотре монитора.

   c. Для настройки параметров событий выполните одно из следующих действий:

   - Если вы хотите загрузить события по конкретным значениям параметров событий, в раскрывающихся списках выберите значение соответствующего параметра события. Начните вводить нужное значение, чтобы все подходящие значения параметров отобразились в списках.

   - Если вы хотите загрузить события по шаблону значений, нажмите на кнопку .* в ячейках нужных параметров события, в раскрывающихся списках введите шаблон значения с помощью регулярного выражения и выберите указанный шаблон значения.

     В регулярных выражениях используется формат, поддерживаемый на языке программирования Python. Подробнее о популярных специальных символах регулярных выражений см. в Приложении.

   Для каждого объекта мониторинга количество и имена параметров событий индивидуальны.

3. Нажмите на кнопку **Выполнить запрос**.

   В центральной части страницы в виде графа отобразятся данные о найденных программой событиях.

4. Если требуется просмотреть полученные события в виде таблицы, выберите вкладку **Таблица**.

   В центральной части страницы отобразится таблица, которая содержит информацию о выявленных событиях.

Просмотр истории паттернов

В разделе **Процессор событий** → **История паттернов** вы можете просматривать структуру устойчиво повторяющихся и/или новых паттернов.

Процессор событий формирует паттерны только по определенным направлениям, которые необходимо предварительно задать в конфигурации внимания. Перед просмотром паттернов также необходимо настроить отображение параметров событий.

Функциональность доступна после добавления лицензионного ключа для коммерческой лицензии с процессором событий.

Вы можете просматривать структуру выявленных паттернов до уровня событий. Процессор событий представляет паттерны, события и значения параметров событий как послойную иерархию вложенных элементов. Например, паттерн четвертого слоя состоит из вложенных паттернов третьего слоя, в свою очередь паттерн третьего слоя состоит из паттернов второго слоя, а паттерн второго слоя состоит из событий – элементов первого слоя. Значения параметров события являются элементами нулевого терминального слоя.

Для каждого объекта мониторинга поступающие события и их параметры индивидуальны. Список параметров событий определяется в файле конфигурации для службы Event Processor. Работы по созданию и загрузке файла конфигурации выполняет системный администратор на этапе настройки службы Event Processor.

Чтобы просмотреть зарегистрированные паттерны:

1. В основном меню выберите раздел **Процессор событий** → **История паттернов**.
2. В блоке параметров **Фильтры** настройте следующие параметры отображения паттернов на странице:
   a. В раскрывающемся списке **Интервал истории** выберите даты и время начала и окончания периода, за который вы хотите загрузить и просмотреть паттерны, нажав на кнопку .
   b. В раскрывающемся списке **Тип паттернов** выберите одно из следующих значений:
      - **Стабильные** – паттерны, которые были зарегистрированы службой Event Processor два и более раза.
      - **Новые** – новые паттерны, зарегистрированные службой Event Processor впервые.
      - **Все** – все паттерны, зарегистрированные службой Event Processor.
   c. В раскрывающемся списке **Голова внимания** выберите голову внимания, по которой требуется просмотреть зарегистрированные паттерны.

      Требуется выбрать одну из голов внимания, заданных при настройке конфигурации внимания. Если вы выбрали голову внимания с обобщенным вниманием и обобщенными параметрами условий, при загрузке истории отобразятся обобщенные паттерны, соответствующие критериям фильтрации.
   d. Для настройки параметров событий выполните одно из следующих действий:
      - Если вы хотите просматривать паттерны по конкретным значениям параметров событий, в раскрывающихся списках выберите значение параметра события. Начните вводить нужное значение, чтобы все подходящие значения параметров отобразились в списках.
      - Если вы хотите просматривать паттерны по шаблону значений, нажмите на кнопку .* в ячейках нужных параметров события, в раскрывающихся списках введите шаблон значения с помощью регулярного выражения и выберите указанный шаблон значения.

        В регулярных выражениях используется формат, поддерживаемый на языке программирования Python. Подробнее о популярных специальных символах регулярных выражений см. в Приложении.

   Для правильного выполнения запроса требуется ввести значения для параметра события, на котором сфокусировано внимание модели. Если в параметре события, на котором сфокусировано внимание, задано несколько значений, процессор событий сформирует паттерны для каждого значения параметра.

   Параметры событий, заданные в качестве обобщенных в выбранной голове внимания, недоступны для настройки.

3. Нажмите на кнопку **Выполнить запрос**.

   В центральной части страницы отобразится таблица, которая содержит **данные о зарегистрированных паттернах**.

   - **ID паттерна** – идентификатор паттерна. Число в начале идентификатора паттерна до знака нижнего подчеркивания соответствует номеру слоя, на котором этот паттерн был обнаружен.
   - **Последнее обнаружение в интервале** – дата и время последнего обнаружения паттерна в потоке событий объекта мониторинга за заданный период.
   - **Количество обнаружений в интервале** – количество обнаружений паттерна в потоке событий объекта мониторинга за заданный период.
   - **Количество событий** – количество событий, составляющих паттерн.
   - **Последняя активация** – дата и время последнего обнаружения паттерна в потоке событий объекта мониторинга или в режиме сна.

4. Если требуется перейти к просмотру структуры паттерна, нажмите на нужную строку паттерна.

   Откроется страница с **подробной информацией о паттерне**.

- **ID паттерна** – идентификатор выбранного паттерна. Число в начале идентификатора паттерна до знака нижнего подчеркивания соответствует номеру слоя, на котором этот паттерн был обнаружен.

- **Общее количество активаций** – количество обнаружений выбранного паттерна в потоке событий за заданный период.

- **Интервал от предыдущего элемента** – временной интервал между выбранным паттерном и паттерном, выявленным в последовательности паттернов на текущем слое до выбранного паттерна. Kaspersky MLAD отображает временные интервалы между элементами выбранного паттерна при его первом обнаружении. При повторном обнаружении паттерна процессор событий учитывает указанный администратором коэффициент допустимой дисперсии интервалов между элементами этого паттерна.

- **Количество событий** – количество событий, составляющих паттерн.

- **Время окончания паттерна** – дата и время окончания выбранного паттерна в последовательности паттернов на текущем слое.

- **Последняя активация** – дата и время последнего обнаружения паттерна в потоке событий или в режиме сна.

- **Паттерны** – вкладка, содержащая таблицу с информацией о паттернах, входящих в состав выбранного паттерна. На вкладке **Паттерны** отображаются следующие данные:

  - **ID паттерна** – идентификатор вложенного паттерна. Число в начале идентификатора паттерна до знака нижнего подчеркивания соответствует номеру слоя, на котором этот паттерн был обнаружен.

  - **Время окончания паттерна** – дата и время окончания вложенного паттерна в последовательности паттернов на выбранном слое.

  - **Общее количество активаций** – количество обнаружений вложенного паттерна в структуре выбранного паттерна.

  - **Количество событий** – количество событий, составляющих вложенный паттерн.

  - **Интервал от предыдущего элемента** – временной интервал между вложенным паттерном и предыдущим паттерном в таблице. Kaspersky MLAD отображает временные интервалы между элементами вложенного паттерна при его первом обнаружении. При повторном обнаружении паттерна процессор событий учитывает указанный администратором коэффициент допустимой дисперсии интервалов между элементами этого паттерна.

  - **Последняя активация** – дата и время последнего обнаружения вложенного паттерна в последовательности паттернов на выбранном слое или в режиме сна.

- **События** – вкладка, содержащая таблицу событий, входящих в состав выбранного паттерна. Для каждого события отображаются следующие данные:

  - **ID события** – идентификатор события.

  - **Системные параметры** – параметр, содержащий следующую информацию о событии:

    - **Дата и время события** – дата и время обнаружения события в структуре паттерна.

- **Интервал от предыдущего элемента** – временной интервал между текущим событием и предыдущим событием в таблице. Kaspersky MLAD отображает временные интервалы между событиями выбранного паттерна при его первом обнаружении. При повторном обнаружении паттерна процессор событий учитывает указанный администратором коэффициент допустимой дисперсии интервалов между событиями этого паттерна.
- **Общее количество активаций** – количество повторений события в структуре выбранного паттерна за заданный период.
- **Количество параметров** – количество параметров события, для которых поступили значения от объекта мониторинга.
- **Последняя активация** – дата и время последнего обнаружения события в потоке событий.

- **Параметры события** – значения параметров события, поступившего от объекта мониторинга.

5. Для просмотра структуры паттерна выполните одно из следующих действий:

- Если требуется посмотреть структуру определенного вложенного паттерна, на вкладке **Паттерны** блока **Вложенные элементы** нажмите на нужную строку паттерна.

  Вы можете вернуться к просмотру структуры паттерна верхнего уровня вложенности, нажав на идентификатор нужного паттерна над блоком **Информация о паттерне**.

- Если требуется просмотреть события, составляющие паттерн на втором уровне вложенности, нажмите на вкладку **События**.

Kaspersky MLAD отображает структуру паттерна с верхнего уровня вложенности.

Управление инцидентами и группами инцидентов

Веб-интерфейс Kaspersky MLAD предоставляет возможность исследования зарегистрированных инцидентов. В зависимости от типа источника зарегистрированного инцидента информация об инциденте и методы его исследования могут отличаться.

Функциональность доступна после добавления лицензионного ключа.

Для любого инцидента вы можете выполнить следующие действия:

- Изучить детали инцидента.
- Выяснить, были ли ранее обнаружены похожие инциденты.
- Исследовать поведение объекта мониторинга в момент обнаружения инцидента.
- Оставить комментарии или экспертные рекомендации к зарегистрированному инциденту или к группе инцидентов.

В разделе **Инциденты** в виде столбчатой диаграммы отображаются инциденты, которые соответствуют критериям фильтрации, установленным под диаграммой. Диаграмма отображает статистику по зарегистрированным инцидентам за период, установленный над диаграммой.

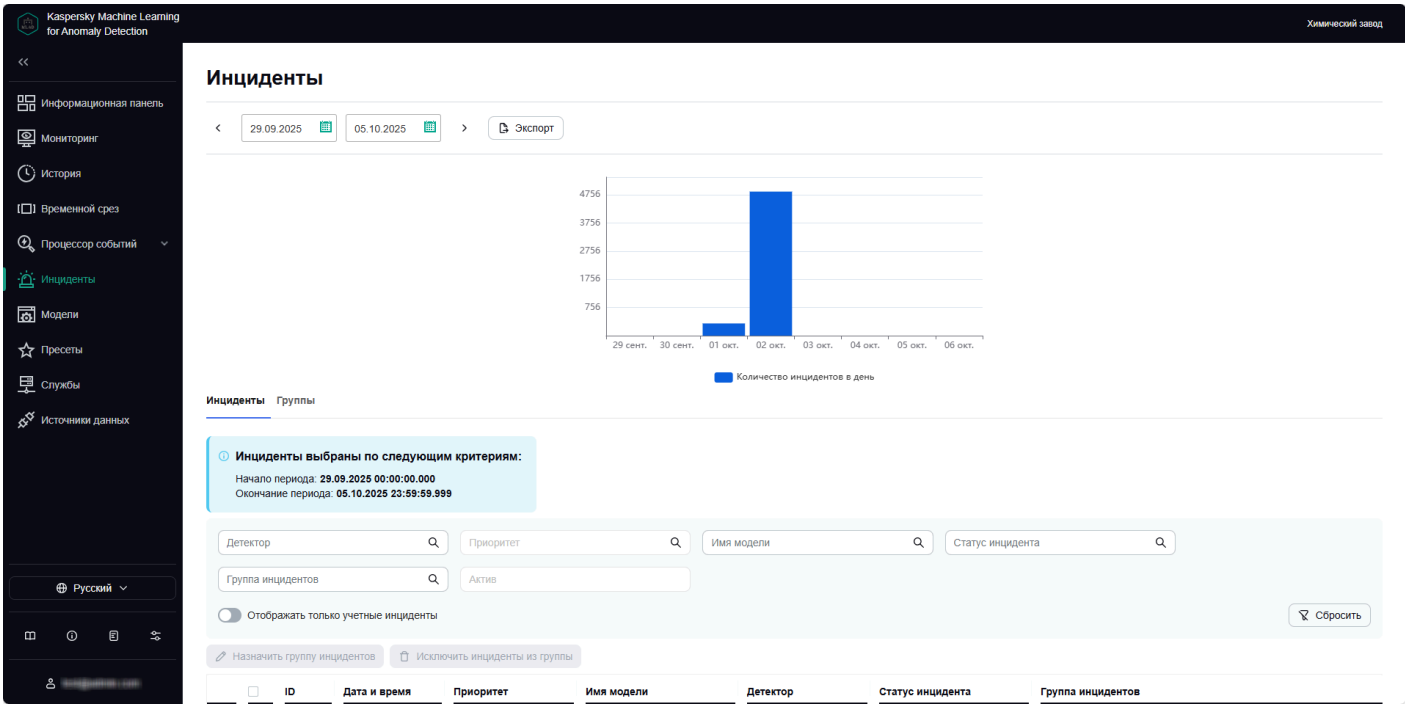
Диаграмма может отображать не более 60 столбцов. Если длительность заданного периода не превышает 60 дней, то инциденты на диаграмме сгруппированы по дням. Если длительность заданного периода составляет от 60 дней до 60 недель, то инциденты на диаграмме сгруппированы по неделям. В случае, когда длительность заданного периода составляет больше 60 недель, инциденты на диаграмме сгруппированы по месяцам.

При наведении курсора мыши на столбец диаграммы отображается окно с указанием количества зарегистрированных инцидентов за единицу времени, соответствующую группировке инцидентов на диаграмме. При нажатии на столбец на диаграмме и в таблице ниже отображается информация об инцидентах, зарегистрированных в период, соответствующий интервалу времени выбранного столбца.

В этом разделе вы можете просматривать как отдельные инциденты, так и группы инцидентов.

Вкладка Инциденты

На вкладке **Инциденты** представлена таблица зарегистрированных инцидентов. Инциденты отсортированы в порядке убывания даты: первыми показаны самые новые инциденты.



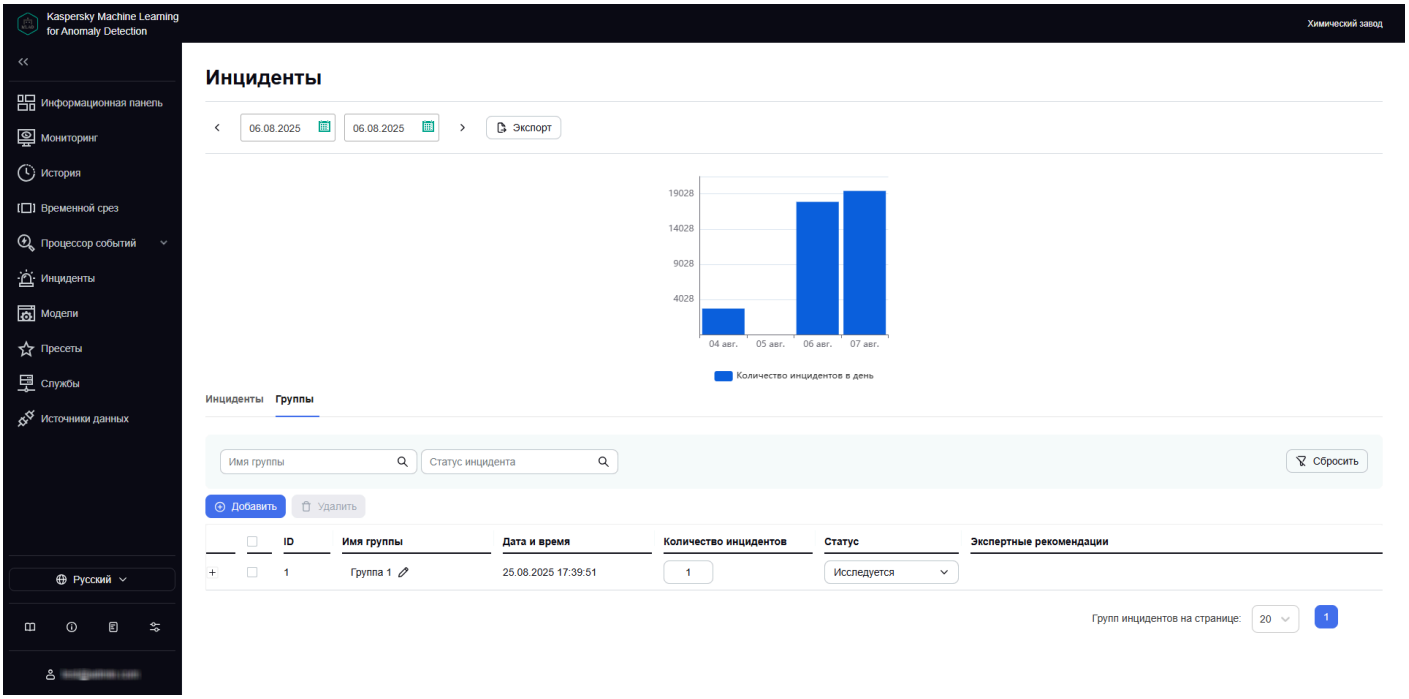
Вкладка **Инциденты**

Вы можете перейти в раздел **История**, нажав на дату и время начала инцидента.

Вкладка Группы

На вкладке **Группы** представлена таблица групп инцидентов. Вы также можете создавать группы самостоятельно и наполнять их нужными инцидентами. Kaspersky MLAD также может автоматически формировать группы похожих инцидентов.

Вы можете изменить имя группы и установить статус инцидентов, которые входят в эту группу. Также вы можете указать экспертные рекомендации, содержащие, например, рекомендуемые действия при возникновении новых инцидентов в этой группе.



Вкладка **Группы**

Об инцидентах

Инцидент – это обнаруженное отклонение от ожидаемого (нормального) поведения объекта мониторинга.

В Kaspersky MLAD поддерживает регистрацию инцидентов для следующих источников:

- Элементы ML-моделей. Инцидент регистрируется при достижении значения артефакта элемента ML-модели порога регистрации инцидентов, заданного для этого элемента. Инциденты могут быть зарегистрированы предиктивными элементами ML-модели, элементами на основе диагностических правил и элементами на основе эллиптического конверта.

  В зависимости от заданных параметров элемента ML-модели инцидент может быть зарегистрирован не сразу после достижения заданного порога. При достижении порога регистрации инцидента элемент ML-модели наблюдает за аномальным поведением объекта мониторинга в течение интервала времени, заданного в параметрах соответствующего элемента. Если аномальное поведение объекта мониторинга сохранялось в течение некоторой заданной доли времени от этого интервала, тогда элемент ML-модели регистрирует инцидент.

  Kaspersky MLAD может подавлять регистрацию следующих друг за другом инцидентов от одного и того же элемента ML-модели, если они произошли вскоре после первого инцидента в серии. Для этого используется параметр **Период подавления повторных срабатываний (сек.)**, который вы можете задать в параметрах соответствующего элемента.

  Элемент ML-модели также может повторно регистрировать один и тот же инцидент вплоть до исчезновения аномального поведения. Вы можете регулировать частоту регистрации повторных инцидентов с помощью параметров **Период напоминания (сек.)** путем изменения соответствующего элемента.

- Детектор Limit Detector. Инцидент регистрируется при достижении значения тега верхнего или нижнего порога блокировки.

- Служба Stream Processor. Инцидент регистрируется при обнаружении потерь данных телеметрии или поступлении наблюдений в Kaspersky MLAD слишком рано или поздно.

При обнаружении отклонения соответствующий источник фиксирует дату, время, релевантные параметры отклонения и сохраняет их в виде записи в разделе **Инциденты**. Если в Kaspersky MLAD для пользователей или внешних систем созданы подписки на уведомления об инцидентах, то информация об инциденте отправляется адресатам через соответствующие службы Kaspersky MLAD.

Об инцидентах, обнаруженных предиктивным элементом ML-модели

Предиктивный элемент ML-модели обучен на определенном подмножестве тегов и может прогнозировать поведение тегов в текущий момент. Инцидентом в этом случае считается существенное расхождение между наблюдаемыми (фактическими) значениями тегов и прогнозируемыми значениями тегов, полученными в результате работы элемента ML-модели. В параметрах элемента модели вы можете просмотреть, какие теги анализируются элементом ML-модели (входные теги) и поведение каких тегов прогнозируется (выходные теги).

ML-модель может включать в себя один или несколько элементов, функционирующих параллельно. В разделах **История** и **Мониторинг** вы можете выбрать определенный элемент ML-модели для отображения инцидентов, зарегистрированных этим элементом модели. Зарегистрированные инциденты отображаются в нижней части графика артефакта элемента ML-модели в виде цветных точек-индикаторов.

На графике артефакта отображается общая ошибка прогноза выбранного элемента ML-модели. *Общая ошибка прогноза* – это показатель отличия прогнозируемых значений от фактических, суммарно по всем тегам, включенным в выбранный элемент ML-модели. Чем выше значение ошибки прогноза, тем сильнее поведение тегов отличается от ожидаемого (нормального). *Порог ошибки прогноза* – это критический уровень значения общей ошибки прогноза, при достижении которого предиктивный элемент ML-модели регистрирует инцидент. Общая ошибка прогноза на графике артефакта отображается в виде красной линии, а порог ошибки прогноза отображается в виде оранжевой линии. Область графика, в которой ошибка прогноза превышает заданный порог, окрашивается в красный цвет.

График артефакта элемента ML-модели отображается в нижней части раздела **История** (см. рисунок ниже).

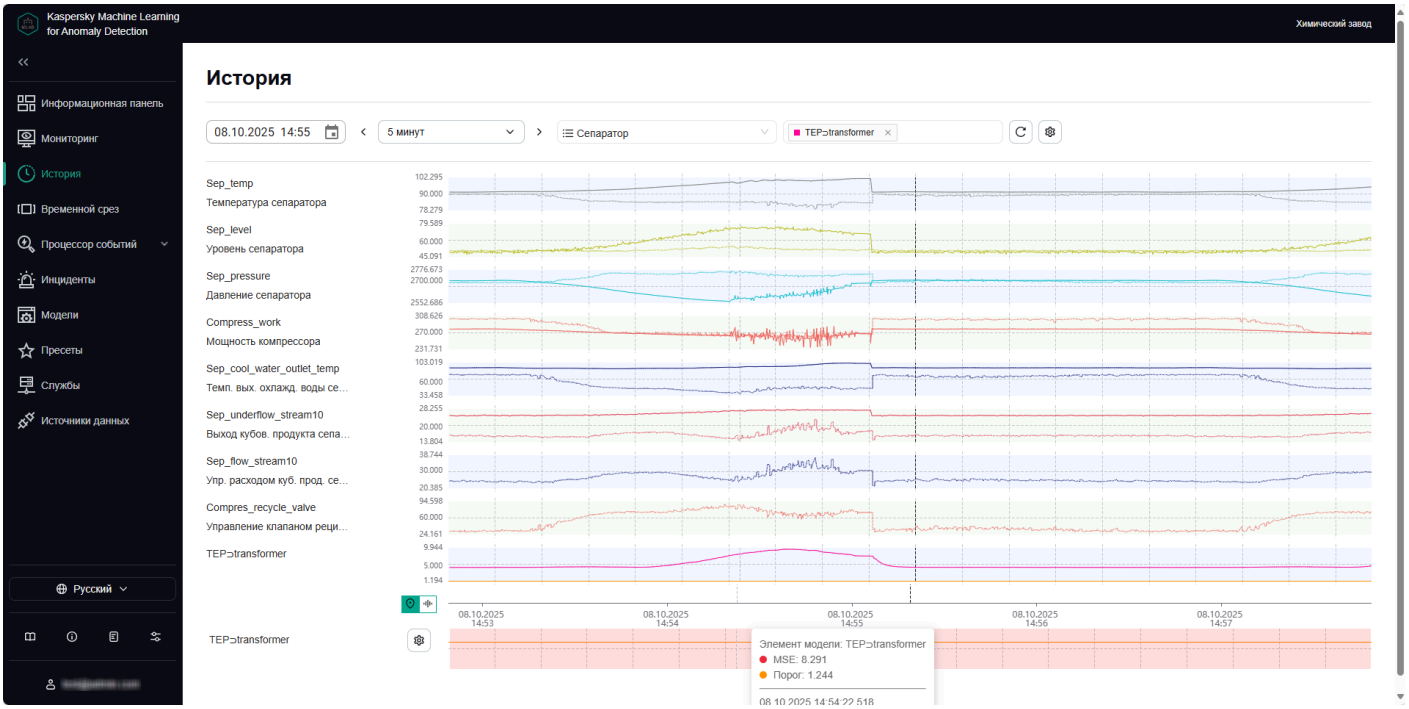


График артефакта элемента ML-модели в разделе **История**

Для каждого инцидента автоматически определяются теги с наибольшими отклонениями фактических значений от прогнозируемых ML-моделью. Из этих тегов формируется динамический пресет по инциденту, который отображается в разделе **История** при переходе в него из таблицы инцидентов по нажатию на дату и время начала конкретного инцидента. Теги в составе динамического пресета по инциденту отсортированы в порядке убывания отклонения их поведения от ожидаемого. Тег с наибольшим отклонением от прогнозируемого значения выводится в таблице инцидентов в разделе **Инциденты**. В таблице инцидентов также указывается порог ошибки прогноза и фактическое значение ошибки прогноза в момент регистрации инцидента.

Информация, полученная при просмотре динамического пресета по инциденту, не является диагностической с точки зрения определения причин инцидента, но ее можно использовать при анализе значений тегов с наибольшими отклонениями в поведении. Тег, поведение которого первым отклонилось от нормы и повлекло дальнейшие отклонения в других тегах, является тегом-причиной. В некоторых случаях тег-причина может находиться не на первом месте в динамическом пресете по инциденту или отсутствовать в нем. Это может произойти по следующим причинам:

- Незначительные по амплитуде изменения в поведении тега-причины произвели мультипликативный эффект и вызвали существенные отклонения других тегов, которые попали в динамический пресет по инциденту.

- Тег-причина не анализируется ML-моделью, и Kaspersky MLAD регистрирует вторичные изменения поведения тегов, вызванные отклонением тега-причины.

- Изменения в поведении тега-причины имели отложенный эффект, и к моменту возникновения аномалии в работе объекта мониторинга поведение тега-причины вернулось в нормальный режим.

Об инцидентах, обнаруженных элементом ML-модели на основе диагностического правила

ML-модель может включать в себя один или несколько элементов на основе диагностических правил. Артефакт диагностического правила рассчитывается в каждом узле РИВС и может принимать следующие значения:

- Значение `0`. Диагностическое правило в текущий момент не сработало.
- Значение `1`. Диагностическое правило в текущий момент сработало.
- В отдельных случаях артефакт диагностического правила может принимать произвольное значение. Например, если в правиле определены вычислимые теги, но отсутствуют условия на поведение тегов, артефакт правила примет значение последнего из сконфигурированных в правиле вычислимых тегов.

Порог регистрации инцидентов для диагностического правила по умолчанию равен единице. Вы можете изменить порог в параметрах правила. Это может быть необходимо, если артефакт правила принимает произвольные (небинарные) значения.

По каждому инциденту, зарегистрированному диагностическим правилом, автоматически формируется динамический пресет, который доступен для выбора в разделе **История** при переходе в него из таблицы инцидентов по нажатию на дату и время начала конкретного инцидента. В составе этого пресета присутствует значение артефакта диагностического правила, а также входящие теги в составе этого правила. Вычислимые теги, определенные в составе правила, на графиках не отображаются.

Об инцидентах, обнаруженных элементом ML-модели на основе эллиптического конверта

Эллиптический конверт ML-модели обучен на определенном подмножестве тегов и может выявлять выбросы (аномалии) в наборе данных. В результате обучения ML-модели в фазовом пространстве формируется эллиптическая область такая, что состояния, попадающими в эту область, считаются нормальными. При выявлении состояний, удаление которых от центра эллиптической области сравнялось или превысило установленный порог, элемент на основе эллиптического конверта регистрирует инцидент. В параметрах элемента модели вы можете просмотреть, какие теги анализируются элементом (параметр **Входные теги**).

Для каждого инцидента, зарегистрированного элементом на основе эллиптического конверта, автоматически определяются теги, при исключении которых из состава ML-модели наблюдаются наименьшие отклонения от нормального состояния. Из этих тегов формируется динамический пресет по инциденту, который доступен для выбора в разделе **История** при переходе в него из таблицы инцидентов по нажатию на дату и время начала конкретного инцидента. Теги в составе динамического пресета по инциденту отсортированы в порядке убывания отклонения их поведения от ожидаемого. Тег с наибольшим влиянием на регистрацию инцидента выводится в таблице инцидентов в разделе **Инциденты**.

ML-модель может включать в себя один или несколько элементов ML-модели, функционирующих параллельно. В разделах **История** и **Мониторинг** вы можете выбрать определенный элемент ML-модели для отображения инцидентов, зарегистрированных в результате работы определенного элемента модели. Зарегистрированные инциденты отображаются в нижней части графика артефакта элемента ML-модели в виде цветных точек-индикаторов.

Об инцидентах, обнаруженных детектором Limit Detector

Если включен детектор *Limit Detector*, то при использовании любой ML-модели Kaspersky MLAD автоматически отслеживает все теги, для которых указаны пороги блокировки тега. Пороги блокировки могут быть указаны в конфигурации тегов, импортируемой в Kaspersky MLAD в начале работы. Вы можете изменить пороги блокировки тега в веб-интерфейсе программы.

Для визуального контроля положения графика тега относительно порогов блокировки на единичных графических областях в разделах **История** и **Мониторинг** вы можете включить функции **Пороги блокировки** и **Всегда показывать пороги блокировки**. Если функция **Всегда показывать пороги блокировки** выключена, то верхняя или нижняя пороговая линия отображается только, если значения тега достигали соответствующего порога на промежутке времени, который в настоящий момент выводится на экране. Детектор Limit Detector определяет и регистрирует события независимо от работы функции **Всегда показывать пороги блокировки**.

В момент, когда значение тега достигает верхнего или нижнего порога блокировки, детектор Limit Detector регистрирует инцидент. Этот тег отображается в таблице инцидентов в разделе **Инциденты**. В таблице инцидентов указаны также пороги блокировки тега и фактическое значение тега, нарушившего один их этих порогов. По каждому инциденту, зарегистрированному детектором Limit Detector, автоматически формируется динамический пресет, который доступен для выбора в разделе **История** при переходе в него из таблицы инцидентов по нажатию на дату и время начала конкретного инцидента. В состав этого пресета включается единственный тег-причина возникновения инцидента.

Об инцидентах, обнаруженных службой Stream Processor

Служба *Stream Processor* собирает данные телеметрии, поступающие от объекта мониторинга в произвольные моменты реального времени, и приводит их к равноинтервальной временной сетке (далее также "РИВС"). При анализе поступающих данных служба Stream Processor может обнаруживать потери данных телеметрии, а также наблюдения, поступившие в Kaspersky MLAD слишком рано или поздно. В таких случаях служба Stream Processor регистрирует инцидент.

Инциденты, обнаруженные службой Stream Processor, отображаются в таблице инцидентов раздела **Инциденты**. Каждому инциденту, зарегистрированному службой Stream Processor, автоматически присваивается один из следующих типов инцидента:

- **Нет данных** – в случае прекращения или прерывания входного потока данных определенного тега.
- **Сбой часов** – в случае обнаружения наблюдений, поступивших в Kaspersky MLAD слишком рано.
- **Позднее поступление наблюдения** – в случае обнаружения наблюдений, поступивших в Kaspersky MLAD поздно.

Служба Stream Processor передает данные, приведенные к РИВС, в ML-модель службы Anomaly Detector.

Об аномалиях

Аномалия – это нештатное, не предусмотренное регламентом работы и не обусловленное производственным процессом отклонение в поведении объекта мониторинга.

Kaspersky MLAD регистрирует только инциденты. Является тот или иной инцидент аномалией определяет специалист АСУ ТП после проведения анализа зарегистрированных программой инцидентов. В результате анализа инцидента может быть сделан один из следующих выводов:

- Инцидент является аномалией, требующей ответных действий со стороны специалиста АСУ ТП.
- Инцидент не является аномалией, это ложно-положительное срабатывание ML-модели.

  При устойчивом повторном ложно-положительном срабатывании ML-модели нужно определить причину ухудшения качества работы используемой ML-модели, скорректировать параметры ML-модели и/или ее элементов или дополнительно обучить элементы ML-модели.
- ML-модель отработала правильно, но инцидент не является аномалией.

  Инцидент является следствием временного перевода объекта мониторинга в нетипичный режим функционирования (профилактика, испытания) или кратковременного влияния нетипичных внешних факторов (необычных погодных условий, запуска соседней установки). В такой ситуации ответных действий со стороны специалиста АСУ ТП не требуется.

Анализ и оценка инцидентов производится предметным экспертом. В некоторых случаях (при регистрации инцидентов, выявленных диагностическими правилами, или инцидентов, случившихся повторно) возможна автоматическая оценка и группирование похожих инцидентов.

ML-модель может не обнаружить объективно существовавшую аномалию. В этом случае аномалия не будет соответствовать ни одному из зарегистрированных инцидентов и не отразится в истории Kaspersky MLAD. Если из наблюдений эксперта, специалиста АСУ ТП или сторонних источников станет известно о неоднократных фактах отсутствия срабатывания ML-модели, необходимо определить причину ухудшения качества работы ML-модели, скорректировать параметры ML-модели и/или ее элементов и провести дополнительное обучение элементов ML-модели.

На аномалию в работе объекта мониторинга также могут указывать новые события, паттерны и значения параметров событий, обнаруженные службой Event Processor (далее также "процессор событий") в потоке поступающих событий. При обнаружении новых событий, паттернов или значений параметров событий служба Event Processor не регистрирует инциденты. Для просмотра новых обнаружений в разделе **Процессор событий** вы можете просмотреть историю регистрации паттернов, выполнив фильтрацию по типу **Новые**. Вы также можете создать монитор для отслеживания новых событий, паттернов или значений параметров событий. Служба Event Processor активирует монитор при каждом выявлении событий, паттернов или значений параметров событий, соответствующих заданным критериям поиска. При достижении заданного порога количества активаций монитора на скользящем окне служба Event Processor отправит оповещение об активации монитора во внешнюю систему с помощью коннектора CEF Connector.

Сценарий: анализ инцидентов

В этом разделе приводится последовательность действий, которые требуется выполнить при анализе зарегистрированных Kaspersky MLAD инцидентов.

Функциональность доступна после добавления лицензионного ключа.

Описанный в этом разделе сценарий анализа инцидентов не является четко регламентированным процессом. Состав и порядок действий, предпринимаемых для исследования инцидента и выявления причины его возникновения, зависят от предметной области, уровня знаний технолога или специалиста АСУ ТП, исследующего инцидент, а также наличия дополнительной информации об объекте мониторинга.

Сценарий анализа инцидентов состоит из следующих этапов:

1. **Просмотр информации о зарегистрированном инциденте**

   В разделе **Инциденты** отображаются все зарегистрированные Kaspersky MLAD инциденты, а также подробная информация о времени их начала, ML-модели, которая зарегистрировала инцидент, и экспертные рекомендации, если они были добавлены. Вы можете перейти к просмотру информации об инцидентах одним из следующих способов:

   - **Просмотр последних инцидентов в разделе Информационная панель**

     Если вы хотите просмотреть недавно обнаруженный инцидент, в разделе **Информационная панель** найдите интересующий вас инцидента в таблице **Последние инциденты**. Для просмотра подробной информации об инциденте нажмите на кнопку `+`.

   - **Просмотр инцидентов в разделе Инциденты**

     Если вам известны дата и время начала инцидента, в разделе **Инциденты** выберите соответствующий период и при необходимости отфильтруйте инциденты. Вы можете изменить интервал времени, в котором отображаются инциденты, используя столбчатую диаграмму или поле выбора даты в верхней части страницы. Для просмотра подробной информации об инциденте нажмите на кнопку `+`.

   - **Переход из раздела История или Мониторинг**

     В разделе **История** или **Мониторинг** в нижней части страницы нажмите на точку-индикатор в блоке графика артефакта элемента ML-модели для просмотра определенного инцидента. Откроется раздел **Инциденты**, в котором отобразятся только те инциденты выбранных для просмотра элементов, которые были зарегистрированы в период, представленный выбранной точкой-индикатором (период указан над таблицей инцидентов). Для просмотра подробной информации об инциденте нажмите на кнопку `+`.

   - **Просмотр подробной информации об инциденте в уведомлении, поступившем по электронной почте**

     Если для вас была создана подписка на уведомления, при регистрации инцидента вы получите уведомление по электронной почте. Сообщение электронной почты содержит подробную информацию об инциденте и ссылку для перехода в раздел **История** в веб-интерфейсе Kaspersky MLAD.

2. **Просмотр информации о группе, к которой отнесен инцидент**

   В таблице инцидентов в разделе **Инциденты** информация о группе (при наличии) отображается в столбце **Группа инцидентов**. Для просмотра всех инцидентов группы выберите вкладку **Группы** и нажмите на кнопку `+` рядом с нужной группой. В таблице отобразится информация об инцидентах, отнесенных к выбранной группе, а также экспертные рекомендации, если они были добавлены. Ознакомьтесь с экспертными рекомендациями для отдельных инцидентов и для группы.

3. **Исследование поведения объекта мониторинга в момент обнаружения инцидента**

   Исследуйте поведение объекта мониторинга в момент обнаружения инцидента.

4. **Анализ инцидента**

   Проведите анализ инцидента, учитывая особенности регистрации инцидента в зависимости от типа источника, который его зарегистрировал:

   - **Forecaster**. Предиктивный элемент ML-модели регистрирует инциденты при существенном расхождении между наблюдаемыми (фактическими) значениями тегов и прогнозируемыми значениями тегов. Основываясь на информации, полученной при просмотре динамического пресета по инциденту, а также используя экспертное знание об объекте мониторинга, сформулируйте гипотезу о том, какие теги могли вызвать возникновение инцидента, и изучите их поведение, выбрав соответствующий пресет. Проанализируйте график артефакта элемента ML-модели, переместитесь назад по времени от момента достижения порога ошибки прогноза и изучите поведение тегов в момент начала роста значений ошибки прогноза.

- **Rule Detector**. По каждому инциденту, зарегистрированному элементом ML-модели на основе диагностического правила, автоматически формируется динамический пресет, в составе которого присутствуют теги, участвующие в критериях правила, и вызвавшие регистрацию инцидента.

- **Elliptic Envelope**. Эллиптический конверт ML-модели регистрирует инциденты при выявлении состояний, удаление которых от центра области концентрации нормальных состояний сравнялось или превысило установленный порог. При регистрации инцидента формируется динамический пресет, в состав которого включаются теги, при исключении которых из состава ML-модели наблюдается наименьшее отклонение наблюдений от нормального состояния. Проанализируйте график артефакта элемента ML-модели, переместитесь назад по времени от момента достижения порога и изучите поведение тегов в момент начала роста значений отклонения.

- **Limit Detector**. По каждому инциденту, зарегистрированному детектором Limit Detector, автоматически формируется динамический пресет, в состав которого включается единственный тег-причина возникновения инцидента.

- **Stream Processor**. Служба Stream Processor регистрирует инциденты до передачи данных телеметрии на обработку в ML-модель. Инциденты регистрируются в случае обнаружения потери данных или наблюдений, поступивших в Kaspersky MLAD слишком рано или поздно.

5. **Добавление статуса, причины, приоритета, экспертных рекомендаций и комментариев к инциденту**

   Для каждого инцидента добавьте экспертные рекомендации или комментарии, в которых вы можете указать, является ли инцидент аномалией. Если требуется, вы можете указать приоритет, статус и причину инцидента. Экспертные рекомендации, комментарии к инциденту и причина инцидента отображаются только при просмотре определенного инцидента.

   Если вы заранее знаете экспертные рекомендации, приоритет, причину, и/или статус по инцидентам, зарегистрированным конкретным элементом ML-модели, вы можете указать эту информацию в параметрах соответствующего элемента. Заданные экспертные рекомендации, приоритет, причина и/или статус будут автоматически присвоены инцидентам в момент их регистрации этим элементом.

6. **Изменение группы инцидентов**

   Укажите для группы статус ее инцидентов и экспертные рекомендации. При необходимости вы можете изменить имя группы. При изменении статуса группы Kaspersky MLAD автоматически изменит статус всех ее инцидентов. Инциденты сохраняют свой статус, если для группы указан статус по умолчанию **Не установлен**.

   Если Kaspersky MLAD некорректно отнес инциденты к группе, вы можете исключить нужные инциденты из ее состава. Вы также можете самостоятельно создать группу и включить в нее нужные инциденты.

Просмотр инцидентов

Функциональность доступна после добавления лицензионного ключа.

Чтобы просмотреть инциденты, зарегистрированные за определенный период:

1. В основном меню выберите раздел **Инциденты**.

2. В верхней части открывшейся страницы выберите даты начала и окончания периода.

   Вы также можете уточнить период, за который требуется просмотреть инциденты, нажатием на столбец столбчатой диаграммы. Столбец может соответствовать месяцу, неделе или одному дню в зависимости от длительности периода, установленного над диаграммой.

3. Если требуется, отфильтруйте инциденты по группам инцидентов, типам, статусам и приоритетам инцидентов, именам ML-моделей, которые зарегистрировали инциденты, а также активам, содержащим теги и/или элементы ML-моделей, для которых были зарегистрированы инциденты, выбрав нужные значения в соответствующих раскрывающихся списках.

4. Если требуется отобразить только учетные инциденты, включите переключатель **Отображать только учетные инциденты**.

   В таблице, расположенной в центральной области страницы, будут показаны инциденты, зарегистрированные за выбранный период в соответствии с заданными критериями фильтрации. При нажатии на кнопку **Сбросить** в таблице и на столбчатой диаграмме будут показаны все зарегистрированные инциденты.

Для каждого инцидента, представленного в таблице, отображается следующая информация:

- **ID** – идентификатор зарегистрированного инцидента.
- **Дата и время** – дата и время начала инцидента по часам объекта мониторинга, отображенное в часовом поясе компьютера.

  Нажав на значение даты и времени начала инцидента, вы перейдете в раздел **История**, где вы можете посмотреть информацию о динамическом пресете по зарегистрированному инциденту.
- **Приоритет** – приоритет зарегистрированного инцидента.

  Приоритет присваивается автоматически в соответствии с приоритетом, заданным в параметрах элемента ML-модели, зарегистрировавшего этот инцидент. Если в параметрах элемента ML-модели приоритет инцидента не задан, инцидентам присваивается приоритет, соответствующий уровню критичности актива, к которому относится элемент ML-модели, зарегистрировавший инцидент. Иначе инциденту присваивается приоритет **Средний**.
- **Имя модели** – имя ML-модели, элемент которой зарегистрировал инцидент. Отсутствует, если инцидент зарегистрирован службой Stream Processor.
- **Детектор** – тип зарегистрированного инцидента: Elliptic Envelope, Forecaster, Limit Detector, Rule Detector, Stream Processor.
- **Статус инцидента** – статус зарегистрированного инцидента, указанный экспертом (технологом или специалистом АСУ ТП) по результатам анализа инцидента или присвоенный автоматически в соответствии со статусом инцидента, заданным для элемента ML-модели, зарегистрировавшего инцидент.

  Вы можете установить статус инцидента по результатам анализа инцидента, выбрав нужное значение в раскрывающемся списке. По умолчанию при установке Kaspersky MLAD доступны следующие статусы инцидентов и групп инцидентов: **Исследуется**, **Ожидается решение**, **Инструкции даны**, **Проблема закрыта**, **Причина неизвестна**, **Игнорировать** и **Ложное срабатывание**. Если требуется, системный администратор может создать, изменить или удалить статусы инцидентов.
- **Группа инцидентов** – имя группы инцидентов, в которую входит зарегистрированный инцидент.

  Вы можете просмотреть инциденты, которые входят в определенную группу, выбрав имя группы в раскрывающемся списке **Группа инцидентов** над таблицей инцидентов.

Просмотр технических характеристик зарегистрированного инцидента

Функциональность доступна после добавления лицензионного ключа.

В разделе **Инциденты** вы можете просмотреть технические характеристики зарегистрированных инцидентов. Для этого нажмите на кнопку + около нужного инцидента в таблице инцидентов. Для выбранного инцидента отобразятся следующие технические характеристики:

- **Инцидент** – блок, содержащий **информацию об инциденте**.

  - **Уровень критичности** – степень влияния отказа единицы оборудования, для которого зарегистрирован инцидент, на ход производственного процесса объекта мониторинга. Уровень критичности присваивается автоматически в соответствии с уровнем критичности, заданным в параметрах актива.
  - **Имя актива** – имя актива, содержащего тег или элемент ML-модели, для которых зарегистрирован инцидент.
  - **Имя модели** – имя ML-модели, элемент которой зарегистрировал инцидент. Отсутствует, если инцидент зарегистрирован службой Stream Processor.
  - **Элемент модели** – имя элемента ML-модели, который зарегистрировал инцидент. Отсутствует, если инцидент зарегистрирован детектором Limit Detector или службой Stream Processor.
  - **Детектор** – тип зарегистрированного инцидента: Elliptic Envelope, Forecaster, Limit Detector, Rule Detector, Stream Processor.
  - **Значение артефакта элемента ML-модели** – значение отклонения поведения объекта мониторинга от нормального на момент регистрации инцидента. Отсутствует, если инцидент зарегистрирован детектором Limit Detector или службой Stream Processor.
  - **Пороговое значение** – пороговое значение, при достижении которого элементом ML-модели был зарегистрирован инцидент. Если инцидент зарегистрирован детектором Limit Detector, для этого параметра указывается значение верхнего или нижнего порога блокировки, которое было достигнуто тегом.

- **Топ-тег** – блок, содержащий **информацию о теге**, оказавшем наибольшее влияние на регистрацию инцидента.

- **Имя топ-тега (ID топ-тега)** – имя и идентификатор тега, оказавшего наибольшее влияние на регистрацию инцидента.

  Если инцидент зарегистрирован предиктивным элементом ML-модели, отображается имя тега, для которого зафиксировано наибольшее отклонение от прогноза. При регистрации инцидента эллиптическим конвертом отображается имя тега, при исключении которого из состава ML-модели наблюдается наименьшее отклонение наблюдения от нормального состояния. При регистрации инцидента детектором Limit Detector отображается тег, значение которого вышло за установленные для этого тега пороги блокировки.

- **Значение топ-тега** – зарегистрированное в момент инцидента значение топ-тега.

- **Пороги блокировки** – предельно допустимые значения топ-тега.

  Пределы блокировки требуются для правильной работы детектора Limit Detector. В момент, когда значение тега достигает верхнего или нижнего порога блокировки, детектор Limit Detector регистрирует инцидент.

- **Описание** – описание топ-тега.

- **Единица измерения** – единица измерения значений топ-тега.

- **Параметры инцидента службы Stream Processor** – блок, содержащий **информацию о параметрах инцидента, зарегистрированного службой Stream Processor**. Этот блок параметров отображается, только если текущий инцидент был зарегистрирован службой Stream Processor.

  - **Тип инцидента** – тип инцидента, зарегистрированного службой Stream Processor. Служба Stream Processor регистрирует инциденты в случае обнаружения наблюдений, поступивших слишком рано или поздно, а также в случае прекращения или прерывания входного потока данных определенного тега.

  - **Дата и время данных** – дата и время формирования наблюдения по часам объекта мониторинга. Этот параметр отображается только для типов инцидентов **Позднее поступление наблюдения** и **Сбой часов**.

  - **Отставание / Опережение** – количество времени, на которое время формирования наблюдения отстает от времени поступления этого наблюдения в Kaspersky MLAD или опережает его. При поступлении данных слишком рано значение параметра отображается со знаком плюс (+). При поступлении данных в программу поздно значение параметра отображается со знаком минус (-). Этот параметр отображается только для типов инцидентов **Позднее поступление наблюдения** и **Сбой часов**.

- **Причина инцидента** – поле для выбора причины инцидента. Это поле заполняет эксперт (технолог или специалист АСУ ТП). Если требуется, системный администратор может создать, изменить или удалить причины инцидентов.

  Причина инцидента может быть присвоена автоматически, если в параметрах элемента ML-модели, зарегистрировавшего инцидент, задана причина инцидента.

- **Экспертные рекомендации** – поле для ввода экспертных рекомендаций по анализу зарегистрированного инцидента. Это поле заполняет эксперт (технолог или специалист АСУ ТП).

  Экспертные рекомендации могут быть присвоены автоматически, если в параметрах элемента ML-модели, зарегистрировавшего инцидент, заданы экспертные рекомендации.

- **Комментарии к инциденту** – поле для ввода комментария для выбранного инцидента. Если требуется, вы можете указать комментарий для инцидента.

Исследование поведения объекта мониторинга в момент обнаружения инцидента

В этом разделе приводится последовательность действий, которые требуется выполнить для исследования поведения объекта мониторинга в момент обнаружения инцидента.

Функциональность доступна после добавления лицензионного ключа.

Сценарий исследования поведения объекта мониторинга состоит из следующих этапов:

1. **Просмотр истории полученных тегов для объекта мониторинга в разделе История**

   Вы можете перейти к просмотру информации об инциденте одним из следующих способов:

   - Если вы хотите просмотреть недавно обнаруженный инцидент, в разделе **Информационная панель** нажмите на дату и время интересующего вас инцидента в таблице **Последние инциденты**.
   - В разделе **Инциденты** нажмите на дату и время интересующего вас инцидента в таблице инцидентов.
   - Если для вас была создана подписка на уведомления об инцидентах, вы можете перейти к инциденту по ссылке из уведомления, полученному по электронной почте. Сообщение электронной почты содержит время начала инцидента, топ-тег и ссылку для перехода в раздел **История** в веб-интерфейсе Kaspersky MLAD.

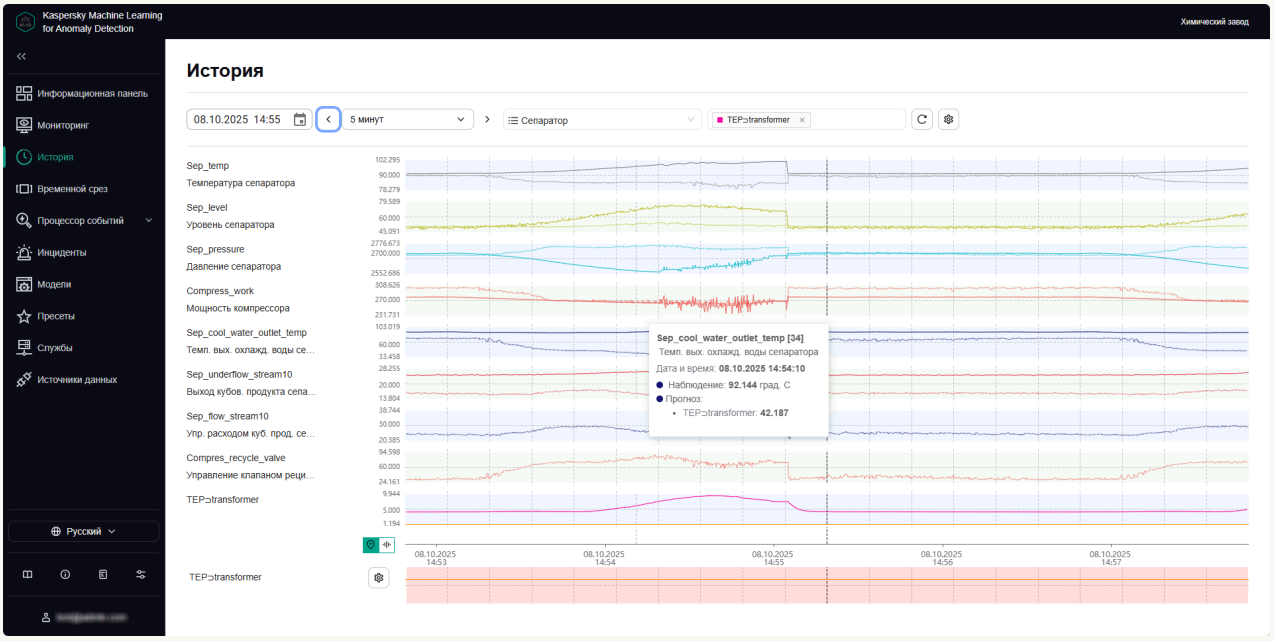
   В разделе **История** Kaspersky MLAD отображает графики тегов, полученных от объекта мониторинга, для которого зарегистрирован выбранный инцидент. На графиках отображаются данные по динамическому пресету, сформированному по дате и времени начала выбранного инцидента. В этот пресет входят теги, поведение которых привело к регистрации инцидента. В зависимости от типа источника, который зарегистрировал инцидент, это могут быть следующие теги:

   - Теги, для фактических значений которых были зафиксированы наибольшие отклонения от прогноза ML-модели, если инцидент был зарегистрирован предиктивным элементом ML-модели.
   - Теги, входящие в диагностическое правило, и значение, полученное в результате работы этого правила, если инцидент был зарегистрирован элементом ML-модели на основе диагностического правила.
   - Теги, при исключении которых из ML-модели наблюдаются наименьшие отклонения наблюдений от нормального состояния, если инцидент был зарегистрирован элементом ML-модели на основе эллиптического конверта.
   - Тег, значение которого вышло за заданные пороги блокировки, если инцидент был зарегистрирован детектором Limit Detector.

   Если требуется, вы можете выбрать другой пресет для отображения данных, полученных от объекта мониторинга в момент регистрации инцидента. На дату и время начала инцидента на графике указывает вертикальная синяя пунктирная линия.

[Пример графиков тегов для зарегистрированного инцидента в разделе История](#).

Графики тегов отображаются в верхней части раздела **История**. В нижней части раздела **История** отображается график артефакта элемента ML-модели.



Графики тегов в разделе **История**

2 Настройка параметров отображения данных на графиках в разделе История

В разделе **История** вы можете включить отображение прогнозируемых значений тегов, полученные в результате работы предиктивных элементов ML-модели. Это позволяет оценить расхождение между фактическими и прогнозируемыми значениями тегов. Информация о теге (имя, описание, дата и время наблюдения, значение и единица измерения тега) отображается при наведении курсора мыши на график определенного тега. Также вы можете включить отображение имени и описания тега слева от графиков каждого тега.

Вы также можете настроить высоту отображаемых графиков. При выборе высоты графика 190 px и более слева от графических областей появятся ползунки, с помощью которых вы можете изменять масштаб отображения графиков.

3 Настройка параметров времени для отображения данных в разделе История

При исследовании поведения тегов вы можете изменять масштаб оси времени или перемещаться по графикам вперед или назад по времени. При отображении более коротких интервалов времени на графиках тегов в разделе **История** могут проявляться детали поведения тегов, которые усреднялись, когда графики тега отображались за более длительный период.

4 Изменение вертикальных границ отображения данных в разделе История

Если отображаются единичные графические области, то выбор вертикального масштаба графика по умолчанию производится автоматически, исходя из минимального и максимального значений тега в отображаемой области. Если для тега установлены минимальное и максимальное допустимые значения (пороги блокировки), вы можете контролировать масштаб графиков по шкале значений на вертикальной оси, включив функцию **Всегда показывать пороги блокировки**. При условии, что значения тега находятся в допустимом диапазоне, вертикальный масштаб графика будет зафиксирован пороговыми линиями, выводимыми по нижней и верхней границам графика тега. Если значения тега выйдут за заданные пороги блокировки, то вертикальный масштаб будет автоматически изменен для отображения запредельных значений тега.

Если отображаются графические области для нескольких тегов, то вертикальный масштаб их отображения регулируется с помощью параметров соответствующей графической области, которые вы можете задать при изменении выбранного пресета.

Изменение приоритета, статуса, причины, экспертных рекомендаций и комментариев к инциденту

Функциональность доступна после добавления лицензионного ключа.

Kaspersky MLAD позволяет добавлять экспертные рекомендации или комментарии к зарегистрированному инциденту.

Экспертные рекомендации, как правило, добавляет эксперт (технолог или специалист АСУ ТП), и они могут содержать рекомендации по устранению проблемы, на которую указывает выявленный инцидент, или анализ инцидента.

Комментарии предназначены для обсуждения между экспертами или операторами предпринятых по инциденту действий: анализ, расследование, исправление. Для каждого комментария фиксируется информация о том, кто и когда его добавил.

Вы также можете добавлять причины возникновения инцидентов и статусы инцидентов, установленные экспертом по результатам их анализа. Статус инцидента может быть присвоен как инциденту, так и группе инцидентов. При изменении статуса группы инцидентов Kaspersky MLAD изменяет статус инцидентов, входящих в эту группу. Статус инцидента также влияет на то, будет ли отображаться точка-индикатор для этого инцидента в разделах **Мониторинг** и **История** и будет ли отправлено уведомление об инциденте с этим статусом. Если для статуса инцидента снят флажок **Уведомлять об инциденте**, то точки-индикаторы инцидентов, которым этот статус был присвоен автоматически, не будут отображаться в разделах **Мониторинг** и **История**, а уведомления об инцидентах не будут отправляться по электронной почте. Статус инцидента может быть присвоен автоматически в одном из следующих случаев:

- Если инцидент был отнесен к группе, для которой установлен статус.
- Если инцидент зарегистрирован элементом ML-модели, в параметрах которого задан статус инцидента по умолчанию.

Для статусов **Проблема закрыта** и **Игнорировать** по умолчанию снят флажок **Уведомлять об инциденте**. Если при регистрации инцидентам автоматически присваивается один из этих статусов в соответствии со статусом, заданным для элемента ML-модели, зарегистрировавшего этот инцидент, то уведомления об этих инцидентах не будут отправлены.

Если вы заранее знаете экспертные рекомендации, приоритет, причину и/или статус по инцидентам, зарегистрированным конкретным элементом ML-модели, вы можете указать эту информацию в параметрах соответствующего элемента. Заданные экспертные рекомендации, приоритет, причина и/или статус будут автоматически присвоены инцидентам в момент их регистрации этим элементом.

Если в параметрах элемента ML-модели приоритет инцидента не задан, инцидентам присваивается приоритет, соответствующий уровню критичности актива, к которому относится элемент ML-модели, зарегистрировавший инцидент. Иначе инциденту присваивается приоритет **Средний**. При необходимости вы можете изменить приоритет инцидента.

Перед изменением приоритета, причины, статуса, комментариев или экспертных рекомендаций требуется провести анализ зарегистрированного инцидента.

Чтобы изменить приоритет, статус, причину, экспертные рекомендации и комментарий к инциденту:

1. В основном меню выберите раздел **Инциденты**.

2. При необходимости измените приоритет инцидента, выбрав в раскрывающемся списке **Приоритет** один из следующих приоритетов: **Очень низкий**, **Низкий**, **Средний**, **Высокий**, **Очень высокий**.

3. При необходимости измените статус инцидента, выбрав в раскрывающемся списке **Статус инцидента** один из следующих статусов: **Исследуется**, **Ожидается решение**, **Инструкции даны**, **Проблема закрыта**, **Причина неизвестна**, **Игнорировать** или **Ложное срабатывание**.

   По умолчанию инциденту присваивается статус **Не установлен**. Если требуется, системный администратор может создать, изменить или удалить статусы инцидентов.

4. Для отображения подробных технических характеристик инцидента нажмите на кнопку + около нужного инцидента. В открывшейся области деталей вы можете выполнить следующие действия:

   - Если требуется изменить причину инцидента, в поле **Причина инцидента** выберите нужную причину инцидента.

     При необходимости системный администратор может создать, изменить или удалить причины инцидентов.

   - Если требуется изменить экспертные рекомендации по анализу зарегистрированного инцидента, нажмите на кнопку ✎, расположенную справа от поля **Экспертные рекомендации**, в появившемся поле введите новые рекомендации и нажмите на клавишу **ENTER**.

     Экспертные рекомендации будут изменены для выбранного инцидента и отобразятся в таблице инцидентов разделе **Инциденты**.

   - Если требуется добавить комментарий к инциденту, в поле **Комментарии к инциденту** введите комментарий и нажмите на кнопку **Добавить комментарий**.

     Вы можете указать комментарий длиной не более 512 символов.

Приоритет, статус, причина, экспертные рекомендации и комментарий будут добавлены к инциденту и будут доступны другим пользователям при просмотре этого инцидента.

Работа с группами инцидентов

По результатам анализа инцидентов вы можете самостоятельно объединять инциденты в группы. Для этого требуется создать группу и наполнить ее инцидентами. При добавлении инцидентов в группу присвоенный им ранее статус автоматически изменится на статус, заданный для этой группы. Инциденты сохраняют свой статус, если для группы, к которой вы хотите отнести инциденты, статус не определен.

Kaspersky MLAD также может автоматически объединять похожие инциденты в группу с помощью службы Similar Anomaly. Это позволяет анализировать инциденты с учетом предыстории, а также использовать экспертные рекомендации, сделанные для аналогичных инцидентов. Инциденты могут быть перегруппированы, и при этом экспертные рекомендации, добавленные к этим инцидентам, мигрируют в новую группу. Имя присваивается группе автоматически – Group #N (N – порядковый номер группы).

Для автоматического объединения инцидентов в группу требуется предварительно запустить службу Similar Anomaly.

При необходимости вы можете исключать инциденты из группы, созданной как самостоятельно, так и автоматически службой Similar Anomaly. Добавление инцидентов в группу, созданную автоматически, невозможно.

Если требуется, вы можете изменить имя, экспертные рекомендации и статус для группы инцидентов.

В таблице инцидентов в разделе **Инциденты** группа, к которой отнесен инцидент, отображается в столбце **Группа инцидентов**.

Просмотр групп инцидентов

Функциональность доступна после добавления лицензионного ключа.

Чтобы просмотреть группы инцидентов:

1. В основном меню выберите раздел **Инциденты** и откройте вкладку **Группы**.
2. Если требуется, отфильтруйте группы инцидентов по их именам и/или статусам, присвоенным инцидентам в группе.

В таблице, расположенной в центральной части страницы, отобразятся группы инцидентов в соответствии с заданными критериями фильтрации. При нажатии на кнопку **Сбросить** в таблице будут показаны все группы инцидентов вашего объекта мониторинга.

Для каждой группы инцидентов в таблице, отображается следующая информация:

- **ID** – идентификатор группы инцидентов.
- **Имя группы** – имя группы инцидентов.

  При автоматическом объединении инцидентов в группу с помощью службы Similar Anomaly Kaspersky MLAD присваивает группе имя Group #N (N – порядковый номер группы).
- **Экспертные рекомендации** – рекомендации по анализу группы зарегистрированных инцидентов, добавленные экспертом (технологом или специалистом АСУ ТП).
- **Количество инцидентов** – количество зарегистрированных инцидентов, которые входят в группу.

  Вы можете перейти к просмотру инцидентов группы, нажав на количество инцидентов нужной группы.
- **Дата и время** – дата и время создания группы инцидентов.
- **Статус** – статус зарегистрированных инцидентов в группе.

  При автоматическом объединении инцидентов в группу Kaspersky MLAD присваивает группе статус **Не установлен**.

  Статус группы также указывает эксперт (технолог или специалист АСУ ТП) по результатам анализа инцидентов, выбрав нужное значение в раскрывающемся списке. По умолчанию при установке Kaspersky MLAD доступны следующие статусы инцидентов и групп инцидентов: **Исследуется**, **Ожидается решение**, **Инструкции даны**, **Проблема закрыта**, **Причина неизвестна**, **Игнорировать** и **Ложное срабатывание**. Если требуется, системный администратор может создавать, изменять или удалять статусы инцидентов.

Также вы можете добавить статус и экспертные рекомендации для группы инцидентов.

Добавление группы инцидентов

По результатам анализа инцидентов вы можете самостоятельно создавать группы и включать в них нужные инциденты.

Функциональность доступна после добавления лицензионного ключа.

Чтобы добавить группу инцидентов:

1. В основном меню выберите раздел **Инциденты** и откройте вкладку **Группы**.
2. Нажмите на кнопку **Добавить** над таблицей групп инцидентов.

   Справа отобразится панель **Добавление группы**.
3. В поле **Имя группы** укажите имя группы инцидентов.
4. Если у вас есть экспертные рекомендации, применимые ко всем инцидентам группы, введите их текст в поле **Экспертные рекомендации**.
5. Если вы заранее знаете статус инцидентов группы, выберите нужный статус в раскрывающемся списке **Статус инцидентов группы**.

   Выбранный статус будет автоматически присвоен всем инцидентам, включенным в эту группу. Инциденты сохраняют свой статус, если для группы инцидентов указан статус по умолчанию **Не установлен**.
6. Нажмите на кнопку **Сохранить**.

Созданная группа отобразится в таблице групп инцидентов.

Изменение группы инцидентов

Вы можете изменить имя группы, а также указать статус группы инцидентов и экспертные рекомендации, содержащие, например, рекомендации при анализе похожих инцидентов.

Функциональность доступна после добавления лицензионного ключа.

Чтобы изменить группу инцидентов:

1. В основном меню выберите раздел **Инциденты** и откройте вкладку **Группы**.
2. Нажмите на кнопку рядом с именем группы инцидентов, которую вы хотите изменить.

   Откроется окно **Изменение группы**.

3. Если требуется, измените параметры группы инцидентов. Описание параметров см. в инструкции по добавлению группы инцидентов.

   При изменении статуса группы инцидентов Kaspersky MLAD изменяет статус всех инцидентов, входящих в эту группу.

   Если требуется, системный администратор может создавать, изменять или удалять статусы инцидентов.

4. Нажмите на кнопку **Сохранить**.

Измененная информация о группе инцидентов отобразится в таблице **Группы** в разделе **Инциденты**.

Изменение состава инцидентов в группе

Функциональность доступна после добавления лицензионного ключа.

После создания группы вы можете включить в нее нужные инциденты. Для этого вы можете выбрать как инциденты, которые не были ранее определены в какую-либо группу, так и инциденты, входящие в состав созданных вручную групп. При включении инцидентов в группу Kaspersky MLAD автоматически исключает их из групп, в состав которых эти инциденты ранее входили.

Добавлять инциденты в группы, созданные автоматически с помощью службы Similar Anomaly, невозможно.

При включении инцидентов в группу Kaspersky MLAD автоматически изменяет их статус на статус, заданный для группы. Если для группы указан статус по умолчанию **Не установлен**, инциденты, входящие в группу, сохраняют свой статус.

Экспертные рекомендации, указанные для группы в целом, не заменяют экспертные рекомендации конкретных инцидентов, если таковые были добавлены экспертом.

Чтобы включить инциденты в группу:

1. В основном меню выберите раздел **Инциденты**.
2. Установите флажки рядом с инцидентами, которые необходимо включить в группу.
3. Нажмите на кнопку **Назначить группу инцидентов**.
4. В раскрывающемся списке **Группа инцидентов** выберите нужную группу.
5. Нажмите на кнопку **Сохранить**.

В зависимости от результатов анализа инцидентов вы можете исключить их из группы. Например, вы можете исключить из группы инциденты, которые служба Similar Anomaly ошибочно в нее включила. При исключении всех инцидентов из группы, созданной автоматически службой Similar Anomaly, Kaspersky MLAD удаляет эту группу.

Чтобы исключить инциденты из группы:

1. В основном меню выберите раздел **Инциденты**.
2. Установите флажки рядом с инцидентами, которые необходимо исключить из групп.

3. Нажмите на кнопку **Исключить инциденты из группы**.

4. Подтвердите исключение инцидентов из групп.

Удаление групп инцидентов

При необходимости вы можете удалить созданную вручную группу инцидентов. Удаление группы инцидентов не приводит к удалению ее инцидентов. При удалении группы Kaspersky MLAD автоматически исключает все инциденты в ее составе, и эти инциденты перестают относиться к какой-либо группе.

Удаление группы, созданной автоматически службой Similar Anomaly и включающей в себя инциденты, невозможно. Kaspersky MLAD автоматически удаляет такие группы после исключения всех инцидентов из ее состава.

Функциональность доступна после добавления лицензионного ключа.

Чтобы удалить одну или несколько групп инцидентов:

1. В основном меню выберите раздел **Инциденты** и откройте вкладку **Группы**.

2. В таблице групп инцидентов установите флажки рядом с теми группами инцидентов, которые требуется удалить.

3. Нажмите на кнопку **Удалить** над таблицей групп инцидентов.

4. Подтвердите удаление групп.

Экспорт инцидентов в файл

Вы можете сохранить в файл формата XLSX инциденты, зарегистрированные за определенный период в Kaspersky MLAD.

Функциональность доступна после добавления лицензионного ключа.

Чтобы сохранить в файл зарегистрированные за определенный период инциденты:

1. В основном меню выберите раздел **Инциденты**.

2. В верхней части открывшейся страницы выберите даты начала и окончания периода.

3. Нажмите на кнопку **Экспорт**.

4. Выберите директорию для сохранения на локальном диске и сохраните файл.

Инциденты, зарегистрированные за выбранный период в Kaspersky MLAD, будут сохранены на локальном диске в файл формата XLSX. Файл формата XLSX можно открыть в программе Microsoft® Excel®.

Управление ML-моделями

Этот раздел содержит информацию о работе с ML-моделями, шаблонами ML-моделей и разметками.

Функциональность доступна после добавления лицензионного ключа.

ML-модели, шаблоны ML-моделей и разметки являются функциональными элементами иерархической структуры объекта мониторинга. Иерархическая структура отображается в виде дерева активов. С помощью кнопок › и ⌄ слева от имен активов вы можете отображать и скрывать состав активов. Если вы выбрали элемент дерева для просмотра и затем свернули дерево, вы можете вновь развернуть структуру дерева до уровня выбранного элемента с помощью кнопки ⊗ слева от названия элемента.

В Kaspersky MLAD ML-модели могут быть импортированы, созданы вручную, скопированы или созданы по шаблону. Если вы создали ML-модель вручную, скопировали ML-модель, которая была создана вручную, или создали ML-модель по шаблону модели, созданной вручную, вы можете добавлять в ML-модель предиктивные элементы, элементы на основе эллиптического конверта и/или элементы на основе диагностических правил.

После обучения элементов ML-модели и проверки результатов их обучения вы можете запустить исторический и/или потоковый инференс для ML-модели. В результате инференса элементы ML-модели регистрируют инциденты, а также формируют артефакты, которые можно просмотреть в разделах **Мониторинг** и **История**.

При необходимости вы можете опубликовать ML-модель. Для опубликованной ML-модели вы также можете запускать исторический и/или потоковый инференс.

В разделе **Модели** вы можете создавать разметки для формирования индикаторов обучения или индикаторов инференса. При необходимости вы можете изменять разметки, копировать и удалять их.

Об ML-моделях

ML-модель – это алгоритм, основанный на методах машинного обучения, задачей которого является анализ телеметрии объекта мониторинга и обнаружение аномалий.

ML-модель создается для конкретного объекта мониторинга с учетом особенностей объекта и характеристик данных телеметрии. При создании ML-модели формируется общая структура алгоритма (архитектура), после чего ML-модель обучается на исторических данных телеметрии, таким образом настраиваясь на особенности поведения конкретного объекта.

ML-модель состоит из одного или нескольких элементов, каждый из которых самостоятельно анализирует телеметрию для выявления аномалий. Как правило, чем сложнее технологические процессы объекта мониторинга, тем больше элементов будет содержать ML-модель. ML-модель может включать в себя элементы следующих типов:

- Предиктивный элемент;
- Элемент на основе диагностического правила;
- Элемент на основе эллиптического конверта.

Элементов каждого типа может быть несколько в ML-модели. Все элементы работают параллельно.

Предиктивные элементы и элементы на основе эллиптического конверта требуется обучить. Элементы на основе диагностического правила обучать не требуется, поэтому они считаются обученными.

Процесс работы ML-модели с данными телеметрии для выявления аномального поведения называется *инференсом*. В Kaspersky MLAD инференс ML-модели может выполняться как на исторических данных (*исторический инференс*), так и данных телеметрии, поступающих в режиме реального времени (*потоковый инференс*).

В случае запуска исторического инференса для нескольких ML-моделей, Kaspersky MLAD выполняет инференс всех этих ML-моделей в порядке очереди их запуска. Вы можете запускать инференс на исторических данных для нескольких ML-моделей одновременно. Рекомендуется запускать исторический инференс на не более трех ML-моделях одновременно. Длительность выполнения исторического инференса определяется интервалом времени данных, которые анализирует ML-модель.

В случае запуска потокового инференса для нескольких ML-моделей, Kaspersky MLAD выполняет инференс этих ML-моделей одновременно. Выполнение исторического и потокового инференса происходит параллельно и независимо друг от друга. В процессе инференса ML-модель регистрирует инциденты, которые можно просмотреть в разделе **Инциденты**.

Помимо инцидентов в результате инференса ML-модель также формирует *артефакты*. Артефакт представляет собой последовательность числовых значений (временной ряд). ML-модель может сформировать следующие артефакты:

- Артефакты, связанные с тегами. Элемент ML-модели формирует эти артефакты для каждого из своих выходных тегов. Эти артефакты формируются только предиктивными элементами ML-модели и представляют собой прогнозируемое значение тега и ошибку этого прогноза.

- Артефакты элементов ML-моделей. Артефакт такого типа формируется каждым элементом ML-модели и является основным результатом работы этого элемента. Математическая природа артефакта зависит от аналитических алгоритмов, используемых элементом, при этом артефакт для элемента ML-модели любого типа интерпретируется одинаково как степень отклонения поведения объекта мониторинга от ожидаемого (нормального). У каждого артефакта есть пороговое значение, при достижении которого регистрируется инцидент.

Вы можете просматривать сформированные артефакты в разделах **Мониторинг** и **История**.

Если в результате инференса были сформированы артефакты и инциденты, не соответствующие ожиданиям, вы можете скорректировать параметры индикатора инференса и/или элементов ML-модели, заново обучить элементы и повторно запустить инференс. При повторном запуске инференса на данных, на которых ранее был проведен инференс, программа удаляет предыдущие результаты инференса на этих данных, если у элементов ML-модели были изменены только общие параметры.

Kaspersky MLAD позволяет выполнить быстрый повторный инференс на исторических данных. Быстрый инференс выполняется на уже готовом артефакте, сформированным предыдущим полным инференсом. ML-модель только удалит ранее зарегистрированные инциденты и сформирует новые, в соответствии с измененными общими параметрами элементов ML-модели.

Вы можете самостоятельно создавать ML-модели и добавлять в них нужные элементы с помощью конструктора моделей. ML-модели также могут быть созданы специалистами "Лаборатории Касперского" или сертифицированным интегратором в рамках *Услуги построения модели и внедрения Kaspersky MLAD*. Для использования таких ML-моделей требуется импортировать их в Kaspersky MLAD.

О предиктивных элементах ML-модели

Предиктивные элементы ML-модели прогнозируют поведение объекта на основе данных о его поведении в ближайшем прошлом. К предиктивным элементам ML-модели относятся нейросетевые элементы и элементы на основе линейной регрессии. Перед добавлением предиктивных элементов в ML-модель изучите рекомендации по использованию элементов ML-моделей.

Конструктор моделей Kaspersky MLAD поддерживает следующие архитектуры для предиктивных элементов ML-модели:

- *Dense*. Нейросетевой элемент ML-модели с полносвязной архитектурой. При создании элемента ML-модели указываются множители для вычисления количества нейронов на внутренних слоях и функции активации на них.
- *TCN*. Нейросетевой элемент ML-модели с иерархической по времени сверточной архитектурой. При создании элемента ML-модели указывается размер и количество фильтров, расширения на слоях, функции активации на них и количество слоев в остаточном блоке.
- *CNN*. Нейросетевой элемент ML-модели со сверточной архитектурой. При создании элемента ML-модели указывается количество нейронов на слоях декодирующего блока, размер и количество фильтров на слоях и размер окна выборки максимума (MaxPooling).
- *RNN*. Нейросетевой элемент ML-модели с рекуррентной архитектурой. При создании элемента ML-модели указывается количество GRU-нейронов на слоях, а также количество распределенных по времени нейронов на слоях декодирующего блока.
- *Transformer*. Нейросетевой элемент ML-модели с архитектурой Transformer. При создании элемента ML-модели указывается количество голов внимания и количество кодирующих блоков Transformer.
- *Линейная регрессия*. Элемент ML-модели на основе линейной регрессии.

В результате инференса предиктивный элемент ML-модели формирует следующие артефакты:

- Прогнозируемые значения тегов. Отображаются в центральной части разделов **Мониторинг** и **История** на единичных графических областях выбранного пресета.
- Индивидуальные ошибки прогнозов – отличия прогнозируемых значений от фактических по каждому тегу. Отображаются в центральной части разделов **Мониторинг** и **История** на единичных графических областях выбранного пресета.
- Суммарная ошибка прогнозов (далее также "общая ошибка прогноза") – суммарный показатель отличия прогнозируемых значений от фактических. Общая ошибка прогноза и порог общей ошибки прогноза отображается на графической области в центральной части разделов **Мониторинг** и **История** после графических областей выбранного пресета, а также на графике артефакта элемента ML-модели, расположенном в нижней части разделов.

  Если общая ошибка прогноза превышает порог общей ошибки прогноза, то предиктивный элемент ML-модели считает, что обнаружил отклонение в поведении объекта мониторинга, и регистрирует инцидент.

Об элементах ML-модели на основе диагностического правила

Диагностические правила описывают заранее известные особенности поведения объекта мониторинга, проявление которых вы считаете аномалией. Диагностические правила должны быть формализованы и должны вычисляться на основе доступной телеметрии объекта. Помимо тегов, поступающих от объекта мониторинга в Kaspersky MLAD, вы можете задать правило на основе вычислимых тегов.

Примеры диагностических правил:

- уровень тега A резко изменился (критерий поведения тега **Ступенька**);
- за последние 12 часов тег Б имеет тренд на повышение, при этом тег В имеет тренд на понижение, а тег С не имеет выраженной динамики;
- значение тега X упало ниже 2800 при условии, что до этого оно поднималось выше 2900.

Об элементах ML-модели на основе эллиптического конверта

Эллиптические конверты используются для выявления аномальных состояний объекта мониторинга.

В отличие от предиктивного элемента эллиптический конверт не пытается установить, как поведение входных тегов ML-модели влияет на поведение выходных тегов. Эллиптический конверт использует предположение, что совокупность тегов, включенных в ML-модель, в каждый конкретный момент времени описывает состояние объекта мониторинга, и наблюдаемые состояния имеют нормальное распределение (далее также "распределение по Гауссу") в фазовом пространстве.

Во время обучения эллиптический конверт подбирает параметры этого нормального распределения с учетом того, что обучающая выборка может содержать некоторый процент аномальных состояний. В результате обучения ML-модели в фазовом пространстве формируется такая эллиптическая область, что состояния, попадающие в эту область, считаются нормальными, а все остальные считаются выбросами (аномалией). Чем дальше от границ эллипса находится состояние, тем более аномальным оно является. Тег, значение которого в составе аномального состояния, внесло наибольший вклад в удаление от эллипса, считается топ-тегом.

Перед добавлением эллиптических конвертов в ML-модель изучите рекомендации по использованию элементов ML-моделей.

О статусах и состояниях ML-моделей и их элементов

Статусы и состояния ML-моделей и их элементов позволяют отобразить в программе последовательность действий, совершенных пользователем в разделе **Модели**.

После обучения элемента ML-модели или исторического инференса ML-модели вы можете оценить результаты обучения или инференса. Выставленные оценки будут отображаться в виде меток в дереве активов, а также под именами ML-моделей при их просмотре.

Для элементов ML-модели предусмотрены следующие статусы:

- **Не обучен**. Этот статус присваивается элементу ML-модели, если для него еще не было запущено обучение или обучение было завершено с ошибкой. Этот статус также отображается для элементов, которые были ранее обучены, но параметры их обучения были изменены. В дереве активов слева от имен необученных элементов отображается значок .
- **Обучен**. Этот статус присваивается элементу ML-модели, если его обучение было успешно завершено или если элемент не подлежит обучению. В дереве активов слева от имен обученных элементов отображается значок .

ML-модели может быть присвоен один из следующих статусов:

- **Не активирована**. ML-модель импортирована, но не активирована. В дереве активов слева от имени ML-модели отображается значок .
- **Не обучена**. ML-модель активирована или создана вручную. В составе ML-модели есть необученные элементы. В дереве активов слева от имени ML-модели отображается значок .
- **Обучена**. Все элементы в составе ML-модели обучены или их обучение не требуется. Для обученной ML-модели может быть запущен инференс. В дереве активов слева от имени ML-модели отображается значок .
- **Готова к публикации**. ML-модель подготовлена к публикации или снята с публикации. ML-модель с таким статусом недоступна для изменений. В дереве активов слева от имени ML-модели отображается значок .
- **Опубликована**. ML-модель опубликована. Для опубликованной ML-модели может быть запущен инференс. В дереве активов слева от имени ML-модели отображается значок .

Состояния ML-моделей и их элементов отображаются в виде меток в дереве активов, а также под именами ML-моделей и элементов ML-моделей при их просмотре. В таблице ниже перечислены состояния ML-моделей и их элементов, предусмотренные в Kaspersky MLAD.

Состояния ML-моделей и элементов ML-моделей

Название состояния при просмотре ML-модели	Обозначение состояния в дереве активов	ML-модель	Элемент ML-модели	Описание
Не используется	—	✓	—	Это состояние присваивается ML-модели, если для нее ранее не были запущены инференс или обучение. Это состояние не отображается в дереве активов.
Обучение завершено с ошибкой	TRN ERR	✓	✓	Это состояние присваивается элементам ML-модели, обучение которых завершилось с ошибкой. Если в составе ML-модели есть хотя бы один элемент, обучение которого завершилось с ошибкой, ей также присваивается это состояние.
Идет обучение	TRN	✓	✓	Это состояние присваивается элементу ML-модели, который в настоящий момент находится в процессе обучения. Если в составе ML-модели имеются элемент в состоянии обучения и при этом отсутствуют элементы, обучение которых завершилось с ошибкой, ей также присваивается это состояние.
В очереди на обучение	TRN Q	✓	✓	Это состояние присваивается элементу ML-модели, для которой было запущено обучение, при этом в текущий момент выполняется обучение другого элемента. ML-модели это состояние присваивается, если все ее элементы поставлены в очередь на обучение.

Обучение завершено успешно	TRN DONE	✓	✓	Это состояние присваивается элементу ML-модели, обучение которого было успешно завершено. ML-модели это состояние присваивается, если все ее элементы были успешно обучены. После оценки результатов обучения вместо состояния **Обучение завершено успешно** отображается выставленная оценка.
Идет исторический инференс	INFR HIST	✓	—	Это состояние присваивается ML-модели, для которой запущен инференс на исторических данных. Вы можете просматривать результаты инференса в разделе **История**. Инциденты, зарегистрированные в процессе инференса, отображаются в разделе **Инциденты**.
В очереди на инференс	INFR Q	✓	—	Это состояние присваивается ML-модели, для которой в настоящий момент выполняется инференс на исторических данных, при этом в текущий момент выполняется исторический инференс для другой ML-модели.
Завершен исторический инференс	INFR DONE	✓	—	Это состояние присваивается ML-модели, для которой был завершен инференс на исторических данных. Вы можете просматривать результаты инференса в разделе **История**. Инциденты, зарегистрированные в процессе инференса, отображаются в разделе **Инциденты**. После оценки результатов инференса ML-модели вместо состояния **Завершен исторический инференс** отображается выставленная оценка.
Идет потоковый инференс	INFR STRM	✓	—	Это состояние присваивается ML-модели, для которой запущен инференс на потоковых данных. Вы можете просматривать результаты инференса в разделе **Мониторинг**. Инциденты, зарегистрированные в процессе инференса, отображаются в разделе **Инциденты**.

О шаблонах ML-моделей

Шаблоны ML-моделей создаются на основе ML-моделей, ранее добавленных в Kaspersky MLAD или созданных с помощью функциональности конструктора моделей. В шаблонах ML-моделей сохраняется структура алгоритма, набор элементов и состояние ML-модели, по которой был создан шаблон. Состояние обучения созданной ML-модели будет соответствовать состоянию обучения исходной ML-модели в момент создания ее шаблона.

С помощью шаблонов вы можете добавлять в Kaspersky MLAD однотипные ML-модели, которые будут анализировать данные, поступающие с оборудования одного типа с похожим набором тегов. При создании ML-модели по шаблону можно изменить состав используемых в ML-модели тегов, указав идентификаторы тегов, отличные от идентификаторов тегов исходной ML-модели.

О разметках

Разметка – это инструмент для отбора интервалов времени. Разметки используются для формирования индикаторов обучения и инференса ML-модели. Разметки в составе индикаторов обучения определяют интервалы времени данных, из которых ML-модель берет данные для обучения. В составе индикаторов инференса разметки определяют интервалы времени, в течение которых ML-модель выполняет инференс.

В составе разметки могут быть использованы два вида критериев: условия на поведение конкретных тегов (отбираются интервалы времени, в которых эти условия соблюдаются) и фильтр по времени (интервалы времени отбираются независимо от поведения тегов). Условия на поведение тегов могут быть определены как для тегов, поступающих от объекта мониторинга, так и для вычислимых тегов. Выражение для расчета вычислимых тегов задается при создании разметки.

Разметка является функциональным элементом иерархической структуры. Разметки могут быть созданы вручную или импортированы в Kaspersky MLAD вместе с ML-моделью.

Об условиях в составе разметок и диагностических правил

Отбор интервалов времени данных для индикаторов обучения или инференса в разметке, а также выполнение диагностического правила в составе ML-модели регулируется условиями, которые задаются при создании разметки и/или элемента ML-модели на основе диагностического правила. В процессе создания разметки и элемента ML-модели на основе диагностического правила вы можете задавать следующие типы условий:

- Фильтрация по времени.

  Фильтр по времени позволяет задать последовательность повторяющихся календарных интервалов (например, интервал с учетом рабочих дней в неделе и часов работы) или набор интервалов с точно определенными моментами начала и окончания.

  Если условия на поведение тегов не заданы, то отобранные фильтром интервалы будут результатом работы разметки или диагностического правила. Во всех узлах РИВС внутри отобранных интервалов правило будет считаться выполненным.

- Условия на поведение тегов.

  Условия на поведение тегов проверяются в узлах РИВС, попавших внутрь интервалов, отобранных фильтром по времени. Если фильтрация по времени не применена, то условия на поведение тегов проверяются во всех узлах РИВС.

  Критерии поведения тегов описываются в блоках условий и связаны между собой логическими операторами **AND** и/или **OR**. Оператор **AND** отслеживает одновременное выполнение всех связанных критериев, а оператор **OR** отслеживает выполнение хотя бы одного из связанных критериев. К критериям в составе блока условия может быть индивидуально применен оператор отрицания **NOT**, который отслеживает поведение, обратное описанному в критерии. В свою очередь блоки условий также могут быть связаны логическими операторами **AND** и/или **OR**.

  Проверка любого условия приводит к одному из трех результатов:

  - Положительный результат (TRUE) – в случае выполнения условия. Если критерии связаны между собой логическим оператором **OR** и проверка критериев дали результаты TRUE и UNDEFINED, то проверка всего блока условий даст положительный результат.

  - Отрицательный результат (FALSE) – в случае невыполнения условия.

  - Неопределенный результат (UNDEFINED) – в случае невозможности проверить выполнение условия (например, из-за нехватки необходимого количества данных). Проверка всего блока условий дает неопределенный результат в следующих случаях:

    - Если критерии блока условий связаны между собой логическим оператором **OR** и проверка отдельных критериев дали результаты FALSE и UNDEFINED.

    - Если критерии блока условий связаны между собой логическим оператором **AND** и проверка отдельных критериев дали результаты UNDEFINED и TRUE и/или FALSE.

  При необходимости вы можете связать два блока условия темпоральным оператором **Пауза** или **Если далее**. Блок условий, предшествующий темпоральному оператору, называется *предварительным условием*. Блок условий, следующий за темпоральным оператором, называется *пост-условием*. В отличие от логических операторов **AND** и **OR**, требующего одновременной проверки условий, темпоральный оператор связывает блоки условий, выполнение которых проверяется в разные моменты времени.

Предварительное условие проверяется в одном узле РИВС, а пост-условие проверяется в одном или нескольких подряд следующих узлах РИВС. Промежуток между узлом проверки предварительного условия и узлами, в которых проверяется пост-условия, соответствует интервалу ожидания. Проверка пост-условия регулируется следующими параметрами:

- Минимальный интервал ожидания – интервал между узлом проверки предварительного условия и узлом РИВС, с которого начнется проверка пост-условия.
- Максимальный интервал ожидания – интервал между узлом проверки предварительного условия и узлом РИВС, в котором закончится проверка пост-условия.
- Групповой оператор, который определяет, требуется ли, чтобы пост-условие было выполнено во всех узлах проверки пост-условия или хотя бы в одном из них.

Если проверка предварительного условия дала отрицательный результат (FALSE) или неопределенный результат (UNDEFINED), то это же значение станет результатом применения всего темпорального оператора. Если проверка предварительного условия дала положительный результат (TRUE), то проверка пост-условия проводится в каждом узле РИВС между минимальным и максимальным интервалом ожидания, при этом результат применения темпорального оператора определяется результатами проверок пост-условия с учетом значения группового оператора.

Если проводится более одной проверки условия с помощью темпорального оператора, то предварительным условием для каждого следующего темпорального оператора является результат применения предыдущего темпорального оператора.

Результат применения темпорального оператора **Если далее** формируется в узле проверки предварительного условия. Темпоральный оператор **Если далее** может быть использован только в составе индикатора обучения, так как для его выполнения требуются данные из будущего, которые в процессе инференса еще не доступны.

Результат применения темпорального оператора **Пауза** формируется в последнем узле РИВС проверки пост-условия. Поскольку в этот момент все узлы, участвующие в операторе находятся в прошлом, то оператор **Пауза** может быть использован как в составе индикатора обучения, так и в составе индикатора инференса.

Общий результат проверки всех условий разметки или диагностического правила может быть либо положительным (TRUE), либо отрицательным (FALSE). Если в каком-то узле РИВС проверка всех заданных условий на поведение тегов привела к неопределенному результату (UNDEFINED), то общий результат применения разметки или диагностического правила в этом узле определяется значением параметра **Интерпретировать невозможность оценки условия как выполнение правила**.

О вычислимых тегах в составе разметок и диагностических правил

Вычислимый тег – это тег, значение которого вычисляется из значений тегов, поступающих от объекта мониторинга, или других вычислимых тегов в соответствии с выражением, заданным пользователем при его создании. Вычислимые теги не сохраняются в базе данных и существуют только в рамках диагностических правил и разметок, в которых они были определены. Вычислимые теги могут быть использованы для расчета некоторого производного значения или для сравнения нескольких значений на протяжении некоторого времени.

Для расчета вычислимого тега вы можете использовать как арифметические действия, так и логические операции, операции сравнения и функции. При написании выражений следует учитывать следующие особенности:

- Для проведения операций над значениями конкретных тегов необходимо прописать имена этих тегов либо в одинарных ('), либо двойных (") кавычках. Если имя тега уже содержит кавычки одного типа, то для применения этого тега в выражении необходимо использовать кавычки другого типа.
- Вы можете использовать значок звездочки в кавычках ("*") для проведения операций над значениями всех тегов, выбранных для расчета вычислимого тега. Например, для вычисления в текущем узле РИВС среднего значения всех выбранных тегов вы можете прописать выражение `mean("*")`. Если для вычислимого тега выбраны теги x и y, это выражение соответствует выражению `mean("x", "y")`.
- Вы можете использовать круглые скобки для явного указания порядка выполнения операций.
- Унарные минус и плюс могут быть использованы как перед числовыми значениями, так и перед конкретными функциями или всем выражением.
- В качестве разделителя целой и дробной частей числа необходимо использовать точку.
- Пробелы между частями выражения игнорируются, вы можете добавлять их по своему усмотрению для читаемости.
- Вы можете комбинировать функции и арифметические действия.
- Результатом выражения должно быть вещественное число. Если результатом вычисления функции является массив чисел, его необходимо передать в другую функцию для получения вещественного числа.

Значение вычислимого тега рассчитывается для каждого узла РИВС в процессе инференса ML-модели с элементом на основе диагностического правила или применения разметки.

По умолчанию для вычисления выражения используются значения аргументов (входящих тегов или других вычислимых тегов) в этом же узле РИВС. Например, значение вычислимого тега с выражением `"x" - "y"` в узле РИВС 12:00 будет равно разности значений тегов x и y, взятых в момент времени 12:00. Аналогично, выражение `max("x", "y")` в узле 12:00 вернет максимальное из значений тегов x и y, взятых в момент времени 12:00.

При необходимости в расчете значения вычислимого тега могут использоваться значения аргументов не только в текущем, но и в предшествующих узлах РИВС. Для этого необходимо определить *окно* – число предшествующих узлов РИВС, включая текущий, из которых будут браться значения аргументов для участия в вычислениях. Длина окна определяется параметром `w`, который может быть указан как для каждой отдельной функции, так и для выражения в целом. По умолчанию `w=1`, что соответствует текущему узлу РИВС. Например, предполагая шаг сетки равным 10 минут, выражение `max("x", "y", "z", w=3)` в узле 12:00 вернет максимальное из значений тегов x, y и z, взятых в моменты времени 11:40, 11:50 и 12:00 (то есть максимальное из 9 значений).

Для применения значения окна сразу ко всем частям выражения необходимо прописать выражение в следующем формате:

`w=<длина окна>: <выражение для расчета>`

Например, `w=3: max("x", "y")`. При вызове конкретной функции длина ее окна может быть переопределена с помощью параметра `w`.

При проведении вычислений с применением окна может оказаться, что результатом является не одно число, а окно (последовательность значений) или даже несколько последовательностей в одном окне. Например, результатом вычисления выражения `w=3: "x" * "y"` в узле 12:00 будет последовательность из трех чисел, являющихся произведениями значений тегов x и y, взятых, соответственно, в 11:40, 11:50 и 12:00.

Некоторые функции предназначены специально для работы с окнами и возвращают последовательности значений. Например, `maxtag("x", "y", "z", w=3)` в узле 12:00 вернет последовательность из трех чисел: максимум из значений тегов x, y и z в момент 11:40, максимум из значений этих же тегов в 11:50, и максимум из значений этих же тегов в 12:00.

Поскольку значением вычислимого тега в каждом отдельном узле РИВС является одно число, то выражение для вычисления тега должно быть построено так, чтобы возвращать одно число даже при проведении вычислений с окнами. Этого можно достигнуть, например, использовав функцию, которая всегда возвращает одно число, независимо от длины окна и числа своих аргументов. Такая функция называется *редуктором*. Редукторами являются функции `min`, `max`, `mean`, `all`, `any`.

Примеры редукторов:

- `min("x" * "y", w=3)`. Выражение возвращает одно число – минимум из произведений значений тегов x и y, взятых, соответственно, в 11:40, 11:50 и 12:00.

- `mean(maxtag("x", "y", "z", w=3))`. Выражение возвращает одно число – среднее из максимумов значений тегов x, y и z в трех последних узлах РИВС.

Если выражение для вычислимого тега все же возвращает последовательность чисел (окно), то оно будет автоматически редуцировано. В этом случае в качестве значения вычислимого тега будет взято последнее из этих значений. Если выражение для вычислимого тега возвращает несколько чисел, не являющихся одним окном (одной временной последовательностью), как например, попарные разности `pwd("x", "y", "z")`, то такое выражение не может быть автоматически редуцировано до одного числа и не пройдет проверку на корректность. В этом случае корректным выражением было бы, например, `max(pwd("x", "y", "z"))` или `all(pwd("x", "y", "z") < 10)`.

Операции в выражениях для расчета вычислимых тегов

Аргументом функции может быть тег, число или вектор, который может быть либо окном, взятым из значений явно указанного тега, либо результатом применения другой вложенной функции. Функция принимает произвольное число аргументов, если явно не указано иное. Длина входного окна функции по умолчанию равна 1, если не задан общий параметр `w` выражения или не определен параметр `w` самой функции.

Функция-редуктор всегда возвращает одно число, независимо от числа аргументов и длины входного окна функции. Другие функции возвращают окно из одной или нескольких последовательностей значений. В таком случае операция выполняется поэлементно, то есть отдельно на каждом шаге окна, при этом результатом операции также является окно. Размерность результата зависит от выполняемого вычисления, числа аргументов функции и/или длины ее входного окна.

Размерности аргументов (длины окон) должны быть одинаковы. Если результат одной функции используется в качестве аргумента другой, то длина окна результата первой должна быть не меньше размера входного окна второй. Если один из аргументов операции является окном, а второй – числом, то число автоматически превращается в окно необходимой длины, состоящее из одинаковых значений.

Действия, которые вы можете использовать в выражениях для расчета перечислены в таблице ниже.

Операция	Описание	Пример выражения
Арифметические действия		
Сложение	Сложение двух или более аргументов.	`"x" + "y"`
Вычитание	Вычитание двух или более аргументов.	`"x" - "y"`
Умножение	Умножение двух или более аргументов.	`"x" * 2`
Деление	Деление двух или более аргументов.	`"x" / 6`
Возведение в степень	Возведение аргумента в степень.	`"x" ** 3`
Операции сравнения		
Равно (==)	Возвращает 1.0, если части выражения равны, иначе возвращает 0.0.	`"y" - "z" == -90`
Больше (>)	Возвращает 1.0, если левая часть выражения больше правой части выражения, иначе возвращает 0.0.	`"y" > 5`
Меньше (<)	Возвращает 1.0, если левая часть выражения меньше правой части выражения, иначе возвращает 0.0.	`99 < "y" ** 2`
Больше или равно (>=)	Возвращает 1.0, если левая часть больше или равна правой части выражения, иначе возвращает 0.0.	`"y" ** 2 >= "z"`
Меньше или равно (<=)	Возвращает 1.0, если левая часть меньше или равна правой части выражения, иначе возвращает 0.0.	`"y" ** 2 <= "z"`
Не равно (!=)	Возвращает 1.0, если части выражения не равны, иначе возвращает 0.0.	`"y" ** 2 != "z"`
Логические операции		
ИЛИ (|)	Возвращает значение 1.0, если хотя бы один из операндов истинен. Возвращает 0.0, если все операнды ложны.	`("x" != 0) | (("y" + "z") > 105.5)`
И (&)	Возвращает значение 1.0, если все операнды выражения истинны. Возвращает 0.0, если хотя бы один из операндов ложен.	`("x" != 0) & (("y" + "z") > 105.5)`
Функции		
`all()`	Функция-редуктор. Возвращает значение 1.0, если значения всех аргументов функции истинны в каждом узле РИВС в рамках окна. Возвращает значение 0.0, если хотя бы в одном узле РИВС какое-либо значение аргумента функции ложно.	`all("y" > 11, w=3)`
`any()`	Функция-редуктор. Возвращает значение 1.0, если значение хотя бы одного аргумента функции истинно хотя бы в одном узле РИВС. Возвращает 0.0, если значение всех аргументов функции ложно во всех узлах РИВС.	`any("y" > 11, w=3)`
`max()`	Функция-редуктор. Возвращает наибольшее из значений, переданных в функцию аргументов. Рассматриваются все значения аргументов в рамках заданного окна.	`max("x", 12, -"y" + 7)`
`min()`	Функция-редуктор. Возвращает наименьшее из значений, переданных в функцию аргументов. Рассматриваются все значения аргументов в рамках заданного окна.	`min("x", 12, -"y" + 7)`
`mean()`	Функция-редуктор. Возвращает среднее арифметическое значение набора переданных в функцию аргументов. Рассматриваются все значения аргументов в рамках заданного окна.	`mean("x", 12, -"y" + 7)`
`maxtag()`	Для каждого узла РИВС в рамках окна возвращает наибольшее значение среди переданных в функцию аргументов. Результатом работы функции является вектор длиной `w`.	`maxtag("x", "y" w=3)` Результатом вычисления функции будет вектор наибольших значений для тегов `x` и `y` в каждом узле заданного окна.
`mintag()`	Для каждого узла РИВС в рамках окна возвращает наименьшее значение среди переданных в функцию аргументов. Результатом работы функции является вектор длиной `w`.	`mintag("x", "y" w=3)` Результатом вычисления функции будет вектор наименьших значений для тегов `x` и `y` на каждом узле заданного окна.

Операция	Описание	Пример выражения
`meantag()`	Для каждого узла РИВС в рамках окна возвращает среднее арифметическое значение среди переданных в функцию аргументов. Результатом работы функции является вектор длиной `w`.	`meantag("x", "y", w=3)` Результатом вычисления функции будет вектор средних арифметических значений для тегов `x` и `y` в каждом узле заданного окна.
`grad()`	Вычисляет градиент массива переданных в функцию аргументов. Под градиентом аргумента в узле РИВС понимается разность между значением аргумента в этом узле и значением этого же аргумента в предыдущем узле РИВС. Функция может быть использована с параметрами `w` и `order`. Параметр `order` используется для указания порядка при расчете градиента. Например, `order=2` соответствует второму порядку. По умолчанию параметр `order` имеет значение `1`. Градиент первого порядка (order=1) вычисляется над значениями аргументов функции (над каждым аргументом отдельно). Результат представляет собой вектор длины w – 1. Градиент более высокого порядка вычисляется над результатами вычисления градиента предыдущего порядка. Результатов применения функции является один или несколько (по числу аргументов) векторов длиной w – order.	• `grad("x", w=5, order=2)` Результатом вычисления функции будет вектор из трех значений. • `grad("x", "y", w=5, order=2)` На вход подано окно из пяти значений. Градиент первого порядка на этом окне вернет результат длиной 4, а градиент второго порядка вернет результат длиной 3. Результатом вычисления функции будут два вектора из трех значений.
`pwd()`	Вычисляет попарные расстояния между аргументами, переданными в функцию. Попарные расстояния вычисляются в произвольном порядке. Функция используется с параметрами `w`, `how` и `absolute`. Параметр `how` регулирует принцип сравнения тегов. Предусмотрены следующие значения параметра: • `auto` (по умолчанию). Регулирует автоматическое использование значений `over_tags` и `over_time` в зависимости от количества тегов, переданных в функцию в виде аргументов, и длины окна. Если в функцию передан один тег в качестве аргумента, параметру автоматически присваивается значение `over_time`. Иначе параметру автоматически присваивается значение `over_tags`. • `over_tags`. Операция выполняется над значениями всех аргументов отдельно в каждом узле РИВС в рамках окна. Результатом операции является `w` окон длиной `n * (n - 1) / 2`, где `n` соответствует числу аргументов, а `w` – длине входного окна. • `over_time`. Операция выполняется над значениями каждого аргумента, полученными за промежуток времени длиной в заданное окно. Результатом операции является `n` окон длиной `w * (w - 1) / 2`, где `n` соответствует числу аргументов, а `w` – длине входного окна. Аргумент `over_time` необходимо использовать при окне с длиной более одного узла. Параметр `absolute` регулирует приведение переданных значений к модулю. Предусмотрены следующие значения параметра: • `true` (по умолчанию), если требуется привести результат вычисления функции к модулю. • `false`, если приведение результата вычисления функции к модулю не требуется.	• `pwd("w", "x", "y", "z")` Результатом вычисления функции будут попарные расстояния, а именно строка из чисел ("x"-"w", "y"-"w", "z"-"w", "y"-"x", "z"-"x", "z"-"y"), при этом значения всех тегов взяты в текущем узле РИВС, и результат вычисления приводится к модулю. • `pwd("x", "y", "z", w=3, how=over_time)` Результатом вычисления функции будут три вектора, каждый из которых содержит набор попарных расстояний между значениями одного и того же тега в разных узлах РИВС в рамках окна.
`take()`	Возвращает значения аргументов в заданном окне. Функция используется с параметрами `w`, `n` и `default`. Параметр `n` определяет длину возвращаемого окна, считая от начала входного окна `w`. Например, функция `take("x", w=4, n=2)` вернет вектор из двух значений тега `x` в первом и втором узлах окна `w`. По умолчанию `n=-1`, что соответствует всем узлам входного окна. Параметр `default` используется для заполнения значений тегов, не поступивших в узлах РИВС на заданном окне.	`take("x", w=3, default=10)` Результатом функции будет вектор со значениями тега `x` в трех последних узлах РИВС. При этом, если для какого-то узла РИВС значение тега еще не поступило, в этом узле для тега будет использовано значение 10.

Операция	Описание	Пример выражения
`abs()`	Возвращает абсолютное значение аргумента, не изменяя его размерности.	`abs("x")` `abs("x", w=3)`
`latest()`	Возвращает последнее (текущее) значение аргумента. Функция принимает только один аргумент. Функция `latest()` неявно применяется ко всему выражению, если результатом вычисления выражения является вектор (окно).	—

Примеры вычисления комбинированных функций см. в Приложении.

Рекомендации по использованию элементов ML-моделей

Этот раздел содержит рекомендации по использованию следующих элементов ML-моделей:

- Элементов ML-модели на основе эллиптического конверта.
- Предиктивных элементов: элементов ML-модели на основе линейной регрессии и нейросетевых элементов.

Рекомендации по использованию элементов ML-модели на основе эллиптического конверта

Элемент ML-модели на основе эллиптического конверта рекомендуется использовать, когда технологический процесс работает в стабильном режиме без резких изменений параметров, и требуется выявление корреляционных аномалий между тегами, когда поведение одного или нескольких тегов стало отличаться от остальных.

При добавлении элемента рекомендуется выбрать теги, которые в штатном режиме работы оборудования должны изменяться синхронно, при этом у каждого тега есть некоторое центральное значение, вокруг которого он колеблется. Центральные значения разных тегов могут отличаться. Визуально, если такие теги отобразить на одном графике, получится волнистая полоса, состоящая из нескольких линий.

Часто в эллиптический конверт отбирают теги, измеряющие один и тот же параметр у смежных компонент одного агрегата, например, температуры разных цилиндров одного компрессора или температуры подшипников с разных сторон вала.

Преимущества и ограничения элементов ML-модели на основе эллиптического конверта

Элементы ML-модели на основе эллиптического конверта имеют следующие преимущества:

- Элементы просты в построении и быстро обучаются.
- Для обучающей выборки требуется относительно небольшой объем наблюдений. Минимальное количество наблюдений в обучающей выборке – 100, рекомендуемое количество наблюдений – от 1000.
- Потребляется небольшое количество вычислительных ресурсов сервера во время инференса ML-модели.
- Элементы эффективны при многомерных корреляциях между тегами.
- Хорошая интерпретируемость результатов инференса.

Элементы ML-модели на основе эллиптического конверта имеют следующие ограничения:

- Подходят только для стационарных режимов работы.
- Требуют близкого к нормальному распределения данных по каждому тегу.
- Неэффективны при множественных рабочих диапазонах или резких изменениях тегов.
- Рассматривают каждый момент времени как обособленный от других, поэтому не способны выявлять связи между тегами во времени.

Рекомендации по использованию элементов ML-модели на основе линейной регрессии

Линейная регрессия является простейшим предиктивным элементом. Она применяется для выявления аномалий в поведении тегов, если есть обоснованное предположение о линейной зависимости между тегами. Линейная зависимость может проявляться в тот же момент времени или с задержкой. Предполагается, что каждый из выходных тегов в выходном окне линейно зависит от совокупности входных тегов во входном окне.

При добавлении элемента рекомендуется задать параметры следующим образом:

- Укажите значение 1 для параметров **Входное окно (шаги)** и **Выходное окно (шаги)**.
- Для выявления одновременной зависимости между тегами укажите значение 0 для параметра **Смещение выходного окна** и выберите разные входные и выходные теги.
- Для выявления зависимости между тегами с задержкой укажите ненулевое значение для параметра **Смещение выходного окна** и выберите входные и выходные теги, при этом теги могут пересекаться.

Преимущества и ограничения элементов ML-модели на основе линейной регрессии

Элементы ML-модели на основе линейной регрессии имеют следующие преимущества:

- Для обучающей выборки требуется малый объем наблюдений. Рекомендуемое количество наблюдений – от 100.
- Потребляется небольшое количество вычислительных ресурсов сервера во время инференса ML-модели.
- Очевидная интерпретация результатов инференса.

Элементы ML-модели на основе линейной регрессии имеют следующие ограничения:

- Элементы подходят только для линейно зависимых тегов.
- Необходимо заранее экспертно установить природу линейной зависимости и определить сдвиг по времени (при наличии).
- Элементы не способны выявлять связи между тегами за пределами заданных параметров линейной зависимости.

Рекомендации по использованию нейросетевых элементов

Все нейросетевые элементы могут выявлять сложные взаимосвязи между тегами, поэтому их рекомендуется использовать, когда логика взаимного влияния параметров системы неочевидна и/или наблюдается динамика процесса во времени (изменения в поведении одних тегов влияют на поведение других с задержкой). Отличия между архитектурами нейросетевых элементов проявляются, в основном, в их способности выучивать динамику во времени, а также в их требованиях к ресурсам и в скорости обучения или инференса.

Все нейросетевые элементы принимают на вход окно из последовательности точек во времени и преобразуют ее на выходе в другое окно из последовательности точек во времени. Выходное окно может быть смещено вперед относительно входного окна. В таком случае выходное окно дает прогноз на будущее относительно текущего входного окна. Длину окна рекомендуется выбирать в диапазоне от 5 до 200 узлов РИВС, при этом окно должно охватывать как минимум половину характерного событийного интервала. Например, если период РИВС равен одной минуте, а существенное изменение в процессе развивается за 10 минут (характерный событийный интервал), то рекомендуется начать с 10 или 20 шагов для длины входного окна (параметр **Входное окно (шаги)**).

На основе архитектур **Dense**, **CNN** и **Transformer** вы можете создать также и автоэнкодерные элементы, для которых длина входного окна равна длине выходного окна, и выходное окно не смещено относительно входного окна. В этом случае нейросетевой элемент выучивает внутренние закономерности тегов во времени, в зависимости друг от друга сжимает входную информацию в выученный сетью внутренний узкий слой, а потом пытается восстановить ту же информацию. Восстановление информации нейросетевому элементу хорошо удается, если выученное поведение соответствует наблюдаемому, иначе восстановление информации происходит с ошибками, при этом вы можете увидеть, где ожидание сети отличалось от реальных наблюдений.

Автоэнкодерные элементы хорошо подходят на начальном этапе подбора архитектуры. В таком случае рекомендуется попробовать создать автоэнкодерный элемент с архитектурой **Dense** или **CNN** и выбрать в качестве входных и выходных одни и те же теги.

Если же причинная логика влияния тегов друг на друга понятна, то рекомендуется добавлять элементы согласно описаниям поддерживаемых архитектур, приведенным в таблице ниже. При этом в качестве входных рекомендуется выбирать те теги, которые являются причиной, а в качестве выходных – теги, которые являются следствием. При этом вы можете выбрать теги, которые являются следствием, в качестве входных и выходных, что может помочь выявить более длительные корреляции тегов.

Рекомендуемое общее количество тегов в одном элементе – до 200. При подготовке данных необходимо убедиться, что на каждый характерный событийный интервал приходится минимум 10 наблюдений по каждому тегу, участвующему в модели.

Общие сведения о поддерживаемых нейросетевых архитектурах

Архитектура нейросетевого элемента	Особенности работы со временем	Относительная потребность в вычислительных ресурсах	Рекомендации по использованию
Dense	Понимание времени ограничено рамками одного окна.	Для архитектуры характерны низкая потребность в вычислительных ресурсах и высокая скорость обучения и инференса.	Используйте эту архитектуру, если нужно выучить зависимости между выходными и выходными тегами без сдвига во времени. Рекомендуемая длина входного и выходного окна – в диапазоне от 5 до 200 шагов. Рекомендуемое смещение – 0.
CNN	Для архитектуры характерны следующие особенности: • Выявление зависимостей во времени ограничено рамками одного входного окна. • Результат сильно зависит от длины окна и ее соотнесения с характерным событийным интервалом. • Если разные теги имеют разные событийные интервалы, и часть из интервалов не вкладывается во входное и/или выходное окно, элемент может не выучить зависимости между тегами. • Может преувеличивать локальные эффекты, игнорируя долгосрочные. • Хорошо отсеивает нерелевантные данные.	Для архитектуры характеры высокая скорость обучения и инференса и большое потребление памяти на длинных окнах.	Используйте эту архитектуру, если предполагается возможность небольшого (много меньше длины событийного интервала) сдвига по времени в зависимости между выходными и выходными тегами. Рекомендуется задавать длину входного и выходного окон равную характерному событийному интервалу, а смещение равное нулю. Вы можете сравнить результаты работы с результатами работы элемента с архитектурой Dense и выбрать лучший вариант.
TCN	Для архитектуры характерны следующие особенности: • Хорошо понимает и короткие, и длинные временные зависимости, особенно устойчиво повторяющиеся; хуже понимает зависимости переменной длины. • Может пропускать спорадические незначительные отклонения.	Для архитектуры характерны средняя потребность в вычислительных ресурсах и средняя скорость обучения и инференса.	Используйте эту архитектуру, если нужно выучить устойчивые повторяющиеся временные зависимости, в том числе длительные (протяженностью в много событийных интервалов), и обнаруживать плавно нарастающие отклонения от них. Рекомендуется задавать длину входного окна, выходного окна и смещения равную половине характерного событийного интервала. Качество модели чувствительно к объему обучающей выборки, поэтому рекомендуется использовать как можно больше данных для обучения. Рекомендуемая длина выборки – от 10 000 событийных интервалов.

Архитектура нейросетевого элемента	Особенности работы со временем	Относительная потребность в вычислительных ресурсах	Рекомендации по использованию
RNN	Для архитектуры характерны следующие особенности: • Хорошо понимает зависимости переменной длины, хуже справляется с длинными зависимостями и/или большим числом тегов. • Лучше подходит для гладких изменений параметров, описываемых дифференциальными уравнениями. • Быстрые случайные колебание могут сильно сглаживаться на входных и/или выходных окнах.	Для архитектуры характерны высокая потребность в вычислительных ресурсах и длительное обучение.	Используйте эту архитектуру, если нужно выучить относительно короткие зависимости (один или два событийных интервала), но при этом возникающие без четкой периодичности и имеющие переменную длину. Рекомендуется задавать длину входного окна, выходного окна и смещения равную половине характерного событийного интервала. В частности, архитектура применима для выявления зависимостей в работе ПИД-регуляторов и подобных регулировочных воздействиях с обратной связью.
Transformer	Для архитектуры характерны следующие особенности: • Выявляет любые зависимости, в том числе длинные зависимости переменной длины. • Остро реагирует даже на незначительные отклонения. • Имеется склонность к переобучению при простых зависимостях и коротких последовательностях.	Для архитектуры характерна высокая потребность в вычислительных ресурсах (квадратичный рост при увеличении длины окна).	Используйте эту архитектуру, если нужно выучить сложные зависимости и построить модель, чувствительную даже к незначительным отклонениям. Рекомендуется задавать длину входного окна, выходного окна и смещения равную половине характерного событийного интервала. Качество модели чувствительно к объему обучающей выборки, поэтому рекомендуется использовать как можно больше данных для обучения. Рекомендуемая длина выборки – от 10 000 событийных интервалов. Не используйте архитектуру для простых одновременных или коротких зависимостей. Это приведет к ложным срабатываниям.

Сценарий: работа с ML-моделями

В этом разделе приводится последовательность действий, которые требуется выполнять при работе с ML-моделями.

Функциональность доступна после добавления лицензионного ключа.

Сценарий работы с ML-моделями состоит из следующих этапов:

1. **Добавление разметок**

   Создайте разметки для отбора интервалов времени, на которых требуется выполнить инференс и/или обучение ML-модели.

2. **Добавление ML-модели**

   Вы можете добавить ML-модель в Kaspersky MLAD одним из следующих способов:

   - Создать ML-модель вручную.

Функциональность доступна после добавления лицензионного ключа для коммерческой лицензии с конструктором моделей.

- Создать ML-модель по шаблону. Предварительно создайте шаблон по нужной ML-модели. Если ML-модель создается по шаблону импортированной ML-модели, вы не можете изменять состав элементов этой ML-модели.

  Функциональность доступна после добавления лицензионного ключа для коммерческой лицензии с конструктором моделей.

- Импортировать ML-модель, созданную специалистами "Лаборатории Касперского" или сертифицированным интегратором в рамках *Услуги построения модели и внедрения Kaspersky MLAD*. Если такая ML-модель использует разметки, они будут импортированы в тот же актив вместе с ML-моделью. После импорта ML-модель нужно активировать.

- Скопировать ранее добавленную ML-модель. Если ML-модель была скопирована с импортированной ML-модели или создана по шаблону импортированной ML-модели, вы не можете изменять состав элементов этой ML-модели.

3. **Работа с элементами ML-модели**

   Вы можете добавлять элементы в состав ML-модели и управлять ими в следующий случаях:

   - ML-модель создана вручную.
   - ML-модель создана по шаблону ML-модели, созданной вручную.
   - ML-модель скопирована с ML-модели, созданной вручную или по шаблону ML-модели, созданной вручную.

   В состав ML-модели вы можете добавить следующие элементы:

   - элементы на основе диагностического правила;
   - элементы на основе эллиптического конверта;
   - предиктивные элементы.

   Управление элементами ML-моделей доступно после добавления лицензионного ключа для коммерческой лицензии с конструктором моделей.

   Изучите рекомендации по использованию элементов ML-модели, добавьте необходимые элементы в ML-модель и задайте их параметры.

   Для проведения инференса ML-модель должна быть обучена. Для этого требуется предварительно обучить все предиктивные элементы и элементы на основе эллиптического конверта в составе ML-модели. Элементы на основе диагностических правил в составе ML-модели обучать не требуется, поэтому они всегда считаются обученными.

   После обучения элементов изучите результаты обучения и оцените их. При необходимости скорректируйте параметры индикатора обучения и/или элементов ML-модели и обучите нужные элементы заново.

ML-модель, импортированная в Kaspersky MLAD, предварительно обучена специалистами "Лаборатории Касперского" или сертифицированным интегратором. ML-модели, созданные по шаблону импортированной ML-модели или созданные путем копирования импортированной ML-модели, также считаются обученными. При необходимости вы можете изменить параметры обучения элементов в составе импортированной ML-модели, указать другие разметки для обучения и обучить элементы заново.

4. **Инференс ML-модели**

   Запустите инференс ML-модели. Вы можете запустить инференс ML-модели на исторических данных и/или данных, поступающих в Kaspersky MLAD в режиме реального времени.

5. **Анализ результатов инференса ML-модели**

   Изучите инциденты и артефакты, сформированные элементами ML-модели в результате инференса, в следующих разделах:

   - **Мониторинг** или **История**, если для ML-модели запущен потоковый инференс.
   - **История**, если для ML-модели был запущен исторический инференс.

   Для отображения прогнозируемых значений тегов и индивидуальных ошибок прогнозов, сформированных предиктивными элементами ML-модели, на единичных графических областях в нужном разделе необходимо предварительно настроить отображение графиков.

   Если запускался исторический инференс, оцените его результаты. Если требуется улучшить качество работы ML-модели, скорректируйте параметры ML-модели, разметок и/или элементов ML-модели. Если ML-модель была импортирована в Kaspersky MLAD, создана по шаблону импортированной ML-модели или скопирована с импортированной ML-модели, вы также можете изменить некоторые параметры ее элементов.

   При необходимости повторно обучите элементы ML-модели. Проведите повторный инференс ML-модели. При повторном запуске инференса на данных, на которых он ранее был проведен, предыдущие результаты инференса на этих данных будут удалены. В случае проведения быстрого исторического инференса будут удалены только инциденты, зарегистрированные ранее на выбранном интервале времени, и для формирования новых инцидентов будут использованы уже существующие артефакты.

6. **Публикация ML-модели**

   Если ML-модель протестирована и готова к продуктивной работе, вы можете опубликовать ее. После публикации ML-модели вы не сможете изменить ее параметры, параметры ее элементов, состав элементов в ML-модели, а сформированные ML-моделью инциденты станут учетными. В отличие от инцидентов, сформированных в процессе инференса неопубликованной ML-моделью, учетные инциденты предполагают принятие мер и ведение отчетности по ним в рамках производственного процесса.

   > Если публикация ML-модели не требуется, пропустите этап 6.

   После завершения обучения и проверки результатов инференса ML-модели подготовьте ML-модель к публикации.

   После подготовки ML-модели к публикации сообщите сотруднику, ответственному за публикацию ML-моделей, о ее готовности, или, если у вас есть необходимые права, опубликуйте ML-модель. Системный администратор может создать роль, которой предоставлено право для публикации ML-моделей, и назначить ее нужному сотруднику.

   При выполнении повторного инференса опубликованной ML-модели на данных, на которых он ранее был проведен, инциденты от предыдущего инференса удалены не будут.

   Вы также можете настроить отправку уведомлений об инцидентах, зарегистрированных опубликованной ML-моделью. Для этого при создании или изменении ранее созданной подписки на уведомления об инцидентах необходимо включить переключатель **Отправлять уведомления только об учетных инцидентах**.

7. **Инференс готовой ML-модели**

   Запустите инференс ML-модели. В процессе инференса ML-модель, анализируя исторические или потоковые данные, формирует артефакты и регистрирует инциденты.

Сценарий: работа с элементами ML-модели на основе диагностического правила

Вы можете добавлять элементы на основе диагностического правила в ML-модель и управлять ими в следующих случаях:

- ML-модель создана вручную.
- ML-модель создана по шаблону ML-модели, созданной вручную.
- ML-модель скопирована с ML-модели, созданной вручную или по шаблону ML-модели, созданной вручную.

Функциональность доступна после добавления лицензионного ключа.

Сценарий работы с диагностическими правилами ML-модели состоит из следующих этапов:

1. **Создание диагностического правила**

   В созданную ранее ML-модель добавьте диагностическое правило. При добавлении элемента задайте общие параметры, шаг сетки, интервалы времени, в течение которых требуется отслеживать поведение тегов, и критерии поведения тегов.

   Элементы на основе диагностических правил в составе ML-модели обучать не требуется, поэтому они считаются обученными.

2. **Инференс ML-модели**

   Запустите инференс ML-модели, в состав которой было добавлено диагностическое правило. Вы можете запустить инференс ML-модели на исторических данных и/или данных, поступающих в Kaspersky MLAD в режиме реального времени.

3. **Анализ результатов инференса ML-модели**

   Изучите инциденты и артефакты, сформированные диагностическим правилом в результате инференса, в следующих разделах:

   - **Мониторинг** или **История**, если для ML-модели запущен потоковый инференс.
   - **История**, если для ML-модели был запущен исторический инференс.

   Если требуется улучшить качество работы ML-модели, скорректируйте параметры индикатора инференса и/или диагностического правила. Проведите повторный инференс ML-модели. При повторном запуске инференса на данных, на которых ранее был проведен инференс, предыдущие результаты инференса на этих данных будут удалены.

Сценарий: работа с элементами ML-модели на основе эллиптического конверта

Вы можете добавлять элементы на основе эллиптического конверта в ML-модель и управлять ими в следующих случаях:

- ML-модель создана вручную.
- ML-модель создана по шаблону ML-модели, созданной вручную.
- ML-модель скопирована с ML-модели, созданной вручную или по шаблону ML-модели, созданной вручную.

Функциональность доступна после добавления лицензионного ключа.

Сценарий работы с элементами ML-модели на основе эллиптического конверта состоит из следующих этапов:

1. **Добавление разметки**

   Создайте разметку для отбора интервалов времени, на которых необходимо выполнить обучение элемента ML-модели на основе эллиптического конверта. Вы можете пропустить этот этап в следующих случаях:

   - Обучение элемента будет проводиться без разметки.
   - Для обучения используется та же разметка, что и для инференса ML-модели.
   - Нужная разметка была создана ранее для обучения другого элемента ML-модели.

2. **Создание элемента ML-модели на основе эллиптического конверта**

   В созданную ранее ML-модель добавьте элемент на основе эллиптического конверта. При добавлении элемента задайте общие параметры, шаг сетки и входные теги.

3. **Обучение элемента ML-модели на основе эллиптического конверта**

   Перед проведением инференса элементы на основе эллиптического конверта необходимо обучить. Задайте параметры обучения элемента. При необходимости для формирования индикатора обучения выберите одну или несколько разметок в параметрах обучения элемента. Если выбрано более одной разметки, то для формирования индикатора обучения используются пересечения выбранных интервалов данных. Если для ML-модели ранее был сформирован индикатор инференса, то разметку инференса следует включить в индикатор обучения. Запустите обучение.

   Изучите результаты обучения и оцените их. При необходимости скорректируйте параметры обучения и обучите элемент заново. Корректировка параметров обучения необходима в следующих случаях:

   - Красная линия на графике **Степень отклонения тегов** является плоской, на графике не прослеживается динамика изменения состояния объекта мониторинга.
   - Красная линия имеет горизонтальные участки вдоль верхней границы графика **Степень отклонения тегов**.
   - Изменения тренда красной линии на графике **Степень отклонения тегов** не соответствуют ожидаемому поведению объекта мониторинга.

- На графике **Степень отклонения тегов** красная линия в основном прижата к нижней части графика, а оранжевая линия проходит в верхней части графика.
- На графике **Распределение значений тегов** отображается более одного пика.

4. **Инференс ML-модели**

   Запустите инференс ML-модели, в состав которой был добавлен элемент на основе эллиптического конверта. Вы можете запустить инференс ML-модели на исторических данных и/или данных, поступающих в Kaspersky MLAD в режиме реального времени.

5. **Анализ результатов инференса ML-модели**

   Изучите инциденты и артефакты, сформированные элементом в результате инференса, в следующих разделах:

   - **Мониторинг** или **История**, если для ML-модели запущен потоковый инференс.
   - **История**, если для ML-модели был запущен исторический инференс.

   Если запускался исторический инференс, оцените его результаты. Если требуется улучшить качество работы ML-модели, скорректируйте параметры индикатора инференса и/или элемента на основе эллиптического конверта. При необходимости повторно обучите элемент и выполните инференс ML-модели. При повторном запуске инференса на данных, на которых он ранее был проведен, предыдущие результаты инференса на этих данных будут удалены.

Сценарий: работа с предиктивными элементами ML-модели

Вы можете добавлять предиктивные элементы в ML-модель и управлять ими в следующих случаях:

- ML-модель создана вручную.
- ML-модель создана по шаблону ML-модели, созданной вручную.
- ML-модель скопирована с ML-модели, созданной вручную или по шаблону ML-модели, созданной вручную.

Функциональность доступна после добавления лицензионного ключа.

Сценарий работы с предиктивными элементами ML-модели состоит из следующих этапов:

1. **Добавление разметки**

   Создайте разметку для отбора интервалов времени, на которых необходимо выполнить обучение предиктивного элемента. Вы можете пропустить этот этап в следующих случаях:

   - Обучение элемента будет проводиться без разметки.
   - Для обучения используется та же разметка, что и для инференса ML-модели.
   - Нужная разметка была создана ранее для обучения другого элемента ML-модели.

2. **Создание предиктивного элемента ML-модели**

В созданную ранее ML-модель добавьте предиктивный элемент. При добавлении элемента задайте общие параметры, шаг сетки, входные и выходные теги, а также выберите архитектуру элемента и задайте параметры архитектуры.

3. **Обучение предиктивного элемента ML-модели**

Перед проведением инференса предиктивные элементы необходимо обучить. Задайте параметры обучения предиктивного элемента. При необходимости для формирования индикатора обучения выберите одну или несколько разметок в параметрах обучения элемента. Если выбрано более одной разметки, то для формирования индикатора обучения используются пересечения интервалов данных, отобранных разметками. Если для ML-модели ранее был сформирован индикатор инференса, то разметку инференса следует включить в индикатор обучения. Запустите обучение.

Изучите результаты обучения и оцените их. При необходимости скорректируйте параметры обучения и обучите предиктивный элемент заново. Корректировка параметров обучения необходима в следующих случаях:

- На графике **Ошибки обучения и валидации** ошибка валидации растет или не изменяется на протяжении всего обучения.
- На графике **Ошибки обучения и валидации** ошибка валидации начала расти под конец обучения.
- В блоке **Прогноз обученной модели** на определенном интервале времени одного или нескольких графиков выходных тегов предсказанное значение начинает систематически отличаться от полученного значения.
- На графике общей ошибки прогноза в блоке **Прогноз обученной модели** не прослеживается динамика изменения состояния объекта мониторинга, красная линия является плоской.
- На графике общей ошибки прогноза в блоке **Прогноз обученной модели** изменения тренда красной линии не соответствуют ожидаемому поведению объекта мониторинга.
- В блоке **Прогноз обученной модели** на графике общей ошибки прогноза красная линия в основном прижата к нижней части графика, а оранжевая линия проходит в верхней части графика.

Корректировка параметров обучения может также понадобиться для предиктивного элемента с нейросетевой архитектурой, если количество узлов РИВС, отобранных для обучения, меньше 10 000.

4. **Инференс ML-модели**

Запустите инференс ML-модели, в состав которой был добавлен предиктивный элемент. Вы можете запустить инференс ML-модели на исторических данных и/или данных, поступающих в Kaspersky MLAD в режиме реального времени.

5. **Анализ результатов инференса ML-модели**

Изучите инциденты и артефакты, сформированные предиктивным элементом в результате инференса, в следующих разделах:

- **Мониторинг** или **История**, если для ML-модели запущен потоковый инференс.
- **История**, если для ML-модели был запущен исторический инференс.

Для отображения прогнозируемых значений тегов и индивидуальных ошибок прогнозов на единичных графических областях необходимо предварительно настроить отображение графиков в нужном разделе.

Если запускался исторический инференс, оцените его результаты. Если требуется улучшить качество работы ML-модели, скорректируйте параметры индикатора инференса и/или предиктивного элемента. При необходимости повторно обучите предиктивный элемент и выполните инференс ML-модели.

Поиск и фильтрация объектов в разделе Модели

В разделе **Модели** в дереве активов вы можете выполнять поиск и фильтрацию следующих объектов:

- ML-моделей;
- шаблонов ML-моделей;
- элементов ML-моделей;
- разметок;
- активов;
- тегов.

Поиск выполняется по именам объектов.

Чтобы найти нужные объекты в дереве активов,

в разделе **Модели** введите поисковый запрос в поле **Поиск**. Поиск выполняется по мере ввода символов в строку поиска. В результаты поиска автоматически включаются омоглифы поисковой строки.

Если найдены объекты, удовлетворяющие поисковому запросу, в дереве отобразятся найденные объекты, а также разделы дерева активов, в составе которых были найдены эти объекты.

Если требуется сбросить поисковый запрос, нажмите на кнопку ⊗ в строке поиска.

Вы также можете выполнять фильтрацию объектов в дереве активов. Для ML-моделей и элементов ML-моделей вы можете выбрать нужные статусы и состояния объектов, оценки исторического инференса ML-моделей и обучения их элементов, а также архитектуры предиктивных элементов и разметки, используемые для обучения элементов или инференса ML-моделей.

Фильтрация применяется к объектам, найденным в соответствии с поисковым запросом. Если поисковый запрос не задан, фильтрация применяется ко всем объектам в дереве активов.

Чтобы отфильтровать объекты в дереве активов:

1. В разделе **Модели** нажмите на кнопку ▽, расположенную над деревом активов.

   Справа отобразятся параметры фильтрации.

2. В раскрывающемся списке **Тип раздела** выберите один или несколько типов разделов дерева актива.

   Вы можете выбрать следующие типы разделов: **Модели**, **Шаблоны моделей**, **Элементы моделей**, **Разметки**, **Активы** и **Теги**.

3. Если вы выбрали тип раздела **Модели**, при необходимости выполните следующие действия:

   - В раскрывающемся списке **Статус модели** выберите нужные статусы ML-моделей.
   - В раскрывающемся списке **Состояние модели** выберите нужные состояния ML-моделей.
   - В раскрывающемся списке **Оценка модели** выберите нужные оценки исторического инференса ML-моделей и/или обучения их элементов.
   - В раскрывающемся списке **Индикатор инференса модели** выберите нужные разметки, используемые в ML-моделях для инференса.

4. Если вы выбрали тип раздела **Элементы моделей**, при необходимости выполните следующие действия:

   - В раскрывающемся списке **Тип элемента модели** выберите один или несколько типов элементов ML-моделей.

     Вы можете выбрать следующие типы элементов ML-моделей: **Предиктивный элемент**, **Правило** и **Эллиптический конверт**.
   - В раскрывающемся списке **Статус элемента модели** выберите нужные статусы элементов ML-моделей.
   - В раскрывающемся списке **Состояние модели** выберите нужные состояния элементов ML-моделей.
   - В раскрывающемся списке **Оценка обучения элемента** выберите нужные оценки обучения элементов ML-моделей.
   - В раскрывающемся списке **Индикатор обучения элемента** выберите нужные разметки, используемые в элементах ML-моделей для обучения.
   - В раскрывающемся списке **Архитектура предиктивного элемента** выберите нужные архитектуры для предиктивных элементов ML-моделей.

5. Если требуется сбросить параметры фильтрации, выполните одно из следующих действий:

   - Для сброса конкретного параметра фильтрации нажмите на кнопку ✕ рядом с нужным параметром.
   - Для сброса всех параметров фильтрации нажмите на кнопку **Очистить фильтры** в правом верхнем углу страницы.

6. Если требуется скрыть отображение параметров фильтрации, нажмите на кнопку ✕ рядом с полем **Поиск**.

Фильтрация объектов выполняется по мере выбора параметров фильтрации. Если найдены объекты, удовлетворяющие параметрам фильтрации, в дереве отобразятся найденные объекты, а также разделы дерева активов, в составе которых были найдены эти объекты.

Если к дереву активов применены какие-либо параметры фильтрации, над деревом активов отображается кнопка .

Работа с разметками

Этот раздел содержит информацию о работе с разметками.

Функциональность доступна после добавления лицензионного ключа.

В разделе **Модели** вы можете создавать, изменять и удалять разметки. Если требуется, вы можете просмотреть на графике интервалы времени данных, на основании которых ML-модель будет выполнять обучение и/или инференс.

Разметки используются в качестве индикаторов обучения или инференса, указывая ML-модели интервалы времени данных, на которых ML-модель может выполнять обучение или инференс. При создании или изменении параметров ML-модели вы можете сформировать индикатор инференса, выбрав одну или несколько ранее созданных разметок. При настройке параметров обучения элементов ML-модели вы можете сформировать индикатор обучения, выбран одну или несколько ранее созданных разметок. Вы можете просмотреть сведения об ML-моделях и/или их элементах, в которых разметка используется в качестве индикаторов инференса и/или обучения.

Создание разметки

Вы можете использовать разметки для формирования индикаторов обучения или инференса ML-модели.

Управление разметками доступно системным администраторам и пользователям с правом **Управление разметками** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы создать разметку:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов рядом с именем актива, для которого требуется создать разметку, откройте вертикальное меню **...** и выберите пункт **Создать разметку**.

   Справа отобразится панель **Создание разметки**.
3. В поле **Имя** укажите имя разметки.
4. В поле **Описание** укажите описание разметки.
5. В поле **Шаг сетки (сек.)** укажите период РИВС в секундах в виде десятичной дроби для разметки.
6. В поле **Цвет разметки** выберите цвет, которым будут выделены интервалы данных, отобранные этой разметкой.
7. Если требуется, включите переключатель **Интерпретировать невозможность оценки условия как выполнение правила**.

   Если Kaspersky MLAD не может однозначно оценить выполнение критериев, заданных в блоках параметров **Фильтрация по времени** и **Условия на теги**, например, вследствие отсутствия наблюдений по тегам, то при включенном параметре программа будет считать заданные критерии выполненными.

8. В блоке параметров **Фильтрация по времени** выполните одно из следующих действий:

   - Для добавления интервала нажмите на кнопку **Добавить интервал** и в раскрывающемся списке **Тип интервала** выберите один из следующих типов временного интервала:

     - **Однократный**. При выборе этого типа интервала укажите дни недели и интервал времени, в течение которого требуется проверять входные данные в соответствии с заданными критериями.

     - **Повторяющийся**. При выборе этого типа интервала укажите годы, даты, дни недели и интервал времени суток, в течение которого требуется периодически проверять входные данные в соответствии с заданными критериями.

   - Для удаления интервала нажмите на кнопку ✕ справа от нужного интервала.

   Вы можете добавить один или несколько временных интервалов.

9. Если требуется добавить вычислимые теги, в блоке параметров **Вычислимые теги** выполните следующие действия:

   a. Нажмите на кнопку **Добавить вычислимый тег**.

   b. В поле **Имя вычислимого тега** укажите имя вычислимого тега.

      Имя вычислимого тега должно быть уникальным среди входящих и вычислимых тегов, используемых в разметке.

   c. В блоке **Теги для вычислений** выполните следующие действия:

      a. Нажмите на значок плюса.

      b. Если в разметке уже определен хотя бы один вычислимый тег, в раскрывающемся списке **Тип тега** выберите одно из следующих значений:

         - **Входящий тег** – для расчета значения на основе значений тегов, поступающих в Kaspersky MLAD.

         - **Вычислимый тег** – для расчета значения на основе значений других вычислимых тегов.

      c. Выберите тег, на основе значений которого необходимо получить значение вычислимого тега.

      d. Если требуется добавить еще один тег для расчета выражения, нажмите на значок плюса.

         Если требуется удалить тег, нажмите на кнопку ✕ справа от нужного тега. Если тег используется в блоке параметров **Условия на теги**, его нельзя удалить.

   d. В поле **Выражение для расчета** введите выражение для расчета вычислимого тега.

   e. Для проверки введенного выражения нажмите на кнопку **Проверить выражение для расчета**.

      Если выражение содержит ошибки, будет выведено соответствующее сообщение. Исправьте ошибки и выполните повторную проверку. Только проверенные вычислимые теги могут быть использованы в разметке.

      Если проверка вычислимого тега не выполнена, разметку не получится сохранить.

   При успешной проверке выражения тегу будет присвоен статус **Проверен**, и его можно использовать для расчета других вычислимых тегов или в критериях поведения тегов.

10. Если требуется добавить критерии поведения тегов, выполните следующие действия:

    a. В блоке параметров **Условия на теги** нажмите на кнопку **Условие**.

    b. Если в разметке уже определен хотя бы один вычислимый тег, в раскрывающемся списке **Тип тега** выберите одно из следующих значений:

    - **Входящий тег** – для добавления критериев поведения для тега, поступающего в Kaspersky MLAD.
    - **Вычислимый тег** – для добавления критериев поведения для вычислимого тега.

    c. В раскрывающемся списке **Тег** выберите тег объекта мониторинга или вычислимый тег, для которого вы хотите добавить критерий поведения.

    Если требуется проверить поведение, прямо противоположное выбранному критерию поведения из блока условий, нажмите на кнопку **NOT** слева от выбранного тега. Надпись **NOT** в кнопке выделится жирным.

    Например, нажмите на кнопку **NOT**, если требуется добавить условие отсутствия ступеньки с заданными параметрами.

    d. В раскрывающемся списке **Поведение** выберите одно из следующих поведений тега, которое требуется отслеживать:

    - **Выше** – значение тега превышает определенный порог.
    - **Ниже** – значение тега опускается ниже определенного порога.
    - **Растет** – линия тренда значений тега растет.
    - **Падает** – линия тренда значений тега падает.
    - **Без динамики** – в линии тренда значений тега отсутствуют выраженные изменения.
    - **Ступенька** – в линии тренда выбранного тега наблюдаются резкие смещения вверх или вниз.
    - **Залипание** – выбранный тег передает одно и то же значение.
    - **Разброс** – вокруг линии тренда выбранного тега наблюдаются резкие изменения разброса значений.

    e. В поле **Окно** укажите продолжительность интервала для анализа поведения тегов в шагах РИВС.

    f. В зависимости от значения выбранного для параметра **Поведение** выполните одно из следующих действий:

    - Если вы выбрали **Выше** или **Ниже**, в поле **Порог** укажите пороговое значение тега и в поле **Срабатывание** минимальное количество выходов за пороговое значение в рамках окна.
    - Если вы выбрали **Растет**, **Падает** или **Без динамики**, в поле **Пороговый уклон** укажите значение уклона тренда в процентах, при превышении которого тренд считается растущим или падающим, и интервал времени между соседними оценками тренда в поле **Период оценки**.

      По умолчанию параметр **Пороговый уклон** не задан. Если значение параметра не задано, Kaspersky MLAD определит направление тренда автоматически.

      По умолчанию параметр **Период оценки** имеет значение `1`. При этом значении оценка тренда происходит в каждом узле РИВС.

- Если вы выбрали **Разброс**, в поле **Порог изменения** укажите минимальное значение, на которое может измениться разброс значений тега вокруг линии тренда, и выберите одно из следующих направлений изменения разброса в раскрывающемся списке **Направление**: **Любое**, **Увеличение**, **Уменьшение**.

  По умолчанию параметр **Порог изменения** не задан. Если значение параметра не задано, Kaspersky MLAD определит его автоматически.

  Критерий поведения тега будет выполнен в момент увеличения и/или уменьшения разброса значения тега вокруг линии тренда.

- Если вы выбрали **Ступенька**, в поле **Порог изменения** укажите минимальное значение, на которое может сместиться линия тренда, и выберите одно из следующих направлений изменения значений тега в раскрывающемся списке **Направление**: **Любое**, **Вверх** или **Вниз**.

  По умолчанию параметр **Порог изменения** не задан. Если значение параметра не задано, Kaspersky MLAD определит его автоматически.

- Если вы выбрали **Залипание**, в поле **Значение** укажите значение, которое должен передавать тег, и допустимый разброс значений тега в поле **Разброс**.

  По умолчанию значение параметра **Разброс** равно нулю. При таком значении любое повторяющееся значение тега вызывает срабатывание критерия.

g. Если требуется добавить критерий поведения тегов в блок условий, нажмите на значок плюса в нижней части блока условий и повторите шаги с 9b по 9e.

h. Если блок условий содержит более одного критерия поведения тегов, выберите один из следующих логических операторов между строками критериев нажатием на кнопку логического оператора:

   - **AND**, если требуется, чтобы одновременно выполнялись все критерии блока.

   - **OR**, если достаточно выполнения хотя бы одного из критериев блока.

i. Если требуется удалить критерий на поведение тегов из блока условий, нажмите на кнопку ✕ в строке с нужным критерием.

11. Если требуется проверить, вызвало ли выполнение предварительного условия выполнение пост-условия, выполните следующие действия:

    a. Добавьте один из следующих темпоральных операторов:

    - **Пауза**, если требуется сформировать результат проверки критериев в последнем узле максимального интервала ожидания.
    - **Если далее**, если требуется сформировать результат проверки критериев в момент проверки предварительного условия.

    Кнопки **Пауза** и **Если далее** доступны после добавления хотя бы одного условия.

    Разметка с темпоральным оператором **Если далее** может быть использована только в индикаторах обучения.

    b. В поле **Продолжительность (шаги)** укажите следующие интервалы ожидания:

    - **от** – интервал между узлом проверки предварительного условия и узлом РИВС, с которого начнется проверка пост-условия (минимальный интервал ожидания).
    - **до** – интервал между узлом проверки предварительного условия и узлом РИВС, в котором закончится проверка пост-условия (максимальный интервал ожидания).

    Проверка пост-условия проводится в узлах РИВС между минимальным и максимальным интервалом ожидания.

    c. В раскрывающемся списке **Проверить** выберите один из следующих групповых операторов:

    - Если требуется выполнение критериев поведения тегов из пост-условия во всех узлах РИВС между минимальным и максимальным интервалом ожидания, выберите групповой оператор **Все шаги**.
    - Если требуется выполнение критериев поведения тегов из пост-условия хотя бы в одном узле РИВС между минимальным и максимальным интервалом ожидания, выберите групповой оператор **Любой шаг**.

    В случае добавления темпорального оператора **Пауза** результат проверки критериев определяется в последнем узле максимального интервала ожидания. Если проводится более одной проверки условия с помощью темпорального оператора **Пауза**, то предварительным условием для каждой следующей проверки темпорального условия **Пауза** является результат проверки предыдущего темпорального условия.

    В случае добавления темпорального оператора **Если далее** результат проверки критериев формируется в момент проверки предварительного условия.

12. Выберите один из следующих логических операторов между блоками разметки нажатием на кнопку логического оператора:

    - **AND**, если требуется, чтобы были выполнены критерии обоих блоков условий.
    - **OR**, если требуется, чтобы был выполнен критерий хотя бы одного из блоков условий.

13. Нажмите на кнопку **Сохранить**.

Новая разметка отобразится в группе **Разметки** дерева активов. Группа **Разметки** создается автоматически и отображается в составе выбранного раздела дерева активов.

Просмотр графика разметок

После создания разметки вы можете просмотреть на графике интервалы времени данных, отобранные разметкой.

Функциональность доступна после добавления лицензионного ключа.

Чтобы просмотреть график разметок:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите разметку, график которой вы хотите просмотреть.

   Справа отобразится список параметров.
3. Нажмите на кнопку **На графике**.

   Справа отобразится панель с графиком разметки.
4. В раскрывающемся списке **Пресет** выберите необходимый пресет.
5. Если требуется, в поле **Разметки** выберите дополнительные разметки.

   Если выбрана одна разметка, то на графике отобразятся интервалы, отобранные разметкой, в указанном при создании цвете. Если выбрано более одной разметки, пересечения отобранных разными разметками интервалов отобразятся с серым фоном.

6. Если требуется выбрать дату и время для отображения данных, выполните одно из следующих действий:

   - В поле **Центр графика** выберите дату и время, на которое требуется отображать данные на графике.

     Вертикальная черная пунктирная линия будет указывать на выбранную дату и время (центр графика).

   - Нажмите на кнопку ⊙, которая расположена слева от оси времени, и выберите на оси времени нужную точку.

     Выбранная точка станет новым центром графика. Вертикальная черная пунктирная линия будет указывать на новые дату и время.

7. Если требуется выбрать интервал времени для отображения данных на графике, выполните одно из следующих действий:

   - Если требуется отображать данные за фиксированный интервал времени, в раскрывающемся списке **Масштаб** выберите необходимый интервал времени. По умолчанию доступны следующие временные интервалы:

     - 1, 5, 10, 15 и 30 минут;
     - 1, 3, 6 и 12 часов;
     - 1, 2, 15 и 30 дней;
     - 3 и 6 месяцев;
     - 1, 2 и 3 года.

     При необходимости системный администратор может создать, изменить или удалить временные интервалы.

   - Если требуется отображать данные за произвольный интервал времени, нажмите на кнопку , которая расположена слева от оси времени, выберите на оси времени нужный интервал и нажмите на кнопку **Применить**. Если требуется еще раз изменить масштаб, повторите это действие.

Просмотр сведений об элементах, связанных с разметками

Разметки могут быть связаны с ML-моделями и/или их элементами, если разметки используются в них в качестве индикаторов инференса и/или обучения. Вы можете просмотреть информацию об ML-моделях и/или элементах ML-моделей, связанных с разметкой.

Пока разметка связана с ML-моделями и/или их элементами, вы не можете ее удалить.

> Функциональность доступна после добавления лицензионного ключа.

Чтобы просмотреть сведения о связанных элементах:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите разметку, связи с которой вы хотите просмотреть.

   Справа отобразится список параметров.
3. Нажмите на кнопку **Показать связи**.

   Отобразится окно **Связанные элементы**. В этом окне отобразится информация, в каких ML-моделях и/или их элементах выбранная разметка используется в качестве индикаторов инференса и/или обучения соответственно.

   Кнопка не отображается, если у разметки отсутствуют связи с ML-моделями и их элементами.

Копирование разметки

Вы можете создать разметку, скопировав ранее созданную разметку. При копировании будет создана разметка, параметры которой идентичны параметрам исходной разметки в момент ее копирования.

> Управление разметками доступно системным администраторам и пользователям с правом **Управление разметками** из группы прав **Управление ML-моделями**.
> Функциональность доступна после добавления лицензионного ключа.

Чтобы скопировать разметку:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите разметку, которую вы хотите скопировать.

   Справа отобразится список параметров.
3. В правом верхнем углу страницы нажмите на кнопку .

   Справа отобразится панель **Копирование разметки**.
4. В поле **Имя** укажите имя разметки.

   По умолчанию разметке присваивается имя в формате `<имя исходной разметки>_Cloned_<дата и время копирования>`.
5. В раскрывающемся списке **Актив** выберите актив, к которому вы хотите отнести разметку.
6. Нажмите на кнопку **Сохранить**.

   Новая разметка отобразится в группе **Разметки** дерева активов. Группа **Разметки** создается автоматически и отображается в составе выбранного раздела дерева активов.

Вы также можете перейти к копированию разметки, нажав на вертикальное меню **...** и выбрав пункт **Копировать разметку**.

Изменение разметки

Вы можете изменять параметры разметок.

Изменение параметров разметки недоступно для импортированных ML-моделей и ML-моделей, созданных путем копирования импортированных ML-моделей или по шаблону импортированных ML-моделей.

Управление разметками доступно системным администраторам и пользователям с правом **Управление разметками** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы изменить разметку:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите разметку, которую вы хотите изменить.

   Справа отобразится список параметров.
3. Нажмите на кнопку **Изменить**.
4. Если требуется, измените параметры разметки. Описание параметров см. в инструкции по созданию разметки.
5. В правом верхнем углу страницы нажмите на кнопку **Сохранить**.

Удаление разметки

Вы можете удалить разметку, если она не используется для обучения или инференса какой-либо ML-модели, а также не была импортирована в Kaspersky MLAD вместе с ML-моделью.

Управление разметками доступно системным администраторам и пользователям с правом **Управление разметками** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы удалить разметку:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите разметку, которую вы хотите удалить.

   Справа отобразится список параметров.
3. В правом верхнем углу страницы нажмите на кнопку .

   Если разметка используется в качестве индикаторов инференса и/или обучения в ML-моделях и/или их элементах, отобразится информация об элементах, с которыми связана выбранная разметка. Удаление разметки в таком случае невозможно.
4. Если у разметки отсутствуют связи с ML-моделями или их элементами, в открывшемся окне подтвердите удаление разметки.

Вы также можете перейти к удалению разметки, нажав на вертикальное меню **...** и выбрав пункт **Удалить разметку**.

Работа с импортированными ML-моделями

Этот раздел содержит информацию о работе с импортированными ML-моделями и их элементами.

Функциональность доступна после добавления лицензионного ключа.

ML-модель может быть предоставлена специалистами "Лаборатории Касперского" или сертифицированным интегратором в рамках *Услуги построения модели и внедрения Kaspersky MLAD*. Такую ML-модель требуется импортировать в Kaspersky MLAD и активировать. Вы не можете создавать новые элементы для импортированной ML-модели, а также удалять уже существующие элементы.

ML-модель импортируется в Kaspersky MLAD уже обученной. Если требуется, вы можете дополнительно обучить предиктивные элементы и элементы на основе эллиптического конверта в составе импортированной ML-модели перед выполнением инференса и/или ее публикацией.

Импорт ML-модели

Если ML-модель была создана специалистами "Лаборатории Касперского" или сертифицированным интегратором, вы можете импортировать эту ML-модель в Kaspersky MLAD. Вместе с ML-моделью в Kaspersky MLAD будут импортированы разметки, использованные для ее обучения.

При импорте ML-модели, размер которой превышает 1 ГБ, работа Kaspersky MLAD может замедлиться.

Импорт ML-моделей доступен системным администраторам и пользователям с правом **Загрузка моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы импортировать ML-модель:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов рядом с именем актива, для которого требуется импортировать ML-модель, откройте вертикальное меню **...** и выберите пункт **Импортировать модель**.
3. В открывшемся окне выберите файл ML-модели.

   Файл ML-модели поставляется в виде архива формата TAR размером не более 1,5 ГБ.

ML-модель будет импортирована в Kaspersky MLAD. Новая ML-модель отобразится в группе **Модели** дерева активов. Группа **Модели** создается автоматически и отображается в составе выбранного раздела дерева активов. Если в составе импортированной ML-модели есть предиктивные элементы, элементы на основе эллиптического конверта и/или элементы на основе диагностических правил, в группе **Модели** будут отображаться подгруппы **Предиктивные элементы**, **Эллиптические конверты** и/или **Правила** соответственно.

После импорта ML-модели присваивается статус **Не активирована**. Требуется активировать ML-модель. При повторном импорте ML-модели, которая ранее была активирована и затем удалена, повторная активация ML-модели не требуется.

Активация импортированной ML-модели

После импорта в Kaspersky MLAD ML-модели, подготовленной специалистами "Лаборатории Касперского" или сертифицированным интегратором, ее требуется активировать.

При потере кода для активации ML-модели требуется отправить запрос специалисту "Лаборатории Касперского" для получения нового кода.

Активация импортированных ML-моделей доступна системным администраторам и пользователям с правом **Активация моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы активировать импортированную ML-модель:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите импортированную ML-модель.

   Справа появится область деталей.
3. В поле **Код для активации модели** введите код, полученный от сотрудников "Лаборатории Касперского", и нажмите на кнопку **Активировать** в правом верхнем углу страницы.

   ML-модель активирована. Ей будет присвоен статус **Обучена**. При необходимости вы можете обучить ML-модель повторно, например, на новых данных.

   Для запуска анализа данных телеметрии от объекта мониторинга вы можете запустить инференс ML-модели.

Изменение параметров элемента импортированной ML-модели

Вы можете изменять некоторые параметры элементов импортированной ML-модели.

Изменение параметров недоступно, если ML-модели присвоен статус **Готова к публикации** или **Опубликована**, а также во время инференса ML-модели.

Изменение параметров элементов импортированных ML-моделей доступно системным администраторам и пользователям с правом **Изменение моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы изменить параметры элемента импортированной ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите элемент ML-модели, который вы хотите изменить.

   Справа отобразится список параметров.
3. В правом верхнем углу страницы нажмите на кнопку **Изменить**.
4. Если требуется, измените следующие параметры элемента:

   - Имя и описание элемента ML-модели.
   - Период напоминания.
   - Период подавления повторных срабатываний.
   - Интервал наблюдения за аномалией.
   - Доля длительности аномалии в интервале.
   - Порог регистрации инцидентов.
   - Цвет точек-индикаторов инцидентов.
   - Статус и причину инцидента.
   - Приоритет инцидента.
   - Экспертные рекомендации.
   - Степень сглаживания.

   Изменение параметров **Период напоминания (сек.)**, **Период подавления повторных срабатываний (сек.)**, **Интервал наблюдения за аномалией (сек.)**, **Доля длительности аномалии в интервале**, **Порог регистрации инцидентов** и **Степень сглаживания** приводит к изменению чувствительности обнаружения аномалий.
5. В правом верхнем углу страницы нажмите на кнопку **Сохранить**.

Работа с ML-моделями, созданными вручную

Этот раздел содержит информацию о работе с ML-моделями, созданными вручную и их элементами.

> Функциональность доступна после добавления лицензионного ключа.

В случае создания ML-модели вручную вы можете добавлять предиктивные элементы ML-моделей, элементы на основе эллиптических конвертов и/или элементы на основе диагностических правил, изменять и удалять их.

Для проведения инференса ML-модель должна быть обучена. Для этого все предиктивные элементы и элементы на основе эллиптического конверта в составе ML-модели требуется предварительно обучить. При необходимости вы можете просмотреть результаты обучения элементов. Элементы на основе диагностических правил обучать не требуется, поэтому они считаются обученными.

Создание ML-модели

Вы можете самостоятельно создавать ML-модели при приобретении Kaspersky MLAD с функциональностью конструктора моделей.

Создание ML-моделей доступно системным администраторам и пользователям с правом **Создание моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы создать ML-модель:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов рядом с именем актива, для которого вы хотите создать ML-модель, откройте вертикальное меню **...** и выберите пункт **Создать модель**.

   Справа отобразится список параметров.
3. В поле **Имя** укажите имя ML-модели.

   Вы можете указать имя ML-модели длиной не более 100 символов.
4. В поле **Описание** укажите описание ML-модели.
5. Если требуется применить разметки для отбора данных для выполнения инференса ML-модели, в блоке параметров **Индикатор инференса** выберите нужные разметки.

   Выбранные разметки сформируют индикатор инференса.

   Если выбрано более одной разметки, то для формирования индикатора инференса используются пересечения выбранных интервалов данных.
6. Если требуется просмотреть, какие данные будут отобраны разметками, нажмите на кнопку **На графике**.

   Если выбрана одна разметка, то на графике отобразятся интервалы данных разметки в указанном при создании цвете. Если выбрано более одной разметки, на графике отобразятся пересечения интервалов данных разметок.
7. В правом верхнем углу страницы нажмите на кнопку **Сохранить**.

Новая ML-модель отобразится в группе **Модели** дерева активов. Группа **Модели** создается автоматически и отображается в составе выбранного раздела дерева активов.

Добавление предиктивного элемента ML-модели

Добавление элементов ML-моделей доступно системным администраторам и пользователям с правом **Создание моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы добавить предиктивный элемент ML-модели:

1. В основном меню выберите раздел **Модели**.
2. Для добавления предиктивного элемента выполните следующие действия:
   a. В дереве активов рядом с именем ML-модели, к которой вы хотите добавить предиктивный элемент, откройте вертикальное меню **...** и выберите пункт **Создать элемент**.
   b. В открывшемся окне выберите тип элемента **Предиктивный элемент**.
   c. Нажмите на кнопку **Создать**.

   Справа отобразится список параметров.
3. В поле **Имя** укажите имя элемента ML-модели.
4. В поле **Описание** укажите описание элемента ML-модели.

5. В блоке параметров **Общие параметры элемента** выполните следующие действия:

   a. В поле **Период напоминания (сек.)** укажите период в секундах, при достижении которого ML-модель сгенерирует повторный инцидент при сохранении аномального поведения в каждом узле РИВС.

      По умолчанию этот параметр имеет значение `0`, что соответствует отсутствию напоминаний.

   b. В поле **Период подавления повторных срабатываний (сек.)** укажите период в секундах, в течение которого ML-модель не регистрирует повторные инциденты от одного и того же элемента.

      По умолчанию этот параметр имеет значение `0` (повторные инциденты регистрируются).

   c. В поле **Интервал наблюдения за аномалией (сек.)** укажите период в секундах, в течение которого отслеживается аномальное поведение тега для принятия решения о регистрации инцидента.

   d. В поле **Доля длительности аномалии в интервале** укажите в виде десятичной дроби долю от периода, заданного в параметре **Интервал наблюдения за аномалией (сек.)**, при достижении которой элемент ML-модели зарегистрирует инцидент.

      Вы можете указать значение в диапазоне от `0` до `1`.

   e. В поле **Порог регистрации инцидентов** укажите пороговое значение ошибки прогноза, при достижении которого происходит регистрация инцидента.

      По умолчанию значение порога автоматически корректируется после каждого обучения элемента. Если после завершения обучения вы включите переключатель **Зафиксировать порог регистрации инцидентов**, то значение порога будет зафиксировано и не изменится после повторного обучения элемента. При необходимости вы можете изменить значение этого параметра.

   f. В поле **Цвет точек-индикаторов инцидентов** выберите цвет точек-индикаторов инцидентов, зарегистрированных элементом ML-модели, на графиках в разделах **Мониторинг** и **История**. В этом цвете также будет отображаться график артефакта, сформированный этим элементом.

   g. Если требуется, в раскрывающемся списке **Статус инцидента** выберите статус инцидента, который будет автоматически присвоен инцидентам, зарегистрированным элементом ML-модели.

      По умолчанию статус не установлен.

   h. Если требуется, в раскрывающемся списке **Причина инцидента** выберите причину инцидента, которая будет автоматически задана для инцидентов, зарегистрированных элементом ML-модели, если эта причина заранее известна.

   i. Если требуется, в раскрывающемся списке **Приоритет инцидента** выберите приоритет, который будет автоматически присвоен инцидентам, зарегистрированным элементом ML-модели.

      По умолчанию инциденту присваивается приоритет **Средний**.

   j. Если требуется, в поле **Экспертные рекомендации** укажите экспертные рекомендации, которые будут автоматически добавлены инцидентам, зарегистрированным элементом ML-модели, если содержание этих рекомендаций заранее известно.

6. Выберите одну из следующих архитектур предиктивного элемента ML-модели: **Dense**, **RNN**, **CNN**, **TCN**, **Transformer** или **LR**.

7. Если требуется, включите переключатель **Расширенные параметры нейронной сети**.

   Переключатель доступен только для элементов с архитектурой **Dense**, **RNN**, **CNN**, **TCN** или **Transformer**.

8. В блоке параметров **Основные параметры** выполните следующие действия:

   a. В поле **Шаг сетки (сек.)** укажите период РИВС для элемента в секундах в виде целого числа или десятичной дроби.

   b. В поле **Степень сглаживания** укажите коэффициент сглаживания суммарной ошибки прогноза в виде десятичной дроби.

      Чем больше значение коэффициента, тем меньше применяется сглаживание к данным.

   c. В поле **Степенной показатель ошибки прогноза** укажите степень, в которую возводится значение ошибки прогноза в каждом узле РИВС перед вычислением суммарной ошибки.

      Значение параметра влияет на значение суммарной ошибки прогноза, формируемой предиктивным элементом во время инференса ML-модели. Значение параметра также влияет на отображение суммарной ошибки прогноза на графике артефакта элемента ML-модели в разделах **Мониторинг** и **История**. Чем выше значение параметра, тем больше значение суммарной ошибки прогноза и тем выше красная линия на графике артефакта элемента.

9. В блоке параметров **Параметры окон** выполните следующие действия:

   a. В поле **Входное окно (шаги)** укажите размер окна для входных значений, на основе которых элемент ML-модели прогнозирует выходные значения.

      Размер окна указывается в количестве шагов РИВС.

   b. В поле **Смещение выходного окна** укажите количество шагов РИВС, на которое начало выходного окна будет смещено относительно начала входного окна.

   c. В поле **Выходное окно (шаги)** укажите длину прогнозирования выходных тегов, вычисляемых на основании входных тегов на входном окне.

10. В блоке параметров **Входные и выходные теги** выполните следующие действия:

    a. Нажмите на кнопку **Выбрать теги**.

    Откроется панель **Выбор тегов модели**, отображающая **таблицу с деревом активов**.

    В таблице с деревом активов отображается следующая информация:

    - **Имя** – имя актива или тега в дереве активов.
    - **Описание** – описание актива или тега в дереве активов.
    - **Входной тег** – переключатель, позволяющий включить тег во входные теги элемента ML-модели или исключить тег из входных тегов.
    - **Выходной тег** – переключатель, позволяющий включить тег в выходные теги элемента ML-модели или исключить тег из выходных тегов.

    b. Если требуется настроить отображение таблицы с деревом активов, выполните следующие действия:

    a. Нажмите на кнопку , расположенную в правом верхнем углу панели.

    b. Установите флажки рядом с теми столбцами таблицы, которые необходимо отображать.

    c. Нажмите на кнопку **Сохранить**.

    c. Если требуется использовать теги, входящие в определенные пресеты, выполните следующие действия:

    a. Нажмите на кнопку , расположенную в правом верхнем углу панели.

    b. Выберите нужные пресеты.

    При необходимости введите поисковый запрос в поле **Поиск**. Поиск выполняется по мере ввода символов в строку поиска.

    c. Нажмите на кнопку **Применить**.

    В панели **Выбор тегов модели** отобразятся теги, входящие в выбранные пресеты.

    d. Для выбора тегов, которые служат исходными данными для прогнозирования значений выходных тегов, выполните одно из следующих действий:

    - Если требуется выбрать определенный тег, включите переключатель в столбце **Входной тег** для нужного тега.
    - Если требуется выбрать несколько тегов, установите флажки рядом с нужными тегами и в раскрывающемся списке **Массовые действия** выберите элемент **Включить** в блоке **Входные теги**.

    e. Для выбора тегов, поведение которых прогнозируется элементом модели, выполните одно из следующих действий:

    - Если требуется выбрать определенный тег, включите переключатель в столбце **Выходной тег** для нужного тега.
    - Если требуется выбрать несколько тегов, установите флажки рядом с нужными тегами и в раскрывающемся списке **Массовые действия** выберите элемент **Включить** в блоке **Выходные теги**.

f. Если требуется отобразить только теги, которые были выбраны в качестве входных и/или выходных, включите переключатель **Используемые теги** над деревом активов.

g. Если требуется исключить выбранные теги из входных или выходных, установите флажки рядом с нужными тегами и в раскрывающемся списке **Массовые действия** выберите элемент **Исключить** в блоке **Входные теги** или **Выходные теги**.

h. Если требуется поменять местами входные и выходные теги, установите флажки рядом с нужными тегами и в раскрывающемся списке **Массовые действия** выберите элемент **Поменять местами**.

Теги, выбранные ранее в качестве входных, станут выходными, а теги, выбранные ранее в качестве выходных, станут входными.

i. Нажмите на кнопку **Сохранить**.

11. Если включен режим расширенной настройки и вы добавляете элемент с Dense-архитектурой, выполните следующие действия:

a. В поле **Множители для вычисления количества нейронов на слоях** укажите через запятую без пробелов множители, при умножении которых на количество входных тегов будет рассчитано количество нейронов на каждом слое элемента ML-модели.

По умолчанию этот параметр имеет значение `8,4,8`.

b. В поле **Функции активации на слоях** укажите одну из следующих функций активации на каждом слое элемента ML-модели через запятую без пробелов:

- `relu` – нелинейная функция активации, которая преобразует входное значение в значение от `0` до положительной бесконечности.
- `selu` – монотонно возрастающая функция, которая включает нормализацию, основанную на центральной предельной теореме.
- `linear` – линейная функция, представляющая собой прямую линию и пропорциональная входным данным.
- `sigmoid` – нелинейная функция, которая преобразует входные значения в значения от `0` до `1`.
- `tanh` – функция гиперболического тангенса, которая преобразует входные значения в значения от `-1` до `1`.
- `softmax` – функция для преобразования вектора значений в вероятностное распределение, которое суммируется до `1`.

По умолчанию этот параметр имеет значение `relu,relu,relu`.

c. В поле **Регуляризация** укажите коэффициент регуляризации в виде десятичной дроби для предотвращения переобучения элемента ML-модели.

По умолчанию этот параметр имеет значение `0`.

12. Если включен режим расширенной настройки и вы добавляете элемент с RNN-архитектурой, выполните следующие действия:

    a. В поле **Количество GRU-нейронов на слоях** укажите количество GRU-нейронов на слоях через запятую без пробелов.

    По умолчанию этот параметр имеет значение `40,40`.

    b. В поле **Количество распределенных по времени нейронов на слоях декодирующего блока** укажите количество нейронов, распределенных по времени на слоях декодирующего блока, через запятую без пробелов.

    По умолчанию этот параметр имеет значение `40,20`.

    c. Если требуется восстанавливать данные, принимаемые на вход сети, включите переключатель **Использовать автокодировщик**.

    d. В поле **Регуляризация** укажите коэффициент регуляризации в виде десятичной дроби для предотвращения переобучения элемента ML-модели.

    По умолчанию этот параметр имеет значение `0`.

13. Если включен режим расширенной настройки и вы добавляете элемент с CNN-архитектурой, выполните следующие действия:

    a. В поле **Размер фильтров на слоях** укажите размер фильтров для каждого слоя элемента через запятую без пробелов.

    По умолчанию этот параметр имеет значение `2,2,2`.

    b. В поле **Количество фильтров на слоях** укажите количество фильтров для каждого слоя элемента ML-модели через запятую без пробелов.

    По умолчанию этот параметр имеет значение `50,50,50`.

    c. В поле **Регуляризация** укажите коэффициент регуляризации в виде десятичной дроби для предотвращения переобучения элемента ML-модели.

    По умолчанию этот параметр имеет значение `0`.

    d. В поле **Размер окна выборки максимума (MaxPooling)** укажите размер окна выборки максимального значения на каждом слое через запятую без пробелов.

    По умолчанию этот параметр имеет значение `2,2,2`.

    e. В поле **Количество нейронов на слоях декодирующего блока** укажите количество нейронов на слоях декодирующего блока.

    f. Если требуется восстанавливать данные, принимаемые на вход сети, включите переключатель **Использовать автокодировщик**.

14. Если включен режим расширенной настройки и вы добавляете элемент с TCN-архитектурой, выполните следующие действия:

    a. В поле **Регуляризация** укажите коэффициент регуляризации в виде десятичной дроби для предотвращения переобучения элемента ML-модели.

    По умолчанию этот параметр имеет значение `0`.

    b. В поле **Размер фильтров** укажите размер фильтров элемента ML-модели.

    По умолчанию этот параметр имеет значение `3`.

    c. В поле **Количество слоев в остаточном блоке (residual block)** укажите количество слоев в остаточном блоке.

    По умолчанию этот параметр имеет значение `1`.

    d. В поле **Количество фильтров на слоях** укажите количество фильтров на каждом слое элемента ML-модели.

    По умолчанию этот параметр имеет значение `64`.

    e. В поле **Расширения на слоях (dilations)** укажите экспоненциальные значения расширения выходных данных на слоях в виде списка, элементы которого перечислены через запятую.

    По умолчанию этот параметр имеет значение `1,2,4,8,16`.

    f. В поле **Тип слоя перед выходным** выберите один из следующих типов слоя, предшествующего выходному слою:

    - **TimeDistributedDense** (по умолчанию) – слой с полносвязной архитектурой.
    - **GRU** – слой с рекуррентной архитектурой.

    g. В раскрывающемся списке **Функция активации** выберите одну из следующих функций активации:

    - **linear** – линейная функция активации, результат которой пропорционален входному значению.
    - **relu** – нелинейная функция активации, которая преобразует входное значение в значение от нуля до положительной бесконечности. Если входное значение меньше или равно нулю, функция возвращает значение ноль, иначе функция возвращает входное значение.

    По умолчанию этот параметр имеет значение `linear`.

15. Если включен режим расширенной настройки и вы добавляете элемент с Transformer-архитектурой, выполните следующие действия:

    a. В поле **Регуляризация в кодирующем блоке** укажите коэффициент регуляризации в кодирующем блоке в виде десятичной дроби.

    По умолчанию этот параметр имеет значение `0.01`.

    b. В поле **Количество голов внимания** укажите количество голов внимания (англ. attention heads).

    По умолчанию этот параметр имеет значение `1`.

    c. В поле **Количество кодирующих блоков** укажите количество кодирующих блоков.

    По умолчанию этот параметр имеет значение `1`.

    d. В поле **Множители для вычисления количества нейронов на слоях** укажите через запятую без пробелов множители, при умножении которых на количество входных тегов будет рассчитано количество нейронов на слоях декодирующего блока.

    По умолчанию этот параметр имеет значение `10,5,10`.

16. В правом верхнем углу страницы нажмите на кнопку **Сохранить**.

    При создании первого элемента в составе ML-модели в дереве активов будет автоматически создана группа **Предиктивные элементы**. Созданный элемент отобразится в этой группе.

Элементу ML-модели будет присвоен статус **Не обучен**, а ML-модели, к которой относится добавленный элемент, будет присвоен статус **Не обучена**. Для запуска инференса ML-модели требуется обучить все ее предиктивные элементы и элементы на основе эллиптического конверта.

Изменение предиктивного элемента ML-модели

Вы можете изменять параметры предиктивных элементов ML-модели.

Изменение параметров недоступно, если ML-модели присвоен статус **Готова к публикации** или **Опубликована**, а также во время инференса ML-модели и обучения элемента.

> Изменение элементов ML-моделей доступно системным администраторам и пользователям с правом **Изменение моделей** из группы прав **Управление ML-моделями**.
> Функциональность доступна после добавления лицензионного ключа.

Чтобы изменить предиктивный элемент ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите предиктивный элемент, который вы хотите изменить.

   Справа отобразится список параметров.
3. В правом верхнем углу страницы нажмите на кнопку **Изменить**.
4. Если требуется, измените параметры предиктивного элемента ML-модели. Описание параметров см. в инструкции по добавлению предиктивного элемента ML-модели.

5. В правом верхнем углу страницы нажмите на кнопку **Сохранить**.

6. Подтвердите сохранение изменений.

   Если были изменены архитектура и параметры архитектуры элемента, а также параметры элемента в блоках **Основные параметры** (кроме параметра **Степень сглаживания**), **Параметры окон** и/или **Входные и выходные теги**, элемент ML-модели необходимо повторно обучить. После внесения изменений в эти параметры элементу будет присвоен статус **Не обучен**.

Добавление элемента ML-модели на основе диагностического правила

Результатом работы (артефактом) диагностического правила в узле РИВС является число 0 или 1 в зависимости от того, выполнены ли заданные в правиле условия на теги в этом узле. Однако, если в составе диагностического правила созданы один или несколько вычислимых тегов, но не задано ни одного критерия на поведение тегов, то результатом работы (артефактом) диагностического правила в каждом узле РИВС будет значение последнего из сконфигурированных в правиле вычислимых тегов, вычисленное для этого узла РИВС. Для принятия решения о регистрации инцидента это значение будет сравниваться с порогом, заданным в параметрах элемента модели. По умолчанию значение порога равно 1. При необходимости вы можете его изменить.

> Добавление элементов ML-моделей доступно системным администраторам и пользователям с правом **Создание моделей** из группы прав **Управление ML-моделями**.
> Функциональность доступна после добавления лицензионного ключа.

Чтобы добавить элемент ML-модели на основе диагностического правила:

1. В основном меню выберите раздел **Модели**.

2. Для добавления диагностического правила выполните следующие действия:

   a. В дереве активов рядом с именем ML-модели, к которой вы хотите добавить диагностическое правило, откройте вертикальное меню ••• и выберите пункт **Создать элемент**.

   b. В открывшемся окне выберите тип элемента **Правило**.

   c. Нажмите на кнопку **Создать**.

   Справа отобразится список параметров.

3. В поле **Имя** укажите имя диагностического правила.

4. В поле **Описание** укажите описание диагностического правила.

5. В блоке параметров **Общие параметры элемента** выполните следующие действия:

   a. В поле **Период напоминания (сек.)** укажите период в секундах, при достижении которого ML-модель сгенерирует повторный инцидент при сохранении аномального поведения в каждом узле РИВС.

      По умолчанию этот параметр имеет значение `0`, что соответствует отсутствию напоминаний.

   b. В поле **Период подавления повторных срабатываний (сек.)** укажите период в секундах, в течение которого ML-модель не регистрирует повторные инциденты от одного и того же элемента.

      По умолчанию этот параметр имеет значение `0` (повторные инциденты не подавляются).

   c. В поле **Интервал наблюдения за аномалией (сек.)** укажите период в секундах, в течение которого отслеживается аномальное поведение тега для принятия решения о регистрации инцидента.

   d. В поле **Доля длительности аномалии в интервале** укажите в виде десятичной дроби долю от периода, заданного в параметре **Интервал наблюдения за аномалией (сек.)**, при достижении которой элемент ML-модели зарегистрирует инцидент.

      Вы можете указать значение в диапазоне от `0` до `1`.

   e. В поле **Порог регистрации инцидентов** укажите пороговое значение, при достижении которого происходит регистрация инцидента.

   f. В поле **Цвет точек-индикаторов инцидентов** выберите цвет точек-индикаторов инцидентов, зарегистрированных элементом ML-модели, на графиках в разделах **Мониторинг** и **История**. В этом цвете также будет отображаться график артефакта, сформированный этим элементом.

   g. Если требуется, в раскрывающемся списке **Статус инцидента** выберите статус инцидента, который будет автоматически присвоен инцидентам, зарегистрированным элементом ML-модели.

      По умолчанию статус не установлен.

   h. Если требуется, в раскрывающемся списке **Причина инцидента** выберите причину инцидента, которая будет автоматически задана для инцидентов, зарегистрированных элементом ML-модели, если эта причина заранее известна.

   i. Если требуется, в раскрывающемся списке **Приоритет инцидента** выберите приоритет, который будет автоматически присвоен инцидентам, зарегистрированным элементом ML-модели.

      По умолчанию инциденту присваивается приоритет **Средний**.

   j. Если требуется, в поле **Экспертные рекомендации** укажите экспертные рекомендации, которое будет автоматически добавлены инцидентам, зарегистрированным элементом ML-модели, если содержание этих рекомендаций заранее известно.

6. В блоке параметров **Параметры правила** выполните следующие действия:

   a. В поле **Шаг сетки (сек.)** укажите период РИВС для элемента в секундах в целого числа или виде десятичной дроби.

   b. Если требуется, включите переключатель **Интерпретировать невозможность оценки условия как выполнение правила**.

      Если Kaspersky MLAD не может однозначно оценить выполнение критериев, заданных в блоках параметров **Фильтрация по времени** и **Условия на теги**, например, вследствие отсутствия наблюдений по тегам, то при включенном параметре программа будет считать правило выполненным.

7. В блоке параметров **Фильтрация по времени** выполните следующие действия:

   a. Нажмите на кнопку **Добавить интервал**.

   b. В раскрывающемся списке **Тип интервала** выберите один из следующих типов временного интервала:

      - **Однократный**. При выборе этого типа интервала укажите дни недели и интервал времени, в течение которого требуется проверять входные данные в соответствии с заданными критериями.

      - **Повторяющийся**. При выборе этого типа интервала укажите годы, даты, дни недели и интервал времени суток, в течение которого требуется периодически проверять входные данные в соответствии с заданными критериями.

   c. Если требуется добавить еще один интервал, нажмите на кнопку **Добавить интервал** и выполните шаг 7b.

   d. Если требуется удалить интервал, нажмите на кнопку ✕ справа от нужного интервала.

Вы можете добавить один или несколько временных интервалов. Если временной интервал не указан, то диагностическое правило применяется в каждом узле РИВС.

8. Если требуется добавить вычислимые теги, в блоке параметров **Вычислимые теги** выполните следующие действия:

   a. Нажмите на кнопку **Добавить вычислимый тег**.

   b. В поле **Имя вычислимого тега** укажите имя вычислимого тега.

      Имя вычислимого тега должно быть уникальным среди входящих и вычислимых тегов, используемых в правиле.

   c. В блоке **Теги для вычислений** выполните следующие действия:

      a. Нажмите на значок плюса.

      b. Если в правиле определен хотя бы один вычислимый тег, в раскрывающемся списке **Тип тега** выберите одно из следующих значений:

         - **Входящий тег** – для расчета значения на основе значений тегов, поступающих в Kaspersky MLAD.
         - **Вычислимый тег** – для расчета значения на основе значений других вычислимых тегов.

      c. Выберите тег, на основе значений которого необходимо получить значение вычислимого тега.

      d. Если требуется добавить еще один тег для расчета выражения, нажмите на значок плюса.

         Если требуется удалить тег, нажмите на кнопку ✕ справа от нужного тега. Если тег используется в блоке параметров **Условия на теги**, его нельзя удалить.

   d. В поле **Выражение для расчета** введите выражение для расчета вычислимого тега.

   e. Для проверки введенного выражения нажмите на кнопку **Проверить выражение для расчета**.

      Если выражение содержит ошибки, будет выведено соответствующее сообщение. Исправьте ошибки и выполните повторную проверку. Только проверенные вычислимые теги могут быть использованы в правиле.

      Если проверка вычислимого тега не выполнена, правило не получится сохранить.

При успешной проверке выражения тегу будет присвоен статус **Проверен**, и его можно использовать для расчета других вычислимых тегов или в критериях поведения тегов.

9. Если требуется добавить критерии поведения тегов, выполните следующие действия:

a. В блоке параметров **Условия на теги** нажмите на кнопку **Условие**.

b. Если в правиле определен хотя бы один вычислимый тег, в раскрывающемся списке **Тип тега** выберите одно из следующих значений:

- **Входящий тег** – для добавления критериев поведения для тега, поступающего в Kaspersky MLAD.
- **Вычислимый тег** – для добавления критериев поведения для вычислимого тега.

c. В раскрывающемся списке **Тег** выберите тег объекта мониторинга или вычислимый тег, для которого вы хотите добавить критерий поведения.

Если требуется проверить поведение, прямо противоположное выбранному критерию поведения из блока условий, нажмите на кнопку **NOT** слева от выбранного тега. Надпись **NOT** в кнопке выделится жирным.

Например, нажмите на кнопку **NOT**, если требуется добавить условие отсутствия ступеньки с заданными параметрами.

d. В раскрывающемся списке **Поведение** выберите одно из следующих поведений тега, которое требуется отслеживать:

- **Выше** – значение тега превышает определенный порог.
- **Ниже** – значение тега опускается ниже определенного порога.
- **Растет** – линия тренда значений тега растет.
- **Падает** – линия тренда значений тега падает.
- **Без динамики** – в линии тренда значений тега отсутствуют выраженные изменения.
- **Ступенька** – в линии тренда выбранного тега наблюдаются резкие смещения вверх или вниз.
- **Залипание** – выбранный тег передает одно и то же значение.
- **Разброс** – вокруг линии тренда выбранного тега наблюдаются резкие изменения разброса значений.

e. В поле **Окно** укажите количество шагов РИВС.

f. В зависимости от значения выбранного для параметра **Поведение** выполните одно из следующих действий:

- Если вы выбрали **Выше** или **Ниже**, в поле **Порог** укажите пороговое значение тега и в поле **Срабатывание** минимальное количество выходов за пороговое значение в рамках окна.
- Если вы выбрали **Растет**, **Падает** или **Без динамики**, в поле **Пороговый уклон** укажите значение уклона тренда в процентах, при превышении которого тренд считается растущим или падающим, и интервал времени между соседними оценками тренда в поле **Период оценки**.

  По умолчанию параметр **Пороговый уклон** не задан. Если значение параметра не задано, Kaspersky MLAD определит направление тренда автоматически.

  По умолчанию параметр **Период оценки** имеет значение `1`. При этом значении оценка тренда происходит в каждом узле РИВС.

- Если вы выбрали **Разброс**, в поле **Порог изменения** укажите минимальное значение, на которое может измениться разброс значений тега вокруг линии тренда, и выберите одно из следующих направлений изменения разброса в раскрывающемся списке **Направление**: **Любое**, **Увеличение**, **Уменьшение**.

  По умолчанию параметр **Порог изменения** не задан. Если значение параметра не задано, Kaspersky MLAD определит его автоматически.

  Критерий поведения тега будет выполнен в момент увеличения и/или уменьшения разброса значения тега вокруг линии тренда.

- Если вы выбрали **Ступенька**, в поле **Порог изменения** укажите минимальное значение, на которое может сместиться линия тренда, и выберите одно из следующих направлений изменения значений тега в раскрывающемся списке **Направление**: **Любое**, **Вверх** или **Вниз**.

  По умолчанию параметр **Порог изменения** не задан. Если значение параметра не задано, Kaspersky MLAD определит его автоматически.

- Если вы выбрали **Залипание**, в поле **Значение** укажите значение, которое должен передавать тег, и допустимый разброс значений тега в поле **Разброс**.

  По умолчанию значение параметра **Разброс** равно нулю. При таком значении любое повторяющееся значение тега вызывает срабатывание критерия.

g. Если требуется добавить критерий поведения тегов в блок условий, нажмите на значок плюса в нижней части блока условий и повторите шаги с 8b по 8e.

h. Если блок условий содержит более одного критерия поведения тегов, выберите один из следующих логических операторов между строками критериев нажатием на кнопку логического оператора:

- **AND**, если требуется, чтобы одновременно выполнялись все критерии блока.

- **OR**, если достаточно выполнения хотя бы одного из критериев блока.

10. Если требуется проверить, вызвало ли выполнение предварительного условия выполнение пост-условия в будущем узле РИВС, добавьте темпоральный оператор:

    a. В блоке параметров **Условия на теги** нажмите на кнопку **Пауза**.

    Кнопка **Пауза** доступна после добавления хотя бы одного условия.

    b. В поле **Продолжительность (шаги)** укажите следующие интервалы ожидания:

    - **от** – интервал между узлом проверки предварительного условия и узлом РИВС, с которого начнется проверка пост-условия (минимальный интервал ожидания).
    - **до** – интервал между узлом проверки предварительного условия и узлом РИВС, в котором закончится проверка пост-условия (максимальный интервал ожидания).

    Проверка пост-условия проводится в узлах РИВС между минимальным и максимальным интервалом ожидания.

    c. В раскрывающемся списке **Проверить** выберите один из следующих групповых операторов:

    - Если требуется выполнение критериев поведения тегов из пост-условия во всех узлах РИВС между минимальным и максимальным интервалом ожидания, выберите групповой оператор **Все шаги**.
    - Если требуется выполнение критериев поведения тегов из пост-условия хотя бы в одном узле РИВС между минимальным и максимальным интервалом ожидания, выберите групповой оператор **Любой шаг**.

    Результат проверки критериев определяется в последнем узле максимального интервала ожидания.

    Если проводится более одной проверки условия с помощью темпорального оператора, то предварительным условием для каждой следующей проверки темпорального условия является результат проверки предыдущего темпорального условия.

11. Выберите один из следующих логических операторов между блоками правила нажатием на кнопку логического оператора:

    - **AND**, если требуется, чтобы были выполнены критерии обоих блоков условий.
    - **OR**, если требуется, чтобы был выполнен критерий хотя бы одного из блоков условий.

12. В правом верхнем углу страницы нажмите на кнопку **Сохранить**.

    При создании первого элемента в составе ML-модели в дереве активов будет автоматически создана группа **Правила**. Созданный элемент отобразится в этой группе.

Если в составе ML-модели есть только элементы на основе диагностических правил, ей будет присвоен статус **Обучена**. Вы можете запустить инференс для такой ML-модели. Если в составе ML-модели есть необученные предиктивные элементы и/или элементы на основе эллиптического конверта, перед запуском инференса их требуется обучить.

Изменение элемента ML-модели на основе диагностического правила

Вы можете изменять параметры элементов ML-модели на основе диагностического правила.

Изменение параметров недоступно, если ML-модели присвоен статус **Готова к публикации** или **Опубликована**, а также во время инференса ML-модели.

Изменение элементов ML-моделей доступно системным администраторам и пользователям с правом **Изменение моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы изменить элемент ML-модели на основе диагностического правила:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите элемент на основе диагностического правила, который вы хотите изменить.

   Справа отобразится список параметров.
3. В правом верхнем углу страницы нажмите на кнопку **Изменить**.
4. Если требуется, измените параметры диагностического правила. Описание параметров см. в инструкции по добавлению элемента ML-модели на основе диагностического правила.
5. В правом верхнем углу страницы нажмите на кнопку **Сохранить**.
6. Если был изменен параметр **Шаг сетки (сек.)**, подтвердите сохранение изменений.

Добавление элемента ML-модели на основе эллиптического конверта

Добавление элементов ML-моделей доступно системным администраторам и пользователям с правом **Создание моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы добавить элемент ML-модели на основе эллиптического конверта:

1. В основном меню выберите раздел **Модели**.
2. Для добавления эллиптического конверта выполните следующие действия:

   a. В дереве активов рядом с именем ML-модели, к которой вы хотите добавить эллиптический конверт, откройте вертикальное меню **...** и выберите пункт **Создать элемент**.

   b. В открывшемся окне выберите тип элемента **Эллиптический конверт**.

   c. Нажмите на кнопку **Создать**.

   Справа отобразится список параметров.
3. В поле **Имя** укажите имя элемента ML-модели.
4. В поле **Описание** укажите описание элемента ML-модели.

5. В блоке параметров **Общие параметры элемента** выполните следующие действия:

   a. В поле **Период напоминания (сек.)** укажите период в секундах, при достижении которого ML-модель сгенерирует повторный инцидент при сохранении аномального поведения в каждом узле РИВС.

      По умолчанию этот параметр имеет значение `0`, что соответствует отсутствию напоминаний.

   b. В поле **Период подавления повторных срабатываний (сек.)** укажите период в секундах, в течение которого ML-модель не регистрирует повторные инциденты от одного и того же элемента.

      По умолчанию этот параметр имеет значение `0` (повторные инциденты не подавляются).

   c. В поле **Интервал наблюдения за аномалией (сек.)** укажите период в секундах, в течение которого отслеживается аномальное поведение тега для принятия решения о регистрации инцидента.

   d. В поле **Доля длительности аномалии в интервале** укажите в виде десятичной дроби долю от периода, заданного в параметре **Интервал наблюдения за аномалией (сек.)**, при достижении которой элемент ML-модели зарегистрирует инцидент.

      Вы можете указать значение в диапазоне от `0` до `1`.

   e. В поле **Порог регистрации инцидентов** укажите пороговое значение, при достижении которого происходит регистрация инцидента.

      По умолчанию значение порога автоматически корректируется после каждого обучения элемента. Если после завершения обучения вы включите переключатель **Зафиксировать порог регистрации инцидентов**, то значение порога будет зафиксировано и не изменится после повторного обучения элемента. При необходимости вы можете изменить значение этого параметра.

   f. В поле **Цвет точек-индикаторов инцидентов** выберите цвет точек-индикаторов инцидентов, зарегистрированных элементом ML-модели, на графиках в разделах **Мониторинг** и **История**. В этом цвете также будет отображаться график артефакта, сформированный этим элементом.

   g. Если требуется, в раскрывающемся списке **Статус инцидента** выберите статус инцидента, который будет автоматически присвоен инцидентам, зарегистрированным элементом ML-модели.

      По умолчанию статус не установлен.

   h. Если требуется, в раскрывающемся списке **Причина инцидента** выберите причину инцидента, которая будет автоматически задана для инцидентов, зарегистрированных элементом ML-модели, если эта причина заранее известна.

   i. Если требуется, в раскрывающемся списке **Приоритет инцидента** выберите приоритет, который будет автоматически присвоен инцидентам, зарегистрированным элементом ML-модели.

      По умолчанию инциденту присваивается приоритет **Средний**.

   j. Если требуется, в поле **Экспертные рекомендации** укажите экспертные рекомендации, которые будет автоматически добавлены инцидентам, зарегистрированным элементом ML-модели, если содержание этих рекомендаций заранее известно.

6. В поле **Шаг сетки (сек.)** укажите период РИВС для элемента в секундах в виде целого числа или десятичной дроби.

7. В блоке параметров **Входные теги** выполните следующие действия:

   a. Нажмите на кнопку **Выбрать теги**.

      Откроется панель **Выбор тегов модели**, отображающая **таблицу с деревом активов**.

      В таблице с деревом активов отображается следующая информация:

      - **Имя** – имя актива или тега в дереве активов.
      - **Описание** – описание актива или тега в дереве активов.
      - **Входной тег** – переключатель, позволяющий включить тег во входные теги элемента ML-модели или исключить тег из входных тегов.

   b. Если требуется настроить отображение таблицы с деревом активов, выполните следующие действия:

      a. Нажмите на кнопку , расположенную в правом верхнем углу панели.

      b. Установите флажки рядом с теми столбцами таблицы, которые необходимо отображать.

      c. Нажмите на кнопку **Сохранить**.

   c. Если требуется использовать теги, входящие в определенные пресеты, выполните следующие действия:

      a. Нажмите на кнопку , расположенную в правом верхнем углу панели.

      b. Выберите нужные пресеты.

         При необходимости введите поисковый запрос в поле **Поиск**. Поиск выполняется по мере ввода символов в строку поиска.

      c. Нажмите на кнопку **Применить**.

      В панели **Выбор тегов модели** отобразятся теги, входящие в выбранные пресеты.

   d. Для выбора тегов, выполните одно из следующих действий:

      - Если требуется выбрать определенный тег, включите переключатель в столбце **Входной тег** для нужного тега.
      - Если требуется выбрать несколько тегов, установите флажки рядом с нужными тегами и в раскрывающемся списке **Массовые действия** выберите элемент **Включить**.

   e. Если требуется отобразить только теги, которые были выбраны в качестве входных, включите переключатель **Используемые теги** над деревом активов.

   f. Если требуется исключить выбранные теги из входных, установите флажки рядом с нужными тегами и в раскрывающемся списке **Массовые действия** выберите элемент **Исключить**.

   g. Нажмите на кнопку **Сохранить**.

8. В правом верхнем углу страницы нажмите на кнопку **Сохранить**.

При создании первого элемента в составе ML-модели в дереве активов будет автоматически создана группа **Эллиптические конверты**. Созданный элемент отобразится в этой группе.

Элементу ML-модели будет присвоен статус **Не обучен**, а ML-модели, к которой относится добавленный элемент, будет присвоен статус **Не обучена**. Для запуска инференса ML-модели требуется обучить все ее предиктивные элементы и элементы на основе эллиптического конверта.

Изменение элемента ML-модели на основе эллиптического конверта

Вы можете изменять параметры элементов ML-модели на основе эллиптического конверта.

Изменение параметров недоступно, если ML-модели присвоен статус **Готова к публикации** или **Опубликована**, а также во время инференса ML-модели и обучения элемента.

Изменение элементов ML-моделей доступно системным администраторам и пользователям с правом **Изменение моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы изменить элемент ML-модели на основе эллиптического конверта:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите элемент на основе эллиптического конверта, который вы хотите изменить.

   Справа отобразится список параметров.
3. В правом верхнем углу страницы нажмите на кнопку **Изменить**.
4. Если требуется, измените параметры эллиптического конверта. Описание параметров см. в инструкции по добавлению элемента ML-модели на основе эллиптического конверта.
5. В правом верхнем углу страницы нажмите на кнопку **Сохранить**.
6. Подтвердите сохранение изменений.

   Если были изменены параметры **Шаг сетки (сек.)** и/или **Входные теги**, элемент ML-модели необходимо повторно обучить. После внесения изменений в эти параметры элементу будет присвоен статус **Не обучен**.

Копирование элемента ML-модели

Вы можете создать элемент ML-модели, скопировав элемент любой ML-модели. При копировании будет создан элемент ML-модели, в котором статус и состояние элемента, параметры архитектуры и обучения соответствуют статусу и состоянию, параметрам архитектуры и обучения исходного элемента в момент его копирования. Если исходный элемент ML-модели в момент его копирования является обученным, то в новом элементе ML-модели будут отображаться результаты обучения исходного элемента.

Копирование элемента ML-модели невозможно в следующих случаях:

- ML-модель, в которую копируется элемент, импортирована.
- ML-модель, в которую копируется элемент, находится в состоянии **Идет исторический инференс** и/или **Идет потоковый инференс**.
- ML-модели, в которую копируется элемент, присвоен статус **Готова к публикации** или **Опубликована**.

Функциональность доступна после добавления лицензионного ключа.

Чтобы скопировать элемент ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите элемент ML-модели, который вы хотите скопировать.

   Справа отобразится список параметров.
3. В правом верхнем углу страницы нажмите на кнопку .

   Справа отобразится панель **Копирование элемента**.
4. В поле **Имя** укажите имя элемента.

   По умолчанию элементу ML-модели присваивается имя в формате `<имя исходного элемента ML-модели>_Cloned_<дата и время копирования>`.
5. В раскрывающемся списке **Модель** выберите ML-модель, в состав которой вы хотите скопировать выбранный элемент.
6. Нажмите на кнопку **Сохранить**.

Новый элемент ML-модели отобразится в соответствующей группе элементов выбранной ML-модели.

Удаление элемента ML-модели

При удалении элемента ML-модели Kaspersky MLAD также удаляет результаты инференса выбранного элемента ML-модели.

Удаление элементов ML-моделей доступно системным администраторам и пользователям с правом **Удаление моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.
Удаление элемента, используемого в импортированной ML-модели, невозможно.

Чтобы удалить элемент ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите элемент ML-модели, который вы хотите удалить.

   Справа отобразится список параметров.

3. В правом верхнем углу страницы нажмите на кнопку .

4. В открывшемся окне подтвердите удаление элемента ML-модели.

Копирование ML-модели

Копирование ML-моделей доступно системным администраторам и пользователям с правом **Копирование моделей** из группы прав **Управление ML-моделями**.

Функциональность доступна после добавления лицензионного ключа.

Вы можете создать ML-модель, скопировав ранее добавленную ML-модель. При копировании будет создана ML-модель, в которой состав элементов, статусы и параметры ML-модели и ее элементов, а также состояние обучения элементов будут идентичны составу элементов, статусам и параметрам ML-модели и ее элементов, состоянию обучения элементов ML-модели в момент ее копирования.

После копирования ML-модели, которая была создана вручную или по шаблону на основе ML-модели, созданной вручную, вы можете добавлять в скопированную ML-модель предиктивные элементы, элементы на основе эллиптического конверта и/или элементы на основе диагностических правил, изменять и удалять их.

После копирования ML-модели, которая была импортирована в программу или создана по шаблону на основе импортированной ML-модели, вы не можете изменять состав элементов скопированной ML-модели.

Перед выполнением инференса вы можете изменить параметры обучения и обучить элементы скопированной ML-модели заново.

Чтобы скопировать ML-модель:

1. В основном меню выберите раздел **Модели**.

2. В дереве активов выберите ML-модель, которую вы хотите скопировать.

   Справа отобразится список параметров.

3. В правом верхнем углу страницы нажмите на кнопку .

   Справа отобразится панель **Копирование модели**.

4. В поле **Имя** укажите имя ML-модели.

   Вы можете указать имя ML-модели длиной не более 100 символов.

   По умолчанию ML-модели присваивается имя в формате `<имя исходной ML-модели>_Cloned_<дата и время копирования>`.

5. В раскрывающемся списке **Актив** выберите актив, к которому вы хотите отнести новую ML-модель.

6. Нажмите на кнопку **Сохранить**.

   Новая ML-модель отобразится в группе **Модели** дерева активов. Группа **Модели** создается автоматически и отображается в составе выбранного раздела дерева активов. Если в составе скопированной ML-модели есть предиктивные элементы, элементы на основе эллиптического конверта и/или элементы на основе диагностических правил, в группе **Модели** будут отображаться подгруппы **Предиктивные элементы**, **Эллиптические конверты** и/или **Правила** соответственно.

Вы также можете перейти к копированию ML-модели, нажав на вертикальное меню **...** и выбрав пункт **Копировать модель**.

Работа с шаблонами ML-моделей

Этот раздел содержит информацию о работе с шаблонами ML-моделей.

Функциональность доступна после добавления лицензионного ключа.

Вы можете создать шаблон существующей ML-модели для многократного переиспользования ее структуры алгоритма, набора элементов и состояния обучения в момент создания шаблона. Вы можете использовать созданный шаблон для добавления новых ML-моделей.

Если исходная ML-модель, по которой был создан шаблон, была создана вручную, то вы можете добавлять в ML-модель, созданную по такому шаблону, предиктивные элементы, элементы на основе эллиптического конверта и/или элементы на основе диагностических правил, изменять и удалять их.

Если исходная ML-модель, по которой был создан шаблон, была импортирована в Kaspersky MLAD, то вы не можете изменять состав элементов ML-модели, созданной по такому шаблону.

Перед инференсом ML-модели требуется обучить все ее предиктивные элементы и элементы на основе эллиптического конверта.

Создание шаблона по ML-модели

Создание шаблонов по ML-моделям доступно системным администраторами пользователям с правом **Создание шаблонов моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Вы можете создать шаблон ML-модели на основе ранее добавленной ML-модели. В созданных шаблонах будет сохранена структура алгоритма, набор элементов, состав тегов и состояние обучения исходной ML-модели.

Вы можете создать шаблон по ранее добавленной ML-модели, если все ее предиктивные элементы и элементы на основе эллиптического конверта обучены и для всех элементов на основе диагностического правила сформированы условия правил.

Чтобы создать шаблон по ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов рядом с именем ML-модели, по которой вы хотите создать шаблон, откройте вертикальное меню **...** и выберите пункт **Создать шаблон**.

   Справа отобразится список параметров.

3. В поле **Имя** укажите имя шаблона.

   Вы можете ввести не более 100 символов.

   По умолчанию шаблону присваивается имя в формате `Шаблон_<имя ML-модели>_<дата и время создания шаблона>`.

4. Если требуется изменить имена тегов шаблона, в столбце **Имя тега шаблона** укажите новые имена для нужных тегов.

   Тегам шаблона автоматически присваиваются имена тегов, используемых в ML-модели, по которой создается шаблон. Вы можете указать для тегов шаблона любые другие имена, например, использовать функциональные описания ролей тегов. Имена тегов шаблона не обязаны совпадать с именами тегов ML-модели, на основе которой сформирован шаблон.

5. Нажмите на кнопку **Сохранить**.

Новый шаблон ML-модели отобразится в группе **Шаблоны** дерева активов. Группа **Шаблоны** создается автоматически и отображается в составе выбранного раздела дерева активов.

Изменение шаблона ML-модели

Вы можете изменить параметры созданного шаблона ML-модели.

Изменение шаблона ML-модели доступно системным администраторам и пользователям с правом **Изменение шаблонов моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы изменить шаблон ML-модели:

1. В основном меню выберите раздел **Модели**.

2. В дереве активов выберите шаблон, который вы хотите изменить.

   Справа отобразится список параметров.

3. В правом верхнем углу страницы нажмите на кнопку **Изменить**.

4. Если требуется, измените параметры шаблона ML-модели. Описание параметров см. в инструкции по созданию шаблона ML-модели.

5. Нажмите на кнопку **Сохранить**.

Создание ML-модели по шаблону

Создание ML-моделей по шаблонам доступно системным администраторами пользователям с правом **Создание моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Вы можете создавать новые ML-модели на основе доступных шаблонов. При создании ML-модели вы можете указать идентификаторы тегов, которые требуется использовать в новой ML-модели.

Чтобы создать ML-модель по шаблону:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов рядом с именем шаблона, по которому вы хотите создать ML-модель, откройте вертикальное меню **...** и выберите пункт **Создать модель**.

   Справа откроется панель **Создание модели**.
3. В поле **Имя модели** укажите имя новой ML-модели.

   Вы можете указать имя ML-модели длиной не более 100 символов.
4. В столбце **Имя тега модели** для каждого тега шаблона выберите из дерева активов тег, который будет использоваться создаваемой по шаблону ML-моделью.
5. Нажмите на кнопку **Сохранить**.

Новая ML-модель отобразится в группе **Модели** дерева активов. Группа **Модели** создается автоматически и отображается в составе выбранного раздела дерева активов. Если в составе ML-модели есть предиктивные элементы, элементы на основе эллиптического конверта и/или элементы на основе диагностических правил, в группе **Модели** будут отображаться подгруппы **Предиктивные элементы**, **Эллиптические конверты** и/или **Правила** соответственно.

Состояние созданной ML-модели будет соответствовать состоянию обучения исходной ML-модели в момент создания ее шаблона.

Удаление шаблона ML-модели

Удаление шаблонов ML-моделей доступно системным администраторами пользователям с правом **Удаление шаблонов моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Вы можете удалить шаблон ML-модели из Kaspersky MLAD. Удаление шаблона не приводит к удалению ML-моделей, созданных на основе этого шаблона.

Чтобы удалить шаблон ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите шаблон ML-модели, который требуется удалить.

   Справа отобразится список параметров.
3. В правом верхнем углу страницы нажмите на кнопку .
4. Подтвердите удаление шаблона ML-модели.

Выбранный шаблон ML-модели будет удален из Kaspersky MLAD.

Изменение параметров ML-модели

Изменение разметки недоступно для импортированных ML-моделей и ML-моделей, созданных путем копирования импортированных ML-моделей или по шаблону импортированных ML-моделей.

Изменение параметров ML-моделей доступно системным администраторам и пользователям с правом **Изменение моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы изменить параметры ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите ML-модель, параметры которой требуется изменить

   Справа отобразится список параметров.
3. В правом верхнем углу страницы нажмите на кнопку **Изменить**.
4. Если требуется, измените параметры ML-модели. Описание параметров см. в инструкции по созданию ML-модели.

   Если ML-модели присвоен статус **Готова к публикации** или **Опубликована** или для нее выполняется инференс, вы можете изменить только описание ML-модели.
5. В правом верхнем углу страницы нажмите на кнопку **Сохранить**.

Обучение предиктивного элемента ML-модели

Процесс обучения предиктивного элемента может состоять из одной или нескольких эпох. *Эпоха* – это цикл, в течение которого предиктивный элемент обучается на всем наборе обучающих данных. Вы можете задать количество эпох для обучения в параметрах обучения элемента.

Для обучения элементов ML-моделей должна быть запущена служба Trainer. При необходимости системный администратор может изменить количество элементов, которое служба может обучать одновременно, в параметрах службы Trainer.

Изменение параметров обучения и запуск повторного обучения недоступны, если ML-модели присвоен статус **Готова к публикации** или **Опубликована**.
Обучение элементов ML-моделей доступно системным администраторам и пользователям с правом **Обучение моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы обучить элемент ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите предиктивный элемент, который вы хотите обучить.

   Справа отобразится список параметров.
3. Откройте вкладку **Обучение** и нажмите на кнопку **Изменить** в правом верхнем углу страницы.
4. В поле **Интервал отбора данных** укажите интервал времени данных, на которых требуется обучить ML-модель.
5. Если требуется применить разметки для отбора данных для обучения ML-модели в рамках выбранного интервала, в поле **Разметки** выберите одну или несколько разметок.

   Выбранные разметки сформируют индикатор обучения.

   Если выбрано более одной разметки, то для формирования индикатора обучения используются пересечения выбранных интервалов данных.
6. Если требуется просмотреть, какие данные будут отобраны разметками, нажмите на кнопку **На графике**.

   Если выбрана одна разметка, то на графике отобразятся интервалы, отобранные разметкой, в указанном при создании цвете. Если выбрано более одной разметки, на графике отобразятся пересечения интервалов, отобранных разметками.

   При просмотре данных на графике вы можете выбрать определенный пресет.
7. Если требуется зафиксировать порог регистрации инцидентов, заданный в параметрах элемента, включите переключатель **Зафиксировать порог регистрации инцидентов**.

   По умолчанию переключатель выключен. Корректировка порога регистрации инцидентов выполняется на основе результатов обучения. При необходимости вы можете вручную изменить значение порога регистрации инцидентов после корректировки.
8. Если требуется задать расширенные параметры обучения, включите переключатель **Расширенные параметры обучения**.
9. В поле **Максимальная продолжительность обучения (сек.)** укажите в секундах максимальное время, которое сервер Kaspersky MLAD может затратить на обучение ML-модели.
10. В поле **Размер валидационной выборки** укажите в виде десятичной дроби долю валидационной выборки относительно всего набора данных для обучения ML-модели.

    Вы можете указать значение в диапазоне от `0` до `1`.

    По умолчанию этот параметр имеет значение `0.2`.
11. В поле **Максимальное количество эпох** укажите максимальное количество эпох для обучения ML-модели.

    По умолчанию этот параметр имеет значение `500`.
12. В поле **Количество эпох для ранней остановки обучения** укажите количество эпох, в течение которых качество обучения не улучшается для ранней остановки обучения ML-модели.

    Ранняя остановка обучения ML-модели применяется для избежания переобучения модели. При этом обучение ML-модели считается успешно завершившимся.

    По умолчанию этот параметр имеет значение `15`.

13. В поле **Разрешение графиков результатов обучения** укажите в виде десятичной дроби разрешение графиков для отображения результатов обучения на вкладке **Результаты обучения**.

    Вы можете указать значение в диапазоне от `0` до `1`.

14. В поле **Размер пакета** укажите количество элементов выборки, которое требуется передать на обучение в рамках итерации.

    По умолчанию этот параметр имеет значение `16`.

    > Этот параметр недоступен для элемента с TCN-архитектурой.

15. В поле **Количество блоков** укажите количество блоков, на которое требуется разбить данные для обучения ML-модели.

    По умолчанию этот параметр имеет значение `4`.

16. В раскрывающемся списке **Режим инференса** выберите одно из следующих значений:

    - Если требуется загрузить все пакеты данных для обучения в оперативную память, выберите **Быстрый инференс**.

      Этот режим инференса позволяет выполнить инференс быстрее.

    - Если требуется загружать в оперативную память по одному пакету данных, выберите **Экономия памяти**.

      Этот режим инференса позволяет выполнить инференс с минимальными затратами оперативной памяти, но медленнее, чем в режиме **Быстрый инференс**.

17. В раскрывающемся списке **Режим обучения** выберите одно из следующих значений:

    - Если требуется загрузить все данные для обучения модели в оперативную память, выберите **Загрузить все данные в оперативную память**.

    - Если требуется загружать в оперативную память по одному блоку данных и сформировать валидационные блоки из конца набора данных, выберите **Сформировать валидационные блоки из конца данных**.

    - Если требуется загружать в оперативную память по одному блоку данных без формирования валидационных блоков, выберите **Проводить валидацию в каждом блоке обучающих данных**.

      Валидационные данные формируются из каждого обучающего блока данных.

18. В раскрывающемся списке **Режим распределения памяти** выберите один из следующих параметров:

    - **Зарезервировать минимальный объем свободной памяти**. При выборе этого параметра при обучении ML-модели служба Trainer будет оставлять свободным минимальный объем памяти, указанный в поле **Объем памяти, МБ**.

    - **Зарезервировать максимальный объем памяти на обучение модели**. При выборе этого параметра для обучения ML-модели служба Trainer будет использовать максимальный объем оперативной памяти, указанный в поле **Объем памяти, МБ**.

19. Если требуется учесть результаты предыдущего обучения при обучении ML-модели на новых данных, включите параметр **Инициализировать веса модели значениями из результатов предыдущего обучения**.

20. Если требуется перемешать данные для улучшения качества обучения ML-модели, включите параметр **Перемешать данные**.

21. В поле **Инициализация генератора псевдослучайных чисел** укажите значение, на основании которого будет сгенерирована последовательность псевдослучайных чисел.

22. В поле **Коэффициент скорости обучения** укажите коэффициент, с помощью которого будут корректироваться веса элемента ML-модели на каждой итерации обучения.

    По умолчанию этот параметр имеет значение `0.0001`.

23. В раскрывающемся списке **Алгоритм оптимизации обучения** выберите один из следующих алгоритмов, который будет использоваться для оптимизации обучения:

    - **Adadelta** – алгоритм, основанный на адаптивной скорости обучения для каждого измерения.
    - **Adagrad** – алгоритм, в котором скорость обучения зависит от частоты обновления параметров во время обучения.
    - **Adam** – алгоритм, основанный на адаптивной оценке первого и второго момента распределения параметров.
    - **RMSprop** – алгоритм, использующий скользящее среднее квадратов градиента для адаптивного нормирования скорости обучения на каждом шаге.
    - **SGD** – алгоритм стохастического градиентного спуска.

24. В раскрывающемся списке **Функция потерь** выберите одну из следующих функций, которая будет использоваться для расчета ошибки прогноза во время обучения:

    - **MSE** – для расчета среднеквадратичной ошибки.
    - **MSLE** – для расчета средней логарифмической ошибки.
    - **MAE** – для расчета средней абсолютной ошибки.
    - **MAPE** – для расчета средней абсолютной процентной ошибки.

25. В правом верхнем углу страницы нажмите на кнопку **Сохранить**.

    В случае изменения параметров обучения для ранее обученного элемента необходимо подтвердить сохранение изменений.

26. В информационном блоке, расположенном над параметрами обучения, нажмите на кнопку **Обучить элемент**.

    Kaspersky MLAD добавит элемент в очередь на обучение. Во время обучения в информационном блоке будет отображаться номер текущей эпохи обучения элемента.

После завершения обучения вы можете просмотреть результаты обучения элемента ML-модели на вкладке **Результаты обучения**.

После успешного обучения всех предиктивных элементов и элементов на основе эллиптического конверта в составе ML-модели ей будет присвоен статус **Обучена**. Если требуется, вы можете повторно обучить элемент ML-модели, нажав на кнопку **Перезапустить обучение**.

Обучение элемента ML-модели на основе эллиптического конверта

Kaspersky MLAD позволяет выполнить обучение элемента на основе эллиптического конверта для ML-модели, созданной вручную, импортированной в Kaspersky MLAD, созданной по шаблону, а также для скопированной ML-модели.

Для обучения элементов ML-моделей должна быть запущена служба Trainer. При необходимости системный администратор может изменить количество элементов, которое служба может обучать одновременно, в параметрах службы Trainer.

Изменение параметров обучения и запуск повторного обучения недоступны, если ML-модели присвоен статус **Готова к публикации** или **Опубликована**.
Обучение элементов ML-моделей доступно системным администраторам и пользователям с правом **Обучение моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы обучить элемент ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите элемент на основе эллиптического конверта, который вы хотите обучить.

   Справа отобразится список параметров.
3. Откройте вкладку **Обучение** и нажмите на кнопку **Изменить** в правом верхнем углу страницы.
4. В поле **Интервал отбора данных** укажите интервал времени данных, на которых требуется обучить ML-модель.
5. Если требуется применить разметки для отбора данных для обучения ML-модели в рамках выбранного интервала, в поле **Разметки** выберите одну или несколько разметок.

   Выбранные разметки сформируют индикатор обучения.

   Если выбрано более одной разметки, то для формирования индикатора обучения используются пересечения выбранных интервалов данных.
6. Если требуется просмотреть, какие данные будут отобраны разметками, нажмите на кнопку **На графике**.

   Если выбрана одна разметка, то на графике отобразятся интервалы, отобранные разметкой, в указанном при создании цвете. Если выбрано более одной разметки, на графике отобразятся пересечения интервалов, отобранных разметками.

   При просмотре данных на графике вы можете выбрать определенный пресет.
7. Если требуется зафиксировать порог регистрации инцидентов, заданный в параметрах элемента, включите переключатель **Зафиксировать порог регистрации инцидентов**.

   По умолчанию переключатель выключен. Корректировка порога регистрации инцидентов выполняется на основе результатов обучения. При необходимости вы можете вручную изменить значение порога регистрации инцидентов после корректировки.

8. Если требуется задать расширенные параметры обучения, включите переключатель **Расширенные параметры обучения**.

9. Если требуется, в поле **Доля выборки для оценки среднего и ковариации** укажите в виде десятичной дроби долю обучающей выборки, на которой производится расчет ковариации и среднего значения.

   Вы можете указать значение в диапазоне от `0` до `1`. Чем выше значение параметра, тем ниже чувствительность эллиптического конверта к аномалиям.

10. В поле **Доля выбросов в выборке** укажите в виде десятичной дроби долю выбросов (аномалий) в обучающей выборке.

    Вы можете указать значение в диапазоне от `0` до `0.5` включительно. Этот параметр автоматически переопределяет значение параметра **Порог регистрации инцидентов**, заданного при создании элемента. Чем выше значение доли выбросов в обучающей выборке, тем ниже значение порога регистрации инцидентов. После обучения элемента вы можете отрегулировать порог регистрации инцидентов вручную.

11. Если требуется, в поле **Инициализация генератора псевдослучайных чисел** укажите значение, на основании которого будет сгенерирована последовательность псевдослучайных чисел.

12. В поле **Разрешение графиков результатов обучения** укажите в виде десятичной дроби разрешение графиков для отображения результатов обучения на вкладке **Результаты обучения**.

    Вы можете указать значение в диапазоне от `0` до `1`. Чем выше указанное значение, тем лучше качество графиков.

13. Если предполагается, что значения тегов центрированы, и их среднее значение равно нулю, включите переключатель **Данные центрированы**.

14. В правом верхнем углу страницы нажмите на кнопку **Сохранить**.

    В случае изменения параметров обучения для ранее обученного элемента необходимо подтвердить сохранение изменений.

15. В информационном блоке, расположенном над параметрами обучения, нажмите на кнопку **Обучить элемент**.

    Kaspersky MLAD добавит элемент в очередь на обучение.

После завершения обучения вы можете просмотреть результаты обучения элемента ML-модели на вкладке **Результаты обучения**.

После успешного обучения всех предиктивных элементов и элементов на основе эллиптического конверта в составе ML-модели ей будет присвоен статус **Обучена**. Если требуется, вы можете повторно обучить элемент ML-модели, нажав на кнопку **Перезапустить обучение**.

Просмотр результатов обучения элемента ML-модели

Вы можете просмотреть результаты обучения предиктивных элементов и элементов на основе эллиптического конверта.

Просмотр результатов обучения элементов ML-моделей доступен системным администраторам и пользователям с правом **Обучение моделей** из группы прав **Управление ML-моделями**. Функциональность доступна после добавления лицензионного ключа.

Чтобы просмотреть результаты обучения элемента ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите элемент ML-модели, результат обучения которого вы хотите просмотреть.

   Справа отобразится панель с параметрами выбранного элемента.
3. Выберите вкладку **Результаты обучения**.

В случае успешного обучения элемента ML-модели на вкладке **Результаты обучения** отображается следующие сведения:

- Сообщение об успешном завершении обучения элемента ML-модели.

  Если требуется просмотреть параметры обучения элемента, указанные при его создании, нажмите на кнопку **Параметры обучения**.
- Блок параметров **Оценка обучения** для оценки результатов обучения элемента ML-модели.
- Блок параметров **Результаты обучения** со следующими сведениями:
  - **Пользователь** – имя пользователя, который запустил обучение элемента ML-модели.
  - **Начало обучения** – дата и время начала обучения элемента ML-модели.
  - **Окончание обучения** – дата и время окончания обучения элемента ML-модели.
  - **Продолжительность обучения** – общая продолжительность обучения элемента ML-модели.
  - **Начало обучающей выборки** – начало времени данных, отобранных в обучающую выборку.
  - **Окончание обучающей выборки** – окончание времени данных, отобранных в обучающую выборку.
  - **Общий интервал времени** – общая продолжительность интервала отбора данных.
  - **Продолжительность интервалов** – суммарная продолжительность интервалов времени данных, отобранных в обучающую выборку после применения разметки индикатора обучения к интервалу отбора данных.
  - **Число узлов РИВС** – количество узлов РИВС, входящих в обучающую выборку после применения разметки индикатора обучения к интервалу отбора данных.

    Обучение предиктивного элемента ML-модели с нейросетевой архитектурой рекомендуется проводить на не менее чем 10 000 узлах РИВС. Если узлов РИВС в обучающей выборке меньше, необходимо увеличить интервал времени данных для обучения и обучить элемент заново.

- Графики с результатами обучения для предиктивных элементов ML-модели:

  - **Ошибки обучения и валидации** – график, отображающий ошибки обучения и валидации в зависимости от эпохи обучения. Синяя линия на графике соответствует ошибке обучения, а красная линия соответствует ошибке валидации.

    В зависимости от динамики ошибок обучения и валидации вы можете принять решение о том, требуется ли увеличить или сократить количество эпох обучения и обучить элемент заново. Корректировка параметров обучения элемента ML-модели необходима в следующих случаях:

    - Ошибка валидации растет или не изменяется на протяжении всего обучения. Для улучшения качества работы необходимо использовать другие данные для обучения и/или использовать другую архитектуру элемента ML-модели и обучить элемент заново.

    - Ошибка валидации начала расти под конец обучения. Небольшой рост ошибки валидации может быть временным и не зависеть от качества данных и/или выбранной архитектуры элемента. В таком случае рекомендуется убедиться, является ли рост ошибки валидации временным. Для этого в параметре **Количество эпох для ранней остановки обучения** нужно указать умноженный на два номер эпохи, на которой начался рост ошибки валидации. Например, если рост ошибки валидации начался на десятой эпохе, укажите в этом параметре значение `20`.

      Если после повторного обучения элемента ошибка валидации не снизилась на дополнительных эпохах обучения, для улучшения качества работы элемента необходимо сократить количество эпох для обучения до эпохи, на которой наблюдалась минимальная ошибка валидации.

  - **Прогноз обученной модели** – графики, отображающие прогноз обученной модели для выходных тегов и общую ошибку прогноза.

    На каждом графике выходного тега полученное значение тега отображается в виде синей линии, а предсказанное значение тега отображается в виде зеленой линии. Если на определенном интервале времени предсказанное значение тега начинает систематически отличаться от полученного значения тега, это может указывать на то, что в выборку для обучения были включены данные для разных режимов работы агрегата или были изменены свойства оборудования (например, был проведен ремонт оборудования). В таком случае перед повторным обучением элемента необходимо выбрать разметку, в которой определены критерии поведения тегов в нужном режиме работы, и/или скорректировать интервал времени данных, на которых обучается элемент ML-модели.

    График общей ошибки прогноза отображается последним. На графике красная линия соответствует общей ошибке прогноза, а горизонтальная оранжевая линия соответствует порогу, при превышении которого элемент ML-модели считает поведение объекта мониторинга аномальным и регистрирует инцидент. С помощью графика общей ошибки прогноза вы можете принять решение о том, требуется ли скорректировать параметры обучения и обучить элемент заново. Корректировка параметров обучения элемента ML-модели необходима в следующих случаях:

    - Красная линия является плоской, на графике не прослеживается динамика изменения состояния объекта мониторинга. Для улучшения качества работы необходимо выбрать другой интервал времени данных, которые отражают нормальную работу объекта мониторинга с незначительными отклонениями, и/или изменить архитектуру элемента.

    - Изменения тренда красной линии не соответствуют ожидаемому поведению объекта мониторинга. Для улучшения качества работы элемента необходимо выбрать другой интервал времени данных, которые отражают нормальную работу объекта мониторинга с незначительными отклонениями, и/или изменить архитектуру элемента.

    - Значение порога значительно больше типового уровня ошибки. На графике красная линия в основном прижата к нижней части графика, а оранжевая линия проходит в верхней части графика. Такое поведение означает, что предиктивный элемент не смог автоматически выбрать адекватное значение порога, так как обучающая выборка либо не содержит аномалий, либо содержит небольшое количество очень интенсивных аномалий. Для улучшения работы элемента необходимо снизить значение параметра **Порог регистрации инцидентов** перед запуском инференса.

- Графики с результатами обучения для эллиптических конвертов ML-модели:

  - **Степень отклонения тегов** – график, отображающий удаление точки, описывающей состояние объекта мониторинга в определенный момент времени в фазовом пространстве, от центра эллиптической области нормальных состояний. Изменение состояния объекта мониторинга отображается в виде красной линии. Горизонтальная оранжевая линия соответствует порогу и показывает максимальное удаление, при котором состояние считается принадлежащим области нормальных состояний.

    С помощью графика вы можете принять решение о том, требуется ли скорректировать параметры обучения и обучить элемент заново. Корректировка параметров обучения элемента ML-модели необходима в следующих случаях:

    - Красная линия является плоской, на графике не прослеживается динамика изменения состояния объекта мониторинга. Для улучшения качества работы элемента необходимо выбрать другой интервал времени данных, которые отражают нормальную работу объекта мониторинга с незначительными отклонениями, и обучить элемент заново.

    - Красная линия имеет горизонтальные участки вдоль верхней границы графика. Для улучшения качества работы элемента необходимо отрегулировать значение параметра **Доля выборки для оценки среднего и ковариации** и обучить элемент заново. Чем выше значение параметра, тем ниже чувствительность эллиптического конверта к аномалиям и тем ниже красная линия на графике.

    - Изменения тренда красной линии не соответствуют ожидаемому поведению объекта мониторинга. Для улучшения качества работы элемента необходимо выбрать другой интервал времени данных, которые отражают нормальную работу объекта мониторинга с незначительными отклонениями, и обучить элемент заново.

    - Значение порога значительно больше типового уровня ошибки. На графике красная линия в основном прижата к нижней части графика, а оранжевая линия проходит в верхней части графика. Такое поведение означает, что эллиптический конверт не смог автоматически выбрать адекватное значение порога, так как обучающая выборка либо не содержит аномалий, либо содержит небольшое количество очень интенсивных аномалий. Для улучшения качества выявления аномальных состояний элементом необходимо отрегулировать значение параметра **Доля выбросов в выборке** и обучить элемент заново. Чем выше значение доли выбросов в обучающей выборке, тем ниже значение порога регистрации инцидентов.

  - **Значения тегов** – графики, отображающие значения каждого тега во время обучения.

  - **Распределение значений тегов** – гистограммы распределения значений каждого тега во время обучения. Пики графика соответствуют наиболее часто наблюдаемым значениям, проанализированным элементом во время обучения.

    Количество пиков на графике является признаком качества данных, отобранных для обучения. Если для обучения элемента были правильно выбраны разметки и интервал времени данных, то на графике должен отображаться один пик. Если пиков на графике несколько, это может указывать на то, что в выборку для обучения были включены данные для разных режимов работы агрегата (например, до и после его ремонта). В таком случае перед повторным обучением элемента необходимо выбрать разметку, в которой определены критерии поведения тегов в нужном режиме работы, и/или скорректировать интервал времени данных, на которых обучается элемент ML-модели.

  - **Корреляция тегов** – матрица, отображающая взаимосвязи тегов, используемых при обучении элемента ML-модели.

Оценка результатов обучения элемента ML-модели

После анализа результатов обучения вы можете оценить результаты обучения, а также оставить комментарий к выставленной оценке. Выставленные оценки отображаются в виде меток в дереве активов, а также под именами ML-моделей и элементов ML-моделей при их просмотре. Выставленная оценка отображается до повторного обучения элемента.

В таблице ниже перечислены оценки обучения элементов ML-моделей, предусмотренные в Kaspersky MLAD.

Оценки обучения элементов ML-моделей

Название оценки	Обозначение оценки в дереве активов	Описание
Хорошие результаты обучения	**TRN OK**	Эта оценка отображается для элемента ML-модели, если результаты его обучения были оценены как хорошие. Оценка обучения также отображается при просмотре ML-модели, если отсутствует оценка ее исторического инференса и при этом отсутствуют элементы с плохими результатами обучения.
Плохие результаты обучения	**TRN POOR**	Эта оценка отображается для элемента ML-модели, если результаты его обучения были оценены как плохие. Оценка обучения также отображается при просмотре ML-модели, если отсутствует оценка ее исторического инференса и при этом в ее составе есть хотя бы один элемент с плохими результатами обучения.

Оценка результатов обучения элементов ML-моделей доступна системным администраторам и пользователям с правом **Обучение моделей** из группы прав **Управление ML-моделями**. Функциональность доступна после добавления лицензионного ключа.

Чтобы оценить результаты обучения элемента ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите элемент ML-модели, результаты обучения которого вы хотите оценить.

   Справа отобразится список параметров.
3. Выберите вкладку **Результаты обучения**.
4. В блоке параметров **Оценка обучения** выполните одно из следующих действий:
   - Если элемент ML-модели обучен хорошо, нажмите на кнопку **Да**.
   - Если элемент ML-модели обучен плохо, нажмите на кнопку **Нет**.
5. При необходимости в поле **Комментарий к оценке** введите краткий комментарий к выставленной оценке.

   Например, вы можете указать причину, по которой результаты обучения считаются плохими.
6. Нажмите на кнопку **Добавить**.

Запуск и остановка инференса ML-модели

Вы можете запускать и останавливать инференс ML-модели со статусами **Обучена** или **Опубликована** на поступающих данных телеметрии.

Kaspersky MLAD поддерживает одновременное выполнение инференса на исторических и поступающих данных.

Kaspersky MLAD позволяет выполнять как полный, так и быстрый инференс на исторических данных. В результате полного исторического инференса ML-модель формирует артефакты и регистрирует инциденты.

Если вам нужно пересчитать инциденты на основе сформированных ранее артефактов, вы можете запустить быстрый исторический инференс. Быстрый исторический инференс выполняется на интервале данных, на котором ранее проводился полный исторический инференс. Быстрый инференс возможен, если были изменены следующие параметры элементов ML-модели:

- **Период напоминания (сек.)**;
- **Период подавления повторных срабатываний (сек.)**;
- **Интервал наблюдения за аномалией (сек.)**;
- **Доля длительности аномалии в интервале**;
- **Порог регистрации инцидентов**.

Функциональность доступна после добавления лицензионного ключа.

Чтобы запустить инференс ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите ML-модель, инференс которой вы хотите запустить.

   Справа отобразится список параметров.
3. Выберите вкладку **Инференс**.

4. Если требуется запустить инференс на данных телеметрии, поступающих в режиме реального времени, в блоке параметров **Потоковый инференс** нажмите на кнопку **Запустить**.

5. Если требуется запустить инференс на исторических данных телеметрии, в блоке параметров **Исторический инференс** укажите интервал времени данных для работы ML-модели и нажмите на одну из следующих кнопок:

   - **Запустить**, если требуется выполнить полный исторический инференс. При запуске полного инференса на интервале инференса заново создаются артефакты.

   - **Пересчитать инциденты**, если требуется выполнить быстрый исторический инференс. При запуске быстрого инференса используется существующие артефакты на интервале инференса.

   При запуске повторного инференса неопубликованной ML-модели с интервала инференса удаляются инциденты элементов ML-модели, сформированные предыдущим инференсом, в том числе и учетные инциденты, если эта ML-модель была ранее опубликована, а затем снята с публикации. При запуске повторного инференса опубликованной ML-модели инциденты элементов этой ML-модели не удаляются, даже если они не являются учетными, то есть они были сформированы, когда эта ML-модель еще не была опубликована или была снята с публикации.

Если был запущен исторический инференс, Kaspersky MLAD добавит ML-модель в очередь на инференс.

Исторический инференс завершается автоматически после обработки всех данных телеметрии в соответствии с заданным интервалом времени. При необходимости вы можете прервать исторический и/или потоковый инференс ML-модели.

Чтобы остановить инференс ML-модели:

1. В основном меню выберите раздел **Модели**.

2. В дереве активов выберите ML-модель, инференс которой вы хотите остановить.

   Справа отобразится список параметров.

3. Выберите вкладку **Инференс**.

4. Нажмите на кнопку **Остановить** в блоке параметров нужного типа инференса.

Kaspersky MLAD остановит инференс для выбранной ML-модели.

Оценка результатов исторического инференса ML-модели

После анализа результатов исторического инференса вы можете оценить результаты последнего запущенного инференса, а также оставить комментарий к выставленной оценке. Выставленные оценки отображаются в виде меток в дереве активов, а также под именами ML-моделей при их просмотре. Выставленная оценка отображается до повторного запуска исторического инференса.

В таблице ниже перечислены оценки исторического инференса ML-моделей, предусмотренные в Kaspersky MLAD.

Оценки исторического инференса ML-моделей

Название оценки	Обозначение оценки в дереве активов	Описание
Хорошие результаты исторического инференса	INFR OK	Эта оценка отображается для ML-модели, если результаты ее исторического инференса были оценены как хорошие.
Плохие результаты исторического инференса	INFR POOR	Эта оценка отображается для ML-модели, если результаты ее исторического инференса были оценены как плохие.

Функциональность доступна после добавления лицензионного ключа.

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите ML-модель, результаты инференса которой вы хотите оценить.

   Справа отобразится список параметров.
3. Выберите вкладку **Инференс**.
4. В блоке параметров **Оценка инференса** выполните одно из следующих действий:
   - Если результаты исторического инференс ML-модели хорошие, нажмите на кнопку **Да**.
   - Если результаты исторического инференс ML-модели плохие, нажмите на кнопку **Нет**.
5. При необходимости в поле **Комментарий к оценке** введите краткий комментарий к выставленной оценке.

   Например, вы можете указать причину, по которой результаты инференса считаются плохими.
6. Нажмите на кнопку **Добавить**.

Просмотр графа потока данных в ML-модели

Вы можете просматривать граф потока данных в ML-моделях.

Функциональность доступна после добавления лицензионного ключа.

Чтобы просмотреть граф потоков данных в ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите ML-модель, граф потока данных который вы хотите просмотреть.

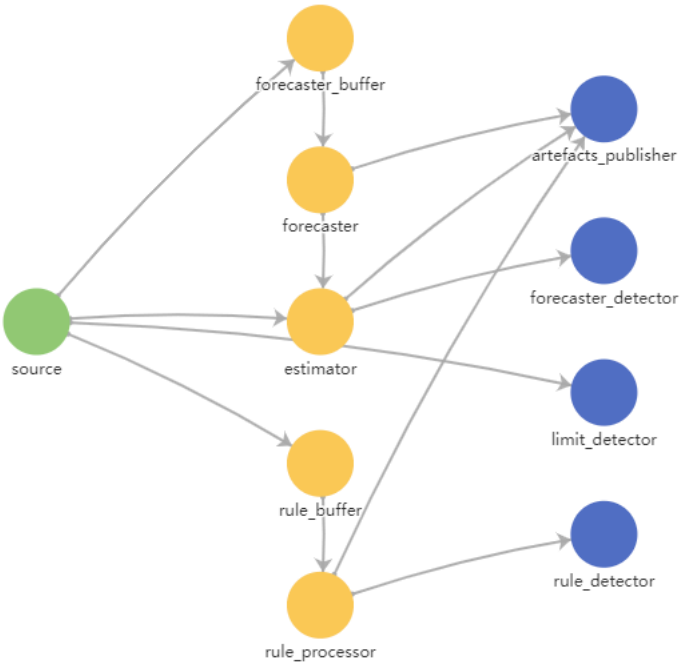
   Справа отобразится список параметров.

3. Выберите вкладку **Граф потока данных**.

   Справа отобразится граф потока данных в ML-модели.

4. Если требуется просмотреть параметры элемента графа, наведите на него курсор мыши.

   Отобразится окно, в котором перечислены значения параметров выбранного элемента.



Граф потока данных в ML-модели

Подготовка ML-модели к публикации

Если ML-модель протестирована и готова к продуктивной работе, вы можете опубликовать ее. Параметры опубликованной модели будут зафиксированы, а сформированные ей инциденты станут учетными. Перед публикацией ML-модель необходимо подготовить к публикации. Подготовка к публикации является промежуточным шагом в процессе публикации ML-модели, в результате которого параметры ML-модели и ее элементов фиксируются, их изменение становится недоступным.

ML-модель, подготовленная к публикации, недоступна для изменения.

> Подготовка ML-модели к публикации может выполняться системным администраторам и пользователям с правом **Изменение моделей** из группы прав **Управление ML-моделями**.
> Функциональность доступна после добавления лицензионного ключа.

Чтобы подготовить ML-модель к публикации:

1. В основном меню выберите раздел **Модели**.

2. В дереве активов выберите ML-модель, которую вы хотите подготовить к публикации.

   Справа отобразится список параметров.

3. Нажмите на кнопку **Подготовить к публикации**.

ML-модели будет присвоен статус **Готова к публикации**. Сообщите сотруднику, ответственному за публикацию ML-моделей, о ее готовности, или, если у вас есть необходимые права, опубликуйте ML-модель.

Если требуется внести изменения в ML-модель перед ее публикацией, нажмите на кнопку **Вернуться в режим правки**. ML-модели будет возвращен статус **Обучена**.

Публикация и снятие ML-модели с публикации

Если ML-модель протестирована и готова к продуктивной работе, вы можете опубликовать ее. Параметры опубликованной модели будут зафиксированы.

После запуска инференса ML-модель будет регистрировать учетные инциденты на рабочих данных от объекта мониторинга. В отличие от инцидентов, сформированных в процессе инференса неопубликованной ML-моделью, учетные инциденты предполагают принятие мер и ведение отчетности по ним в рамках производственного процесса.

Публикация и снятие ML-моделей с публикации доступно системным администраторам и пользователям с правом **Изменение моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы опубликовать ML-модель:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите ML-модель, которую вы хотите опубликовать.

   Справа отобразится список параметров.
3. Нажмите на кнопку **Опубликовать**.

ML-модели будет присвоен статус **Опубликована**.

При необходимости, например, если требуется изменить параметры ML-модели и/или ее элементов или перестать регистрировать учетные инциденты, вы можете снять опубликованную ML-модель с публикации.

Чтобы снять ML-модель с публикации:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите ML-модель, которую вы хотите снять с публикации.

   Справа отобразится список параметров.
3. Нажмите на кнопку **Снять с публикации**.

ML-модели будет присвоен статус **Готова к публикации**.

Удаление ML-модели

Вы можете удалить созданные ранее и/или импортированные ML-модели из Kaspersky MLAD. Если требуется, вы можете повторно загрузить ML-модель, которая была ранее импортирована и затем удалена.

После удаления ML-модели ее артефакты (например, прогнозы, индивидуальные ошибки, ошибки прогноза, индикаторы выполнения правила), а также инциденты, зарегистрированные ML-моделью, будут удалены.

Удаление ML-моделей доступно системным администраторами пользователям с правом **Удаление моделей** из группы прав **Управление ML-моделями**.
Функциональность доступна после добавления лицензионного ключа.

Чтобы удалить ML-модель:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите ML-модель, которую требуется удалить.

   Справа отобразится список параметров.
3. В правом верхнем углу страницы нажмите на кнопку 🗑.
4. Подтвердите удаление ML-модели.

   Выбранная ML-модель будет удалена из Kaspersky MLAD.

Вы также можете перейти к удалению ML-модели, нажав на вертикальное меню ••• и выбрав пункт **Удалить модель**.

Управление пресетами

В разделе **Пресеты** вы можете создавать пользовательские пресеты. Созданные вами пресеты будут отображаться только для вашей учетной записи.

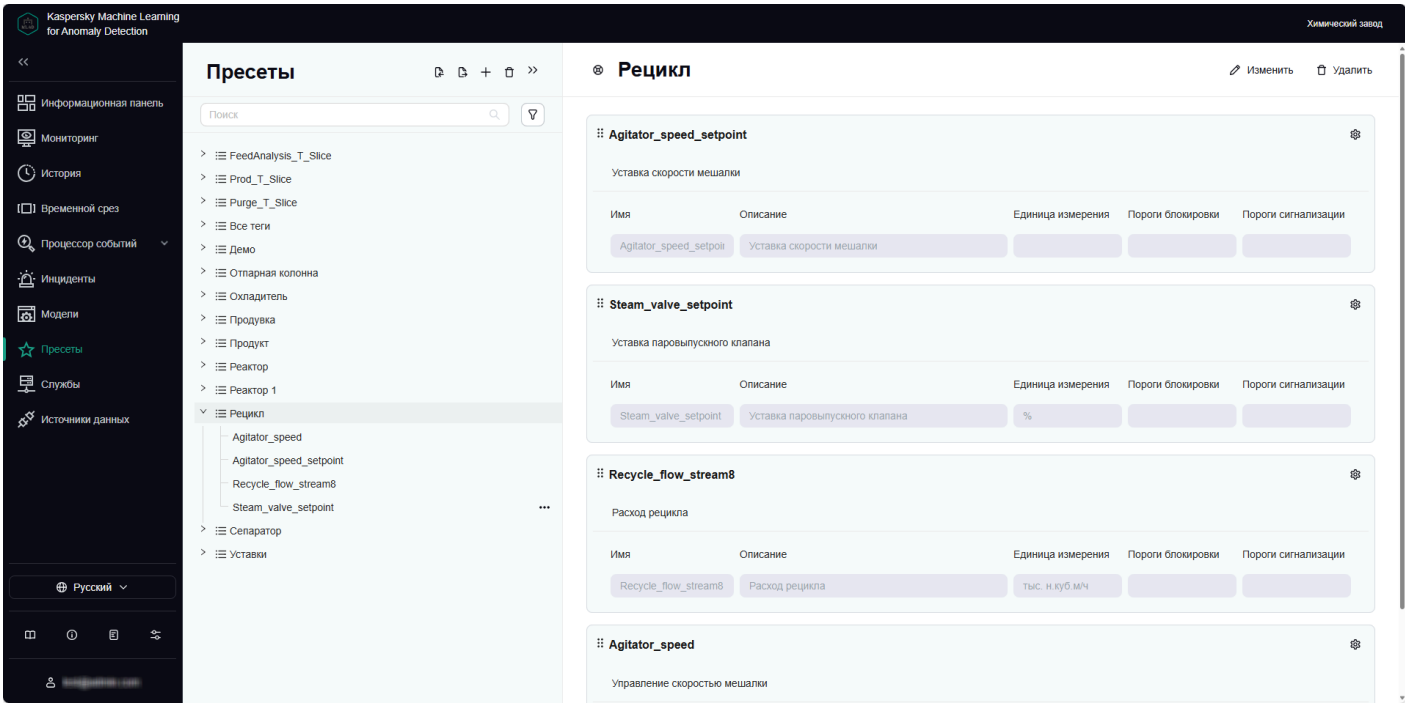
При создании пресетов вы можете выполнять следующие действия:

- Выбирать теги, данные которых будут отображаться на графиках в разделах **История** и **Мониторинг**.
- Управлять графическими областями в составе пресета. *Графическая область* – это совокупность тегов, данные которых совместно отображаются путем наложения на одном графике в разделах **История** и **Мониторинг**. В графической области могут отображаться данные для одного и более тегов пресета. Графические области, в которых указан один тег, называются *единичными*.
- Управлять отображением тегов пресета в разделе **Временной срез**. Для этого вы можете задавать выражения с простыми арифметическими действиями (например, сложение, вычитание, умножение и деление), чтобы рассчитать значения тегов в составе пресета.

Пользовательские пресеты, теги, входящие в их состав, и активы, к которым относятся пресеты, отображаются в левой части окна в виде дерева. Пользовательские пресеты отображаются со значком ☰, а активы, к которым они относятся, отображаются со значком 🗀. С помощью кнопок › и ⌄ слева от имен активов и пресетов вы можете отображать и скрывать состав активов.

Для просмотра получаемых данных на графиках в разделах **История** и **Мониторинг** вы также можете загрузить пресеты в Kaspersky MLAD из JSON-файла.

При необходимости вы можете изменить необходимые пресеты, сохранить их в JSON-файл, а также удалить их.



Раздел **Пресеты**

О пресетах

Пресет – это набор тегов, сформированный пользователем в произвольном порядке или созданный автоматически программой. Пресет является функциональным элементом иерархической структуры.

Пресет, сформированный пользователем, называется *пользовательским*. Набор тегов в составе пользовательского пресета может соответствовать определенному аспекту технологического процесса или участку объекта мониторинга. Созданные пользовательские пресеты отображаются в разделе **Пресеты**.

Пресет, созданный программой автоматически, называется *динамическим*. В Kaspersky MLAD предусмотрены следующие динамические пресеты:

- Динамический пресет по инциденту – динамический пресет, сформированный при регистрации инцидента.

- Динамический пресет по элементу ML-модели – динамический пресет, сформированный при выборе элемента ML-модели в разделе **Мониторинг** или **История**.

Сформированные динамические пресеты отображаются в группе **Динамические пресеты** дерева активов в раскрывающемся списке **Пресет** в разделах **Мониторинг** и **История**.

Динамические пресеты по инцидентам

Динамическому пресету, сформированному при регистрации инцидента, автоматически присваивается название **Теги инцидента #<идентификатор инцидента>**. Динамический пресет по инциденту содержит теги, оказавшие наибольшее влияние на формирование зарегистрированного инцидента.

Набор тегов в динамическом пресете по инциденту зависит от типа зарегистрированного инцидента. Динамические пресеты могут быть сформированы по инцидентам, зарегистрированным предиктивными элементами ML-моделей, элементами ML-моделей на основе диагностических правил и эллиптических конвертов, а также детектором Limit Detector.

Для каждого тега в составе динамического пресета по инциденту формируются единичные графические области. Перейти к просмотру графических областей динамического пресета по инциденту вы можете одним из следующих способов:

- Из таблицы инцидентов по нажатию на дату и время начала конкретного инцидента. При нажатии на дату и время начала инцидента будет осуществлен переход в раздел **История**.
- По нажатию на точку-индикатор инцидента. Точки-индикаторы инцидентов отображаются в нижней части графика артефакта элемента ML-модели в разделах **Мониторинг** и **История**. После нажатия на точку-индикатор инцидента отобразится таблица инцидентов. Нажмите на дату и время начала инцидента для перехода в раздел **История**.

Динамические пресеты по элементам ML-моделей

Динамическому пресету, сформированному по элементу ML-модели, автоматически присваивается название **<имя ML-модели> ⊃ <имя элемента>**. Динамический пресет доступен для выбора в разделах **Мониторинг** и **История**, пока выбран элемент, по которому он был сформирован.

Динамический пресет по элементу ML-модели содержит входные и выходные теги, заданные в параметрах этого элемента, а также теги разметки, используемой в качестве индикатора инференса для ML-модели, которой принадлежит выбранный элемент. Состав тегов в динамическом пресете автоматически изменяется при изменении состава входных и выходных тегов выбранного элемента ML-модели, а также при изменении состава тегов разметки, используемой в качестве индикатора инференса для ML-модели.

Для каждого тега в составе динамического пресета по элементу ML-модели формируются единичные графические области. Графические области динамического пресета отображаются автоматически после выбора нужного элемента в разделе **Мониторинг** или **История**.

Поиск и фильтрация объектов в разделе Пресеты

В разделе **Пресеты** в дереве активов вы можете выполнять поиск и фильтрацию следующих объектов:

- активов;
- пресетов;
- тегов.

Поиск выполняется по именам объектов.

Чтобы найти нужные объекты в дереве активов,

в разделе **Пресеты** введите поисковый запрос в поле **Поиск**. Поиск выполняется по мере ввода символов в строку поиска. В результаты поиска автоматически включаются омоглифы поисковой строки.

Если найдены объекты, удовлетворяющие поисковому запросу, в дереве активов отобразятся найденные объекты, а также разделы дерева активов, в составе которых были найдены эти объекты.

Если требуется сбросить поисковый запрос, нажмите на кнопку в строке поиска.

Вы также можете выполнять фильтрацию объектов в дереве активов. Фильтрация применяется к объектам, найденным в соответствии с поисковым запросом. Если поисковый запрос не задан, фильтрация применяется ко всем объектам в дереве активов.

Чтобы отфильтровать объекты в дереве активов:

1. В разделе **Пресеты** нажмите на кнопку , расположенную над деревом активов.

   Справа отобразятся параметры фильтрации.

2. В раскрывающемся списке **Тип раздела** выберите один или несколько типов разделов дерева активов.

   Вы можете выбрать следующие типы разделов: **Активы**, **Пресеты** и **Теги**.

3. Если требуется сбросить параметры фильтрации, выполните одно из следующих действий:

   - Для сброса конкретного параметра фильтрации нажмите на кнопку рядом с нужным параметром.
   - Для сброса всех параметров фильтрации нажмите на кнопку **Очистить фильтры** в правом верхнем углу страницы.

4. Если требуется скрыть отображение параметров фильтрации, нажмите на кнопку рядом с полем **Поиск**.

Фильтрация объектов выполняется по мере выбора параметров фильтрации. Если найдены объекты, удовлетворяющие параметрам фильтрации, в дереве отобразятся найденные объекты, а также разделы дерева активов, в составе которых были найдены эти объекты.

Если к дереву активов применены какие-либо параметры фильтрации, над деревом активов отображается кнопка .

Просмотр пресета

Вы можете просматривать пресеты, созданные и загруженные вами ранее в Kaspersky MLAD для вашего объекта мониторинга.

Чтобы просмотреть пресет:

1. В основном меню выберите раздел **Пресеты**.
2. На открывшейся странице в дереве активов слева выберите нужный пресет.

   Справа отобразится список графических областей, входящих в состав выбранного пресета.
3. Если требуется просмотреть информацию по тегам, входящим в состав пресета, выполните следующие действия:

   a. Слева от имени нужного пресета нажмите на кнопку ›.

   Под выбранным пресетом отобразится список тегов, входящих в его состав.

   b. Для просмотра параметров тега нажмите на нужный тег в составе пресета.

   Справа отобразится список параметров тега, заданных при его создании.

Если требуется, вы можете изменить пресет или создать новый пресет.

Создание пресета

В Kaspersky MLAD вы можете создавать пресеты и в составе пресетов формировать графические области. Графические области определяют состав тегов, данные которых отображаются на одном графике, а также место отображения графика тегов в разделах **История** и **Мониторинг**. Графические области, в которых указан один тег, называются *единичными*. Единичные графические области создаются автоматически после выбора тегов для пресета, по одной области на каждый выбранный тег.

Если вы используете процессор событий и настроили монитор **Эксфильтрация данных по DNS**, то при активации этого монитора в иерархической структуре объекта мониторинга будет создан актив **DNS Exfiltration**. Программа автоматически наполняет этот актив тегами, содержащими информацию о DNS-запросах, которые привели к активации монитора. При необходимости вы можете создать пресет из этих тегов и использовать его для просмотра графиков тегов монитора в разделах **История** и **Мониторинг**.

Чтобы создать пресет:

1. В основном меню выберите раздел **Пресеты** и нажмите на кнопку +.

   Справа отобразится панель **Создание пресета**. В левой части панели отобразится дерево активов.
2. В поле **Имя пресета** укажите имя пресета.
3. В раскрывающемся списке **Актив пресета** выберите актив, к которому необходимо отнести пресет.
4. В дереве активов установите флажки около тегов, которые необходимо добавить в пресет.

   Для добавления всех тегов, входящих в состав определенного пресета, выберите этот пресет в поле **Выберите пресет**. Для добавления тега по его имени начните вводить имя тега в поле **Поиск по имени тега** и выберите нужный тег.

   Если требуется удалить теги из пресета, в дереве активов снимите флажки около тех тегов, которые требуется удалить.
5. Нажмите на кнопку **Сохранить выбор**.

   Справа отобразятся графические области, созданные автоматически для каждого выбранного тега.

6. Если требуется удалить графические области, выполните одно из следующих действий:

   - Нажмите на кнопку **Удалить все области** в блоке параметров **Графические области** для удаления всех графических областей пресета.

   - Нажмите на кнопку в правом верхнем углу блока нужной графической области и подтвердите удаление графической области.

   Удаление графической области не приводит к удалению тегов в составе этой области из пресета. Вы можете добавить теги из удаленных графических областей в другие области.

7. Если требуется изменить существующую графическую область, выполните одно из следующих действий:

   - Для добавления тега в графическую область нажмите на значок плюса в блоке графической области и выберите тег.

     Если требуется, вы можете скопировать имя выбранного тега, нажав на кнопку справа от нужного имени. Вы можете использовать скопированное имя тега, например, в качестве названия графической области.

   - Для удаления тега из графической области нажмите на кнопку напротив нужного тега в блоке графической области.

8. Если требуется добавить графическую область, выполните следующие действия:

   a. Нажмите на кнопку **Пустая область**.

   b. Выберите тег для добавления в графическую область.

      Если требуется, вы можете скопировать имя выбранного тега, нажав на кнопку справа от нужного имени. Вы можете использовать скопированное имя тега, например, в качестве названия графической области.

   c. Если требуется добавить еще один или более тегов в графическую область, нажмите на значок плюса и выберите теги.

9. Если требуется добавить единичные графические области для тегов, которые не используются в других графических областях пресета, нажмите на кнопку **Единичные графики**.

10. Если требуется изменить расположение графической области внутри пресета, перетащите графическую область вверх или вниз, удерживая за точки ( ) слева от ее названия.

11. Если требуется изменить параметры отображения графической области в разделах **История** и **Мониторинг**, выполните следующие действия:

    a. Нажмите на кнопку ⚙ в правом верхнем углу нужного блока графической области.

    Справа отобразится панель с параметрами отображения графической области.

    b. Укажите название и при необходимости описание графической области.

    Название и описание графической области отображаются слева от графиков в разделах **История** и **Мониторинг**, а также при наведении курсора на график.

    c. В раскрывающемся списке **Режим масштабирования оси** выберите один из следующих режимов:

    - **Режим единой оси** – для отображения тегов области используется общая ось ординат.
    - **Режим приведения** – для каждого тега данные масштабируются по оси ординат индивидуально, независимо от данных других тегов в составе графической области.

    d. Если был выбран режим единой оси в качестве режима масштабирования, выполните одно из следующих действий:

    - Включите переключатель **Автоматический**, если требуется автоматически масштабировать график с учетом минимального и максимального значений всех тегов графической области.
    - Выключите переключатель **Автоматический** и укажите верхнюю и нижнюю границы отображения значений тегов графической области.

      Допустимые границы отображения значений тега имеют больший приоритет над отображением порогов блокировки, даже если включена функция **Всегда показывать пороги блокировки**.

    e. Если требуется добавить горизонтальные контрольные линии для тегов на графике, нажмите на кнопку **Добавить контрольную линию** и укажите контрольное значение и цвет линии для отображения на графике.

    Контрольные линии помогают визуально оценить колебания значений тегов в определенных пределах. Вы можете добавить несколько линий.

    Если требуется удалить контрольную линию, нажмите на кнопку ✕ напротив заданного контрольного значение и цвета нужной линии.

    f. Нажмите на кнопку **Сохранить**.

12. Если требуется настроить отображение пресета в разделе **Временной срез**, выполните следующие действия:

    a. Нажмите на кнопку **Отображение пресета в разделе Временной срез**.

    Справа отобразится панель **Отображение пресета в разделе Временной срез**.

    b. Включите переключатель **Отображать пресет в разделе Временной срез**.

    c. В поле **Подпись оси X** укажите подпись, которая отображается по оси абсцисс.

    d. Для отображения на графике значений тегов пресета, рассчитываемых по выражению, нажмите на кнопку **Добавить график** и укажите следующие значения:

    - В поле **Название** введите название выражения, по которому рассчитываются значения тегов.
    - В поле **Подпись оси Y** введите подпись, которая отображается по оси ординат.
    - В поле **Выражение для расчета** введите выражение, по которому рассчитываются значения тегов.

      С помощью заданных выражений вы можете просмотреть индивидуальные ошибки тегов, прогнозируемые значения тегов, а также значения тегов, полученные от датчиков объекта мониторинга, в один и тот же момент времени. Вы можете задать выражения с простыми арифметическими действиями (например, сложение, вычитание, умножение и деление), а также использовать следующие переменные в выражениях:

      - *$tagValue* – полученное значение тега (по результатам наблюдения);
      - *$tagError* – индивидуальная ошибка тега;
      - *$tagPrediction* – прогнозируемое значения тега;
      - *$tagX* – значение координаты расположения датчика объекта мониторинга по оси абсцисс, заданного при создании тега;
      - *$tagY* – значение координаты расположения датчика объекта мониторинга по оси ординат, заданного при создании тега;
      - *$tagZ* – значение координаты расположения датчика объекта мониторинга по оси аппликат, заданного при создании тега.

      Например, если от датчиков поступают значения температуры по Фаренгейту, для отображения на графике значений температуры по Цельсию вы можете указать следующее выражение:

      ```
      5/9 * ($tagValue - 32)
      ```

    - В поле **Цвет графика** выберите цвет графика, который будет отображаться для пресета в разделе **Временной срез**.

    Если требуется, вы можете добавить несколько выражений для раздела **Временной срез**.

    e. Если требуется удалить выражение в пресете для раздела **Временной срез**, нажмите на кнопку справа от нужного выражения.

    f. Нажмите на кнопку **Сохранить**.

13. Нажмите на кнопку **Сохранить**.

Если какие-либо теги пресета не были добавлены хотя бы в одну графическую область, в окне браузера отобразится соответствующее информационное сообщение. Теги, не использованные в графических областях, не будут отображены на графиках в разделах **История** и **Мониторинг**.

Новый пресет отобразится в разделе **Пресеты** в дереве активов слева и в раскрывающемся списке пресетов в разделах **История** и **Мониторинг**. Пресет, для которого выполнен пункт 12 этой инструкции, также отобразится в раскрывающемся списке пресетов в разделе **Временной срез**.

Загрузка пресетов из файла

Загрузка пресетов выполняется из файла формата JSON. В этом файле с помощью параметра `parent_category_id` задаются идентификаторы активов, в которые необходимо загрузить пресеты. Если идентификатор актива не указан, пресет загружается в головной элемент иерархической структуры.

Если требуется, вы можете загрузить все пресеты из файла JSON в определенный актив. При этом идентификаторы активов, указанные в параметре `parent_category_id` JSON-файла, игнорируются.

Чтобы загрузить пресеты в Kaspersky MLAD:

1. В основном меню выберите раздел **Пресеты**.
2. Выполните одно из следующих действий:
   - Если требуется загрузить пресеты в активы, указанные в JSON-файле, в верхней части открывшейся страницы нажмите на кнопку .
   - Если требуется загрузить пресеты в определенный актив, в дереве активов рядом с разделом, в который требуется загрузить пресеты, откройте вертикальное меню **...** и выберите пункт **Импортировать пресеты**.
3. Выберите файл формата JSON с описанием пресетов на локальном диске.

Выбранный файл будет загружен в Kaspersky MLAD. Новые пресеты отобразятся в списке пресетов в дополнение к ранее созданным пресетам.

Изменение пресета

Вы можете изменять созданные и загруженные вами ранее пресеты.

Если требуется, вы можете удалить теги из состава пресета с помощью вертикального меню в дереве активов. Для этого откройте вертикальное меню **...** справа от нужного тега, выберите пункт **Удалить тег** и подтвердите удаление тега из пресета.

Чтобы изменить пресет:

1. В основном меню выберите раздел **Пресеты**.
2. Выполните одно из следующих действий:
   - В дереве активов слева выберите нужный пресет и нажмите на кнопку **Изменить** в правом верхнем углу страницы.
   - В вертикальном меню **...** справа от нужного пресета выберите пункт **Изменить пресет**.

   Справа отобразится панель **Изменение пресета**. В левой части панели отобразится дерево активов.
3. Если требуется, измените следующие параметры пресета:
   - Имя пресета.
   - Актив, к которому относится пресет.
   - Состав тегов в пресете.

     При удалении тега из пресета Kaspersky MLAD также удаляет его из всех графических областей, в составе которых использовался этот тег. Для каждого тега, добавленного в пресет, будут автоматически созданы единичные графические области.

     > Для сохранения изменений состава тегов пресета необходимо нажать на кнопку **Сохранить выбор**. Нажатие на эту кнопку не приводит к сохранению пресета. Вы остаетесь в режиме изменения пресета.

   - Состав графических областей в пресете.

     Удаление графической области не приводит к удалению тегов в ее составе из пресета. Вы можете добавить теги из удаленных графических областей в другие области.
   - Состав тегов в графических областях.
   - Расположение графической области внутри пресета.
   - Параметры отображения графической области в разделах **История** и **Мониторинг**.
   - Параметры отображения пресета в разделе **Временной срез**.
4. Для сохранения пресета нажмите на кнопку **Сохранить**.

   Если какие-либо теги пресета не были добавлены хотя бы в одну графическую область, в окне браузера отобразится соответствующее информационное сообщение. Теги, не использованные в графических областях, не будут отображены на графиках в разделах **История** и **Мониторинг**.

Измененный пресет обновится в дереве активов в разделе **Пресеты** и в раскрывающемся списке пресетов в разделах **История** и **Мониторинг**. Измененный пресет, для которого заданы параметры отображения в разделе **Временной срез**, также отобразится в раскрывающемся списке пресетов в разделе **Временной срез**.

Сохранение пресетов в файл

Вы можете сохранить в файл формата JSON созданные и загруженные вами ранее в Kaspersky MLAD пресеты.

Чтобы сохранить в файл созданные и загруженные в Kaspersky MLAD пресеты:

1. В основном меню выберите раздел **Пресеты**.
2. В верхней части открывшейся страницы нажмите на кнопку .

   Созданные и загруженные в Kaspersky MLAD пресеты будут сохранены на локальном диске в файл формата JSON.

Удаление пресетов

Вы можете удалить созданные или загруженные вами ранее пресеты.

Чтобы удалить пресет:

1. В основном меню выберите раздел **Пресеты**.
2. Выполните одно из следующих действий:
   - В дереве активов выберите нужный пресет и нажмите на кнопку **Удалить** в правом верхнем углу страницы.
   - В вертикальном меню ••• справа от нужного пресета выберите пункт **Удалить пресет**.
3. Подтвердите удаление пресета.

   Пресет будет удален из списка пресетов.

Чтобы удалить пресеты определенного актива:

1. В основном меню выберите раздел **Пресеты**.
2. В вертикальном меню ••• справа от нужного актива выберите пункт **Удалить пресеты из актива**.
3. Подтвердите удаление пресетов.

   Пресеты выбранного актива будут удалены.

Чтобы удалить все пресеты:

1. В основном меню выберите раздел **Пресеты** и нажмите на кнопку , расположенную над деревом активов.
2. Подтвердите удаление пресетов.

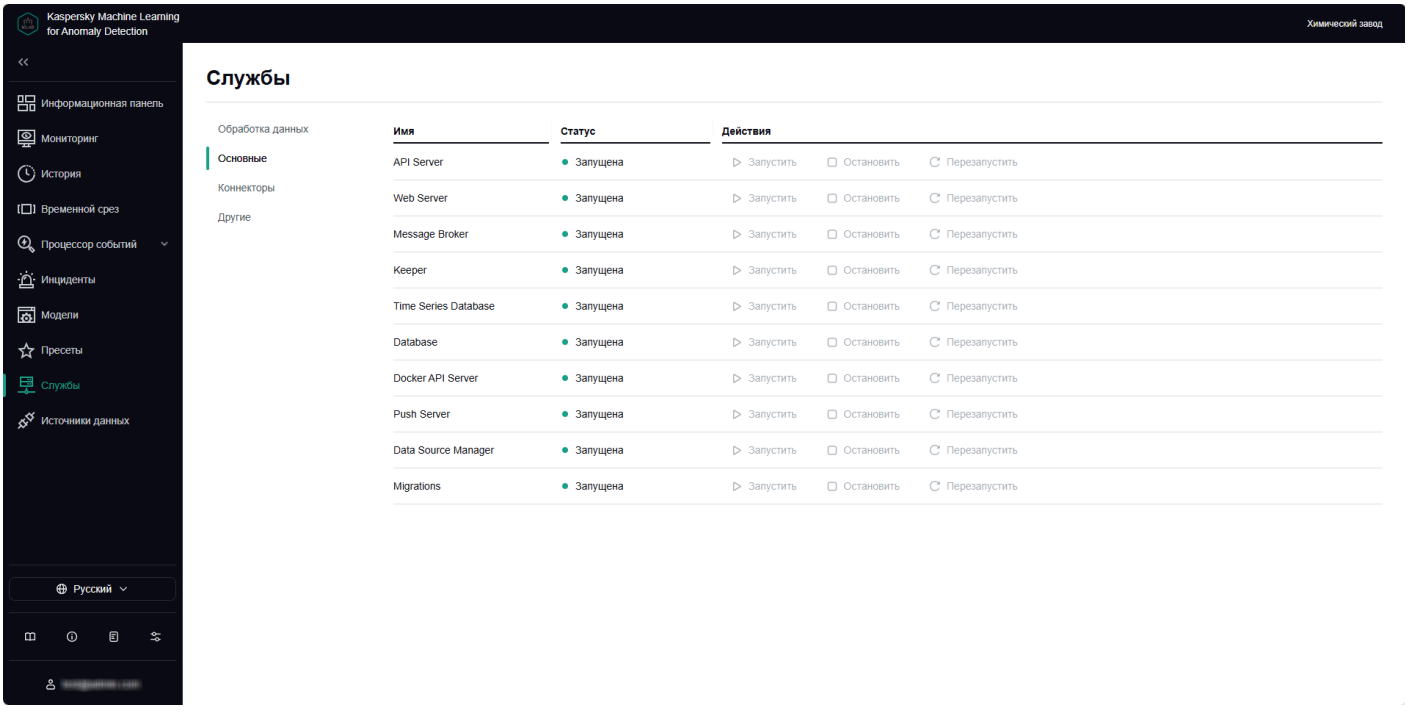
Все пресеты будут удалены.

Управление службами

В разделе **Службы** отображается таблица, содержащая информацию о службах и их статусах. В веб-интерфейсе Kaspersky MLAD службы сгруппированы по их функциональным областям, и для каждой службы отображается следующая информация:

- **Имя** – имя службы.
- **Статус** – текущий статус службы. В Kaspersky MLAD предусмотрены следующие статусы служб:
  - **Обновление** – был инициализирован запуск, перезапуск или остановка службы с помощью одной из кнопок в столбце **Действия**.
  - **Запущена** – служба запущена.
  - **Запускается** – служба в процессе запуска.
  - **Ошибка при запуске** – возникла ошибка при запуске службы.
  - **Остановлена** – служба остановлена.
  - **Перезапускается** – служба в процессе перезапуска.
  - **Не инициализирована** – невозможно запустить службу из-за некорректного запуска Kaspersky MLAD.
- **Действия** – доступные действия (запустить, остановить, перезапустить).

Управление статусами служб из подраздела **Основные** недоступно в веб-интерфейсе Kaspersky MLAD.



Раздел **Службы**

Просмотр статусов служб

Вы можете просматривать статусы служб, чтобы убедиться, что службы успешно запущены или остановлены.

Просмотр статусов служб доступен системным администраторам и пользователям с правом **Просмотр статусов служб программы** из группы прав **Работа со службами программы**.

Kaspersky MLAD проверяет статусы служб каждые 30 секунд.

Чтобы просмотреть статусы служб,

в основном меню выберите раздел **Службы**.

Откроется раздел **Службы**, в котором отображается таблица, содержащая доступные службы, их статусы, а также кнопки для запуска, остановки и перезапуска служб.

Запуск, остановка и перезапуск служб

Kaspersky MLAD позволяет запускать, останавливать и перезапускать службы.

Запуск, остановка и перезапуск служб доступны системным администраторам и пользователям с правом **Управление статусами служб программы** из группы прав **Работа со службами программы**. Функциональность управления статусами служб из подраздела **Обработка данных** доступна после добавления лицензионного ключа.

Управление статусами служб из подраздела **Основные** недоступно в веб-интерфейсе Kaspersky MLAD.

В разделе **Службы** вы можете управлять статусами следующих служб:

- *Anomaly Detector*. Эту службу необходимо включить и настроить, если требуется анализировать данные телеметрии и выявлять аномалии в поведении объекта мониторинга.
- *Trainer*. Эту службу необходимо включить, если требуется обучить элементы ML-моделей на основе данных телеметрии.
- *Similar Anomaly*. Эту службу необходимо включить и настроить, если требуется группировать схожие инциденты.
- *Event Processor*. Эту службу необходимо включить и настроить, если требуется выявлять паттерны и аномальные последовательности событий.

- *Stream Processor*. Эту службу необходимо включить и настроить, если требуется приводить данные телеметрии к равноинтервальной временной сетке и регистрировать инциденты при обнаружении потери данных и поступлении данных слишком рано или поздно.

- *Data Source Manager*. Эту службу необходимо включить и настроить, если требуется получать данные телеметрии по протоколу OPC UA.

- *HTTP Connector*. Этот коннектор необходимо включить и настроить, если требуется получать данные телеметрии по протоколу HTTP или HTTPS.

- *AMQP Connector*. Этот коннектор необходимо включить и настроить, если требуется получать данные телеметрии и принимать сообщения о регистрации инцидентов по протоколу AMQP.

- *KICS Connector*. Этот коннектор необходимо включить и настроить, если требуется получать данные телеметрии от Kaspersky Industrial CyberSecurity for Networks.

- *MQTT Connector*. Этот коннектор необходимо включить и настроить, если требуется получать данные телеметрии и принимать сообщения о регистрации инцидентов по протоколу MQTT.

- *CEF Connector*. Этот коннектор необходимо включить и настроить, если требуется получать данные телеметрии и принимать сообщения о регистрации инцидентов по технологии CEF.

- *WebSocket Connector*. Этот коннектор необходимо включить и настроить, если требуется получать данные телеметрии и принимать сообщения о регистрации инцидентов по протоколу WebSocket.

- *Mail Notifier*. Эту службу необходимо включить и настроить, если требуется отправлять уведомления о зарегистрированных инцидентах по электронной почте.

- *Logger*. Эту службу необходимо включить, если требуется вести и хранить журналы работы Kaspersky MLAD. По умолчанию эта служба включена.

Чтобы запустить, остановить или перезапустить службу:

1. В основном меню выберите раздел **Службы**.

2. На открывшейся странице выберите один из следующих подразделов: **Обработка данных**, **Коннекторы** или **Другие**.

3. Для нужной службы выполните одно из следующих действий:

   - Если вы хотите запустить службу, нажмите на кнопку **Запустить**.

   - Если вы хотите остановить службу, нажмите на кнопку **Остановить**.

   - Если вы хотите перезапустить службу, нажмите на кнопку **Перезапустить**.

   Новый статус службы отобразится в столбце **Статус**.

Управление источниками данных

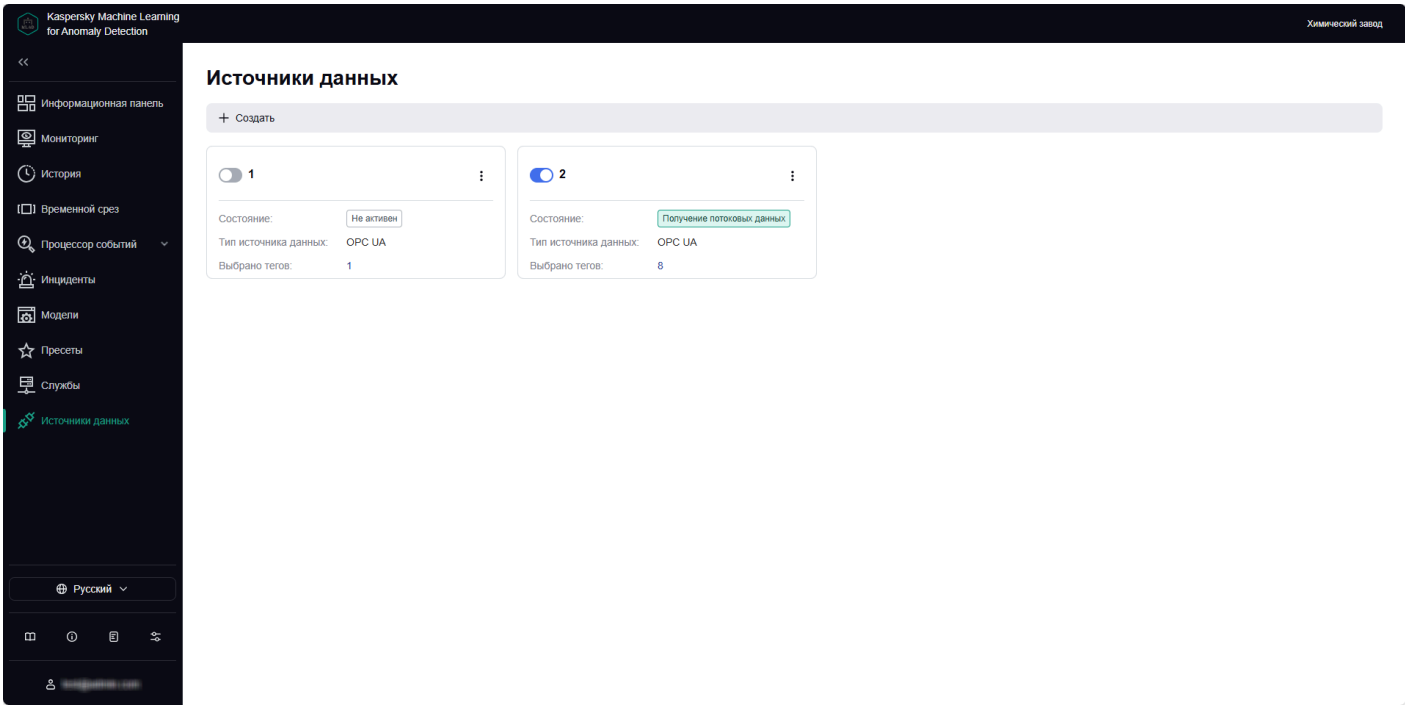
Данные телеметрии могут поступать в Kaspersky MLAD от нескольких источников одновременно. В разделе **Источники данных** вы можете настроить параметры подключения Kaspersky MLAD к разным источникам, а также управлять подключением к ним для получения потоковых данных телеметрии.

На данный момент Kaspersky MLAD поддерживает одновременное подключение к нескольким источникам данных по протоколу OPC UA.

Источники данных представлены в виде карточек. Для каждого источника данных отображается следующая краткая информация:

- Имя источника данных.
- **Состояние** – состояние соединения с источником данных. В Kaspersky MLAD предусмотрены следующие состояния:
  - **Не активен** – Kaspersky MLAD не подключен к источнику данных.
  - **Идет подключение** – устанавливается соединение с источником данных.
  - **Получение потоковых данных** – Kaspersky MLAD получает потоковые данные от источника.
  - **Идет отключение** – соединение с источником данных разрывается.
  - **Ошибка** – возникла ошибка соединения с источником данных.
- **Тип источника данных** – протокол, по которому данные поступают от источника данных.
- **Выбрано тегов** – количество тегов, по которым Kaspersky MLAD ожидает поступление данных от источника.

При необходимости вы можете изменить параметры источника данных или удалить их карточки из программы.



Раздел **Источники данных**

Создание карточки источника данных OPC UA

Kaspersky MLAD использует службу Data Source Manager для подключения к источнику, который передает данные по протоколу, описанному спецификацией OPC Unified Architecture (унифицированная архитектура OPC). Kaspersky MLAD поддерживает подключение к нескольким источникам данных OPC UA одновременно. Для этого необходимо добавить карточки источников данных OPC UA в программу и задать параметры загрузки данных телеметрии от этих источников.

В источнике данных OPC UA теги могут идентифицироваться именами, не совпадающими с именами тегов, добавленных в Kaspersky MLAD. Для сопоставления тегов источников данных с тегами, добавленными в программу, вы можете задать параметры преобразования имен тегов Kaspersky MLAD в идентификаторы тегов, поступающих от источника данных.

С помощью службы Data Source Manager вы можете получать потоковые данные. Потоковые данные начинают поступать в Kaspersky MLAD после подключения к источникам данных OPC UA.

Для получения данных от источников данных необходимо предварительно запустить службу Data Source Manager.
Управление источников данных доступно системным администраторам.

Чтобы создать карточку источника данных OPC UA:

1. Выберите раздел **Источники данных** и нажмите на кнопку **Создать**.

   Справа откроется панель **Создание источника данных**.

2. В открывшейся панели в поле **Имя** укажите имя источника данных.

3. Если требуется, в поле **Описание** укажите описание источника данных.

4. В раскрывающемся списке **Тип источника данных** выберите **OPC UA**.

5. В блоке параметров **Теги источника данных** выполните следующие действия:

   a. Нажмите на кнопку **Выбрать теги**.

      Справа отобразится панель **Выбор тегов для источника данных** с деревом активов.

   b. В дереве активов выберите теги, по которым необходимо получать телеметрию от источника данных.

      При необходимости для выбора тегов отфильтруйте теги, выбрав нужный пресет, или воспользуйтесь строкой поиска над деревом активов.

   c. Нажмите на кнопку **Сохранить**.

   В блоке параметров **Теги источника данных** отобразится информация о количестве выбранных тегов.

6. Для сопоставления имен тегов, добавленных в программу, с идентификаторами тегов, поступающих от источника данных, в блоке параметров **Преобразование имени тега** выполните следующие действия:

   a. В поле **Тип имени тега** выберите одно из следующих значений:

      - **Основное**, если требуется использовать имя тега, указанное в поле **Имя**, для его преобразования в идентификатор тега в источнике данных.

      - **Альтернативное**, если требуется использовать имя тега, указанное в поле **Альтернативное имя**, для его преобразования в идентификатор тега в источнике данных.

   b. В поле **Регулярное выражение для имени тега** укажите регулярное выражение, которое необходимо применить к имени тега, указанному в программе, для его преобразования в идентификатор тега в источнике данных.

      В регулярных выражениях используется формат, поддерживаемый на языке программирования Python. Подробнее о популярных специальных символах регулярных выражений см. в Приложении.

   c. В поле **Шаблон идентификатора тега** укажите шаблон, по которому необходимо сформировать идентификатор тега источника данных.

      В шаблоне используются подстановки типа `$n`, где `n` – неотрицательное целое число. При этом `$0` будет соответствовать части имени тега, отобранной всем регулярным выражением. Подстановки вида `$ <натуральное число>` будут соответствовать части имени тега, отобранными частями регулярного выражения, заключенными в круглые скобки в соответствии с заданным порядком. Например, `$2` будет соответствовать части имени тега, отобранными частью регулярного выражения, заключенного во вторую пару круглых скобок.

   d. В поле **Тип преобразования** выберите одно из следующих значений:

      - **Идентификатор узла данных (параметр NodeId)**, если в источнике данных тег доступен по параметру NodeID.

      - **Путь к тегу (параметр Path)**, если в источнике данных тег доступен по параметру Path.

7. Если требуется проверить преобразование имен тегов Kaspersky MLAD в идентификаторы тегов в источнике данных, в блоке параметров **Проверка преобразования** выполните следующие действия:

   a. В поле **Имя тега для проверки** введите имя любого тега.

   b. Нажмите на кнопку **Проверить**.

   В поле **Результат** отобразится результат преобразования имени тега в идентификатор тега источника данных в соответствии с параметрами преобразования, заданными в блоке параметров **Преобразование имени тега**.

8. При необходимости корректировки параметров повторите шаги 6 и 7.

9. В блоке **Параметры для подключения и загрузки данных** выполните следующие действия:

   a. В поле **Точка подключения** укажите адрес (URL) подключения.

      Например, `opc.tcp://10.0.0.0:8001/freeopcua/server/`.

   b. В поле **Время ожидания подключения к OPC UA-серверу (сек.)** укажите время в секундах, в течение которого служба Data Source Manager будет пытаться установить соединение с OPC UA-сервером.

   c. Если требуется, с помощью кнопки **Обзор** под параметром **Конфигурационный файл** добавьте файл, содержащий описание тегов источника данных.

      Конфигурационный файл в явном виде устанавливает соответствие имен отдельных тегов их идентификаторам в источнике данных. Конфигурационный файл используется, когда соответствие имени тега и его идентификатора в источнике данных нельзя задать с помощью общих параметров преобразования, описанных выше. Кроме того, в конфигурационном файле могут быть указаны индивидуальные параметры преобразования текстовых значений тега в числовые. Правила соответствия, описанные для тегов в конфигурационном файле, являются более приоритетными, чем правила, описанные для этих же тегов в карточке источника данных.

      Если требуется удалить конфигурационный файл, нажмите на кнопку . Если требуется сохранить загруженный конфигурационный файл на компьютере, нажмите на кнопку .

   d. С помощью переключателя **Масштабировать полученные значения тегов** включите или выключите конвертацию значений тегов с учетом параметров **Смещение** и **Множитель**, заданных при создании тега.

      По умолчанию конвертация полученных значений тегов выключена.

   e. В раскрывающемся списке **Политика безопасности соединения** выберите алгоритм шифрования сообщений.

      Для выбора доступны следующие варианты: **Выберите политику безопасности соединения**, **Basic256**, **Basic128Rsa15**, **Basic256Sha256**, **Aes128Sha256RsaOaep**.

   f. В раскрывающемся списке **Режим безопасности соединения** выберите одно из следующий значений:

      - Если требуется не подписывать и не шифровать сообщения, выберите **Выберите режим безопасности соединения**.
      - Если требуется подписывать сообщения, выберите **Подписывать сообщения**.
      - Если требуется подписывать и шифрования сообщения, выберите **Подписывать и шифровать сообщения**.

   g. Если OPC UA-сервер использует аутентификацию клиента, в полях **Имя пользователя для подключения к серверу** и **Пароль для подключения к серверу** укажите имя пользователя и пароль для подключения к OPC UA-серверу.

   h. Если требуется использовать защищенное соединение и на OPC UA-сервере включена аутентификация клиента, выполните следующие действия:

      a. Добавьте сертификат клиентского приложения с помощью кнопки **Обзор** под параметром **Сертификат клиента**.

      b. Добавьте закрытый ключ к сертификату клиентского приложения с помощью кнопки **Обзор** под параметром **Закрытый ключ клиента**.

      c. В поле **Пароль для закрытого ключа клиента** укажите пароль, который будет использован для снятия блокировки закрытого ключа.

Рекомендуется использовать сертификат с длиной ключа к сертификату 4 096 бит при использовании алгоритма RSA или 256 бит при использовании алгоритма ECDH.
Загрузка сертификата и ключа к сертификату возможна только в виде файла в формате DER или PEM.

Если требуется удалить файл сертификата или ключ к сертификату, нажмите на кнопку в соответствующем поле. Если требуется сохранить файл сертификата или ключ к сертификату на компьютере, нажмите на кнопку в соответствующем поле.

i. Если требуется использовать защищенное соединение и вы используете собственный удостоверяющий центр для выпуска сертификатов, добавьте корневой сертификат для проверки подписи сертификата OPC UA-сервера с помощью кнопки **Обзор** под параметром **Сертификат CA OPC UA-сервера**.

Если требуется удалить файл сертификата, нажмите на кнопку . Если требуется сохранить файл сертификата на компьютере, нажмите на кнопку .

10. Нажмите на кнопку **Сохранить**.

Для получения потоковых данных телеметрии от созданного источника данных необходимо к нему подключиться.

Копирование карточки источника данных

Управление источников данных доступно системным администраторам.

Вы можете создать карточку источника данных, скопировав ранее созданную карточку. При копировании будет создана карточка источника данных, параметры которого идентичны параметрам исходного источника в момент копирования.

По умолчанию источнику данных присваивается имя в формате `<имя исходного источника данных>_Cloned_<дата и время копирования карточки>`. Если требуется, вы можете изменить имя источника данных при копировании.

Чтобы скопировать карточку источника данных:

1. Выберите раздел **Источники данных**.

2. В правом верхнем углу карточки источника данных, параметры которого вы хотите скопировать, откройте вертикальное меню и выберите пункт **Копировать**.

   Справа отобразится панель **Копирование источника данных**.

3. При необходимости измените параметры источника данных. Описание параметров см. в инструкции по созданию карточки источника данных.

   Параметр **Тип источника данных** недоступен для изменения.

4. Нажмите на кнопку **Сохранить**.

Изменение параметров источника данных

Управление источников данных доступно системным администраторам.

Чтобы изменить параметры источника данных:

1. Выберите раздел **Источники данных**.
2. В правом верхнем углу карточки источника данных, параметры которого требуется изменить, откройте вертикальное меню ⋮ и выберите пункт **Изменить**.

   Справа отобразится панель **Изменение источника данных**.
3. Измените параметры источника данных. Описание параметров см. в инструкции по созданию карточки источника данных.
4. Нажмите на кнопку **Сохранить**.

Подключение к источнику данных и отключение от него

Управление источниками данных доступно системным администраторам.

Для получения данных телеметрии вы должны выполнить подключение к источнику данных. Если требуется прекратить поступление данных, вам нужно отключиться от источника данных.

Чтобы подключиться к источнику данных или отключиться от него:

1. Выберите раздел **Источники данных**.
2. В карточке нужного источника данных выполните одно из следующих действий:

   - Для подключения к источнику данных включите переключатель слева от названия источника.

     После подключения к источнику данных в Kaspersky MLAD начнут поступать потоковые данные телеметрии.
   - Для отключения от источника данных выключите переключатель слева от названия источника.

Удаление карточки источника данных

Управление источниками данных доступно системным администраторам.

При необходимости вы можете удалить карточку источника данных. Удаление карточки источника в программе не приводит к удалению данных, полученных от источника до его удаления, и не влияет на функционирование самого источника.

Чтобы удалить карточку источника данных:

1. Выберите раздел **Источники данных**.
2. В правом верхнем углу карточки источника данных, который требуется удалить, откройте вертикальное меню ⋮ и выберите пункт **Удалить**.
3. Подтвердите удаление.

Kaspersky MLAD позволяет временно выключить получение данных от источников вместо удаления их карточек. Вы можете снова подключиться к источнику данных в любое время.

Устранение неисправностей

Этот раздел содержит описание возможных неисправностей в работе Kaspersky MLAD и способов их устранения.

При подключении к Kaspersky MLAD браузер выводит предупреждение о сертификате

Проблема

При попытке подключения к Kaspersky MLAD браузер выводит предупреждение о том, что сертификат безопасности или устанавливаемое соединение не являются доверенными. Содержание предупреждения зависит от используемого браузера.

Решение

После установки Kaspersky MLAD для подключения к веб-интерфейсу по умолчанию используется самоподписанный сертификат. При использовании самоподписанного сертификата браузер отображает предупреждение о том, что сертификат безопасности или устанавливаемое соединение не являются доверенными. Для получения доверенного сертификата вам нужно обратиться в отдел информационной безопасности или отдел информационных технологий Заказчика. Обновите сертификаты для подключения к Kaspersky MLAD через веб-интерфейс.

Вы можете временно использовать самоподписанный сертификат для подключения к Kaspersky MLAD (например, при пробной эксплуатации). Для использования самоподписанного сертификата в окне предупреждения браузера выберите вариант, позволяющий продолжить подключение. После подключения к Kaspersky MLAD в окне браузера будет отображаться предупреждающее сообщение о сертификате. Текст сообщения зависит от используемого браузера.

Если браузер отображает предупреждение после установки доверенного сертификата, то могла произойти подмена сертификата злоумышленником. Требуется обратиться в Службу технической поддержки.

Заканчивается свободное пространство на жестком диске

Проблема

На жестком диске компьютера, на котором установлен Kaspersky MLAD, заканчивается свободное пространство.

Решение

Для работы программы компьютер должен удовлетворять аппаратным и программным требованиям.

Не допускайте полного израсходования свободного места на жестком диске. Периодически проверяйте наличие свободного места с помощью команды `df -h`.

Чтобы программа работала правильно,

освободите на жестком диске компьютера достаточный объем пространства, соответствующий минимальным требованиям к объему свободного пространства. Вы можете освободить место на жестком диске следующими способами:

- Перенесите резервные копии Kaspersky MLAD, дистрибутив Kaspersky MLAD и посторонние файлы на другой диск или сервер.
- Создайте образ диска, на котором установлен Kaspersky MLAD, замените жесткий диск на более емкий и разверните образ на новом диске.

Непредвиденная перезагрузка операционной системы

Проблема

Неожиданная перезагрузка компьютера с установленным Kaspersky MLAD.

Решение

Дождитесь окончания загрузки компьютера. Остановите работу Kaspersky MLAD (даже если программа не полностью восстановилась) и снова запустите ее вручную. Если после перезапуска работоспособность Kaspersky MLAD не восстановилась, обратитесь в Службу технической поддержки. Будьте готовы предоставить журналы работы процессов Kaspersky MLAD и другие данные по запросу специалистов Службы технической поддержки. Журналы работы процессов располагаются в директориях, перечисленных в статье Директории для хранения данных программы. Для доступа к журналам нужно иметь root-права в операционной системе.

Не удается подключиться к веб-интерфейсу Kaspersky MLAD

Проблема

При подключении к веб-интерфейсу Kaspersky MLAD после ввода правильного пароля отображается ошибка *Error! Invalid server error.*

Решение

Часто ошибка *Error! Invalid server error* возникает в случае, когда сервер Kaspersky MLAD не может обработать запрос, например, из-за того, что на жестком диске сервера, на котором установлена программа, закончилось свободное место.

Чтобы восстановить правильную работу программы,

освободите на жестком диске сервера достаточный объем пространства, соответствующий минимальным требованиям к объему свободного пространства. Вы можете освободить место на жестком диске следующими способами:

- Перенесите резервные копии Kaspersky MLAD, дистрибутив Kaspersky MLAD и посторонние файлы на другой диск или сервер.
- Если Kaspersky MLAD установлен на виртуальной машине, увеличьте объем виртуального жесткого диска виртуальной машины.
- Создайте образ диска, на котором установлен Kaspersky MLAD, замените жесткий диск на более емкий и разверните образ на новом диске.

Не отображаются графики данных или графические области в разделах История и Мониторинг

Проблема

В разделах **История** и **Мониторинг** не отображаются графики данных или графические области.

Возможны следующие причины:

- Пресеты не импортированы в Kaspersky MLAD.
- Выбранный пресет не содержит теги.
- В выбранном пресете не заданы графические области.
- В разделе **История** выбран интервал времени, для которого отсутствуют данные.
- Не выполнено подключение к источнику данных или не запущен коннектор, используемый для получения данных от объекта мониторинга.
- Объект мониторинга отключен.

Решение

Импортируйте или создайте пресеты, содержащие теги и графические области.

Для отображения данных в разделе **Мониторинг** убедитесь, объект мониторинга включен. Включите коннектор и/или подключитесь к источникам данных, используемым для получения данных от объекта мониторинга. Выберите интервал времени и пресет.

Для отображения данных в разделе **История** выберите пресет, дату и интервал времени, в котором присутствуют данные по тегам пресета.

Не отображается результат применения разметки

Проблема

В разделе **Модели** при просмотре графика разметок отсутствует окраска интервалов данных, которые должны быть отобраны разметкой.

Решение

На выбранном для отображения интервале времени разметка не отобрала ни одного интервала данных. Рассмотрите другой интервал времени, увеличьте рассматриваемый интервал времени для отображения данных на графике разметок в поле **Масштаб** или измените параметры разметки.

Отображается сообщение об остановленной службе Trainer

Проблема

При переходе на вкладку **Обучение** элемента ML-модели отображается сообщение **Служба Trainer остановлена**. При этом служба Trainer была запущена системным администратором или пользователем с правом **Управление статусами служб программы** из группы прав **Работа со службами программы**.

Решение

Подождите около двух секунд. Если служба Trainer запущена, сообщение автоматически исчезнет.

Обучение элемента ML-модели завершилось с ошибкой

Проблема

Обучение элемента ML-модели завершилось с ошибкой. Ошибка обучения может возникнуть как сразу после начала обучения, так и после выполнения некоторого числа эпох обучения.

Решение

Если обучение элемента ML-модели завершилось с ошибкой сразу после начала обучения с сообщением об отсутствии данных по одному или нескольким тегам, это означает, что по указанным тегам отсутствуют данные в рамках интервала обучения, заданного в параметре **Интервал отбора данных**, с учетом применения разметок (индикатора обучения). Нажмите на кнопку **На графике** и визуально проконтролируйте, на каких участках отсутствуют данные, с учетом примененного индикатора обучения. Измените параметры разметки индикатора обучения, исключите проблемные теги из элемента ML-модели или загрузите в программу недостающие данные.

Если обучение элемента ML-модели завершилось с ошибкой после того, как обучение продолжалось некоторое время, то выбранная архитектура элемента, параметры элемента или параметры обучения элемента не подходят для решения вашей задачи с учетом имеющихся данных, так как целевые метрики качества ML-модели не могут быть достигнуты. Попробуйте использовать элемент другого типа или архитектуры или измените параметры элемента или параметры его обучения.

Не приходят уведомления об инцидентах по электронной почте

Проблема

Не приходят уведомления об инцидентах по электронной почте.

Решение

Убедитесь, что выполнены следующие условия:

- Настроено взаимодействие Kaspersky MLAD с SMTP-сервером.
- Запущена служба Mail Notifier.
- Создана подписка на уведомления об инцидентах.
- Нужные адресаты выбраны в подписке. Если выбрана группа контактов, убедитесь, что нужный адресат входит в состав этой группы.
- Нужные типы инцидентов и соответствующие им источники инцидентов (ML-модели, активы и теги) выбраны в подписке.
- Переключатель **Отправлять уведомления только об учетных инцидентах** находится в нужном положении.
- Отправка уведомлений по подписке включена с помощью переключателя **Отправка уведомлений**.

Отсутствует артефакт элемента ML-модели по результатам инференса

Проблема

По результатам инференса ML-модели для ее элемента отсутствует артефакт на определенном интервале времени.

Решение

Проверьте наличие данных по всем тегам, выбранных в элементе ML-модели, на этом интервале времени.

Если используется индикатор инференса, убедитесь, что он отобрал этот интервал времени. Для этого нажмите на кнопку при **На графике** просмотре ML-модели.

Убедитесь, что в разметках индикатора инференса не используется оператор **Если далее**. При наличии этого оператора индикатор инференса всегда возвращает отрицательный результат, даже если на графике интервал данных отобран. Разметки с оператором **Если далее** могут быть использованы только для индикаторов обучения. При необходимости измените параметры разметок индикатора инференса и/или выберите другие разметки для индикатора инференса.

Если вы проводили исторический инференс, убедитесь, что интервал времени инференса включает интервал времени отсутствующего артефакта. При необходимости измените интервал времени инференса.

Не отображаются изменения параметров элемента на графике его артефакта

Проблема

После изменения порога и/или параметров регистрации инцидентов в параметрах элемента ML-модели, изменения не отобразились на графике артефакта в разделе **История**, а также не изменилось положение инцидентов.

Решение

Убедитесь, что после внесения изменений вы провели быстрый инференс на желаемом интервале времени. Если быстрый инференс не проводился, на вкладке **Инференс** нужной ML-модели в блоке параметров **Исторический инференс** укажите нужный интервал времени данных и нажмите на кнопку **Пересчитать инциденты**.

В разделе **История** нажмите на кнопку ⊙ слева от оси времени, и выберите нужную точку для обновления отображение графиков относительно нового центра графиков (вертикальной синей пунктирной линии).

Время точки-индикатора инцидента не совпадает с временем инцидента

Проблема

Время, отображаемое в подсказке при наведении курсора на точку-индикатор инцидента в разделах **История** и **Мониторинг**, не совпадают с временем инцидента в разделе **Инциденты**.

Решение

В зависимости от масштаба времени, выбранного для отображения графиков в разделах **История** и **Мониторинг**, одна точка-индикатор может соответствовать нескольким близко расположенным инцидентам, попадающих в некоторый интервал времени. В подсказке такой точки-индикатора отображается время начала и окончания этого интервала, а не время регистрации определенного инцидента. Инциденты, к которым относится эта точка-индикатор, находятся внутри указанного интервала.

При необходимости увеличьте масштаб отображения данных.

Не выполняется передача событий между Kaspersky MLAD и внешними системами

Проблема

События не поступают в Kaspersky MLAD и/или оповещения об активации мониторов не отправляются во внешние системы.

Решение

Чтобы восстановить обмен событиями с внешними системами:

1. Запустите службу Event Processor и коннектор CEF Connector.
2. При настройке службы Event Processor выполните следующие действия:
    a. В поле **Конфигурационный файл процессора событий** загрузите конфигурационный файл, описывающий параметры событий.
    b. В поле **Интервал получения событий эпизода (сек.)** укажите интервал времени в секундах, необходимый для формирования эпизода, учитывая скорость получения событий от объекта мониторинга.

3. Для получения событий в файле .env укажите IP-адрес и номер порта, по которым требуется осуществлять подключение к внешнему источнику событий.

4. Для отправки событий укажите IP-адрес и номер порта для подключения к внешней системе при настройке коннектора CEF Connector.

Невозможно загрузить данные для просмотра в разделе Процессор событий

Проблема

После перезапуска Kaspersky MLAD невозможно загрузить данные для просмотра истории событий и/или истории паттернов в разделе **Процессор событий** (недоступна кнопка **Выполнить запрос**). Такая же проблема наблюдается после изменения параметров службы Event Processor.

Решение

Подождите некоторое время. После перезапуска Kaspersky MLAD состояние службы Event Processor восстанавливается. Длительность процесса восстановления состояния при значительном объеме обработанных событий и зарегистрированных паттернов может занимать от нескольких минут до нескольких часов (зависит от объема данных).

До момента восстановления состояния службы Event Processor в разделе **Процессор событий** не выполняются запросы и не обновляются данные, а также в это время не обрабатываются данные, поступающие от коннектора CEF Connector. Эти данные временно сохраняются в очереди сообщений системы и обрабатываются после восстановления состояния службы Event Processor.

Также рекомендуется не включать коннектор CEF Connector до полного восстановления состояния службы Event Processor. Контролировать процесс восстановления службы Event Processor вы можете с помощью журналов контейнера службы.

Неправильно обрабатываются данные в разделе Процессор событий

Проблема

Создается большое количество коротких паттернов.

Решение

В параметрах службы Event Processor увеличьте длину эпизода для уменьшения количества регистрации коротких паттернов.

Проблема

Приходит большое количество оповещений об активации монитора.

Решение

Для уменьшения количества оповещений об активации монитора проверьте созданные ранее мониторы и удалите ненужные. Также рекомендуется уточнить параметры активации мониторов: **Скользящее окно** и **Порог**.

Не отображаются события в разделе Процессор событий

Проблема

При выполнении запроса для просмотра истории событий в разделе **Процессор событий** → **История событий** не отображаются события, которые отображались ранее.

Решение

Убедитесь, что Kaspersky MLAD сохраняет состояние службы Event Processor в таблицу базы данных.

Если состояние службы Event Processor сохраняется в файл в битовом формате, то Kaspersky MLAD сохраняет состояние службы с частотой, заданной в поле **Периодичность создания резервных копий компонента**. При перезапуске службы Event Processor результаты обработки потока событий, полученных процессором событий с момента последнего сохранения состояния службы, будут утеряны.

Списки активаций мониторов пустые или частично отсутствуют после перезапуска службы Event Processor

Проблема

После перезапуска или изменения параметров службы Event Processor в разделе **Процессор событий** → **Мониторинг** не отображаются ранее созданные мониторы и заданные параметры конфигурации внимания.

Решение

Процессор событий сохраняет созданные мониторы и заданные параметры конфигурации внимания после сохранения состояния службы Event Processor в таблицу базы данных (основной способ) или файл в битовом формате.

Состояние списков активаций мониторов синхронизируется с таблицей базы данных с определенной частотой (по умолчанию каждые пять минут). При перезапуске службы Event Processor информация об активациях монитора за интервал времени, меньший чем частота синхронизации, может быть утеряна. При этом история событий и паттернов, на которых оповещения о таких активациях могли быть сгенерированы, синхронизируются в базу данных полностью.

Если требуется, вы можете увеличить частоту синхронизации информации об активациях монитора с помощью параметра `monitors_stacks_persistence_interval_minutes` в конфигурационном файле для службы Event Processor и повторно загрузить конфигурационный файл при настройке параметров службы Event Processor.

Требуется изменить язык локализации Справки

Проблема

Требуется изменить язык локализации Справки в веб-интерфейсе Kaspersky MLAD.

Для изменения языка локализации Справки на веб-сайте Службы технической поддержки по адресу https://support.kaspersky.ru/ выберите нужный язык локализации в правом верхнем углу страницы.

Решение

Чтобы изменить язык локализации Справки в веб-интерфейсе программы:

1. Откройте браузер, установленный на вашем компьютере.
2. В адресной строке браузера введите веб-адрес Kaspersky MLAD, полученный от квалифицированного технического специалиста Заказчика, специалиста "Лаборатории Касперского" или сертифицированного интегратора.
3. Для открытия Справки выполните одно из следующих действий:
   - В правом нижнем углу страницы ввода учетных данных нажмите на ссылку **Справка**.
   - На странице ввода учетных данных введите адрес электронной почты пользователя и пароль и в нижнем левом углу открывшейся страницы нажмите на кнопку 🕮.

   Откроется новая вкладка браузера со Справкой программы.
4. В веб-адресе укажите необходимый язык локализации:
   - ru – если вы хотите открыть Справку на русском языке (например, https://<веб-адрес Kaspersky MLAD>/help/**ru**/247959.htm);
   - en – если вы хотите открыть Справку на английском языке (например, https://<веб-адрес Kaspersky MLAD>/help/**en**/247959.htm).

После подключения к программе вы можете изменить язык интерфейса и Справки в меню пользователя.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

Услуги технической поддержки предоставляются при наличии действующего *Договора об оказании технической поддержки*. Объем предоставляемых услуг технической поддержки определяется действующим *Договором об оказании технической поддержки*.

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки, написав сотрудникам Службы технической поддержки по электронной почте mlad-support@kaspersky.com.

Специалисты Службы технической поддержки могут запросить у вас сведения из системы ведения журналов Kaspersky MLAD.

Список ограничений

Kaspersky MLAD имеет ряд ограничений, не критичных для работы программы:

- Оповещения об активации мониторов службы Event Processor отправляются во внешние системы только через коннектор CEF Connector. Отправка оповещений по электронной почте не предусмотрена.
- Служба Event Processor обрабатывает только категориальные данные. Все значения параметров событий представляются или преобразуются в тип данных – строка. Разнообразие значений строк для каждого параметра события может быть большим (до десятков тысяч значений), но конечным.
- Производительность обработки данных для текущей версии процессора событий составляет около пяти тысяч событий в секунду и может уменьшаться при большом количестве голов внимания и мониторов. Для работы с большим потоком событий требуется значительный объем оперативной памяти. Оценка необходимого объема зависит от потока событий, разнообразия событий в потоке и параметров конфигурации внимания и мониторов.
- Режим сохранения состояния службы Event Processor в файл в битовом формате предназначен только для работы в отладочном режиме и не должен использоваться при нормальной эксплуатации программы.
- Kaspersky MLAD совместим с Kaspersky Industrial CyberSecurity for Networks версии 4.0 и выше.
- Kaspersky MLAD рассчитан на работу с потоком тегов, скорость которого не превышает 10 000 тегов в секунду (допустимы кратковременные всплески не более 20%). При скорости потока тегов, превышающей указанное значение, возможна задержка обработки тегов, формирования прогнозов и выявления аномалий.
- Компьютеры, на которых установлены Kaspersky MLAD и Kaspersky Industrial CyberSecurity for Networks, должны находиться в одной сети.
- Обновление программы с сохранением данных поддерживается только для версии Kaspersky MLAD 5.0.0-001 или выше. Для перехода от Kaspersky MLAD 4.0.0 к версии Kaspersky MLAD 6.0.0 и выше необходимо произвести новую установку Kaspersky MLAD и вручную импортировать данные из ранее установленной версии Kaspersky MLAD 4.0.0. Для получения подробной информации о переходе от Kaspersky MLAD 4.0.0 к Kaspersky MLAD версии 6.0.0 или выше рекомендуется обратиться в Службу технической поддержки.
- Откат программы к предыдущей установленной версии поддерживается только для версии Kaspersky MLAD 5.0.0-001 или выше.
- В разделе **Инциденты** в окне выбора периода при перемещении вправо по оси времени в блоках для выбора начала и окончания периода отображается год начала заданного периода.
- После загрузки конфигурации активов и тегов в разделе **Модели** не отображаются разметки, созданные ранее для загруженных активов.
- В разделах **Мониторинг** и **История** вертикальная ось, отображающая при наведении курсора мыши на график артефакта элемента ML-модели в нижней части страницы, не совпадает с вертикальной осью, отображающейся в графических областях в верхней части страницы.
- В разделе **Пресеты** для тега, входящего в состав пресета, отображается снятый флажок при поиске по имени этого тега в дереве активов. Если установить флажок для этого тега, становится доступной кнопка **Сохранить выбор** при фактическом отсутствии изменений в составе тегов пресета. Список тегов, отображающийся в дереве активов в соответствии с поисковым запросом, прокручивается при выборе тега в составе актива с большим количеством тегов.

- В разделе **Модели** в некоторых случаях не нажимается кнопка **Импортировать модель** в вертикальном меню выбранного актива. Для корректной работы необходимо навести курсор мыши на правую часть кнопки и нажать ее.

- В разделе **Модели** невозможен предварительный просмотр разметки, для которой выбран хотя бы один тег, по которым в Kaspersky MLAD не поступали наблюдения.

- В разделе **Активы** после удаления головного элемента иерархической структуры (*Root*) невозможно создать новые активы и/или теги.

- В разделе **История** в раскрывающемся списке для выбора элементов ML-моделей отображаются удаленные элементы ML-моделей.

- Служба Similar Anomaly перестает работать при повторном запуске исторического инференса. При повторном запуске исторического инференса рекомендуется выключить службу Similar Anomaly.

- В разделе **Модели** при увеличении масштаба отображения разметки во время ее просмотра не отображается горизонтальная полоса прокрутки. Часть элементов управления просмотром разметки становится недоступна.

- Kaspersky MLAD хранит всю историю полученных значений тегов, а также прогнозируемых значений тегов. Поэтому требуется предварительно рассчитать размер хранилища, исходя из показателей скорости обновления данных (тегов в секунду) и временного интервала хранения истории мониторинга данных телеметрии.

- В разделе **Модели** не всегда отображаются результаты обучения предиктивного элемента после его успешного обучения. Для отображения результатов необходимо обновить страницу.

- Значение параметра **Часовой пояс объекта мониторинга**, заданного системным администратором в основных параметрах Kaspersky MLAD, применяется только к датам и времени при выборе интервалов времени разметок. В остальных разделах веб-интерфейса, в которых для отображения данных можно выбрать дату и время, этот параметр не применяется.

- В разделе **Временной срез** возникает ошибка при выборе пресета, значения тегов которого рассчитываются по выражению, если в этом выражении используются недопустимые переменные.

- В разделе **Временной срез** возникает ошибка при выборе пресета, если для этого пресета настроено отображение в разделе **Временной срез**, но для тегов пресета не заданы координаты расположения датчика объекта мониторинга в пространстве.

- Не выполняется поиск по омоглифам латинских букв для пресетов и элементов ML-моделей в разделе **История** и для пресетов и разметок при просмотре графика разметки.

- Если в качестве начала интервала времени для исторического инференса выбран 1970 год, то после нажатия на кнопку **Пересчитать инциденты** изменяется дата начала или конца выбранного интервала.

- В системе ведения журналов Grafana не выполняется фильтрация по времени при просмотре журналов событий информационной безопасности.

- Происходит разделение актива после импорта файла конфигурации активов и тегов, в котором для загружаемого актива не указаны идентификатор и родительский актив. Если импорт выполнялся в раздел дерева, в котором уже есть актив с таким же именем как и у загружаемого актива, в режиме **Добавить и обновить** с выключенным переключателем **Рассматривать все элементы как новые**, то после импорта в разделе дерева активов будут отображаться два актива с одинаковым именем, при этом в одном активе будут отображаться все теги, а в другом – ML-модели и разметки, созданные ранее в этом активе.

- В карточке источника данных отображается только информация о количестве тегов, выбранных при создании карточки, не отображается информация о количестве тегов, описанных в конфигурационном файле.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

Параметры конфигурационного файла .env

Изменение параметров конфигурационного файла выполняет только квалифицированный технический специалист Заказчика, сотрудник "Лаборатории Касперского" или сертифицированный интегратор.

Конфигурационный файл .env заполняется для настройки коннектора CEF Connector, а также учетных данных пользователя службы Database и первого пользователя программы. Конфигурационный файл хранится в корневой директории программы.

Конфигурационный файл доступен только пользователям с root-правами.

Конфигурационный файл содержит параметры, приведенные в таблице ниже.

Параметры конфигурационного файла .env

Параметр	Описание
CEF_CONNECTOR_INCOMING_IP	IP-адрес, по которому будет осуществляться подключение внешнего источника событий к коннектору CEF Connector.
CEF_INCOMING_PORT	Номер порта, по которому будет осуществляться подключение внешнего источника событий к коннектору CEF Connector.
AUDIT_LOGGER_LOGIN	Имя пользователя службы Database.
AUDIT_LOGGER_PASSWORD	Пароль пользователя службы Database.
DEFAULT_ADMINISTRATOR_USER	Адрес электронной почты первого пользователя программы с ролью системного администратора.
DEFAULT_ADMINISTRATOR_PASSWORD	Пароль первого пользователя программы с ролью системного администратора.

Для применения изменений, внесенных в конфигурационный файл, требуется перезапустить Kaspersky MLAD.

Параметры конфигурационного файла config.env

Изменение параметров конфигурационного файла выполняет только квалифицированный технический специалист Заказчика, сотрудник "Лаборатории Касперского" или сертифицированный интегратор.

Конфигурационный файл config.env заполняется для настройки параметров хранения данных телеметрии, прокси-сервера и ведения журналов библиотеки TensorFlow. Конфигурационный файл хранится в директории configs/environment.

Конфигурационный файл доступен только пользователям с root-правами.

Конфигурационный файл содержит параметры, приведенные в таблице ниже.

Параметры конфигурационного файла config.env

Параметр	Описание
`KAFKA_TAGS_TOPIC`	Имя топика, в который коннекторы и/или источники данных передают данные телеметрии. Предусмотрены следующие значения: • `tags` – для передачи данных телеметрии в службу Message Broker без их обработки службой Stream Processor; • `sp_tags` – для передачи данных телеметрии в службу Message Broker после их обработки службой Stream Processor.
`EE_SCALE_MULTIPLIER`	Коэффициент корреляции, который линейно изменяет расстояние между точками внутри эллипса относительно его центра. Чем выше множитель, тем выше значение ошибки прогноза.
`EE_SCALE_POWER`	Степенной показатель отклонения, который нелинейно изменяет расстояние между точками внутри эллипса. Чем точки дальше от центра, тем сильнее они стягиваются внутрь эллиптической области, не изменения при этом ее границы. Это позволяет сохранить чувствительность ошибки прогноза при его малых значениях, при этом избежать лишних ложных срабатываний.
`https_proxy` и `HTTPS_PROXY`	Адрес прокси-сервера для работы контейнеров Kaspersky MLAD с использованием защищенного соединения. Для правильной работы программы рекомендуется оставить параметры пустыми.
`http_proxy` и `HTTP_PROXY`	Адрес прокси-сервера для работы контейнеров Kaspersky MLAD без защищенного соединения. Для правильной работы программы рекомендуется оставить параметры пустыми.
`TF_CPP_MIN_LOG_LEVEL`	Уровень ведения журналов для библиотеки TensorFlow. Предусмотрены следующие значения: • `0` – ведение журналов всей информации библиотеки; • `1` – ведение журналов без общей информации о работе библиотеки; • `2` – ведение журналов без общей информации о работе библиотеки и событий, которые могут привести к ошибкам в работе библиотеки; • `3` – ведение журналов без общей информации о работе библиотеки, событий, которые могут привести к ошибкам в работе библиотеки, и ошибок. возникших в работе библиотеки.

Для применения изменений, внесенных в конфигурационный файл, требуется перезапустить Kaspersky MLAD.

Параметры и пример Excel-файла, содержащего конфигурацию активов и тегов

Конфигурационный файл создается квалифицированным техническим специалистом Заказчика, сотрудником "Лаборатории Касперского" или сертифицированным интегратором. Системный администратор загружает конфигурацию активов и тегов иерархической структуры в разделе **Активы** в меню администратора.

Порядок параметров на вкладках конфигурационного файла не важен.

Конфигурационный файл содержит следующие вкладки:

- **readme** – вкладка, содержащая общую информацию о конфигурационном файле.
- **directory_types** – вкладка, описывающая типы активов иерархической структуры с помощью следующих параметров:
  - **directory_type_id** – идентификатор типа актива. Идентификатор присваивается автоматически при экспорте дерева активов.
  - **directory_type** – уникальное имя типа актива.
  - **parameter<номер параметра>_label** – имена специальных параметров, где <номер параметра> соответствует значению из диапазона от 1 до 5. Если у актива заданного типа отсутствует какой-либо специальный параметр, оставьте соответствующее поле в конфигурационном файле пустым.
  - **description** – описание типа актива. Поле не обязательно для заполнения.

- **directories** – вкладка, описывающая активы иерархической структуры с помощью следующих параметров:
  - **directory_id** – идентификатор актива. Идентификатор присваивается автоматически при экспорте дерева активов.
  - **directory_type** – тип актива. Тип выбирается из типов активов, заданных на вкладке **directory_types**.
  - **directory_type row** – номер строки на вкладке **directory_types**, на которой описан выбранный тип актива. Поле заполняется автоматически.
  - **directory_name** – уникальное имя актива в рамках его родительского актива.

    При вводе имени актива не допускается перенос части имени на новую строку и использование обратной косой черты (\).
  - **directory_info** – описание актива. Поле не обязательно для заполнения.
  - **parent** – родительский актив. Если импортируемый актив находится на верхнем уровне иерархии активов, оставьте поле **parent** пустым.

    При вводе имени актива не допускается перенос части имени на новую строку и использование обратной косой черты (\).
  - **parent row** – номер строки, на которой описан выбранный родительский актив. Поле заполняется автоматически.
  - **parent_id** – идентификатор родительского актива. Идентификатор присваивается автоматически при экспорте дерева активов.
  - **parameter<номер параметра>** – имена специальных параметров, где <номер параметра> соответствует значению из диапазона от 1 до 5. Имена специальных параметров заполняются автоматически, если для выбранного типа актива определены специальные параметры.
  - **value<номер параметра>** – значения специальных параметров, где <номер параметра> соответствует значению из диапазона от 1 до 5. Если у актива отсутствует специальный параметр, оставьте поле для ввода соответствующего значения пустым.
  - **criticality** – уровень критичности актива. Поле не обязательно для заполнения. Вы можете указать следующие значения:
    - **very_high** – соответствует значению по умолчанию **Очень высокий**.
    - **high** – соответствует значению по умолчанию **Высокий**.
    - **medium** – соответствует значению по умолчанию **Средний**.
    - **low** – соответствует значению по умолчанию **Низкий**.
    - **very_low** – соответствует значению по умолчанию **Очень низкий**.

    При необходимости вы можете изменить значения уровней критичности.
- **tags** – вкладка, описывающая теги иерархической структуры с помощью следующих параметров:

- **tag_id** – идентификатор тега. Значение идентификатора присваивается автоматически в диапазоне от 1 до 1 000 000 при экспорте первичных элементов иерархической структуры.
- **tag_name** – уникальное имя тега.

  При вводе имени тега не допускается перенос части имени на новую строку и использование обратной косой черты (\).

- **alternate_name** – уникальное альтернативное имя тега. Поле не обязательно для заполнения.

  При вводе альтернативного имени тега не допускается перенос части имени на новую строку и использование обратной косой черты (\).

- **tag_description** – описание тега.
- **parent** – родительский актив, к которому относится тег. Если для импортируемого тега родительским элементом является головной элемент иерархической структуры, оставьте поле **parent** пустым.
- **parent_row** – номер строки на вкладке **directories**, на которой описан выбранный родительский актив. Поле заполняется автоматически.
- **parent_id** – идентификатор родительского актива. Идентификатор присваивается автоматически при экспорте дерева активов.
- **tag_type** – **тип тега**. Поле не обязательно для заполнения.

  - **PV** – для обозначения измерений или наблюдаемых значений физических параметров.
  - **CV** – для обозначения вычисляемых значений физических параметров.
  - **IV** – для обозначения тегов, не зависящих от других тегов.
  - **SV** – для обозначения уставки.
  - **MV** – для обозначения регулируемых значений физических параметров.
  - **B** – для обозначения тегов в битовом формате.
  - **X** – для обозначения наблюдений, не являющимися тегами.

  Если вы затрудняетесь определить тип тега, вы можете использовать вопросительный знак (?) в качестве типа тега.

- **tag_units** – единица измерения тега.
- **red_min** – нижний порог предельно допустимого значения тега. Поле не обязательно для заполнения.
- **red_max** – верхний порог предельно допустимого значения тега. Поле не обязательно для заполнения.

- **yellow_min** – нижний порог сигнализации, при достижении которого оператору следует обратить внимание на поведение тега. Поле не обязательно для заполнения.

- **yellow_max** – верхний порог сигнализации, при достижении которого оператору следует обратить внимание на поведение тега. Поле не обязательно для заполнения.

- **validity_min** – нижний порог физически возможных значений тега. Поле не обязательно для заполнения.

- **validity_max** – верхний порог физически возможных значений тега. Поле не обязательно для заполнения.

- **comment** – комментарий к тегу. Поле не обязательно для заполнения.

- **x** – координата расположения датчика объекта мониторинга по оси абсцисс. Поле не обязательно для заполнения.

- **y** – координата расположения датчика объекта мониторинга по оси ординат. Поле не обязательно для заполнения.

- **z** – координата расположения датчика объекта мониторинга по оси аппликат. Поле не обязательно для заполнения.

- **bias** – значение, которое необходимо добавить к значению тега, переданному в Kaspersky MLAD. Укажите `0`, если конвертация значения не требуется.

  Конвертация значений, поступающих в Kaspersky MLAD выполняется при включенном переключателе **Масштабировать полученные значения тегов** в параметрах используемого коннектора и/или источника данных. Значение **bias** добавляется к результату умножения полученного значения тега на значение **multiplier**.

- **multiplier** – значение, на которое необходимо умножить значение тега, переданное в Kaspersky MLAD. Укажите `1`, если конвертация значения не требуется.

  Конвертация значений, поступающих в Kaspersky MLAD выполняется при включенном переключателе **Масштабировать полученные значения тегов** в параметрах используемого коннектора и/или источника данных. Умножение полученного значения тега на значение **multiplier** выполняется перед добавлением значения **bias**.

На рисунках ниже приведен пример файла в формате XLSX, который содержит описания активов и тегов и их конфигурацию.

	A	B	C	D	E	F	G	H
1	directory_type_id	directory_type	parameter1_label	parameter2_label	parameter3_label	parameter4_label	parameter5_label	description
2		Завод	Процесс	Регион				Отдельная производственная единица
3		Агрегат	Производитель	Модель	Год изготовления	Ответственный		Промышленная установка
4		Уставки						Набор уставок

Вкладка **directory_types**

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	directory_	directory_type	directory_type n	directory_name	directory_info	parent	parent ro	parent_i	parameter	value1	parameter	value2	parameter	value3	parameter	value4	parameter	value5	critica	
2		Завод	2	Химический завод	Tennessee Eastman Process				Процесс=	TEP	Регион=	США								
3		Агрегат	3	Реактор	Химический реактор	2			Производитель=	Chemical Mac	Модель=	R1/12-13	Год изготовления=	2001	Ответственный=	Иванов Иван Иванович				
4		Уставки	4	Уставки	Уставки реактора	3														

Вкладка **directories**

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1	tag_id	tag_name	alternate_name	tag_description	parent	parent_row	parent_id	tag_type	tag_units	red_min	red_max	yellow_min	yellow_max	validity_min	validity_max	commen	t	x	y	z	bias	multiplie
2		Reactor_pressure_setpoint		Уставка давления реактора	Химический завод; Реактор; Уставки	4		SV	кПа												0	6,89476
3		A_feed_stream1		Расход реагента А	Химический завод; Реактор	3		PV	тыс. н.куб.м/ч		0,6										0	1
4		Нет отклика температуры реактора		Правило	Химический завод	2		PV													0	1

Вкладка **tags**

Параметры и пример JSON-файла, описывающего пресеты

Файл формата JSON с описанием пресетов создается квалифицированным техническим специалистом Заказчика, сотрудником "Лаборатории Касперского" или сертифицированным интегратором. Файл с описанием пресетов загружается пользователем в разделе **Пресеты**.

В JSON-файле задается информация о пресетах в параметре `presets`, который в свою очередь содержит следующие параметры:

- `name` – имя пресета.
- `code` – идентификатор пресета в базе данных Kaspersky MLAD. Идентификатор присваивается автоматически при загрузке файла.
- `sort` – порядковый номер отображения пресета в разделе **Пресеты**.
- `tags` – список идентификаторов тегов, входящих в состав пресета.
- `parent_category_id` – идентификатор актива, к которому относится пресет. Идентификатор должен соответствовать значению параметра `directory_id`, указанному в Excel-файле, содержащем конфигурацию активов и тегов. Параметр имеет значение `root`, если пресет относится к головному элементу иерархической структуры.
- `is_display_on_time_slice` – параметр, определяющий, требуется ли отображать пресет в разделе **Временной срез**. Если параметр имеет значение `true`, пресет отображается в разделе **Временной срез**.

- `evaluations` – параметр, описывающий график в разделе **Временной срез**, с помощью следующих параметров:
  - `axis_x_name` – подпись для оси абсцисс на графике.
  - `evaluations` – параметр, описывающий выражение, по которому рассчитываются значения тегов для их отображения на графике, с помощью следующих параметров:
    - `name` – название выражения, по которому рассчитывается значение тегов для их отображения на графике.
    - `yAxis` – подпись для оси ординат на графике.
    - `expression` – выражение, по которому рассчитываются значения тегов.
    - `expression_color` – цвет графика, который будет отображаться для пресета. Цвет графика задается в соответствии с кодированием цвета в аддитивной цветовой модели RGB с альфа-каналом с помощью следующих параметров:
      - `a` – альфа-параметр, определяющий непрозрачность цвета. Вы можете указать значение в диапазоне от `0` до `1`.
      - `b` – координата синего канала модели RGB. Вы можете указать значение в диапазоне от `0` до `255`.
      - `g` – координата зеленого канала модели RGB. Вы можете указать значение в диапазоне от `0` до `255`.
      - `r` – координата красного канала модели RGB. Вы можете указать значение в диапазоне от `0` до `255`.
- `graphic_areas` – группа параметров, описывающих графические области в составе пресета.
  - `name` – название графической области.
  - `description` – описание графической области.
  - `sort` – порядковый номер отображения графической области в пресете в разделах **Пресеты**, **История** и **Мониторинг**.
  - `display_max` – верхняя граница отображения тегов графической области. Если параметр `is_scale_mode_auto` имеет значение `true`, укажите `null` в качестве значение параметра `display_max`.
  - `display_min` – нижняя граница отображения тегов графической области. Если параметр `is_scale_mode_auto` имеет значение `true`, укажите `null` в качестве значение параметра `display_min`.
  - `additional_thresholds` – группа параметров, описывающих контрольные линии.
    - `id` – идентификатор контрольной линии. Идентификатор присваивается автоматически при загрузке файла.
    - `value` – контрольное значение.

- `color` – цвет графика, который будет отображаться для контрольной линии. Цвет графика задается в соответствии с кодированием цвета в аддитивной цветовой модели RGB с альфа-каналом с помощью следующих параметров:
  - `a` – альфа-параметр, определяющий непрозрачность цвета. Вы можете указать значение в диапазоне от `0` до `1`.
  - `r` – координата красного канала модели RGB. Вы можете указать значение в диапазоне от `0` до `255`.
  - `g` – координата зеленого канала модели RGB. Вы можете указать значение в диапазоне от `0` до `255`.
  - `b` – координата синего канала модели RGB. Вы можете указать значение в диапазоне от `0` до `255`.

- `scale_mode` – режим масштабирования оси. Для параметра `scale_mode` вы можете указать одно из следующих значений:
  - `single_axis` – для отображения данных на графике используется общая ось ординат.
  - `cast` – для каждого тега данные масштабируются по оси ординат индивидуально, независимо от данных других тегов в составе графической области.
- `is_scale_mode_auto` – параметр, определяющий способ масштабирования графика в режиме единой оси. Если параметр имеет значение `true`, график тегов масштабируется автоматически с учетом минимального и максимального значений данных среди всех тегов графической области.
- `tag_id_list` – список идентификаторов тегов, входящих в состав графической области.
- `graphic_area_id` – идентификатор графической области. Идентификатор присваивается автоматически при загрузке файла.
- `preset_id` – идентификатор пресета, к которому относится графическая область. Идентификатор присваивается автоматически при загрузке файла.

Ниже приведен пример файла в формате JSON, который содержит описания пресетов.

```
{
    "presets": [
        {
            "name": "Продукт",
            "code": null,
            "sort": 0,
            "tags": [
                51,
                52,
                53,
                49,
                50
            ],
            "is_display_on_time_slice": false,
            "evaluations": {
                "axis_x_name": "",
                "evaluations": []
            },
            "graphic_areas": [
                {
                    "name": "F_product",
                    "description": "Доля pear. F в конечном продукте",
                    "sort": 0,
                    "display_max": null,
                    "display_min": null,
                    "additional_thresholds": [],
                    "scale_mode": "single_axis",
                    "is_scale_mode_auto": true,
                    "tag_id_list": [
                        51
                    ],
                    "graphic_area_id": null,
                    "preset_id": null
                },
                  ...
            ],
        },
        ...
        {
            "name": "Охладитель",
            "code": null,
            "sort": 0,
            "tags": [
                64
            ],
            "is_display_on_time_slice": false,
            "evaluations": {
                "axis_x_name": "",
                "evaluations": []
            },
            "graphic_areas": [
                {
                    "name": "Condenser_cool_water_flow",
                    "description": "Упр. расходом охл. воды конденсатора",
                    "sort": 0,
                    "display_max": null,
                    "display_min": null,
                    "additional_thresholds": [],
                    "scale_mode": "single_axis",
                    "is_scale_mode_auto": true,
                    "tag_id_list": [
                        64
                     ],
                    "graphic_area_id": null,
                    "preset_id": null
                }
            ]
        }
    ]
}
```


Параметры и пример JSON-файла, содержащего конфигурацию параметров для службы Event Processor

Конфигурационный файл создается техническим специалистом Заказчика, сотрудником "Лаборатории Касперского" или сертифицированным интегратором. Системный администратор загружает конфигурационный файл процессора событий при настройке параметров службы Event Processor.

При повторной загрузке конфигурационного файла, в котором определены другие параметры событий, параметры событий, определенные в предыдущем конфигурационном файле, станут недоступны для настройки в веб-интерфейсе программы.

Коннектор CEF Connector получает информацию о каждом обнаруженном событии от внешних систем в CEF-формате:

```
CEF:<версия формата CEF>|<имя поставщика внешней системы>|<название программы внешней системы>|<версия программы внешней системы>|<уникальный идентификатор типа события>|<описание события>|<уровень важности события>|<параметр 1>=<значение параметра 1> ... <параметр N>=<значение параметра N>
```

где:

- `CEF:<версия формата CEF>|<имя поставщика внешней системы>|<название программы внешней системы>|<версия программы внешней системы>|<уникальный идентификатор типа события>|<описание события>|<уровень важности события>|` – заголовок события.
- `<параметр 1>=<значение параметра 1> ... <параметр N>=<значение параметра N>` – тело события, содержащее последовательность пар `<параметр события>=<значение параметра события>`.

Конфигурационный файл описывает параметры в событиях, полученных коннектором CEF Connector. Имена параметров событий в Kaspersky MLAD могут совпадать с именами параметров, полученных в CEF-формате коннектором CEF Connector. При необходимости вы можете указать другие имена параметров, которые необходимо обрабатывать в Kaspersky MLAD, по определенным правилам. Правила соответствия параметров событий задаются в параметре `mapping_fields` конфигурационного файла.

Параметры `nodes` и `links` конфигурационного файла предназначены для описания способа построения графа результатов поиска событий. Граф представляет собой отображение отношений параметров событий, вершины которого задаются в параметре `nodes`, а дуги задаются в параметре `links`.

Конфигурационный файл содержит следующие параметры:

- `timestamp_field` – имя параметра для обозначения даты и времени в событиях, полученных коннектором CEF Connector от внешней системы.
- `timestamp_scale` – единица измерения времени событий.
- `global_episodes_history_interval` – интервал времени, за который Kaspersky MLAD восстанавливает эпизоды после перезапуска службы Event Processor. Интервал времени указывается в виде числа и единицы времени на английском языке (в формате типа данных INTERVAL языка программирования SQL). Например, значение `3 months` соответствует интервалу времени, равному трем месяцам.
- `monitors_stacks_persistence_interval_minutes` – частота (в минутах) синхронизации информации об активациях мониторов в таблицу базы данных службы Event Processor.
- `sep` – разделитель между параметрами значений в событиях, полученных коннектором CEF Connector.
- `sep_kv` – разделитель ключа и значения в событиях, полученных коннектором CEF Connector.
- `sep_cef_caption` – разделитель в заголовке событий, полученных коннектором CEF Connector.
- `mapping_fields` – правила соответствия параметров событий, полученных коннектором CEF Connector, с именами параметров событий для обработки в Kaspersky MLAD. При необходимости вы можете задать условия записи параметров событий в Kaspersky MLAD в зависимости от значений других параметров, полученных коннектором CEF Connector. Этот параметр не является обязательным для заполнения.
- `fields` – список параметров событий, обрабатываемых службой Event Processor. Имена этих параметров могут соответствовать именам параметров, полученных в CEF-формате, так и именам параметров, заданных в правилах с помощью параметра `mapping_fields`.

- `nodes` – группа параметров, описывающих вершины графа отношений параметров событий с помощью следующих параметров:
  - `name` – имя параметра события, соответствующего вершине графа.
  - `depth` – порядковый номер отображения вершины графа слева направо при просмотре истории событий.
  - `tooltip` – параметр, включающий параметр `templates`. В параметре `templates` задается надпись, которая будет отображаться при наведении курсора мыши на вершину графа.
  - `fieldShortCut` – параметр, определяющий альтернативное имя параметра события. На графе отношений параметров событий альтернативное имя отображается в квадратных скобках рядом со значением параметра, соответствующего вершине графа. Этот параметр не является обязательным для заполнения.
- `links` – группа параметров, описывающих дуги графа (отношения параметров событий) с помощью следующих параметров:
  - `source` – имя первого параметра события, образующего связь на графе.
  - `target` – имя второго параметра события, образующего связь на графе.
  - `tooltip` – параметр, включающий параметр `templates`. В параметре `templates` задается надпись, которая будет отображаться при наведении курсора мыши на дугу графа. Вы можете использовать следующие переменные с помощью двойных фигурных скобок:
    - Любой параметр из списка параметров событий `fields`.
    - `onIntervalActivationsCount` – количество обнаружений события в потоке событий за период, заданный при просмотре истории событий.
    - `onIntervalLastActivationTimestamp` – дата и время последнего обнаружения события в потоке событий за период, заданный при просмотре истории событий.
    - `lastActivationTimestamp` – дата и время последнего обнаружения события в потоке событий.
    - `totalActivationsCount` – количество обнаружений события в потоке событий.
  - `isGraphGroup` – параметр, определяющий способ отображения связи на графе отношений параметров событий. Если параметр имеет значение `true`, то события с разными значениями параметров, которые не используются в качестве вершин графа, отображаются как одна группа событий. Если параметр имеет значение `false`, то события с разными значениями параметров отображаются как разные события. По умолчанию этот параметр имеет значение `false`.

Ниже приведен пример файла в формате JSON, который содержит конфигурацию параметров для службы Event Processor. Файл содержит описание параметров событий для процессора событий. В соответствии со значениями, указанными в параметре `mapping_fields`, в Kaspersky MLAD будут отображаться события со следующими параметрами события:

- `EventType` – соответствует параметру `cat` в событии, полученном коннектором CEF Connector.
- `User_Name` – соответствует параметру `cs1`, если для параметра `cs1Label` получено значение `user`.

- `Destination_Host` – соответствует параметру `cs1`, если для параметра `cs1Label` получено значение `destination`.

- `Access_Result` – соответствует параметру `cs1`, если для параметра `cs1Label` получено значение `access`.

```
{
    "timestamp_field": "TimeStamp",
    "timestamp_scale": "ms",
    "global_episodes_history_interval": "3 weeks",
    "monitors_stacks_persistence_interval_minutes": 10,
    "sep": " ",
    "sep_kv": "=",
    "sep_cef_caption": "|",
    "mapping_fields": {
        "cat": "User_Host",
        "cs1": {"map_label": "cs1Label", "values": {"user": "User_Name",
                                                    "destination": "Destination_Host",
                                                    "access": "Access_Result"}}
    },
    "fields": [
        "User_Host",
        "User_Name",
        "Destination_Host",
        "Access_Result"
    ],
    "nodes": [
        {
            "name": "User_Name",
            "depth": 0,
            "tooltip": {
                "templates": [
                    "User: {{User_Name}}"
                ]
            },
            "fieldShortCut": "User"
        },
        {
            "name": "User_Host",
            "depth": 1,
            "tooltip": {
                "templates": [
                    "User host: {{User_Host}}"
                ]
            },
            "fieldShortCut": "Src"
        },
        {
            "name": "Destination_Host",
            "depth": 2,
            "tooltip": {
                "templates": [
                    "Destination: {{Destination_Host}}"
                ]
            },
            "fieldShortCut": "Dst"
        }
    ],
    "links": [
        {
            "source": "User_Name",
            "target": "User_Host",
            "tooltip": {
                "templates": [
                    "{{User_Name}} » {{User_Host}}",
                    "Count: {{onIntervalActivationsCount}}"
                ]
            },
            "isGraphGroup": true
        },        {
            "source": "User_Host",
            "target": "Destination_Host",
            "tooltip": {
                "templates": [
                    "{{User_Host}} » {{Destination_Host}}",
                    "DeviceEventClassID: {{Access_Result}}",
                    "Count: {{onIntervalActivationsCount}}"
                ]
            }
        }
    ]
}
```

Параметры и пример JSON-файла, описывающего теги источника данных OPC UA

Конфигурационный файл создается квалифицированным техническим специалистом Заказчика, сотрудником "Лаборатории Касперского" или сертифицированным интегратором. Системный администратор загружает конфигурационный файл с описанием тегов источника данных OPC UA при создании его карточки.

Конфигурационный файл в явном виде устанавливает соответствие имен отдельных тегов их идентификаторам в источнике данных. Конфигурационный файл используется, когда соответствие имени тега и его идентификатора в источнике данных нельзя задать с помощью общих параметров преобразования, задаваемых при создании карточки источника данных. Кроме того, в конфигурационном файле могут быть заданы преобразования текстовых значений тега в числовые. Конфигурационный файл имеет приоритет над общими параметрами в карточке источника данных.

Конфигурационный файл содержит следующие параметры:

- `opc_variables` – список тегов в источнике данных. Каждый тег задается с помощью следующих параметров:
  - `name` – имя тега в Kaspersky MLAD.
  - `nodeid` – идентификатор узла, по которому доступен тег в источнике данных.
  - `path` – путь к тегу в источнике данных.
  - `conversions` – преобразование текстовых значений конкретного тега в числовые. Преобразования задаются в виде списка пар параметров:
    - `key` – текстовое значение тега в источнике данных.
    - `value` – соответствующее числовое значение тега, которое будет передано в Kaspersky MLAD. Вы также можете использовать знак ~, что соответствует отсутствующему значению.

  Для поиска тега в источнике данных необходимо задать либо параметр `nodeid`, либо параметр `path`.

- `conversions` – преобразование текстовых значений в числовые для всех тегов. Преобразования задаются в виде списка пар параметров:
  - `key` – текстовое значение тега в источнике данных.
  - `value` – соответствующее числовое значение тега, которое будет передано в Kaspersky MLAD. Вы также можете использовать знак ~, что соответствует отсутствующему значению.
- `encoding` – необязательный параметр, определяющий кодек Python, используемый для декодирования текстовых значений тегов.

Ниже приведен пример файла в формате JSON, который содержит описание тегов источника данных.

```
{
    "opc_variables": [
        {
            "name": "Tag1",
            "nodeid": "ns=2;s=Tag1"
        },
        {
            "name": "Tag2",
            "path": ["0:Objects", "0:my_tag2"]
        },
        {
            "name": "Tag3",
            "path": ["0:Objects", "0:my_tag3"],
            "conversions": [
                {
                    "key": "ok",
                    "value": 5
                }
            ]
        }
    ],
    "conversions": [
        {
            "key": "ok",
            "value": 2
        },
        {
            "key": "alarm",
            "value": 7
        }
    ],
    "encoding": "cp1251"
}
```

Просмотр журнала Kaspersky MLAD

В Kaspersky MLAD используется система ведения журналов Grafana для отслеживания состояния служб программы, а также для отслеживания событий информационной безопасности.

Отслеживание событий информационной безопасности Kaspersky MLAD в подсистеме ведения журналов

В таблице ниже приведены типы событий ИБ, которые отслеживаются в Kaspersky MLAD.

Типы событий информационной безопасности

Идентификатор события информационной безопасности в системе ведения журналов	Тип события информационной безопасности
access_control	Проверка прав пользователей при выполнении действий в веб-интерфейсе Kaspersky MLAD
license_control	Добавление и удаление лицензионных ключей
log_control	Удаление журналов событий ИБ из базы данных Kaspersky MLAD при превышении объема хранения журналов или при истечении срока их хранения
login	Подключение и попытки подключения пользователей к Kaspersky MLAD
logout	Завершение подключения пользователей к Kaspersky MLAD
model_control	Создание, импорт, изменение и удаление моделей
role_control	Создание, изменение и удаление ролей
service_control	Запуск, остановка и перезапуск служб Kaspersky MLAD
system_settings_control	Изменение параметров Kaspersky MLAD
tag_control	Импорт, создание, изменение и удаление тегов
user_control	Создание, изменение и удаление учетных записей пользователей

Каждая запись о событии ИБ содержит следующие параметры:

- **event_id** – идентификатор события ИБ.
- **timestamp** – дата и время события ИБ.
- **event_type** – идентификатор типа события ИБ.
- **sub_type** – уточнение типа события ИБ.
- **severity** – важность события ИБ. В Kaspersky MLAD предусмотрены следующие уровни важности событий ИБ:
  - **1** – низкий.

    К этим событиям ИБ относятся записи о предоставлении доступа пользователям на выполнение какого-либо действия в веб-интерфейсе и об успешном выполнении каких-либо действий пользователей.
  - **5** – средний.

    К этим событиям ИБ относятся записи о действиях пользователей в веб-интерфейсе по управлению ML-моделями, тегами, учетными записями и паролями, а также записи о достижении заданных порогов по времени и объему хранения журналов событий ИБ.
  - **8** – высокий.

    К этим событиям ИБ относятся записи об указании пользователями неправильного адреса электронной почты пользователя и/или пароля при подключении к веб-интерфейсу программы, а также записи о неуспешных попытках смены пароля.
  - **10** – высший.

    К этим событиям ИБ относятся записи о попытках подключения к веб-интерфейсу программы с помощью системной или заблокированной учетной записи, а также записи о попытках выполнения каких-либо действий в программе при отсутствии соответствующих прав доступа.
- **username** – адрес электронной почты пользователя, действия которого привели к записи события ИБ.
- **ip_address** – IP-адрес компьютера, с которого пользователем было произведено действие, записанное в журналы событий ИБ.
- **outcome** – результат события ИБ. Результат OK соответствует успешному выполнению операции пользователем. Результат FAIL соответствует отказу в выполнении операции пользователем.
- **msg** – краткое содержание события ИБ.
- **info** – подробное описание события ИБ.

Отслеживание состояния служб Kaspersky MLAD в подсистеме ведения журналов

Для обозначения служб Kaspersky MLAD, состояние которых отслеживается в подсистеме ведения журналов, используются наименования соответствующих им контейнеров или образов в Docker. В качестве имени образа в большинстве случаев используется сокращенное имя службы. Имя контейнера формируется по следующему шаблону:

`<директория программы> - <имя образа> -#,`

где: # – номер контейнера Docker.

По умолчанию Kaspersky MLAD использует директорию `/opt/kaspersky/mlad`.

В журнале Kaspersky MLAD записи о состоянии служб программы хранятся только за последнюю неделю.

Ниже приведена таблица соответствия служб Kaspersky MLAD и имен образов и контейнеров Docker.

Соответствие служб Kaspersky MLAD и имен образов и контейнеров Docker

Служба Kaspersky MLAD	Имя образа	Имя контейнера
Anomaly Detector	anomaly_detector	mlad-anomaly_detector-1
Time Series Database	influxdb	mlad-influxdb-1
Message Broker	kafka	mlad-kafka-1
Keeper	keeper	mlad-keeper-1
Logger	logger	mlad-logger-1
Database	postgres	mlad-postgres-1
Similar Anomaly	similar_anomaly	mlad-similar_anomaly-1
Event Processor	event-processor	mlad-event-processor-1
Stream Processor	stream-processor	mlad-stream-processor-1
Trainer	trainer	mlad-trainer-1
Web Server	nginx-ui	mlad-nginx-ui-1
API Server	web-server	mlad-web-server-1
Mail Notifier	postman	mlad-postman-1
Data Source Manager	datasource-manager	mlad-datasource-manager-1
MQTT Connector	mqtt-connector	mlad-mqtt-connector-1
AMQP Connector	amqp-connector	mlad-amqp-connector-1
HTTP Connector	http-connector	mlad-http-connector-1
KICS Connector	kics3-connector	mlad-kics3-connector-1
CEF Connector	cef-connector	mlad-cef-connector-1
WebSocket Connector	ws-connector	mlad-ws-connector-1
Docker API Server	docker-api-server	mlad-docker-api-server-1
Migrations	migrations	mlad-migrations-1
Push Server	push-server	mlad-push-server-1
	webstatic	mlad-webstatic-1

Для служб Time Series Database, Message Broker, Logger, Database, Web Server, а также образа webstatic используется уровень ведения журналов Инфо. Уровни ведения журналов для остальных служб Kaspersky MLAD задаются системным администратором при настройке параметров программы.

Сценарий: просмотр журналов событий информационной безопасности

Перед началом работы с подсистемой ведения журналов рекомендуется ознакомиться с руководством пользователя системы Grafana.

Объем и время хранения записей событий ИБ задаются при настройке параметров безопасности.

Запись журналов событий информационной безопасности в базу данных Kaspersky MLAD ведется автоматически. Если требуется, системный администратор может указать параметры внешней системы, в которую требуется отправлять журналы событий ИБ.

Сценарий просмотра журналов событий информационной безопасности состоит из следующих этапов:

1. **Переход в подсистему ведения журналов**

   Перейдите в систему ведения журналов нажатием на кнопку . Откроется интерфейс Grafana, в котором требуется указать адрес электронной почты и пароль пользователя Kaspersky MLAD.

   Доступно только системным администраторам и пользователям с правом **Работа с журналами программы**.

2. **Анализ журналов событий информационной безопасности**

   Перейдите в раздел **Security audit** и проанализируйте записи журналов событий ИБ за выбранный период. Вы можете выполнить фильтрацию по параметрам журналов событий ИБ. Для этого в столбце с нужным параметром журналов нажмите на кнопку , установите флажки около нужных критериев фильтрации и нажмите на кнопку **Ok**. Для сброса критериев фильтрации снимите нужные флажки и нажмите на кнопку **Ok**.

3. **Экспорт журналов событий информационной безопасности**

   Для выгрузки в текстовый файл журналов событий ИБ за выбранный период, в разделе **Security audit** в вертикальном меню в правом верхнем углу таблицы журналов событий ИБ выберите **Inspect** → **Data** и в открывшейся панели нажмите на кнопку **Download CSV**.

Сценарий: оценка основных метрик Kaspersky MLAD

Перед началом работы с подсистемой ведения журналов рекомендуется ознакомиться с руководством пользователя системы Grafana.

При первом подключении к подсистеме ведения журналов требуется изменить пароль, установленный по умолчанию.

В этом подразделе приводится последовательность действий, которые требуется выполнить для оценки работоспособности и общего состояния Kaspersky MLAD.

Сценарий оценки работоспособности и общего состояния Kaspersky MLAD состоит из следующих этапов:

1. **Переход в подсистему ведения журналов**

   Перейдите в систему ведения журналов нажатием на кнопку . Откроется интерфейс Grafana, в котором требуется указать адрес электронной почты и пароль пользователя Kaspersky MLAD.

   > Доступно только системным администраторам и пользователям с правом **Работа с журналами программы**.

2. **Анализ основных метрик Kaspersky MLAD**

   Перейдите в раздел **Summary docker metrics** и проанализируйте графики основных метрик Kaspersky MLAD за выбранный период.

   Для каждого контейнера служб Kaspersky MLAD отображаются следующие метрики:

   - *CPU usage* – история загрузки центрального процессора контейнером. Измеряется в процентах.
   - *RAM usage* – история использования контейнером оперативной памяти. Измеряется в байтах.
   - *Disk usage Read/Write* – история нагрузки контейнера на дисковую подсистему (операции записи и чтения). Измеряется в байтах.
   - *Network usage* – история задействования контейнером сетевых ресурсов. Измеряется в байтах в секунду.

Сценарий: просмотр метрик и журналов контейнера

> Перед началом работы с подсистемой ведения журналов рекомендуется ознакомиться с руководством пользователя системы Grafana.

> В журнале Kaspersky MLAD хранятся записи только за последние 48 часов.

В этом подразделе приводится последовательность действий, которые требуется выполнить для оценки работоспособности и просмотра журналов определенного контейнера из комплекта поставки Kaspersky MLAD.

Сценарий оценки работоспособности и просмотра журналов определенного контейнера состоит из следующих этапов:

1. **Переход в подсистему ведения журналов**

   Перейдите в систему ведения журналов нажатием на кнопку . Откроется интерфейс Grafana, в котором требуется указать адрес электронной почты и пароль пользователя Kaspersky MLAD.

   > Доступно только системным администраторам и пользователям с правом **Работа с журналами программы**.

2. **Анализ метрик контейнера**

   Перейдите в раздел **Service detailed monitoring** и в раскрывающемся списке **Container** выберите контейнер, метрики которого вы хотите проанализировать. Проанализируйте графики метрик Kaspersky MLAD для контейнера за необходимый период.

   В разделе **Service detailed monitoring** представлены следующие метрики:

   - *Memory* – история использования контейнером оперативной памяти. Измеряется в байтах.
   - *CPU* – история загрузки центрального процессора контейнером. Измеряется в процентах.
   - *File system* – история нагрузки контейнера на дисковую подсистему (операции записи и чтения). Измеряется в байтах.
   - *Network* – история задействования контейнером сетевых ресурсов. Измеряется в байтах в секунду.

3. **Анализ журналов контейнера**

   Проанализируйте записи журналов контейнера за выбранный период, которые отображаются под информационной панелью с метриками. Вы можете выполнить поиск по записям журналов контейнера. Для этого введите поисковый запрос в поле **Log search** и нажмите на клавишу **ENTER**. Для сброса результатов поиска очистите поле **Log search** и нажмите на клавишу **ENTER**.

4. **Экспорт журналов контейнера**

   Для выгрузки в текстовый файл журналов контейнера за выбранный период, в разделе **Service detailed monitoring** в вертикальном меню ⋮ в правом верхнем углу блока нужной метрики выберите **Inspect** → **Data** и в открывшейся панели нажмите на кнопку **Download CSV**.

Специальные символы регулярных выражений

Для поиска событий, паттернов и значений параметров событий, а также для преобразования имен тегов в их идентификаторы в источнике данных вы можете использовать регулярные выражения. В регулярных выражениях используется формат, поддерживаемый на языке программирования Python.

Наиболее популярными являются следующие специальные символы:

- `^` – Соответствует началу строки. Например, `^A` означает, что поиск будет осуществляться по значениям, начинающимся с символа A.
- `$` – Соответствует концу строки. Например, `A$` означает, что поиск будет осуществляться по значениям, заканчивающимся символом A.
- `.` – Соответствует одному любому символу.
- `|` – Разделяет допустимые варианты символов или совокупности символов в строке. Например, `к(о|и)т` соответствует как строке `кот`, так и `кит`.

- `\` – Символ, указывающий на то, что следующий символ является обычным символом в строке, а не специальным. Вы можете использовать символ `\` для поиска специальных символов. Например, `\.` описывает точку, а `\\` описывает обратную косую черту.

- `[]` – Соответствует любому символу из набора допустимых символов. Например, `[ абв ]` соответствует появлению одного из трех указанных символов.

  Для поиска по диапазону значений вы можете использовать символ `-`. Если требуется найти символы, которые не входят в указанный диапазон, вы можете использовать символ `^` внутри квадратных скобок. Например, `[^0-9]` задает возможность появления любого символа, кроме цифр.

Для указания нужного количества повторений выражения вы можете использовать следующие специальные символы:

- `?` – Символ, определяющий, что предшествующее выражение может встречаться в строке ноль или один раз.

- `*` – Символ, определяющий, что предшествующее выражение может встречаться в строке ноль или более раз.

- `+` – Символ, определяющий, что предшествующее выражение может встречаться в строке один или более раз.

- `{}` – Символьный класс, позволяющий указать нужное количество повторений предшествующего выражения. Вы можете указать количество повторений одним из следующих способов:

  - `{n}` – Выражение, предшествующее фигурным скобкам, встречает в строке параметра ровно `n` раз.

  - `{m,n}` – Выражение, предшествующее фигурным скобкам, встречается в строке от `m` до `n` раз включительно.

  - `{m,}` – Выражение, предшествующее фигурным скобкам, встречается в строке не менее `m` раз.

  - `{,n}` – Выражение, предшествующее фигурным скобкам, встречается в строке не более `n` раз.

Вы также можете использовать скобки `()` для объединения элементов выражения в группу. Например, `( к[ои]т ){2}` найдет вхождения `коткот`, `киткит`, `киткот` и `коткит`.

Наборы шифров для защищенного TLS-соединения

Для защищенного TLS-соединения по протоколу TLS-1.2 рекомендуется использовать следующий набор шифров:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384;

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256;

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256;

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384;

- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256;

- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256;
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384.

Для защищенного TLS-соединения по протоколу TLS-1.3 рекомендуется использовать следующий набор шифров:

- TLS_AES_128_GCM_SHA256;
- TLS_AES_256_GCM_SHA384;
- TLS_CHACHA20_POLY1305_SHA256;
- TLS_AES_128_CCM_SHA256.

Примеры вычисления комбинированных функций в выражениях для расчета вычислимых тегов

В таблице ниже представлены значения тегов, используемых в приведенных примерах.

Значения тегов в примерах

Узел РИВС	Значение тега `x`	Значение тега `y`	Значение тега `z`	Значение тега `y sq`
Узел 1 (`w=1`)	0	10	100	100
Узел 2 (`w=2`)	1	11	101	121
Узел 3 (`w=3`)	2	12	102	144
Узел 4 (`w=4`)	3	13	103	169

Получение максимального абсолютного значения последних трех изменений значений тега

В этом примере рассматривается порядок выполнения операций для получения максимального значения последних трех изменений значений тега `y sq` на окне, равном четырем узлам РИВС.

Выражение для расчета:

```
max(grad("y sq", w=4))
```

Последовательность операций:

1. Вычисление градиента первого порядка. Для вычисления градиента необходимо из значения тега в узле РИВС N вычесть значение в узле N-1.

   - Градиент тега в узле 2 соответствует результату вычитания значения тега в узле 1 из значения тега в узле 2. Результатом вычисления является число 21.
   - Градиент тега в узле 3 соответствует результату вычитания значения тега в узле 2 из значения тега в узле 3. Результатом вычисления является число 23.
   - Градиент тега в узле 4 соответствует результату вычитания значения тега в узле 3 из значения тега в узле 4. Результатом вычисления является число 25.

2. Выбор максимального среди значений. Максимальным значением и результатом расчета всего выражения является число 25.

Получение арифметического среднего максимальных значений среди тегов за промежуток времени

В этом примере рассматривается порядок выполнения операций для получения среднего арифметического максимальных значений среди тегов `x`, `y sq` и результата прибавления единицы к значениям тега `z` на окне, равном трем узлам РИВС. Такое выражение может быть использовано для анализа данных телеметрии по однотипным тегам (например, для сравнения данных телеметрии по нескольким датчикам на одном оборудовании).

Выражение для расчета:

```
mean(maxtag("x", "y sq", "z" + 1, w=3))
```

Последовательность операций:

1. Получение значений для третьего аргумента функции. К каждому значению тега `z` на заданном окне добавляется единица. Результатом вычисления будет вектор из чисел 101, 102 и 103.

2. Получение максимального значения среди тегов в каждом узле РИВС.

   - В узле 1 сравниваются значения 0, 100 и 101, среди которых 101 является максимальным.
   - В узле 2 сравниваются значения 1, 121 и 102, среди которых 121 является максимальным.
   - В узле 3 сравниваются значения 2, 144 и 103, среди которых 144 является максимальным.

3. Вычисление среднего арифметического полученных максимальных значений. Результатом вычисления среднего арифметического чисел 101, 121 и 144 и результатом вычисления всего выражения является число 122.

Получение минимального значения из попарных расстояний максимальных значений среди тегов за промежуток времени

В этом примере рассматривается порядок выполнения операции для получения минимального значения из попарных расстояний максимальных значений среди тегов `x`, `y` и `y sq` на окне, равному трем узлам РИВС.

Выражение для расчета:

```
min(pwd(maxtag("x", "y", "y sq", w=3)))
```

Последовательность операций:

1. Получение максимальных значений среди тегов за промежуток времени.

   - В узле 1 сравниваются значения 0, 10 и 100. Среди полученных значений максимальным является число 100.
   - В узле 2 сравниваются значения 1, 11 и 121. Среди полученных значений максимальным является число 121.
   - В узле 3 сравниваются значения 2, 12 и 144. Среди полученных значений максимальным является число 144.

2. Вычисление попарных расстояний. Результаты вычисления попарных расстояний приводятся к модулю, так как для параметра `absolute` используется значение по умолчанию `true`.

   - Результатом вычисления расстояния между 100 и 121 является число 21.
   - Результатом вычисления расстояния между 100 и 144 является число 44.
   - Результатом вычисления расстояния между 121 и 144 является число 23.

3. Выбор минимального значения из полученных попарных расстояний. Минимальным значением и результатом вычисления всего выражения является число 21.

Глоссарий

ML-модель

Алгоритм, основанный на методах машинного обучения, задачей которого является анализ телеметрии объекта мониторинга и обнаружение аномалий.

Актив

Раздел иерархической структуры, представляющий различные элементы организационной структуры предприятия (цеха, производства, заводы) или технические системы (агрегаты, установки).

Аномалия

Нештатное, неожиданное и не предусмотренное производственным процессом отклонение в поведении объекта мониторинга.

Артефакт

Последовательность числовых значений (временной ряд), сформированная в результате инференса ML-модели. Для каждого элемента ML-модели формируется основной артефакт, характеризующий степень отклонения поведения объекта мониторинга от ожидаемого (нормального). Некоторые типы элементов могут формировать артефакты, связанные с конкретными тегами (например, прогноз значений выходных тегов предиктивного элемента).

АСУ ТП

Аббревиатура от "автоматизированная система управления технологическим процессом". Группа технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях.

Внимание

Специальная конфигурация процессора событий, которую требуется настроить для отслеживания событий и паттернов по отдельным подмножествам истории событий, а также для выявления событий, поступивших в необычное для них время, и общности в поведении объекта мониторинга.

Время данных

Система отсчета времени, в которой идут часы источников данных на объекте мониторинга.

Графическая область

Совокупность тегов, данные которых совместно отображаются путем наложения на одном графике в разделах **История** и **Мониторинг**. В графической области могут отображаться данные для одного и более тегов пресета.

Иерархическая структура объекта мониторинга

Способ представления объекта мониторинга в виде дерева, конечные узлы которого являются тегами, а промежуточные – активами.

Индикатор инференса

Совокупность критериев, на основании которых определяются интервалы времени данных, на которых ML-модель выполняет инференс.

Индикатор обучения

Совокупность критериев, на основании которых определяются интервалы времени данных, на которых ML-модель выполняет обучение.

Инференс

Работа ML-модели с данными телеметрии для выявления аномального поведения.

Инцидент

Обнаруженное отклонение от ожидаемого (нормального) поведения объекта мониторинга.

Коннектор

Служба, которая обеспечивает обмен данными с внешними системами.

Монитор

Источник извещений о выявлении процессором событий паттернов, событий или значений параметров событий в соответствии с заданными критериями мониторинга. Критерии мониторинга определяют голову внимания, дополнительные фильтры на значения параметров событий, а также скользящий временной интервал и количество последовательных активаций монитора на скользящем временном интервале.

Паттерн

Последовательность событий или других паттернов, на которые разбивается поток событий от объекта мониторинга. Последовательность включает как идентификаторы элементов этой последовательности, так и интервалы времени между ними.

Пресет

Набор тегов, сформированный пользователем в произвольном порядке или созданный автоматически программой. Пресет, сформированный пользователем, называется пользовательским. Набор тегов в составе пользовательского пресета может соответствовать определенному аспекту технологического процесса или участку объекта мониторинга. Пресет, созданный программой автоматически, называется динамическим. Динамические пресеты могут быть сформированы по инциденту или по элементу ML-модели.

Равноинтервальная временная сетка (РИВС)

Бесконечная последовательность моментов времени, следующих друг за другом через равные интервалы, к которой приводится поток поступающих данных телеметрии.

Разметка

Инструмент для отбора интервалов времени. Разметки используются для формирования индикаторов обучения и инференса ML-модели. В составе разметки могут быть использованы два вида критериев: условия на поведение конкретных тегов (отбираются интервалы времени, в которых эти условия соблюдаются) и фильтр по времени (интервалы времени отбираются независимо от поведения тегов).

Роль учетной записи

Совокупность прав доступа, определяющая набор доступных пользователю действий при подключении к веб-интерфейсу приложения. В Kaspersky MLAD предусмотрены роль системного администратора и пользовательские роли.

Семплирование

Метод корректировки обучающей выборки с привязкой к шагам временной шкалы в исходном наборе данных.

Событие

Набор значений из заранее заданного перечня параметров, описывающих то, что произошло на объекте мониторинга. История событий формируется как набор пар: идентификаторов событий и меток их времени.

Тег

Именованный параметр технологического процесса, например, измеряемый параметр (температура или давление) или состояние (включено, выключено или номер режима)

Топ-тег

Параметр технологического процесса, который оказал наибольшее влияние на регистрацию инцидента.

Топик AMQP

Иерархический путь к источнику данных, на базе которого отправляются сообщения по протоколу AMQP.

Топик MQTT

Иерархический путь к источнику данных, на базе которого отправляются сообщения по протоколу MQTT.

Уведомление

Сообщение с информацией об инциденте (инцидентах), которое программа отправляет через системы доставки сообщений (например, по электронной почте) на указанные адреса.

Эксфильтрация данных

Несанкционированное копирование, передача или получение данных с компьютера или сервера.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в директории установки программы (в поддиректории legal).

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Ubuntu, LTS являются зарегистрированными товарными знаками Canonical Ltd.

Словесный знак Grafana и логотип Grafana являются зарегистрированными товарными знаками/знаками обслуживания или товарными знаками/знаками обслуживания Coding Instinct AB в США и других странах и используются с разрешения Coding Instinct. Мы не являемся аффилированной, поддерживаемой или спонсируемой со стороны Coding Instinct или сообщества Grafana компанией.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

Google, Chrome, Google Chrome – товарные знаки Google LLC.

TensorFlow и любые связанные с ним обозначения являются товарными знаками Google LLC.

Intel, Core и Xeon являются товарными знаками Intel Corporation или ее дочерних компаний.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft, Excel и Microsoft Edge являются товарными знаками группы компаний Microsoft.

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

PGP – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.