kaspersky

Kaspersky Machine Learning for Anomaly Detection

Содержание

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, некорректные 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 оповещения 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 как машинного обучения, так и произвольных правил для обнаружения аномалий.
- Отображает в виде графиков наблюдаемые и предсказываемые значения тегов и ошибки прогноза как в режиме онлайн-мониторинга, так и в режиме ретроспективного анализа истории телеметрии.
- Обеспечивает работу с журналом обнаруженных инцидентов.
- Предоставляет возможность переобучения и дополнительного обучения используемой ML-модели.
- Позволяет создавать ML-модели и добавлять в нее элементы на основе нейронных сетей и диагностических правил.
- 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, OPC UA, MQTT, AMQP, CEF и WebSocket, а также по специализированному протоколу поверх протокола HTTPS от программы Kaspersky Industrial CyberSecurity for Networks.

- Отображает в виде графиков исторические данные и данные, поступающие в режиме реального времени, в соответствии с заданными наборами тегов.
- 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_4.0.2.<номер сборки>_ru-RU_en-US.tar.xz, который содержит следующие файлы:

- установочный скрипт и все необходимые для установки системы файлы;
- 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.

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:

- 8 ядер;
- 32 ГБ оперативной памяти;
- 200 ГБ 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™ 2.13:

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

Поддерживаемые операционные системы:

- Ubuntu 22.04 LTS и выше.

До развертывания Kaspersky MLAD должно быть установлено следующее программное обеспечение:

- docker 20.10.21 и выше;
- docker compose 2.12.2 и выше.

Устанавливать программное обеспечение 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 107 и выше;
- минимальное разрешение экрана монитора для корректного 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.

Информационная безопасность

Параметры ML-модели напрямую влияют на обнаружение аномалий, и поэтому изменять их могут только системные администраторы. Дата последнего изменения ML-модели (активация, изменение имени, порогового значения MSE, весов MSE) доступна в разделе **Модели**. История изменений доступна только в логах, 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 "Лаборатории Касперского" или сертифицированному интегратору.
- Обеспечить защиту трафика внутри интранет-системы.
- Обеспечить защиту подключений к внешним сетям.

- Использовать защищенное TLS-соединение для передачи данных.
- Изменить имя и пароль первого пользователя программы с ролью системного администратора при установке программы.
- 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.
  - 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 нотификации и системе логирования.
- 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

Этот раздел содержит описание разграничения доступа пользователей 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	Пользовательская

	администратор	роль
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 об инцидентах: • Создание, изменение и удаление уведомления об инцидентах. • Включение и выключение отправки уведомлений об инцидентах.	✓	–
Настройка параметров Kaspersky MLAD	✓	–
Управление активами: • 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.	✓	–
Управление ML-моделями: • Загрузка ML-модели; • Активация импортированной ML-модели; • Создание ML-модели; • Изменение ML-модели;	✓	✓ (по назначению)

• Добавление и изменение нейросетевого элемента ML-модели; • 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 элементов ML-модели и просмотр результатов обучения элементов ML-модели; • Подготовка ML-модели к публикации; • Публикация ML-модели; • Удаление ML-модели.		
Управление службами Kaspersky MLAD: • Просмотр статусов служб; • Запуск, остановка и перезапуск служб.	✓	✓ (по назначению)
Просмотр логов Kaspersky MLAD	✓	✓ (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, причину, экспертного заключения и замечания к инциденту или группе инцидентов;
    - Экспорт инцидентов в файл.
- Следующие действия в разделе **Модели**:
    - Создание, изменение и удаление разметок;
    - Запуск и остановка инференса ML-модели;
    - Просмотр графа потока данных ML-модели.
- Управление пресетами:
    - Просмотр пресетов;
    - 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 4.0 появились следующие возможности и доработки:

- Конструктор моделей – добавлена функциональность, позволяющая создавать, изменять и удалять собственные ML-модели и элементы ML-моделей на основе нейронной сети и/или диагностических правил.

- Разметки – добавлена функциональность, позволяющая создавать, изменять и удалять разметки для обучения и инференса ML-моделей.

- Обучение ML-моделей – в веб-интерфейсе программы добавлена возможность управлять параметрами обучения элементов ML-моделей. Также вы можете запускать и прерывать обучение элементов ML-моделей, просматривать номер текущей эпохи обучения элемента и просматривать результаты последнего обучения в веб-интерфейсе программы.

- Иерархическая структура объекта мониторинга – добавлена функциональность, позволяющая определить в Kaspersky MLAD способ организации активов объекта мониторинга в виде дерева первичных и функциональных элементов. Первичные элементы иерархической структуры представлены активами и тегами, управление которыми доступно в разделе **Активы**. Формат конфигурационного файла для загрузки тегов изменен на XLSX. При загрузке конфигурационного файла также загружаются активы иерархической структуры. Функциональные элементы иерархической структуры представлены ML-моделями, шаблонами ML-моделей и разметками. Иерархическая структура объекта мониторинга отображается в разделах **Активы** и **Модели**, а также в разделе **Пресеты** при создании и изменении пресетов.

- Роли – добавлена функциональность, позволяющая управлять ролями и выбирать для них права доступа к функциям программы. Управление ролями доступно в разделе **Роли**.

- Политика безопасности – добавлена функциональность, позволяющая управлять параметрами безопасности Kaspersky MLAD в соответствии с политикой безопасности на предприятии.

- Логирование событий информационной безопасности – добавлена функциональность, позволяющая управлять параметрами хранения логов событий информационной безопасности, а также просматривать логи событий информационной безопасности в системе логирования Grafana.

- Скрипт обновления программы – добавлена функциональность, позволяющая выполнять резервное копирование Kaspersky MLAD и восстановление программы из резервной копии с помощью скрипта обновления программы. Изменена команда запуска скрипта для обновления программы при выпуске новых версий.

- Коннектор CEF Connector – добавлена функциональность, позволяющая отправлять логи событий информационной безопасности во внешнюю систему.

- Коннектор OPC UA Connector – добавлены новые параметры для настройки коннектора OPC UA Connector.

- Служба Mail Notifier – добавлены новые параметры для настройки службы Mail Notifier.

- Служба Trainer – оптимизирована работа службы Trainer.

- Обновлен веб-интерфейс Kaspersky MLAD.

- Добавлены новые параметры для настройки отображения графиков в разделах **Мониторинг** и **История**.

Основные понятия Kaspersky MLAD

Этот раздел содержит развернутые определения основных понятий в Kaspersky MLAD.

Иерархическая структура объекта мониторинга

Иерархическая структура объекта мониторинга (далее также *иерархическая структура*) – это способ организации данных объекта мониторинга в виде дерева, конечные узлы которого соответствуют исходным тегам и/или тегам, обработанными службой Stream Processor.

Теги объекта мониторинга организованы в виде иерархии активов, представляющих агрегаты, установки, цеха и заводы. Число активов зависит 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, 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 создать их 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.

Теги

Основными объектами наблюдения в Kaspersky MLAD являются теги. *Тег* – это параметр технологического процесса, передаваемый в промышленной сети (например, контролируемая температура). 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.

В Kaspersky MLAD есть следующие типы тегов:

- **Исходные теги**

  Значения этих тегов поступают в Kaspersky MLAD напрямую от объекта мониторинга при условии, что выключено использование службы Stream Processor.

  Исходные теги отображаются в иерархической структуре объекта мониторинга.

- **Теги, обработанные службой Stream Processor**

Значения тегов, полученные в результате обработки входного потока тегов службой Stream Processor.

Служба Stream Processor может привести входной поток тегов к РИВС. Для каждого узла равно-интервальной последовательности служба Stream Processor вычисляет значения тегов для выходного потока. В зависимости от того, сколько входных наблюдений было накоплено для каждого узла и как давно наблюдения поступали в последний раз, служба Stream Processor может вычислять выходные значения тегов путем агрегации (вычисление значения тега на основе нескольких наблюдений тега, накопленных для соответствующего узла равно-интервальной последовательности) или импутации (восстановление значение тега для пустого узла равно-интервальной последовательности на основе значений этого тега, полученных ранее).

Служба Stream Processor также может вычислять значения производных тегов на основе поступающих данных телеметрии. Например, служба Stream Processor может вычислять значения скользящего среднего или среднего значения группы тегов.

Теги, обработанные службой Stream Processor, отображаются в иерархической структуре объекта мониторинга.

Kaspersky MLAD поддерживает несколько способов получения данных телеметрии (тегов). В зависимости от характеристик объекта мониторинга и возможностей передачи тегов вы можете выбрать один из следующих способов получения тегов:

- С помощью коннекторов Kaspersky Industrial CyberSecurity for Networks, которые анализируют зеркалированный трафик и отдают теги в Kaspersky MLAD в онлайн-режиме. Kaspersky MLAD передает обратно информацию об обнаруженных инцидентах.
- С помощью коннектора **OPC UA Connector**, если на объекте мониторинга есть возможность передавать теги от АСУ ТП по протоколу OPC UA в онлайн-режиме.
- С помощью коннектора **MQTT Connector**, если на объекте мониторинга есть возможность передавать теги по протоколу MQTT и принимать оповещения о регистрации инцидентов в онлайн-режиме.
- С помощью коннектора **AMQP Connector**, если на объекте мониторинга есть возможность передавать теги по протоколу AMQP и принимать оповещения о регистрации инцидентов в онлайн-режиме.
- С помощью коннектора **WebSocket Connector**, если на объекте мониторинга есть возможность передавать теги по протоколу WebSocket и принимать оповещения 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 оповещения о регистрации возникновении инцидентов в онлайн-режиме.
- Если первые четыре способа передачи тегов недоступны, с помощью коннектора **HTTP Connector** можно настроить регламентную выгрузку тегов в виде CSV-файлов по протоколу HTTP (например, один раз в час или один раз в минуту), написав скрипт выгрузки тегов.

ML-модели

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 представляет собой самостоятельную ML-модель, а общий результат работы службы Anomaly Detector складывается из объединения результатов инференса элементов ML-модели. Как правило, чем сложнее технологические процессы объекта мониторинга, тем больше элементов будет содержать ML-модель.

Инференс – это работа ML-модели с данными телеметрии для выявления аномального поведения. 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 этих ML-модели в порядке очереди их запуска. 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**.

ML-модели могут быть созданы специалистами "Лаборатории Касперского" или сертифицированным интегратором в рамках *Услуги построения модели и внедрения Kaspersky MLAD*. Для использования таких ML-моделей требуется загрузить их в Kaspersky MLAD. Вы также можете самостоятельно создавать ML-модели и добавлять в них нужные элементы с помощью конструктора моделей.

ML-модель может включать в себя следующие элементы, работающие параллельно:

- Элемент на основе нейронной сети;
- Элемент на основе диагностического правила.

В Kaspersky MLAD ML-модели может быть присвоен один из следующих статусов:

- *Не активирована* – ML-модель импортирована, но не активирована.
- *Черновик* – ML-модель активирована или ML-создана вручную и в составе этой модели есть необученные нейросетевые элементы.
- *Обучена* – Все элементы в составе ML-модели обучены. Для обученной ML-модели может быть запущен инференс.
- *Готова к публикации* – ML-модель подготовлена к публикации и недоступна для изменений.
- *Опубликована* – ML-модель опубликована. Для опубликованной ML-модели может быть запущен инференс.

Элемент ML-модели на основе нейронной сети

Наиболее распространенным типом ML-моделей является нейронная сеть, которая предсказывает поведение объекта на основе данных о его поведении в ближайшем прошлом. В основе этой ML-модели лежит детектор Forecaster.

Если отличие предсказания модели от фактически наблюдаемых значений превышает определенный порог, то детектор Forecaster считает, что обнаружил отклонение в поведении объекта мониторинга и регистрирует инцидент. Суммарный показатель отличия предсказанных значений от фактических (суммарная ошибка прогноза) в пользовательском интерфейсе условно обозначается *MSE* (*mean squared error*).

График значений MSE и порог MSE, при превышении которого детектор Forecaster регистрирует инцидент, выводятся в разделах **Мониторинг** и **История** под графиками тегов. Если в ML-модели содержится несколько элементов, вы можете выбрать элемент модели для просмотра значений MSE, рассчитанных этим элементом.

Конструктор моделей Kaspersky MLAD поддерживает следующие архитектуры нейронной сети для элементов ML-модели:

- *Dense*. Элемент ML-модели с полносвязной архитектурой. При создании элемента ML-модели указывается множители для вычисления количества нейронов на внутренних слоях и функции активации на них.
- *TCN*. Элемент ML-модели с иерархической по времени сверточной архитектурой. При создании элемента ML-модели указывается функция активации, размер фильтров, расширения на слоях и количество кодирующих блоков.
- *CNN*. Элемент ML-модели со сверточной архитектурой. При создании элемента ML-модели указывается количество сверточных слоев, размер и количество фильтров на слоях и размер окна выборки максимума (MaxPooling).
- *RNN*. 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*. Элемент ML-модели с архитектурой Transformer. При создании элемента ML-модели указывается количество голов внимания и количество кодирующих блоков Transformer.

Элемент 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. В основе диагностических правил лежит детектор Rule Detector.

Диагностические правила формулируются предметными экспертами и реализуются специалистами "Лаборатории Касперского" или сертифицированным интегратором в виде сериализованной структуры правила в виде JSON-файла. Вы также можете сформулировать диагностические правила самостоятельно с помощью конструктора моделей.

Примеры диагностических правил:

- значение тега A не меняется в течение минуты;
- 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.

Шаблоны 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 добавить 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.

Разметки

Разметка – это набор интервалов времени, заданных для тегов по определенным правилам. 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.

Разметка является функциональным элементом иерархической структуры. Разметки могут быть импортированы в Kaspersky MLAD вместе с ML-моделью или создана вручную.

Инциденты

Инцидент – это обнаруженное детектором аномалий отклонение от ожидаемого (нормального) поведения объекта мониторинга.

Kaspersky MLAD поддерживает несколько типов детекторов аномалий: Forecaster, Rule Detector, Limit Detector. Детектор Forecaster лежит в основе нейросетевых элементов ML-модели, в свою очередь детектор Rule Detector лежит в основе диагностических правил. Каждый детектор анализирует поступающие от объекта мониторинга данные телеметрии на предмет отклонений от нормального поведения объекта.

Кроме выявления отклонений от нормального поведения объекта Kaspersky MLAD контролирует качество поступающих данных. В случае прекращения или прерывания входного потока данных для определенного тега или обнаружения во входном потоке наблюдений, поступивших в программу слишком рано или поздно, служба Stream Processor регистрирует инциденты.

При обнаружении отклонения соответствующий детектор фиксирует дату, время, релевантные параметры отклонения и сохраняет их в виде записи в разделе **Инциденты**. Если в Kaspersky MLAD для пользователей или внешних систем настроены уведомления об инцидентах, то информация об инциденте отправляется адресатам через соответствующие службы Kaspersky MLAD.

Инциденты, обнаруженные нейросетевым элементом ML-модели

Нейросетевой элемент ML-модели, в основе которого лежит детектор *Forecaster*, обучен на определенном подмножестве тегов и может предсказывать поведение тегов в текущий момент. Инцидентом в этом случае считается существенное расхождение между наблюдаемыми (фактическими) значениями тегов и предсказанными значениями тегов, полученными в результате работы элемента ML-модели. В параметрах элемента модели вы можете просмотреть, какие теги анализируются нейронной сетью (параметр **Входные теги**) и поведение каких тегов предсказывается (параметр **Выходные теги**).

ML-модель, построенная на основе детектора Forecaster, состоит из одного или нескольких элементов ML-модели, функционирующих параллельно. В разделах **История** и **Мониторинг** вы можете выбрать определенную ветку ML-модели для отображения на графиках MSE инцидентов, зарегистрированных в результате работы определенного элемента модели. Зарегистрированные инциденты отображаются в нижней части графика MSE в виде цветных точек-индикаторов.

На графике MSE также отображаются предсказанные значения тегов и ошибки MSE для выбранного элемента ML-модели. *Ошибка MSE* – это показатель отличия предсказанных значений от фактических, суммарно по всем тегам, включенным в выбранный элемент ML-модели. Чем выше значение MSE, тем сильнее поведение тегов отличается от ожидаемого (нормального). *Порог MSE* – это критический уровень значения MSE, при превышении которого детектор Forecaster регистрирует инцидент. Порог MSE на графике MSE отображается в виде оранжевой линии.

График MSE отображается в нижней части раздела **История** (см. рисунок ниже).

График MSE в разделе **История**

Для каждого инцидента автоматически определяются теги, поведение которых сильнее повлияло на регистрацию инцидента. Из этих тегов формируется пресет Tags for event #N, который доступен для выбора в разделе **История**. Теги в составе пресета Tags for event #N отсортированы в порядке убывания отклонения их поведения от ожидаемого. Первый, наиболее аномальный тег также выводится в таблице инцидентов в разделе **Инциденты**. В таблице инцидентов также указывается порог ошибки MSE и фактическое значение ошибки MSE в момент регистрации инцидента.

Информация, полученная при просмотре пресета Tags for event #N, 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 пресете Tags for event #N 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 пресет Tags for event #N.
- 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.

Инциденты, обнаруженные элементом ML-модели на основе диагностического правила

Элемент ML-модели на основе диагностического правила состоит из одного или несколько диагностических правил. В основе этого элемента лежит детектор Rule Detector. Результатом работы каждого диагностического правила является получение следующих значений, которые вычисляются в каждый момент времени:

- Значение `0`. Диагностическое правило в текущий момент не сработало или не применимо.
- Значение `1`. Диагностическое правило в текущий момент сработало.
- В отдельных случаях возможны промежуточные значения от `0` до `1`. Диагностическое правило в текущий момент сработало частично.

В момент, когда полученное значение достигает установленного для диагностического правила порога (как правило, равного единице), детектор Rule Detector регистрирует инцидент. Для каждого инцидента, зарегистрированного детектором Rule Detector автоматически формируется пресет Tags for event #N, который доступен для выбора в разделе **История**. В составе этого пресета присутствует значение, полученное в результате работы диагностического правила, а также теги, входящие в состав этого правила.

Для отображения графиков значений, полученных в результате работы диагностических правил, вы можете включить отображение предсказанных значений тегов в разделе **История**.

Инциденты, обнаруженные 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 при изменении тега.

Для визуального контроля положения графика тега относительно порогов блокировки включите функцию Всегда показывать пороги блокировки. Если эта функция 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. Для каждого инцидента, зарегистрированного детектором Limit Detector автоматически формируется пресет Tags for event #N, который доступен для выбора в разделе **История**. В состав этого пресета включается единственный тег-причина возникновения инцидента.

Инциденты, обнаруженные 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 и 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:

- **Сбой часов** – в случае обнаружения наблюдений, поступивших в Kaspersky MLAD слишком рано.
- **Позднее поступление наблюдения** – в случае обнаружения наблюдений, поступивших в Kaspersky MLAD поздно.
- **Нет данных** – в случае прекращения или прерывания входного потока данных определенного тега.

Служба Stream Processor передает данные, приведенные к РИВС, в ML-модель службы Anomaly Detector.

Аномалии

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 оператора объекта мониторинга.
- **Инцидент не является аномалией, это ложно-положительное срабатывание детектора**.

  При устойчивом повторном ложно-положительном срабатываниях детектора нужно определить причину ухудшения качества работы используемого в ML-модели детектора, провести дополнительную настройку или дополнительное обучение ML-модели. Дополнительную настройку детектора или дополнительное обучение ML-модели осуществляют специалисты "Лаборатории Касперского" в рамках *Услуги построения модели и внедрения Kaspersky MLAD*.

- **Используемый в ML-модели детектор отработал корректно, но инцидент не является аномалией**.

  Инцидент является следствием временного перевода объекта мониторинга в нетипичный режим функционирования (профилактика, испытания) или кратковременного влияния нетипичных внешних факторов (необычные погодные условия, запуск соседней установки). В такой ситуации ответных действий со стороны оператора объекта мониторинга 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.

Используемый в ML-модели детектор 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, оператора или сторонних источников станет известно о неоднократных фактах отсутствия срабатывания детектора, необходимо определить причину ухудшения качества работы детектора и провести дополнительную настройку или дополнительное обучение ML-модели. Дополнительное обучение ML-модели могут выполнять только специалисты "Лаборатории Касперского" или сертифицированные интеграторы.

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.

Процессор событий

Процессор событий в составе Kaspersky MLAD предназначен для выявления в потоке событий, поступающих от объектов мониторинга и от службы Anomaly Detector, 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.

События

Служба Event Processor обрабатывает данные, поступающие от объектов мониторинга и от службы Anomaly Detector, в виде событий. *Событие* – это набор значений, описывающих изменение состояния объекта мониторинга по заранее заданному перечню параметров, с указанием момента времени, когда произошло изменение. Набор параметров событий зависит от объекта мониторинга и задается в конфигурационном файле для службы Event Processor.

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 данных от службы Anomaly Detector 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 просмотреть 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.

Паттерны

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. 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.

Направления внимания

Поток событий, поступающих от объекта мониторинга, как правило, содержит множество несвязанных между собой событий. Служба Event Processor поддерживает механизм направлений 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 (направлениям внимания). Направление внимания определяется значением параметра событий, которое должно присутствовать во всех событиях этого направления. Процессор событий будет выявлять события и паттерны только по тем направлениям внимания, которые задаются в конфигурации внимания.

Вы можете настроить направления внимания в разделе **Процессор событий**.

Режимы 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 в основном режиме (количество событий)** службы Event Processor.

  По полученному в потоке событий эпизоду служба Event Processor выявляет новые и/или повторяющиеся (стабильные) события и паттерны по каждому из заданных направлений внимания. Вы можете настроить направления внимания 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.

Мониторы

Монитор – источник извещений о выявлении процессором событий паттернов, событий или значений параметров событий в соответствии с заданными критериями мониторинга. Критерии мониторинга определяют скользящий временной интервал, число последовательных обнаружений, фильтры для значения параметров событий, а также условие для обнаружения новых событий, паттернов или значений параметров событий.

Вы можете создать 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 указать в параметре события **Пользователь** имя пользователя, действия которого вы хотите отслеживать.

- **Паттерны**. Вы можете создать монитор для оповещения о выявлении новых или ранее встречавшихся паттернов по определенному направлению внимания. 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.

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**) за последние пять минут (значение скользящего временного интервала).

При обнаружении в потоке поступающих данных событий, паттернов или 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**.

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.

Доступ к отдельным службам и коннекторам программы не предусмотрен.

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, которую создается для конкретного объекта защиты на основе алгоритмов машинного обучения и/или диагностических правил с использованием данных телеметрии этого объекта. ML-модель обеспечивает обнаружение инцидентов.

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

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*. Приводит данные телеметрии, поступающие от объекта мониторинга в произвольные моменты реального времени, к равноинтервальной временной сетке.
- *Trainer*. Выполняет повторное или дополнительное обучение уже имеющейся ML-модели на основе новых 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, предсказываемых ML-моделью значений тегов и ошибок предсказания.
- *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 логов работы Kaspersky MLAD.
- *Mail Notifier*. Выполняет рассылку по электронной почте уведомлений о регистрации инцидентов.

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.
- *OPC UA Connector*. Обеспечивает получение тегов от систем АСУ ТП по протоколу, который описан спецификацией OPC Unified Architecture (Унифицированная архитектура OPC).
- *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 протокола HTTP.

На рисунке ниже представлена схема взаимодействия служб Kaspersky MLAD.

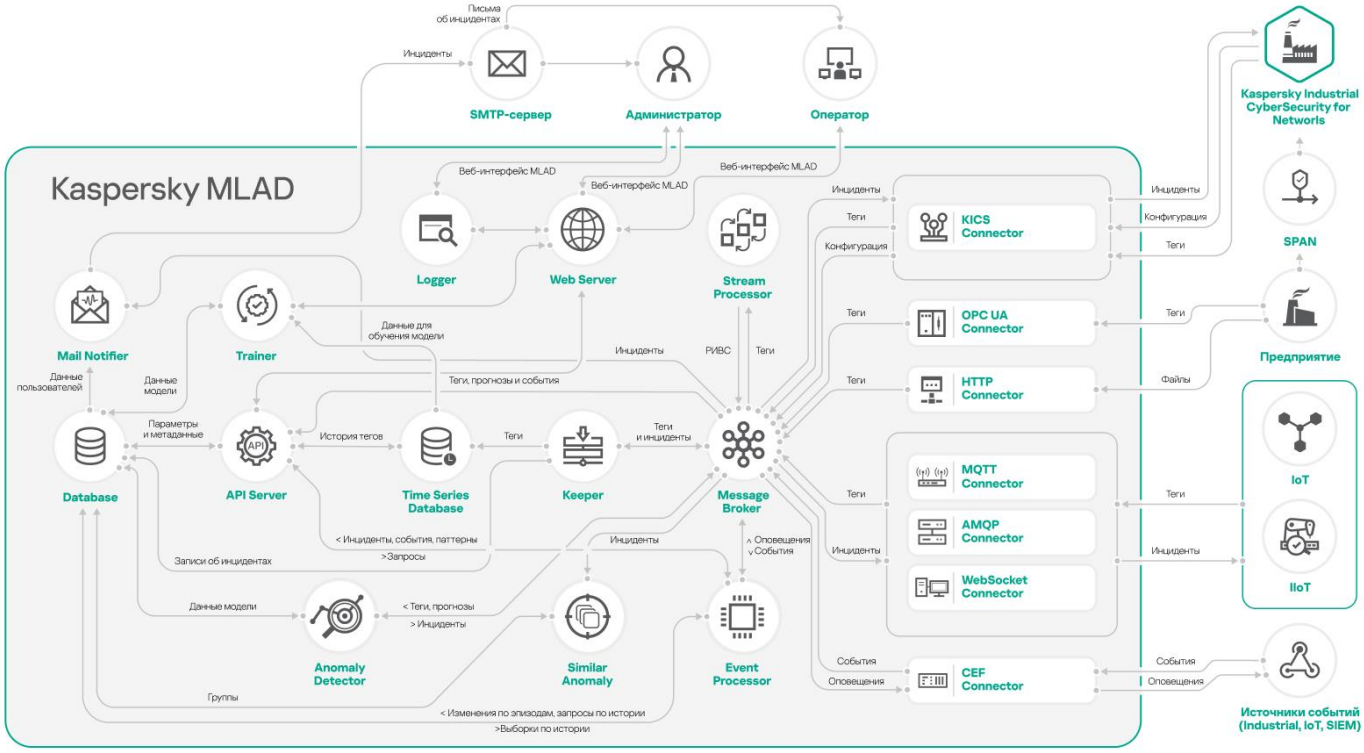


Схема взаимодействия служб Kaspersky MLAD

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:

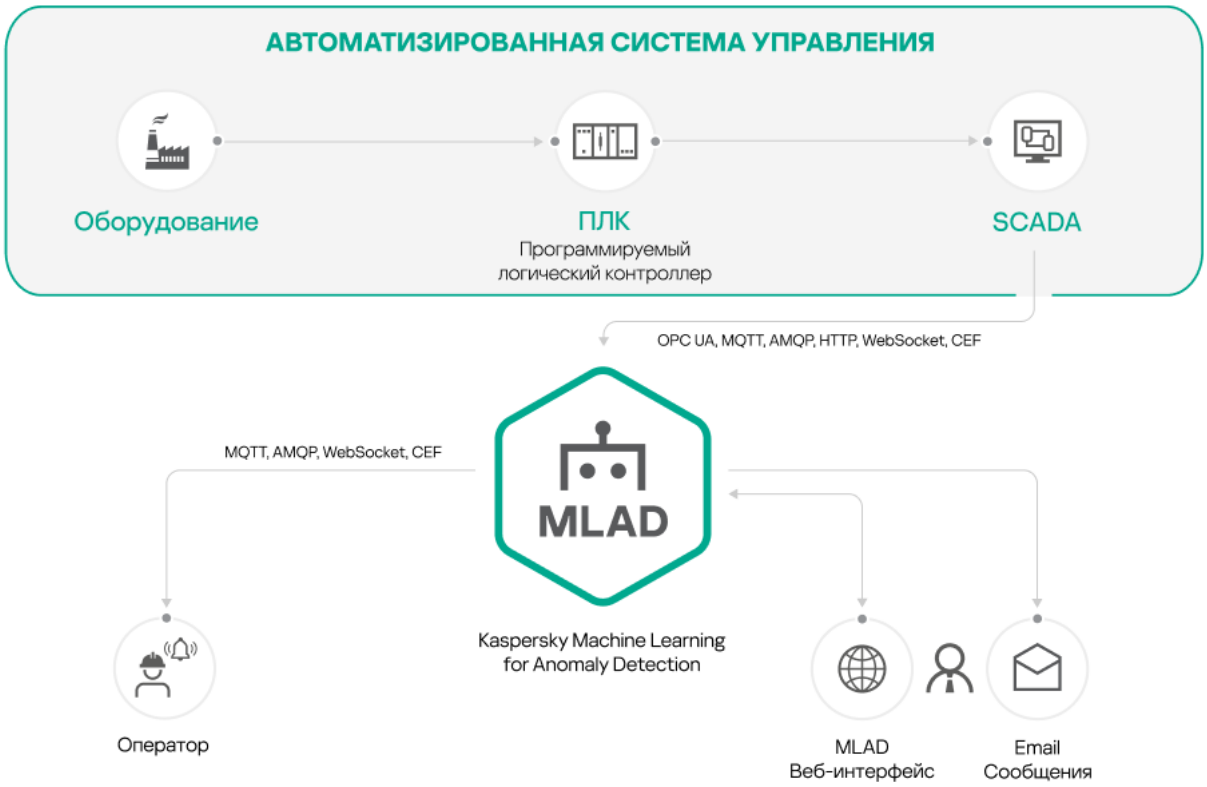
- Одиночная установка.
- Установка с Kaspersky Industrial CyberSecurity for Networks версии 4.0 и выше.

Одиночная установка Kaspersky MLAD

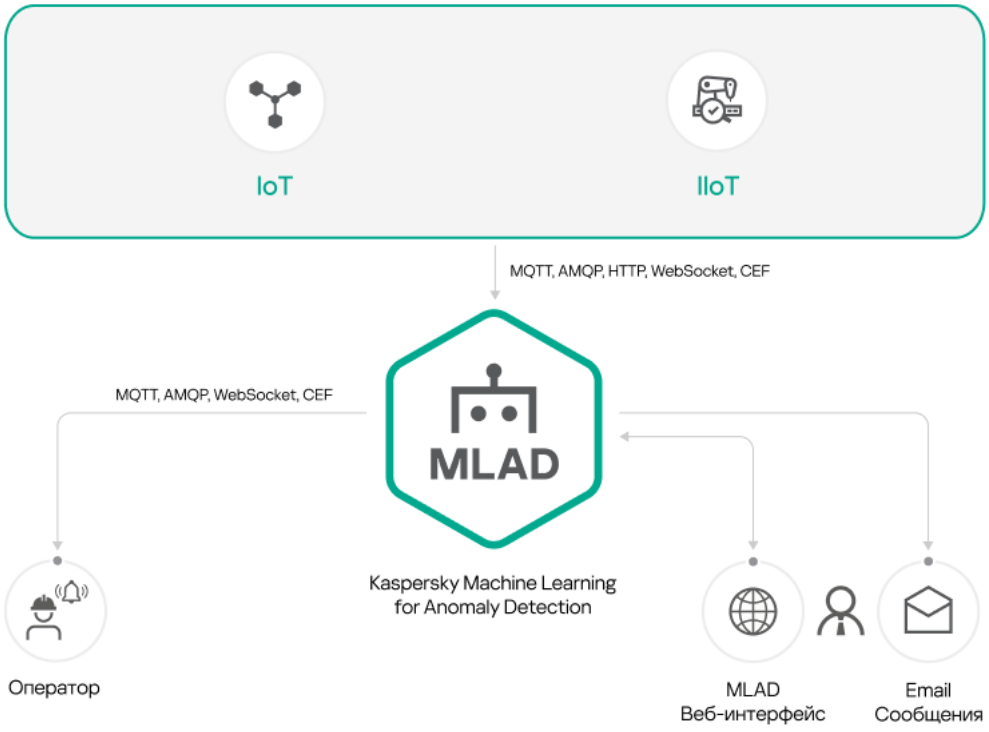
Вы можете установить только Kaspersky MLAD, если планируете использовать в качестве поставщика данных следующие коннекторы:

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

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



Одиночная установка Kaspersky MLAD с использованием коннекторов: OPC UA Connector, MQTT Connector, AMQP Connector, HTTP Connector, WebSocket 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. Для получения данных телеметрии (тегов) и/или событий от внешних систем требуется настроить коннекторы HTTP Connector, MQTT Connector, AMQP Connector, OPC UA Connector, KICS Connector, CEF Connector и WebSocket Connector.

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 потери данных телеметрии и 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 детекторы в основе ML-модели обнаруживают отклонения от нормального поведения объекта мониторинга, то служба Anomaly Detector регистрирует инциденты. При обнаружении схожих инцидентов служба Similar Anomaly формирует группы инцидентов.

Вы можете просмотреть зарегистрированные инциденты и группы инцидентов в разделе **Инциденты**. Kaspersky MLAD также отправляет уведомления об инцидентах на заданные адреса электронной почты 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, а также новые события и паттерны. При активации мониторов служба Event Processor также отправляет оповещения о выявлении событий, паттернов и значений параметров событий 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 логирования (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.

Установка программы

Этот раздел содержит пошаговое описание установки Kaspersky MLAD. При установке Kaspersky MLAD создает первого пользователя программы с ролью системного администратора.

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

На сервере Kaspersky MLAD должно быть установлено только то программное обеспечение, которое указано в аппаратных и программных требованиях.

Установка Kaspersky MLAD выполняется в соответствии с описанной процедурой установки программы. Установка и использование Kaspersky MLAD возможны только на одном сервере. Установка и использование разных служб и коннекторов на нескольких серверах невозможны.

Чтобы установить Kaspersky MLAD:

1. Распакуйте архив Kaspersky_MLAD_4.0.2.<номер сборки>_ru-RU_en-US.tar.xz, входящий в состав комплекта поставки:

   ```
   tar xf Kaspersky_MLAD_4.0.2.<номер сборки>_ru-RU_en-US.tar.xz
   ```

2. Перейдите в директорию mlad-release-4.0.2-<номер сборки>:

   ```
   cd mlad-release-4.0.2-<номер сборки>
   ```

3. Запустите скрипт установки setup.sh:

   ```
   sudo ./setup.sh
   ```

4. Следуйте указаниям мастера установки программы.

   С помощью мастера установки программы вы можете изменить имя и пароль первого пользователя программы с ролью системного администратора.

Чтобы установить Kaspersky MLAD в неинтерактивном режиме:

1. Распакуйте архив Kaspersky_MLAD_4.0.2.<номер сборки>_ru-RU_en-US.tar.xz, входящий в состав комплекта поставки:

   ```
   tar xf Kaspersky_MLAD_4.0.2.<номер сборки>_ru-RU_en-US.tar.xz
   ```

2. Перейдите в директорию mlad-release-4.0.2-<номер сборки>:

   ```
   cd mlad-release-4.0.2-<номер сборки>
   ```

3. Запустите скрипт установки setup.sh со следующими ключами:

   ```
   sudo ./setup.sh -q -e accept
   ```

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 имя пользователя и пароль по умолчанию. Для получения имени 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.

Программа будет установлена на компьютер. После установки программы запустите ее.

Обновление программы

Этот раздел содержит пошаговое описание обновления Kaspersky MLAD.

Обновление Kaspersky MLAD возможно, начиная с версии программы 4.0.1-001. 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.

На сервере Kaspersky MLAD должно быть установлено только то программное обеспечение, которое указано в аппаратных и программных требованиях.

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.

Чтобы обновить Kaspersky MLAD из командной строки:

1. Распакуйте архив mlad-4.0.2-<номер новой сборки>.tar.xz, входящий в состав комплекта поставки:

   `tar xf mlad-4.0.2-<номер новой сборки>.tar.xz`

2. Перейдите в директорию, в которой вы распаковали Kaspersky MLAD:

   `cd mlad-4.0.2-<номер новой сборки>`

3. Запустите скрипт обновления программы upgrade.sh:

   `sudo ./upgrade.sh -u -f <полный путь к файлу release.txt обновляемой сборки программы>`

   Вы можете запустить скрипт upgrade.sh с ключом `-h`, если требуется вызвать помощника в интерфейсе обновления Kaspersky MLAD:

   `sudo ./upgrade.sh -h`

4. Следуйте указаниям мастера 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 – mlad-release-4.0.2-<номер установочной сборки>). Там же будет создана директория с именем upgrade_backup-4.0.2-<номер предыдущей сборки>, которая содержит резервную копию предыдущей версии Kaspersky MLAD.

Вы можете переместить директорию с резервной копией программы в другое место хранения в соответствии с регламентом вашего предприятия.

Резервное копирование программы

Вы можете выполнять резервное копирование программы в соответствии с регламентом вашего предприятия. Kaspersky MLAD также автоматически создает резервную копию при обновлении программы.

Резервное копирование программы выполняется с помощью скрипта обновления upgrade.sh.

Резервное копирование Kaspersky MLAD возможно, начиная с версии программы 4.0.1-001. При резервном копировании Kaspersky MLAD будут сохранены все данные, загруженные, полученные и обработанные Kaspersky MLAD: конфигурации тегов, пресеты, ML-модели и параметры Kaspersky MLAD.

Чтобы выполнить резервное копирование Kaspersky MLAD из командной строки:

1. Перейдите в директорию, в которой установлен Kaspersky MLAD:

   ```
   cd mlad-release-4.0.2-<номер сборки>
   ```

2. Для выполнения резервного копирования программы запустите скрипт обновления upgrade.sh с ключом `-b`:

   ```
   sudo ./upgrade.sh -b
   ```

В директории, в которой установлен Kaspersky MLAD (по умолчанию – mlad-release-4.0.2-<номер сборки>), будет создана директория backup-4.0.2-<дата и время резервного копирования>, в которой будут храниться все файлы резервной копии программы.

Вы можете переместить директорию с резервной копией программы в другое место хранения в соответствии с регламентом вашего предприятия.

Откат программы к предыдущей установленной версии

Этот раздел содержит пошаговое описание отката программы к предыдущей установленной версии с помощью скрипта обновления upgrade.sh.

Откат Kaspersky MLAD возможен, начиная с версии программы 4.0.1-001.

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. Перейдите в одну из следующих директорий, в которой находится резервная копия Kaspersky MLAD, до которой требуется выполнить откат программы:

   - upgrade_backup-4.0.2-<номер сборки> – директория, в которой хранится версия программы, созданная автоматически при обновлении программы. Для перехода в директорию выполните команду:

     ```
     cd upgrade_backup-4.0.2-<номер предыдущей сборки>
     ```

   - backup-4.0.2-<дата и время резервного копирования> – директория, в которой хранится версия программы, созданная при выполнении резервного копирования программы. Для перехода в директорию выполните команду:

     ```
     cd backup-4.0.2-<дата и время резервного копирования>
     ```

     При откате программы к предыдущей версии директория backup-4.0.2-<дата и время резервного копирования> должна находиться в директории, в которой установлен Kaspersky MLAD (по умолчанию – mlad-release-4.0.2-<номер сборки>).

2. Для отката программы к предыдущей версии запустите скрипт обновления программы upgrade.sh с ключом `-r`:

   ```
   sudo ./upgrade.sh -r
   ```

3. Следуйте указаниям мастера обновления программы.

Будет выполнен откат Kaspersky MLAD к предыдущей установленной версии.

Сценарий восстановления Kaspersky MLAD из резервной копии

В случае неисправности сервера, на котором установлен Kaspersky MLAD, вы можете восстановить программу на другом сервере из резервной копии Kaspersky MLAD с помощью скрипта обновления upgrade.sh.

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

1. **Установка Kaspersky MLAD**

   Установите на сервер ту же версию Kaspersky MLAD, для которой выполнялось резервное копирование.

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

   Переместите директорию с резервной копией программы в директорию, в которой установлен Kaspersky MLAD (по умолчанию – mlad-release-4.0.2-<номер установочной сборки>).

3. **Восстановление Kaspersky MLAD**

   Перейдите в директорию, в которой находится резервная копия Kaspersky MLAD, с помощью команды:

```
cd <директория с резервной копией программы>
```

Для восстановления программы из резервной копии запустите скрипт обновления программы upgrade.sh с ключом `-r`:

```
sudo ./upgrade.sh -r
```

Следуйте указаниям мастера обновления программы.

Подготовка к работе

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

1. Источник данных телеметрии включен и настроен на отправку данных в Kaspersky MLAD.
2. Сеть передачи данных подготовлена для доставки данных телеметрии от источника данных к серверу Kaspersky MLAD, сетевое оборудование надлежащим образом настроено, передача данных разрешена.
3. Подготовлены конфигурационные параметры и/или файлы того коннектора, который будет использован в Kaspersky MLAD для приема данных телеметрии или событий от внешних систем. Коннектор должен быть настроен и активирован после запуска Kaspersky MLAD.
4. Описания тегов принимаемой телеметрии и активов иерархической структуры подготовлены для импорта в Kaspersky MLAD в виде файла формата XLSX. Описания пресетов подготовлены в виде файла в формате JSON. Файлы создаются квалифицированным техническим специалистом Заказчика, специалистом "Лаборатории Касперского" или сертифицированным интегратором.
5. ML-модель или несколько ML-моделей созданы, обучены на исторических данных телеметрии. ML-модели подготовлены для импорта в Kaspersky MLAD в виде файлов формата TAR, если файлы созданы специалистом "Лаборатории Касперского" или сертифицированным интегратором в рамках *Услуги построения модели и внедрения Kaspersky MLAD*.
6. Системному администратору Kaspersky MLAD переданы коды для активации ML-моделей. Коды для активации ML-моделей хранятся в надежном хранилище.

Запуск и остановка Kaspersky MLAD

Чтобы запустить остановленную программу:

1. Перейдите в директорию, в которой установлен Kaspersky MLAD (по умолчанию – mlad-release-4.0.2-<номер установочной сборки>).
2. В командной строке выполните команду:

   ```
   ./mlad-start.sh
   ```

Kaspersky MLAD будет запущен.

Чтобы остановить программу:

1. Перейдите в директорию, в которой установлен Kaspersky MLAD (по умолчанию – mlad-release-4.0.2-<номер установочной сборки>).

2. В командной стоке выполните команду:

   ```
   ./mlad-stop.sh
   ```

   Kaspersky MLAD будет остановлен.

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.

Рекомендуется 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.

По умолчанию Kaspersky MLAD использует директорию mlad-4.0.2-<номер установочной сборки>/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> mlad-4.0.2-<номер установочной
сборки>/ssl/nginx/mlad_nginx.crt
sudo cp <ключ к новому сертификату.key> mlad-4.0.2-<номер установочной
сборки>/ssl/nginx/mlad_nginx.key
```

Новый сертификат и его ключ будут сохранены в директории mlad-4.0.2-<номер установочной сборки>/ssl/nginx/ в виде файлов mlad_nginx.crt и mlad_nginx.key соответственно.

4. Перезапустите Kaspersky MLAD, выполнив в командной строке следующие команды:

```
mlad-4.0.2-<номер установочной сборки>/mlad-stop.sh
mlad-4.0.2-<номер установочной сборки>/mlad-start.sh
```

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 MQTT Connector, AMQP Connector и WebSocket Connector, а также службы Mail Notifier. Вы можете обновлять сертификаты для подключения этих коннекторов и службы Mail Notifier по защищенному соединению в разделе **Системные параметры** в меню администратора.

Для подключения коннекторов MQTT Connector, AMQP Connector и WebSocket Connector, а также службы 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. **Запуск Kaspersky MLAD**

   Запустите Kaspersky MLAD. Будут запущены следующие службы, необходимые для работы Kaspersky MLAD:

   - API Server.
   - Web Server.

- Message Broker.
- Keeper.
- Time Series Database.
- Database.
- Logger.

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

   Откройте веб-интерфейс программы в поддерживаемом браузере и введите имя 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 установите доверенный сертификат.

3. **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 корректного обнаружения аномалий должна быть запущена служба *Anomaly Detector*.

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

   Конфигурация тегов, активов и пресетов создается в процессе выполнения работ по внедрению программы и построению ML-модели специалистом "Лаборатории Касперского" или интегратором. Конфигурация тегов и активов описывается в файле в формате XLSX. Конфигурация пресетов описывается в файле в формате JSON. Примеры описания конфигурации тегов и активов, а также конфигурации пресетов см. в Приложении.

   Для дальнейшей работы загрузите конфигурацию тегов и активов в Kaspersky MLAD. Загрузите конфигурацию пресетов или создайте новые пресеты из тегов.

5. **Загрузка и создание ML-моделей**

   > ML-модель не входит в комплект поставки программы и предоставляется в рамках *Услуги построения модели и внедрения Kaspersky MLAD*.

   Загрузите ML-модель, если она была предоставлена в рамках *Услуги построения модели и внедрения Kaspersky MLAD*, или создайте ее самостоятельно с помощью конструктора моделей. Активируйте загруженную ML-модель. Для активации ML-модели требуется ввести код для активации модели.

6. **Настройка коннекторов**

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

   - KICS Connector.
   - OPC UA Connector.
   - CEF Connector.
   - HTTP Connector.
   - MQTT Connector.

- AMQP Connector.
- WebSocket Connector.

7. **Подключение к источнику данных**

   Когда вышеперечисленные коннекторы настроены, запустите коннекторы, используемые для вашего объекта мониторинга. Перейдите в раздел **Информационная панель** и убедитесь, что данные поступают в Kaspersky MLAD в онлайн-режиме.

8. **Настройка конфигурации внимания**

   Для работы с событиями и паттернами настройте параметры конфигурации внимания и отображение параметров событий. Служба Event Processor будет выявлять события и паттерны только по тем направлениям внимания, которые задаются в конфигурации внимания.

9. **Создание учетных записей для пользователей**

   Создайте учетные записи для пользователей программы и назначьте им необходимые роли. Настройте 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. Рекомендуется проверить наличие полной резервной копии всех данных Kaspersky MLAD. При обновлении программы Kaspersky MLAD автоматически создает резервную копию предыдущей версии программы. Вы также можете выполнить резервное копирование программы вручную.

Чтобы удалить Kaspersky MLAD:

1. Перейдите в директорию, в которой установлен Kaspersky MLAD (по умолчанию – mlad-release-4.0.2-<номер установочной сборки>):

   ```
   cd mlad-release-4.0.2-<номер сборки>
   ```

2. Запустите скрипт установки setup.sh с ключом -u:

   ```
   sudo ./setup.sh -u
   ```

3. Подтвердите удаление служб Kaspersky MLAD.

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:

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

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

Системным администраторам доступно меню, предоставляющее возможность настраивать параметры программы, управлять учетными записями пользователей, настраивать уведомления об инцидентах, управлять тегами, а также переходить на страницу системы логирования для просмотра логов.

В нижней части основного меню и меню администратора доступно меню пользователя, предоставляющее возможность выбрать язык веб-интерфейса, изменить пароль своей учетной записи, выйти из своей учетной записи, а также переходить между меню. Переход 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 верхнем левом 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 инцидентах, службах и их статусах.
Мониторинг	Открывает раздел, в котором отображаются данные, поступающие в систему в реальном времени. Вы также можете настраивать параметры отображения поступающих данных на графике.
История	Открывает раздел, который содержит полную историю поступивших в систему данных и результаты их анализа ML-моделями. Вы также можете настраивать параметры отображения исторических данных на графике.
Временной срез	Открывает раздел, который содержит информацию о значениях технологических параметров, полученных от датчиков в один и тот же момент времени. Вы также можете настраивать 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 обнаруженных инцидентов. В рамках анализа инцидентов вы также можете добавить статус, причину, экспертное заключение и замечание к инциденту или группе инцидентов.
Модели	Открывает раздел, который позволяет просмотреть информацию об используемых в системе ML-моделях и шаблонах ML-моделей, а также управлять ими. Управление ML-моделями и шаблонами ML-моделей доступно только системным администраторам.
Пресеты	Открывает раздел, в котором вы можете просматривать информацию о доступных пресетах, изменять их параметры, а также создавать пресеты.
Службы	Открывает раздел, который позволяет просмотреть информацию о службах и их статусах, а также запускать, останавливать и перезапускать службы. Управление статусами служб доступно только системным администраторам.

Меню администратора

В таблице ниже описаны разделы меню администратора Kaspersky MLAD.

Разделы меню администратора

Раздел	Описание
Пользователи	Открывает раздел, в котором вы можете управлять учетными записями пользователей.
Роли	Открывает раздел, который содержит информацию о доступных ролях пользователей.
Права	Открывает раздел, который содержит информацию о правах пользователей.
Уведомления	Открывает раздел, в котором вы можете управлять уведомлениями, которые программа отправляет пользователям при регистрации инцидентов.
Системные параметры	Открывает раздел, в котором вы можете управлять параметрами служб Kaspersky MLAD.
Активы	Открывает раздел, в котором вы можете управлять 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 страницу с краткой информацией о программе.
	Осуществляет переход в систему логирования (Grafana™) в новой вкладке браузера. Этот раздел доступен только системным администраторам.
	Осуществляет переход в меню администратора из основного меню. В меню администратора вы можете управлять учетными данными пользователей, просматривать их

	роли и права, а также настраивать уведомления об инцидентах и управлять тегами. Меню администратора доступно только системным администраторам.
	Осуществляет переход в основное меню из меню администратора. В основном меню вы можете просматривать исторические данные и данные, поступающие в реальном времени, просматривать зарегистрированные инциденты, события и паттерны, а также просматривать сведения о созданных ML-моделях.
	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.

При подключении пользователя к веб-интерфейсу Kaspersky MLAD внутри программы генерируется токен, время действия которого определяет максимальную продолжительность неактивной пользовательской сессии. В течение этого времени при активном использовании Kaspersky MLAD программа не запрашивает учетные данные пользователя, если для подключения используются те же компьютер, браузер и учетная запись. 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.

Если авторизованный пользователь не использует программу дольше, чем указано в параметре **Период неактивности пользователя (мин)**, то Kaspersky MLAD автоматически завершает сессию подключения для этого пользователя. Для завершения сессии подключения до истечения срока действия токена авторизованный пользователь может самостоятельно выйти 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, имя пользователя и пароль для входа в программу 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 имя пользователя и пароль.

   Если вы подключаетесь к веб-интерфейсу впервые, используйте указанные при установке программы имя и пароль первого пользователя с ролью системного администратора.
4. Нажмите на кнопку **Войти** или на клавишу **ENTER**.

   В окне браузера откроется **Информационная панель**.

   При первом подключении 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.

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

  Новый пароль должен удовлетворять следующим требованиям:

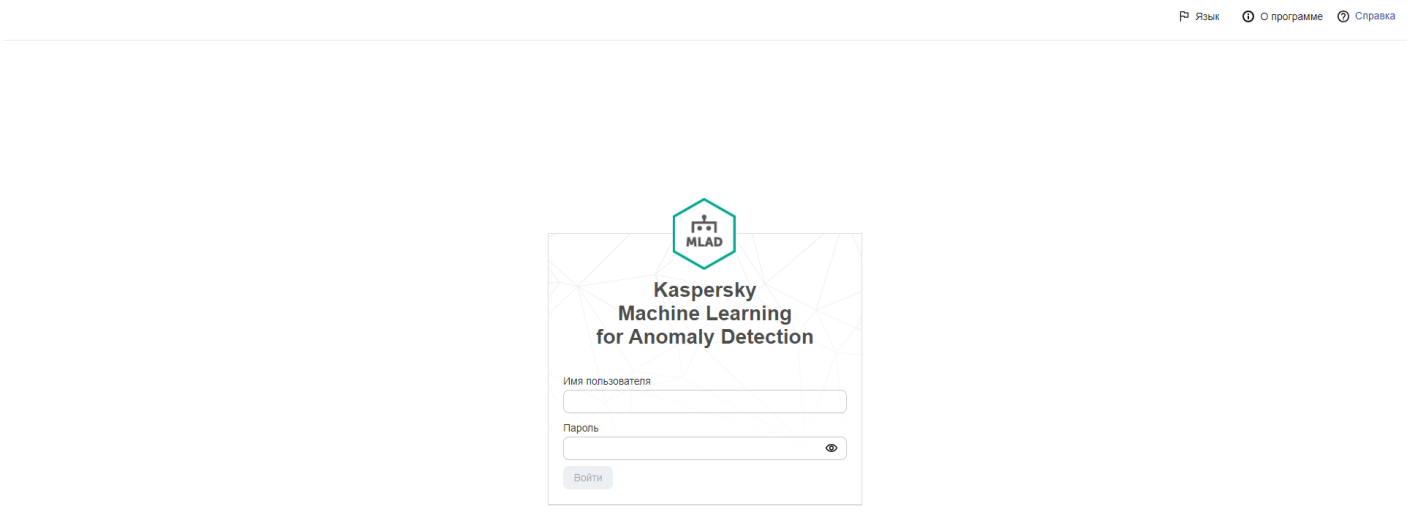
  - Не совпадает с предыдущими паролями. Количество ранее использованных паролей, с которыми новый пароль не должен совпадать, задается пользователем с ролью системного администратора.
  - Содержит минимальное количество символов, заданное администратором при настройке параметров безопасности.
  - Содержит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

- **Подтверждение пароля** – подтвердите пароль для учетной записи пользователя.

При истечении срока действия пароля, заданного при настройке параметров безопасности, в браузере также откроется окно изменения пароля.

Если вы закрыли окно браузера без завершения сессии подключения, сессия останется действующей до истечения времени, заданного 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 параметрах безопасности, Kaspersky MLAD завершает пользовательскую сессию.

В случае 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.



Страница ввода учетных данных 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 в меню администратора.
   - 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 локализации веб-интерфейса Kaspersky MLAD

В Kaspersky MLAD доступны английский и русский языки для веб-интерфейса программы.

Чтобы изменить язык локализации веб-интерфейса программы:

1. В левом нижнем углу страницы веб-интерфейса Kaspersky MLAD нажмите на кнопку **Язык**.
2. Выберите нужный язык локализации: 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.

Лицензия включает в себя право на использование программы в соответствии с условиями Лицензионного соглашения, а также на получение технической поддержки. Срок использования программы зависят от типа лицензии, по которой была приобретена программа.

Предусмотрены следующие типы лицензий:

- Base – для использования функциональности программы при первой покупке Kaspersky MLAD.
- Renewal – для использования функциональности программы при повторном приобретении Kaspersky MLAD.

Каждый тип лицензии может быть бессрочным или быть ограниченным по времени пользования в 1, 2 или 3 года. При приобретении лицензии на определенный срок рекомендуется продлевать срок действия лицензии после даты его окончания.

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:

- лицензионный ключ 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;
- тип лицензии.

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

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

- дата и время регистрации инцидента;
- имя ML-модели, зарегистрировавшей инцидент;
- имя топ-тега;
- описание топ-тега;
- значение топ-тега в момент регистрации инцидента;
- единицы измерения топ-тега;
- ссылка для перехода в раздел **История** в момент начала инцидента;
- идентификатор инцидента;
- имя детектора, зарегистрировавшего инцидент;
- значение суммарной среднеквадратичной ошибки MSE 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;
- дата и время регистрации инцидента;
- дата 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;
- ссылка для перехода в раздел **История** в момент начала инцидента;
- значение суммарной среднеквадратичной ошибки MSE 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);
- экспертное заключение (при наличии);
- идентификаторы релевантных тегов;
- причина инцидента (при наличии).

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

- имя поставщика программы;
- имя программы;
- версия Kaspersky MLAD;
- идентификатор подписи программы;
- дата и время регистрации инцидента;
- дата и время завершения инцидента;
- имя детектора, зарегистрировавшего инцидент;
- имя ML-модели, зарегистрировавшей инцидент;
- ссылка 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;
- имя программы;
- версия Kaspersky MLAD;
- идентификатор подписи программы;
- имя монитора, который зарегистрировал событие;
- идентификатор монитора;
- дата и время регистрации события;
- количество активаций на скользящем окне;
- тип элемента, который вызвал активацию монитора;
- информация, является ли зарегистрированное событие новым для программы;
- последние события или паттерны, которые активировали монитор;
- условие на фильтры для монитора;
- информация, активируется ли монитор только новыми событиями или паттернами.

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

- имя поставщика программы;
- имя программы;
- версия Kaspersky MLAD;
- идентификатор подписи программы;
- идентификатор события ИБ;
- дата 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:

- Информация 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.
- Информация 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.
- 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, фамилия, 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 в качестве имен пользователей при подключении пользователей к веб-интерфейсу программы. Имена 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, имя роли, состояние роли (активна или неактивна), список назначенных прав, дата и время создания роли, дата и время изменения роли.

  Данные о ролях вводит системный администратор в меню администратора.
- Данные об уведомлениях об инцидентах: идентификатор уведомления, адрес электронной почты для отправки уведомления, тип инцидента, пользователь, которому будет отправлено уведомление, состояние уведомления (активно или неактивно).

  Данные об уведомлениях вводит системный администратор в меню администратора.

- Данные о параметрах Kaspersky MLAD:

  - Основные параметры программы: имя объекта мониторинга, веб-адрес программы, IP-адрес для подключения к программе, 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, информация, является ли смена пароля при первом подключении обязательной, количество паролей пользователя, хранящихся в истории, срок действия пароля, минимальная длина пароля, информация, 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: информация, требуется ли использовать детекторы Limit Detector, Forecaster, XGBoost и/или Rule Detector, информация, требуется ли пропускать разрывы в данных, максимальное количество запрашиваемых записей из службы Message Broker, количество сообщений, отправляемых в одном блоке в службу Message Broker, количество одновременно запущенных ML-моделей.

  - Параметры службы Keeper: информация, требуется ли сохранять все теги, время ожидания получения тегов, инцидентов и метрик.

  - Параметры службы Mail Notifier: адрес и порт SMTP-сервера, имя пользователя и пароль для подключения к SMTP-серверу, информация, 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: периодичность равноинтервальной последовательности, 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 коннектора HTTP Connector: информация, требуется ли записывать данные в службу Message Broker, информация, требуется ли сохранять полученный файл, размер записываемого блока, максимальный размер загружаемого файла.

  - Параметры коннектора MQTT Connector: информация, требуется ли использовать TLS-соединение, адрес и порт MQTT-брокера, имя пользователя и пароль для подключения к MQTT-брокеру, корневой сертификат, сертификат клиентского приложения и ключ к сертификату клиентского приложения, список подписок MQTT для получения тегов, топик MQTT для публикации сообщений, формат обработки поступающих данных, конфигурационный файл коннектора, информация, 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: информация, требуется ли использовать TLS-соединение, адрес и порт AMQP-брокера, имя пользователя и пароль для подключения к AMQP-брокеру, корневой сертификат, сертификат клиентского приложения и ключ к сертификату клиентского приложения, виртуальный узел AMQP, имена точек обмена AMQP для получения тегов и для публикации сообщений, топик AMQP для публикации сообщений, формат обработки поступающих данных,

конфигурационный файл коннектора, информация, требуется ли масштабировать полученные значения тегов.

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

- Параметры коннектора OPC UA Connector: имя точки подключения, таймаут (время ожидания) подключения к серверу OPC UA, конфигурационный файл коннектора, интервал исторических данных, начало и окончание периода исторических данных, размер блока исторических данных, отправляемых сервером OPC UA, размер блока исторических данных, отправляемых в службу Message Broker.

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

- Параметры коннектора CEF Connector: информация, требуется ли получать события для службы Event Processor, информация, требуется ли отправлять зарегистрированные инциденты и/или события в SIEM-систему, IP-адрес и порт для отправки событий и инцидентов в SIEM-системы, информация, 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.

- Параметры коннектора WebSocket Connector: веб-адрес WebSocket-сервера, корневой сертификат, сертификат клиентского приложения и ключ к сертификату клиентского приложения, формат обработки поступающих данных, конфигурационный файл коннектора, информация, требуется ли масштабировать полученные значения тегов, информация, требуется ли отправлять инциденты.

- Параметры службы Event Processor: конфигурационный файл службы, информация, требуется ли обрабатывать инциденты как события, максимальное количество слоев сети, коэффициент, определяющий допустимую дисперсию длительности паттерна, интервал получения событий эпизода, размера эпизода в основном режиме, способ сохранения состояния службы Event Processor, периодичность создания резервных копия компонента, резервная копия состояния службы Event Processor, размер эпизода в режиме сна, режим отправки оповещений при активации монитора в режиме сна, периодичность и продолжительность режима сна, интервал истории событий для обработки в режиме сна.

- Параметры статуса инцидентов: идентификатор статуса инцидента, названия статуса инцидента на русском и английском языке, порядковый номер сортировки, информация, 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: информация, 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, значок актива, идентификатор родительского актива, описание и тип актива, идентификатор и имя типа актива, имена и значения специальных параметров типа актива, описание типа актива, идентификатор и имя тега, альтернативное

имя тега, значок тега, описание тега, тип тега, единица измерения тега, верхние и нижние пороги блокировки, сигнализации и достоверности измерений, верхняя и нижняя границы отображения тегов, выражение, по которому требуется рассчитать значение тега из значения, переданного в программу, 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, цвет дополнительных пороговых линий.

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

- Данные о пресетах: имя пресета, идентификатор пресета, значок пресета, имена и идентификаторы тегов, входящих в пресет, информация, требуется ли настроить выражение для раздела **Временной срез**, подписи осей абсцисс и ординат, имя 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**.

- Информация о количестве поступивших в секунду тегов и событий. Данные рассчитывает программа на основании данных, полученных от внешних систем.

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

- Информация о предсказанных значениях тегов, суммарной среднеквадратичной ошибки MSE и индивидуальной ошибке тегов. Данные рассчитывает программа на основании данных, полученных от внешних систем.

- Информация 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, дата и время регистрации инцидента, имя и идентификатор топ-тега, причина инцидента, название детектора, зарегистрировавшего инцидент, название группы инцидентов, статус инцидента, имя ML-модели, ветка ML-модели, значение суммарной среднеквадратичной ошибки MSE, пороговое значение суммарной среднеквадратичной ошибки MSE, значение топ-тега, пороги блокировки, описание и единицы измерения тега, тип инцидента, дата и время формирования наблюдения, время, на которое формирование наблюдения отстает от поступления этого наблюдения в программе или опережает его, экспертное заключение к инциденту и к группе, комментарий к инциденту, название и идентификатор группы инцидентов, количество инцидентов в группе, дата и время создания группы инцидентов, статус зарегистрированных инцидентов в группе, идентификаторы релевантных тегов, 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**: высота графиков, пресет для перехода в раздел **История** (только при настройке параметров отображения графика в разделе **Мониторинг**), информация, требуется ли отображать график наблюдений в выбранном цвете, цвет графиков наблюдений, информация, требуется ли отображать график предсказаний в выбранном цвете, цвет графиков предсказаний, информация, требуется ли отображать на графиках имена и описания тегов, предсказанное значение тега и/или персональную ошибку тега, информация, требуется ли отображать индикаторы для всех инцидентов на графиках, информация, требуется ли отображать на графиках пороги блокировки и/или дополнительные пороговые линии, ветка ML-модели, используемая для формирования предсказанных значений, пресеты, временные интервалы, дата и время для отображения графиков.

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

- Параметры отображения графиков в разделе **Временной срез**: высота графиков, ветка ML-модели, используемая для формирования предсказанных значений, пресеты, временные интервалы, дата и время для отображения графиков.

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

- Параметры обработки и отображения данных для процессора событий: параметры событий, по которым регистрируются паттерны (индивидуальны для каждого объекта мониторинга), информация, требуется ли регистрировать паттерны по шаблону (регулярному выражению), параметры шаблона (индивидуальны для каждого объекта мониторинга).

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

  - название детектора;
  - название используемой ML-модели;
  - имя и идентификатор топ-тега;
  - название 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: название и идентификатор монитора, количество зарегистрированных активаций на скользящем окне, дата и время последней активации, тип элемента, вызвавшей активацию монитора, параметр, определяющий что отслеживает монитор, скользящее окно, порог, названия параметров события, за значениями которых наблюдает монитор, типы значений, которые отслеживает монитор, параметры событий, на которых сфокусировано внимание модели, значения параметров события, за которыми наблюдает монитор, размер стека (упорядоченного во времени списка активаций монитора), идентификатор значения параметра события, обнаружение которого вызвало активацию монитора, идентификатор события, обнаружение которого вызвало активацию монитора, идентификатор паттерна, обнаружение которого вызвало активацию монитора, дата и время обнаружения события в потоке событий, временной интервал между текущим событием и предыдущим событием в поток событий на скользящем окне, количество повторений события в потоке событий на скользящем окне, дата и время последнего обнаружения события в потоке событий на скользящем окне, значения параметров события, поступившего об объекта мониторинга, количество событий, входящих в состав паттерна, который вызвал 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, дата и время последнего обнаружения паттерна на интервале, количество обнаружений паттерна в потоке событий объекта мониторинга за заданный период, количество событий в составе паттерна, дата и время последнего обнаружения паттерна в потоке событий или в режиме сна, дата и время начала и окончания периода загрузки паттернов, тип паттерна, направление внимания, значение параметра события, информация, требуется ли регистрировать паттерны по шаблону (регулярному выражению), параметры шаблона (индивидуальны для каждого объекта мониторинга), временной интервал между выбранный паттерном и паттернов, выявленным в последовательности паттернов на текущем слое до выбранного паттерна, общее количество активаций, дата и время окончания паттерна в последовательности паттернов на текущем слое, номер слоя паттерна, идентификаторы событий, входящих в состав паттерна, дата и время обнаружения события в структуре паттерна, количество параметров события, для которых поступили значения от объекта мониторинга.

  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, дата и время последнего изменения ML-модели, имя пользователя, который создал ML-

модель, дата и время создания или загрузки ML-модели, названия и идентификаторы входящих в нее элементов, интервал времени и разметки для проведения инференса.

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

- Информация об элементах ML-моделей и их параметрах:

  - Общие параметры для всех типов элементов ML-моделей: идентификатор, имя и описание элемента ML-модели, интервал времени, при достижении которого генерируется повторный инцидент, интервал времени, в течение которого не регистрируются повторные инциденты, шаг сетки в секундах, причина и статус инцидента, цвет точек-индикаторов для инцидентов, экспертное заключение.

  - Основные параметры нейросетевых элементов ML-моделей: архитектура элемента, имена и идентификаторы входных тегов, имена и идентификаторы выходных тегов, порог регистрации инцидентов, степенной показатель суммарной среднеквадратичной ошибки MSE, степень сглаживания суммарной среднеквадратичной ошибки MSE, 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, активации на слоях.

  - Параметры нейросетевого элемента с RNN-архитектурой: количество GRU-нейронов на слоях, количество распределенных по времени нейронов на слоях декодирующего блока.

  - Параметры нейросетевого элемента с CNN-архитектурой: размер фильтров на слоях, количество фильтров на слоях, размер окна выборки максимума, количество нейронов на слоях декодирующего блока.

  - Параметры нейросетевого элемента с TCN-архитектурой: регуляризация, размер фильтров, расширения на слоях, активация, количество кодирующих блоков, тип слоя перед выходным.

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

  - Параметры обучения нейросетевого элемента: интервал времени для обучения, названия и идентификаторы разметок для обучения, максимальная 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 батча (пакета данных для обучения), количество блоков, режим инференса, режим обучения, режим автоматического разделения данных на блоки, используемый объем памяти для обучения, информация, требуется ли инициализировать веса модели значениями из результатов предыдущего обучения и/или перемешивать данные.

  - Информация о результатах обучения нейросетевого элемента: очередь обучения (идентификаторы и имена элементов ML-модели, которые ожидают очереди на обучение), статус обучения, имя и идентификаторы обучающихся элементов, количество блоков, на которые разбит набор данных для обучения, имя пользователя, который запустил обучения элемента, продолжительность обучения, дата и время начала и окончания обучения, продолжительность интервалов времени данных в обучающей выборке, количество узлов РИВС, входящий в обучающую выборку, ошибки обучения и валидации, предсказание обученной ML-модели на обучающей выборке.

  - Параметры элементов на основе диагностических правил: информация, 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; параметры условия на поведение

тегов: тег, для которого добавлено условие, поведение тега, условие выполнения правила, количество шагов РИВС, пороговое значение тега, минимальное количество срабатываний правила для регистрации инцидента, значение дифференциала первого уровня, 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, 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**.

- Информация о разметках: идентификатор, имя и описание разметки, интервал, с которым рассчитываются данные на РИВС, цвет разметки, 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; параметры условия на поведение тегов: тег, для которого добавлено условие, поведение тега, условие выполнения правила, количество шагов РИВС, пороговое значение тега, минимальное количество срабатываний правила для регистрации инцидента, значение дифференциала первого уровня, 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, 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, дата 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.

  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 логов событий информационной безопасности (сут)** при настройке параметров безопасности. Программа также удаляет ранние записи журналов событий ИБ при превышении объема для хранения события ИБ, заданного в параметре **Объем логов событий информационной безопасности (МБ)**.

- Журналы контейнеров Kaspersky MLAD: дата и время события, уровень важности события, название 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.

Также 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, ветки ML-моделей и параметров 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 пресетах Tags for event #N, сформированных для зарегистрированного инцидента, 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:

- имя объекта мониторинга;

- период, за который были выгружены инциденты;

- идентификаторы зарегистрированных инцидентов;

- даты и время зарегистрированных инцидентов;

- статусы зарегистрированных инцидентов;

- имена групп, в которые входят зарегистрированные инциденты;

- имена и идентификаторы топ-тегов, оказавших наибольшее влияние на регистрацию инцидентов;

- значения топ-тегов;

- единицы измерения топ-тегов;

- описания топ-тегов;

- имена ML-моделей, зарегистрировавших инциденты;

- имена детекторов, зарегистрировавших инциденты.

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

- идентификаторы событий ИБ;

- даты и время событий ИБ;

- типы событий ИБ;

- уточнения типов событий ИБ;

- уровни важности событий ИБ;
- имена пользователей, действия которых привели к записи событий ИБ;
- IP-адреса компьютеров, с которых пользователями были произведены действия, записанные в журналы событий ИБ;
- результаты событий ИБ;
- краткие содержания событий ИБ;
- подробные описания событий ИБ.

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

- даты и время событий;
- уровни важности событий;
- имя контейнера, для которого зарегистрированы события;
- описания событий.

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

- идентификатор типа актива;
- уникальное имя типа актива;
- имена специальных параметров для типа актива (при наличии);
- описание типа актива (при наличии);
- идентификатор актива;
- имя актива;
- уникальное имя актива в рамках его родительского актива;
- описание актива (при наличии);
- имя родительского актива, к которому относится актив (при наличии);
- идентификатор родительского актива (при наличии);
- имена специальных параметров актива (при наличии);
- значения специальных параметров актива (при наличии);
- идентификатор тега;
- уникальное имя тега;
- уникальное альтернативное имя тега (при наличии);

- описание тега;
- имя родительского актива, к которому относится тег (при наличии);
- идентификатор родительского актива;
- тип тега (при наличии);
- единица измерения тега;
- нижний и верхний пороги блокировки (при наличии);
- нижний и верхний пороги сигнализации (при наличии);
- нижний и верхний пороги достоверности измерений (при наличии);
- нижняя и верхняя границы отображения значений тега на графиках (при наличии);
- выражение, по которому требуется рассчитать значение тега из значения, переданного в Kaspersky MLAD;
- комментарий к тегу;
- координаты расположения датчика объекта мониторинга по осям абсцисс, ординат и аппликат (при наличии).

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

- имя пресета;
- идентификатор пресета;
- идентификатор пользователя, который создал пресет или загрузил его в программу;
- идентификаторы тегов, входящих в состав пресета;
- порядковый номер пресета для сортировки;
- значок пресета;
- при использовании пресета для отображения данных в разделе **Временной срез** программа также сохраняет следующие данные:
  - подпись по оси абсцисс на графике в разделе **Временной срез**;
  - имя 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 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;
  - информация, 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;
  - названия параметров в базе данных Kaspersky MLAD;
  - типы введенных значений;
  - введенные или выбранные значения;
  - название 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;
  - единицы измерения временной метки тегов;
  - тип получаемых данных;
  - формат шаблона для декодирования типа получаемых данных.
- Конфигурационный файл коннектора OPC UA Connector, содержащий следующие данные:
  - идентификатор тега;
  - имя актива, к которому относится тег;
  - тип данных, которые передаются в значении тега.
- Конфигурационный файл службы Event Processor, содержащий следующие данные:
  - список обрабатываемых параметров событий;
  - время и масштаб времени для обработки событий;
  - 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, а также 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 mlad-release-4.0.2-<номер установочной сборки>):

- . – корневая директория программы. Используется для хранения конфигурационных файлов, журнала логов установки и обновления Kaspersky MLAD, скриптов для установки, обновления, запуска и остановки Kaspersky MLAD, подписи дистрибутива. Также в корне директории программы хранятся примечания к текущему выпуску Kaspersky MLAD (Release Notes).

- ./data – директория для хранения данных, которые загружаются с использованием коннектора HTTP Connector.

- ./containers – директория для хранения архива с контейнерами служб Kaspersky MLAD. Контейнеры служб Kaspersky MLAD устанавливаются в Docker из этого архива.

- ./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.

- ./upgrade_backup-<номер версии>-<номер сборки> – директория для хранения резервных копий Kaspersky MLAD, которые создаются в процессе обновления Kaspersky MLAD. Содержимое повторяет структуру корневой директории, в которую установлен Kaspersky MLAD.

- ./backup-<номер версии>-<дата и время резервного копирования> – директория для хранения резервных копий Kaspersky MLAD, созданных при выполнении резервного копирования. Содержимое повторяет структуру корневой директории, в которую установлен Kaspersky MLAD.

- ./volumes_backup_<дата удаления> – директория для хранения резервных копий томов (**volumes**) Docker, которые создаются во время удаления Kaspersky MLAD.

- Директория /var/lib/docker/volumes/:

  - ./mlad-release-<номер версии>-<номер установочной сборки>_postgres-volume – директория для хранения файлов базы данных Postgres.

  - ./mlad-release-<номер версии>-<номер установочной сборки>_influxdb-volume – директория для хранения файлов службы Time Series Database.

  - ./mlad-release-<номер версии>-<номер установочной сборки>_logger-volume – директория для хранения файлов подсистемы логирования.

  - ./mlad-release-<номер версии>-<номер установочной сборки>_webstatic-volume – директория для хранения статических данных веб-интерфейса программы.

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

Изменить файлы программы может администратор программы или пользователь, от имени которого распакован архив, содержащий установочный скрипт и все необходимые для установки Kaspersky MLAD файлы.

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

Этот раздел содержит информацию об управлении учетными записями пользователей Kaspersky MLAD.

Управление учетными записями пользователей Kaspersky MLAD доступно системным администраторам.

Для того чтобы обеспечить безопасную работу пользователей с Kaspersky MLAD, вам нужно установить доверенный сертификат для подключения к веб-интерфейсу и создать учетную запись для каждого пользователя.

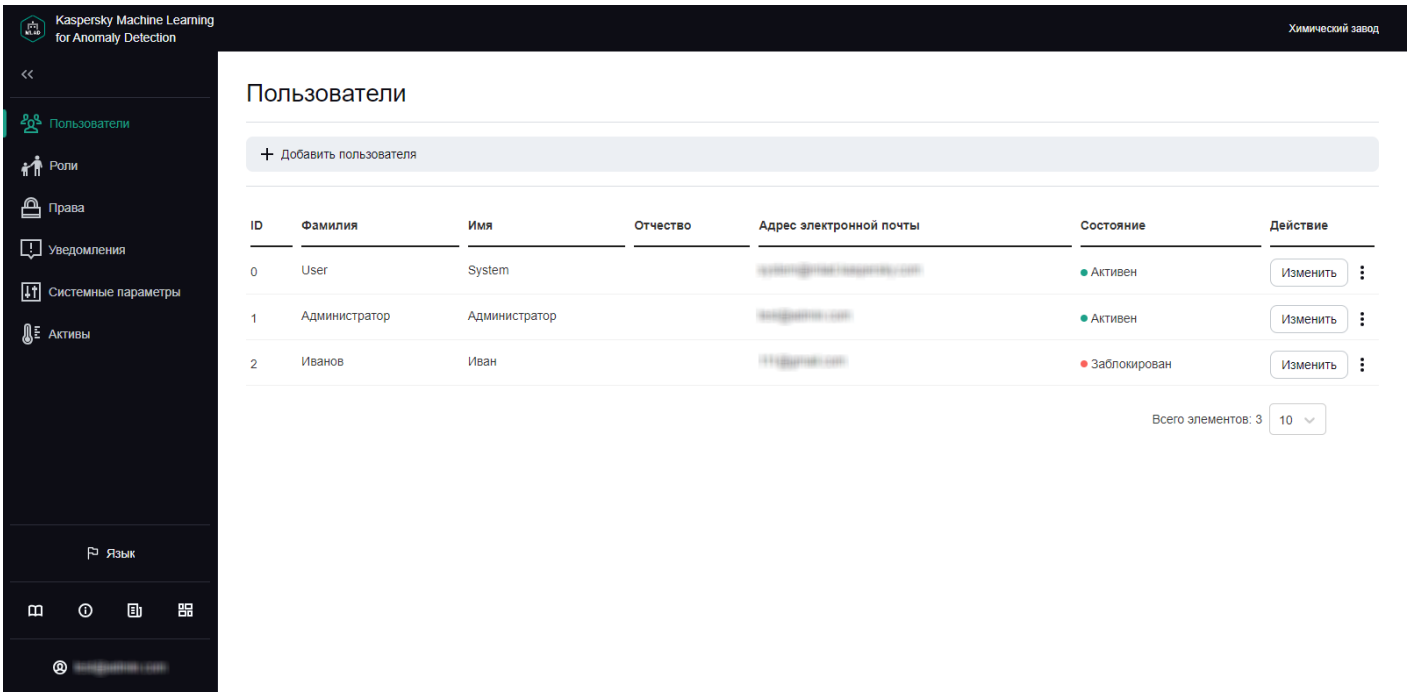
Все созданные учетные записи пользователей и **информация о них** отображаются в таблице разделе **Пользователи** в меню администратора.

- **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 **Заблокирован**. 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 также можете добавлять и 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 количества неудачных попыток авторизации этого пользователя 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 отозвать токены аутентификации или просмотреть 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**.

   Откроется окно **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.

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 изменять учетные записи пользователей и отзывать 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 учетной записи пользователь не может авторизоваться в Kaspersky MLAD.

Если пользователь был авторизован в момент блокировки его учетной записи, сессия работы в программе будет активна до выполнения одного из следующих условий:

- Пользователь вышел из своей учетной записи.
- Программа автоматически завершила сессию подключения по истечении срока действия токена аутентификации для учетной записи пользователя.
- Для учетной записи пользователя были отозваны токены аутентификации.

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**.

   Откроется окно **Изменение пользователя**.

4. Если требуется, выполните следующие действия:

   a. В поле **Фамилия** введите новую фамилию пользователя.

b. В поле **Имя** введите новое имя пользователя.

c. В поле **Отчество** введите новое отчество пользователя.

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

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

7. 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 **Заблокирован**.

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

8. Нажмите на кнопку **Сохранить**.

Измененная информация о пользователе отобразится в таблице. При изменении пароля для какой-либо учетной записи Kaspersky MLAD автоматически завершает пользовательскую сессию пользователя, для которого был изменен пароль.

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 для учетной записи пользователя. В результате для пользователя, чьи токены вы отозвали, будет завершена сессия работы в программе одновременно на всех устройствах, на которых он был авторизован. Отзыв токенов может быть полезен в случае, если требуется принудительно завершить сессии подключения к программе для определенного пользователя.

Чтобы отозвать токен или токены для учетной записи пользователя:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Пользователи**.

3. Нажмите на вертикальное меню ⋮, которое расположено в строке той учетной записи пользователя, для которой требуется отозвать токены аутентификации.

4. Выберите пункт **Отозвать токены**.

5. В открывшемся окне подтверждения нажмите на кнопку **Да**.

Токены 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. Нажмите на вертикальное меню ⋮, которое расположено в строке той учетной записи пользователя, для которой требуется просмотреть список прав доступа.

4. 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 разграничить доступ пользователей к функциям программы в зависимости от задач пользователей, используя типовые роли.

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** – цифровой идентификатор роли пользователя.
- **Роль** – название роли пользователя.
- **Состояние** – признак, указывающий, используется ли 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.

Управление ролями доступно системным администраторам.

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 появится 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. Для включения использования роли для пользователей программы установите переключатель **Состояние** в положение **Активна**.

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. Нажмите на кнопку **Изменить**.

   Справа появится панель **Изменение роли**.

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

   Вы можете ввести не более 30 символов.

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

6. Для изменения прав доступа роли выполните следующие действия:

   a. Нажмите на кнопку **Количество прав**.

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

   b. В списке прав измените выбор прав 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**.

8. Нажмите на кнопку **Сохранить**.

Удаление роли

Управление ролями доступно системным администраторам.

Вы можете удалять пользовательские роли, которые не назначены пользователям Kaspersky MLAD.

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 нажмите на кнопку **Да**, чтобы подтвердить удаление.

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** в строке той роли, для которой требуется просмотреть список прав.

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

Управление уведомлениями об инцидентах

Этот раздел содержит информацию об управлении уведомлениями при регистрации инцидентов. Уведомления отправляются по электронной почте пользователям, для которых они были настроены.

Управление уведомлениями об инцидентах доступно системным администраторам.

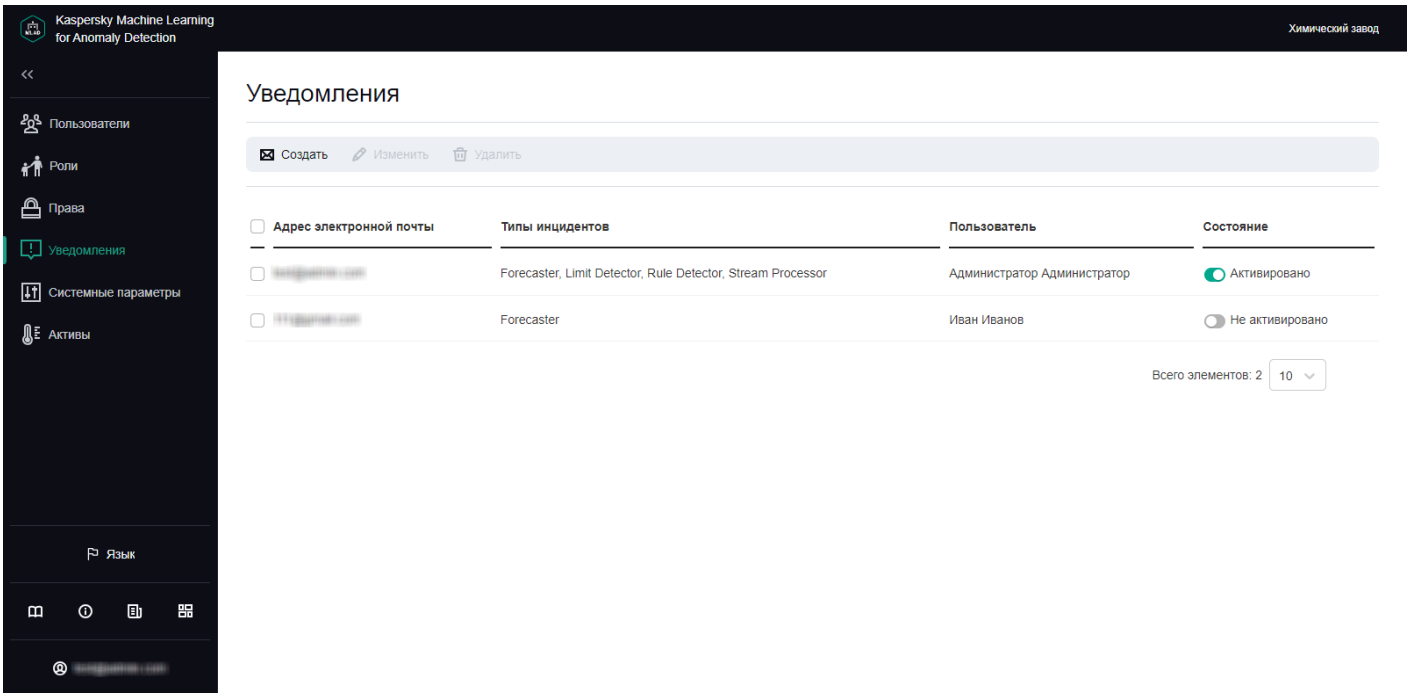
Предварительно требуется настроить и запустить службу Mail Notifier.

Все созданные уведомления об инцидентах и **информация о них** отображается в разделе **Уведомления** в меню администратора.

- **Адрес электронной почты** – адрес электронной почты пользователя, на который приходят уведомления об инцидентах.
- **Типы инцидентов** – тип инцидентов, уведомления о которых получает пользователь. Вы можете получать уведомления об инцидентах, зарегистрированных детекторами Forecaster, Limit Detector и Rule Detector, а также службой Stream Processor.
- **Пользователь** – фамилия и имя пользователя, который получает уведомления об инцидентах.
- **Состояние** – переключатель, позволяющий включить или выключить отправку уведомлений об инцидентах.

Если требуется, вы можете изменять количество уведомлений, отображаемых на одной странице.

Вы можете создавать, изменять и удалять уведомления об определенных инцидентах для пользователей Kaspersky MLAD.



Раздел **Уведомления**

Создание уведомления об инцидентах

Управление уведомлениями об инцидентах доступно системным администраторам.

Чтобы создать уведомление пользователя об инцидентах:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Уведомления**.

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

   Откроется окно **Создание уведомления**.

4. В раскрывающемся списке **Пользователь** выберите пользователя, для которого вы хотите создать уведомление.

   В списке **Пользователь** отображаются фамилии и имена пользователей, заданные при создании их учетных записей.

5. В поле **Адрес электронной почты** измените адрес электронной почты пользователя, на который будут приходить уведомления об инцидентах.

   По умолчанию Kaspersky MLAD автоматически заполняет поле **Адрес электронной почты** адресом, указанным для выбранного пользователя при создании его учетной записи.

6. Укажите типы инцидентов, при регистрации которых программа будет отправлять уведомления:

   - Если вы хотите настроить уведомление о прогнозируемых значениях тега, установите флажок **Forecaster**.
   - Если вы хотите настроить уведомление о приближении значения тега к порогам блокировки, установите флажок **Limit Detector**.
   - Если вы хотите настроить уведомление о достижении тегом порога, установленного для диагностического правила, установите флажок **Rule Detector**.
   - Если вы хотите настроить уведомление о прекращении или прерывании входного потока данных определенного тега, а также об обнаружении наблюдений, поступивших слишком рано или поздно, установите флажок **Stream Processor**.

7. В поле **Язык рассылки** 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.

8. Для включения отправки уведомлений установите переключатель **Состояние** в положение **Активировано**.

9. Нажмите на кнопку **Сохранить**.

Информация о новом уведомлении отобразится в таблице. Если требуется, вы можете изменять или удалять уведомления.

Изменение уведомления об инцидентах

Управление уведомлениями об инцидентах доступно системным администраторам.

Чтобы изменить уведомление об инцидентах:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Уведомления**.

3. Установите флажок около уведомления, которое вы хотите изменить, и нажмите на кнопку **Изменить**.

   Кнопка **Изменить** доступна, если выбрано только одно уведомление.

4. Внесите необходимые изменения.

5. При необходимости включите или выключите отправку уведомлений об инцидентах с помощью переключателя **Состояние**.

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

Измененная информация об уведомлении отобразится в таблице. Если требуется, вы можете удалять уведомления.

Включение и выключение отправки уведомлений об инцидентах

Управление уведомлениями об инцидентах доступно системным администраторам.

Kaspersky MLAD позволяет временно выключить отправку уведомлений вместо удаления их конфигураций. Информация об уведомлении сохраняется в разделе **Уведомления**. Вы можете включить отправку уведомление в любое время.

Чтобы включить или выключить отправку уведомлений об инцидентах:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Уведомления**.

3. Выполните одно из следующих действий:

   - Если требуется включить отправку уведомления об инцидентах, установите переключатель в столбце **Состояние** в положение **Активировано** для нужного уведомления.

   - Если требуется выключить отправку уведомления об инцидентах, установите переключатель в столбце **Состояние** в положение **Не активировано** для нужного уведомления.

Удаление уведомления об инцидентах

Управление уведомлениями об инцидентах доступно системным администраторам.

Чтобы удалить уведомление об инцидентах:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Уведомления**.

3. Установите флажок около уведомления, которое вы хотите удалить, и нажмите на кнопку **Удалить**.

   Кнопка **Удалить** доступна, если выбрано хотя бы одно уведомление. Вы можете выбрать несколько уведомлений одновременно.

4. В открывшемся окне нажмите на кнопку **Да**, чтобы подтвердить удаление.

Информация об уведомлении будет удалена из таблицы.

Kaspersky MLAD позволяет временно выключить отправку уведомлений вместо удаления.

Настройка параметров Kaspersky MLAD

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

Настройка основных параметров Kaspersky MLAD

Kaspersky MLAD позволяет указать название объекта мониторинга, веб-адрес и IP-адрес для подключения пользователей к веб-интерфейсу программы, а также периодичность получения новых данных от объекта мониторинга. Название объекта мониторинга будет отображаться в каждом разделе 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 название объекта мониторинга.

4. В поле **Веб-адрес программы** укажите веб-адрес программы.

5. В поле **IP-адрес для подключения к программе** укажите IP-адрес программы.

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.

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.

8. В раскрывающемся списке **Часовой пояс объекта мониторинга** выберите нужный часовой пояс объекта мониторинга.

9. Нажмите на кнопку **Сохранить**.

Настройка параметров безопасности Kaspersky MLAD

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

   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.

   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.

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

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`.

      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.

   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`.

   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)**.

   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)**.

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

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

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

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

      При незаполненном поле Kaspersky MLAD хранит все логи событий ИБ в течение срока, заданного в параметре **Время хранения логов событий информационной безопасности (сут)**.

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

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

6. Нажмите на кнопку **Сохранить**.

Настройка службы Anomaly Detector

В Kaspersky MLAD ML-модель может содержать следующие детекторы:

- Limit Detector – обнаруживает аномалии по факту выхода значения тега за минимальное или максимальное значение.

- Forecaster – предсказывает поведение объекта в настоящем на основе данных о его поведении в ближайшем прошлом.
- XGBoost – с определенной вероятностью обнаруживает аномалии в данных объекта мониторинга на основе выученной XGBoost-классификатором выборке данных для рассматриваемого отрезка времени.
- Rule Detector – строит прогнозы значений, принимаемых тегами при штатном функционировании объекта мониторинга и регистрирует инцидент при срабатывании одного или нескольких правил.

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

Работы по настройке службы Anomaly Detector могут выполнять системные администраторы.

Чтобы настроить параметры службы Anomaly Detector Kaspersky MLAD:

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.

4. С помощь переключателя **Использовать детектор Forecaster** включите или выключите использование детектора Forecaster.

5. С помощью переключателя **Использовать детектор XGBoost** включите или выключите использование детектора XGBoost.

6. С помощью переключателя **Использовать детектор Rule Detector** включите или выключите использование детектора Rule Detector.

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

8. 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.

9. 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.

10. В поле **Количество одновременно запущенных моделей** введите максимальное количество ML-моделей, которые могут анализировать данные телеметрии одновременно.

    Для максимальной производительности Kaspersky MLAD количество одновременно работающих ML-моделей не должно превышать 80% от количества ядер сервера, на котором установлен Kaspersky MLAD.

11. 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 сохранения этих данных в базе Kaspersky MLAD.

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

Чтобы настроить параметры маршрутизации данных Kaspersky MLAD:

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 как известные, так и неизвестные программе теги, поступающие от внешних источников, включите переключатель **Сохранять все теги**.
   - Если требуется сохранять только известные программе теги, выключите переключатель **Сохранять все теги**.

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

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

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

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 выполняется, если в сети объекта мониторинга настроен 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 SMTP-сервера** укажите IP-адрес SMTP-сервера.

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

5. В поле **Имя пользователя для SMTP-сервера** укажите имя пользователя для SMTP-сервера.

6. В поле **Пароль для SMTP-сервера** укажите пароль для SMTP-сервера.

7. Если требуется, с помощью переключателя **Использовать TLS-соединение** включите использование защищенного TLS-соединения.

   По умолчанию использование защищенного TLS-соединения выключено.

   > Во избежание компрометации получаемых и/или 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:

   - Загрузите сертификат SMTP-сервера с помощью кнопки **Обзор** под параметром **Сертификат SMTP-сервера**.
   - Загрузите ключ к файлу сертификата SMTP-сервера с помощью кнопки **Обзор** под параметром **Ключ к сертификату SMTP-сервера**.

   > Рекомендуется использовать сертификат, созданный по стандарту X.509, с длиной ключа к сертификату не менее 4 096 бит.

   Если требуется удалить файл сертификата или ключ к сертификату, нажмите на значок **Очистить** () в соответствующем поле. Если требуется сохранить файл сертификата или ключ к сертификату на компьютере, нажмите на значок **Скачать** () 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 **Периодичность равноинтервальной последовательности (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 значок **Очистить** ( ). Если требуется сохранить файл конфигурации на компьютере, нажмите на значок **Скачать** ( ).

5. Нажмите на кнопку **Сохранить**.

Настройка коннектора HTTP Connector

Kaspersky MLAD использует коннектор HTTP Connector для получения данных из CSV-файлов при регламентной загрузке данных методом `POST`. Вы можете загружать данные по протоколу HTTP или HTTPS, указав нужный протокол в запросе.

Работы по настройке коннектора HTTP Connector могут выполнять системные администраторы.

Коннектор HTTP Connector не поддерживает защищенное соединение. Если вы хотите использовать защищенное соединение для получения и отправки данных, рекомендуется дополнительными средствами обеспечить защиту сетевого соединения (например, использовать VPN) или другим способом исключить возможный несанкционированный доступ к каналу связи.

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. С помощью переключателя **Записывать данные в службу Message Broker** включите функцию записи данных в службу Message Broker.

4. Если требуется, с помощью переключателя **Сохранять полученный файл** включите функцию сохранения полученных CSV-файлов.

5. В поле **Размер записываемого блока (количество тегов)** укажите количество тегов, которое единовременно записывается в службу Message Broker.

6. 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.

7. 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/"
```

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).

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. Если требуется, с помощью переключателя **Использовать TLS-соединение** включите использование защищенного TLS-соединения.

   По умолчанию использование защищенного TLS-соединения выключено.

   Во избежание компрометации получаемых и/или 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.

4. 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`.

5. В поле **Имя пользователя для MQTT-соединения** укажите имя пользователя.

6. В поле **Пароль для MQTT-соединения** укажите пароль пользователя.

7. Если вы включили использование защищенного TLS-соединения, и на MQTT-брокере установлен самоподписанный сертификат, добавьте корневой сертификат для MQTT-брокера с помощью кнопки **Обзор** под параметром **Сертификат CA**.

   Если требуется удалить файл сертификата, нажмите на значок **Очистить** (). Если требуется сохранить файл сертификата на компьютере, нажмите на значок **Скачать** ().

8. Если вы включили использование защищенного TLS-соединения, и на MQTT-брокере включена аутентификация клиента, выполните следующие действия:

   - Добавьте сертификат клиентского приложения MQTT с помощью кнопки **Обзор** под параметром **Сертификат клиента**.
   - Добавьте ключ к сертификату клиентского приложения MQTT с помощью кнопки **Обзор** под параметром **Ключ к сертификату клиента**.

   > Рекомендуется использовать сертификат, созданный по стандарту X.509, с длиной ключа к сертификату не менее 4 096 бит.

   Если требуется удалить файл сертификата или ключ к сертификату, нажмите на значок **Очистить** () в соответствующем поле. Если требуется сохранить файл сертификата или ключ к сертификату на компьютере, нажмите на значок **Скачать** () 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 оповещения об инцидентах.

    Для выбора доступны следующие варианты: `JSONBatch`, `Topic`, `SmartHome`, `KISG`.

    По умолчанию этот параметр имеет значение `JSONBatch`.

    > Если вам не подходит ни один из форматов данных и оповещений 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 настройки коннектора для этого формата данных, с помощью кнопки **Обзор** под параметром **Конфигурационный файл коннектора**.

    Если требуется удалить файл сертификата, нажмите на значок **Очистить** (). Если требуется сохранить файл сертификата на компьютере, нажмите на значок **Скачать** ().

13. Если требуется пересчитывать значения тегов с учетом параметров, значения которых указаны в файле пресета, включите переключатель **Масштабировать полученные значения тегов**.

По умолчанию масштабирование полученных данных выключено.

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).

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. Если требуется, с помощью переключателя **Использовать TLS-соединение** включите использование защищенного TLS-соединения.

   По умолчанию использование защищенного TLS-соединения выключено.

   Во избежание компрометации получаемых и/или 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.

4. 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`.

5. В поле **Имя пользователя для AMQP-соединения** укажите имя пользователя.

6. В поле **Пароль для AMQP-соединения** укажите пароль пользователя.

7. Если вы включили использование защищенного TLS-соединения, и на AMQP-брокере установлен самоподписанный сертификат, добавьте корневой сертификат для AMQP-брокера с помощью кнопки **Обзор** под параметром **Сертификат CA**.

   Если требуется удалить файл сертификата, нажмите на значок **Очистить** (). Если требуется сохранить файл сертификата на компьютере, нажмите на значок **Скачать** ().

8. Если вы включили использование защищенного TLS-соединения, и на AMQP-брокере включена аутентификация клиента, выполните следующие действия:

   - Добавьте сертификат клиентского приложения AMQP с помощью кнопки **Обзор** под параметром **Сертификат клиента**.

- Добавьте ключ к сертификату клиентского приложения AMQP с помощью кнопки **Обзор** под параметром **Ключ к сертификату клиента**.

Рекомендуется использовать сертификат, созданный по стандарту X.509, с длиной ключа к сертификату не менее 4 096 бит.

Если требуется удалить файл сертификата или ключ к сертификату, нажмите на значок **Очистить** (🗑) в соответствующем поле. Если требуется сохранить файл сертификата или ключ к сертификату на компьютере, нажмите на значок **Скачать** (⬇) 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 тегов** укажите имя точки обмена для получения тегов от внешнего AMQP-брокера.

    Если значение для этого параметра не установлено, то получение тегов через коннектор AMQP Connector не происходит.

    По умолчанию для этого параметра значение не установлено.

11. В поле **Список подписок AMQP для получения тегов** укажите имя списка подписок, от которых коннектор AMQP Connector будет получать значения тегов.

    По умолчанию этот параметр имеет значение `#`.

12. В поле **Очередь AMQP для получения тегов** укажите имя очереди для коннектора AMQP Connector. Поле не является обязательным для заполнения.

13. В поле **Имя точки обмена (exchange) AMQP для публикации сообщений** укажите имя точки обмена для отправки сообщений о возникновении событий.

    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 оповещения об инцидентах.

    Для выбора доступны следующие варианты: `JSONBatch`, `Topic`, `SmartHome`, `KISG`.

    По умолчанию этот параметр имеет значение `JSONBatch`.

Если вам не подходит ни один из форматов данных и оповещений 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 настройки коннектора для этого формата данных, с помощью кнопки **Обзор** под параметром **Конфигурационный файл коннектора**.

    Если требуется удалить конфигурационный файл коннектора, нажмите на значок **Очистить** (🗑). Если требуется сохранить конфигурационный файл коннектора на компьютере, нажмите на значок **Скачать** (⬇).

17. Если требуется пересчитывать значения тегов с учетом параметров, значения которых указаны в файле пресета, включите переключатель **Масштабировать полученные значения тегов**.

    По умолчанию масштабирование полученных данных выключено.

18. Нажмите на кнопку **Сохранить**.

Kaspersky MLAD будет получать данные и отправлять сообщения о регистрации инцидентов по протоколу AMQP.

Настройка коннектора OPC UA Connector

Kaspersky MLAD использует коннектор OPC UA Connector для получения данных по протоколу, который описан спецификацией OPC Unified Architecture (унифицированная архитектура OPC).

Работы по настройке коннектора OPC UA Connector могут выполнять системные администраторы.

Коннектор OPC UA Connector не поддерживает защищенное соединение. Если вы хотите использовать защищенное соединение для получения и отправки данных, рекомендуется дополнительными средствами обеспечить защиту сетевого соединения (например, использовать VPN) или другим способом исключить возможный несанкционированный доступ к каналу связи.

Чтобы настроить работу коннектора OPC UA Connector:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Системные параметры** → **OPC UA Connector**.

   Справа отобразится список параметров.

3. В поле **Точка подключения** укажите адрес подключения.

   Например, `opc.tcp://10.0.0.0:8001/freeopcua/server/`.

4. В поле **Таймаут подключения к OPC UA-серверу (сек.)** укажите время в секундах, в течение которого коннектор OPC UA Connector будет пытаться установить соединение с OPC UA-сервером.

5. С помощью кнопки **Обзор** под параметром **Конфигурационный файл** добавьте файл, содержащий параметры для настройки коннектора OPC UA Connector.

   Если требуется удалить конфигурационный файл коннектора, нажмите на значок **Очистить** (). Если требуется сохранить конфигурационный файл коннектора на компьютере, нажмите на значок **Скачать** ().

6. В поле **Интервал исторических данных (сек.)** укажите время в секундах, за которое коннектор OPC UA Connector запрашивает исторические данные, хранящиеся на OPC UA-сервере.

   Укажите значение `0`, если не требуется загружать исторические данные. Укажите значение `-1`, если требуется загрузить все исторические данные.

7. В поле **Начало периода исторических данных (ГГГГ/ММ/ДД ЧЧ:ММ:СС)** укажите дату и время начала периода, за который требуется загрузить данные с OPC UA-сервера.

8. В поле **Окончание периода исторических данных (ГГГГ/ММ/ДД ЧЧ:ММ:СС)** укажите дату и время окончания периода, за который требуется загрузить данные с OPC UA-сервера.

9. В поле **Размер блока исторических данных, отправляемых OPC UA-сервером (параметр numvalues)** укажите количество тегов, которое будет передаваться в блоке исторических данных коннектору OPC UA Connector от OPC UA-сервера.

10. В поле **Размер блока исторических данных, отправляемых в службу Message Broker** укажите количество тегов, которое будет передаваться в блоке исторических данных от коннектора OPC UA Connector в службу Message Broker.

11. Нажмите на кнопку **Сохранить**.

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 значок **Очистить** (). Если требуется сохранить файл свертки на компьютере, нажмите на значок **Скачать** ().

4. В поле **Пароль для коннектора KICS Connector** введите пароль, который вы указали при добавлении коннектора в Kaspersky Industrial CyberSecurity for Networks.

5. Если требуется отправлять в Kaspersky Industrial CyberSecurity for Networks сообщения о регистрации инцидентов, включите переключатель **Отправлять сообщения в Kaspersky Industrial CyberSecurity for Networks**.

6. В поле **Частота семплирования 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. *Семплирование* (англ. data sampling) – метод корректировки обучающей выборки с целью балансировки распределения классов в исходном наборе данных.

7. Если требуется пересчитывать значения тегов с учетом параметров, значения которых указаны в файле пресета, включите переключатель **Масштабировать полученные значения тегов**.

   По умолчанию масштабирование полученных данных выключено.

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 логов событий информационной безопасности Kaspersky MLAD во внешнюю систему. Запись логов 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.

Коннектор CEF Connector не поддерживает защищенное соединение. Если вы хотите использовать защищенное соединение для получения и отправки данных, рекомендуется дополнительными средствами обеспечить защиту сетевого соединения (например, использовать VPN) или другим способом исключить возможный несанкционированный доступ к каналу связи.

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. Если требуется, с помощью переключателя **Получать события для службы Event Processor** включите использование коннектора CEF Connector для получения событий из внешней системы.

4. Если требуется отправлять во внешнюю систему сообщения об инцидентах, зарегистрированных программой, включите переключатель **Отправлять зарегистрированные инциденты в SIEM-систему**.

5. Если требуется отправлять во внешнюю систему сообщения о событиях, зарегистрированных службой Event Processor, включите переключатель **Отправлять зарегистрированные события в SIEM-систему**.

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 логи событий ИБ Kaspersky MLAD во внешнюю систему, включите переключатель **Отправлять логи 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 логов событий ИБ.

   Kaspersky MLAD поддерживает протоколы TCP и UDP для отправки логов 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 логи событий ИБ.

   c. В поле **Порт syslog-сервера для отправки событий информационной безопасности** укажите номер порта внешней системы, в которую требуется отправлять логи событий ИБ.

9. 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.

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 **Веб-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 на WebSocket-сервере установлен самоподписанный сертификат, добавьте корневой сертификат для WebSocket-сервера с помощью кнопки **Обзор** под параметром **Сертификат CA**.

   Если требуется удалить файл сертификата, нажмите на значок **Очистить** (). Если требуется сохранить файл сертификата на компьютере, нажмите на значок **Скачать** ().

5. Если требуется использовать защищенное соединение, и на WebSocket-сервере включена аутентификация клиента, выполните следующие действия:

   - Добавьте сертификат клиентского приложения WebSocket с помощью кнопки **Обзор** под параметром **Сертификат клиента**.
   - Добавьте ключ к сертификату клиентского приложения WebSocket с помощью кнопки **Обзор** под параметром **Ключ к сертификату клиента**.

   > Рекомендуется использовать сертификат, созданный по стандарту X.509, с длиной ключа к сертификату не менее 4 096 бит.

   Если требуется удалить файл сертификата или ключ к сертификату, нажмите на значок **Очистить** () в соответствующем поле. Если требуется сохранить файл сертификата или ключ к сертификату на компьютере, нажмите на значок **Скачать** () 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 оповещения об инцидентах.

   Для выбора доступны следующие варианты: `JSONBatch`, `Topic`, `SmartHome`, `KISG`.

   По умолчанию этот параметр имеет значение `JSONBatch`.

   > Если вам не подходит ни один из форматов данных и оповещений 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 настройки коннектора для этого формата данных, с помощью кнопки **Обзор** под параметром **Конфигурационный файл коннектора**.

   Если требуется удалить конфигурационный файл коннектора, нажмите на значок **Очистить** (). Если требуется сохранить конфигурационный файл коннектора на компьютере, нажмите на значок **Скачать** ().

8. Если требуется пересчитывать значения тегов с учетом параметров, значения которых указаны в файле пресета, включите переключатель **Масштабировать полученные значения тегов**.

   По умолчанию масштабирование полученных данных выключено.

9. Если требуется отправлять оповещения о зарегистрированных в Kaspersky MLAD инцидентах на WebSocket-сервер, включите переключатель **Отправлять инциденты**.

10. 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. Вы можете настроить параметры службы Event Processor.

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 значок **Очистить** (). Если требуется сохранить файл конфигурации на компьютере, нажмите на значок **Скачать** ().

   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 в основном режиме (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 в основном режиме (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.
- **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**.

> 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 значок **Очистить** (). Если требуется сохранить файл, содержащий резервную копию службы, на компьютере, нажмите на значок **Скачать** ().

4. В блоке **Режим сна** выполните следующие действия:

   a. В поле **Размер эпизода в режиме сна (количество событий)** укажите количество событий для формирования эпизода в режиме сна.

      Служба Event Processor формирует эпизоды на основе истории событий, поступивших на повторную обработку за интервал времени, заданный в поле **Интервал истории событий для обработки в режиме сна**.

   b. 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.

   c. 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.

   d. 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.

   e. 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. Нажмите на кнопку **Сохранить**.

Настройка статусов и причин инцидентов

Kaspersky MLAD позволяет указать причины для инцидентов, а также статусы для инцидентов и групп 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**.

Причина инцидента представляют собой отметку о причине возникновения инцидента, которую добавляет эксперт по результатам анализа инцидента.

Вы можете добавить причины и статусов инцидентов. Созданные причины и статусы инцидентов станут доступными для выбора в разделе **Инциденты**. Вы также можете изменять и удалять статусы и причины инцидентов.

Работы по настройке причин и статусов инцидентов могут выполнять системные администраторы.

Чтобы добавить статусы 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 появится 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** 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 MSE для разделов **Мониторинг** и **История**, установите флажок **Уведомлять об инциденте**.

8. Нажмите на кнопку **Сохранить**.

Чтобы добавить причины инцидентов:

1. В меню администратора выберите раздел **Системные параметры** → **Инциденты**.

2. В блоке **Причины инцидентов** нажмите на кнопку **Создать**.

   Справа появится 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 нажмите на кнопку **Да**, чтобы подтвердить 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 логирования служб Kaspersky MLAD

Вы можете настроить уровни логирования служб Kaspersky MLAD для записи определенной информации о состоянии программы и ее отображения в системе логирования (Grafana). Соответствие служб Kaspersky MLAD и имен образов и контейнеров Docker, см. в Приложении.

Работы по настройке логирования служб Kaspersky MLAD могут выполнять системные администраторы.

Чтобы настроить уровни логирования служб Kaspersky MLAD:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.
2. Выберите раздел **Системные параметры** → **Логирование**.

   Справа отобразится список служб Kaspersky MLAD.
3. Если требуется, в раскрывающихся списках рядом с названием необходимой службы измените уровень логирования службы.

В Kaspersky MLAD доступны следующие уровни логирования:

- **Отладка** – логирование всей информации в программе;
- **Инфо** – логирование общей информации о работе программы;
- **Общие** – логирование важной информации о работе программы;
- **Важные** – логирование ошибок, возникших в работе программы, и событий, которые могут привести к ошибкам в работе программы;
- **Ошибка** – логирование ошибок, возникших в работе программы;
- **Критические** – логирование критических ошибок, возникших в работе программы.

По умолчанию для большинства служб используется уровень логирования **Общие**. Для службы API Server по умолчанию используется уровень логирования **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 добавить временные интервалы отображения данных на графиках. Созданные временные интервалы станут доступными для выбора в разделах **Мониторинг**, **История** и **Временной срез**. Вы также можете изменять и удалять временные интервалы.

Работы по настройке временных интервалов отображения данных на графиках могут выполнять системные администраторы.

Чтобы добавить временные интервалы 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 появится 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 временной интервал 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 нажмите на кнопку **Да**, чтобы подтвердить удаление.

Информация о временном интервале будет удалена из таблицы.

Настройка отображения основного меню Kaspersky MLAD

Работы по настройке параметров отображения основного меню Kaspersky MLAD могут выполнять системные администраторы.

Чтобы настроить отображение основного меню и меню администратора 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 логирования службы программы, параметры отображения меню программы и по управлению типовыми статусами и причинами инцидентов, настраиваемые через веб-интерфейс. Это может сократить время на настройку 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 сохранен 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 в Kaspersky MLAD.

   Файлы конфигурации Kaspersky MLAD будут загружен в программу.

Управление активами и тегами

Управление активами и тегами доступно системным администраторам.

Активы и теги являются первичными элементами иерархической структуры объекта мониторинга. Иерархическая структура отображается в виде дерева активов.

В виде тегов в Kaspersky MLAD передаются наблюдения объекта мониторинга. На основании значений, полученных по созданным тегам, 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. С помощью значков плюс (⊞) и минус (⊟) слева от названий активов вы можете отобразить и скрыть данные дерева активов. Вы можете создавать активы и теги, а также изменять параметры тега, например пороги блокировки тега или границы отображения значений тегов на графике.

Kaspersky MLAD может получать данные от устройств, зарегистрированных во внешних системах (например, Kaspersky Industrial CyberSecurity for Networks). Kaspersky MLAD сохраняет теги, полученные от внешних устройств, в службе Time Series Database. При включенной функции сохранения всех тегов в службе Time Series Database также сохраняются идентификаторы и значения неизвестных тегов (отсутствующих в дереве активов). Вы можете сравнить текущую структуру дерева активов со структурой в службе Time Series Database и при необходимости добавить отсутствующие теги в текущую структуру.

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.

Также вы можете удалять существующие в системе теги, импортировать теги и активы из файла в формате XLSX и экспортировать их в файл в формате XLSX.

Создание актива в дереве активов

Управление активами и тегами доступно системным администраторам.

В Kaspersky MLAD вы можете создавать активы в дереве активов и распределять теги по активам наиболее удобным для вас способом. Например, вы можете создать активы в соответствии с устройствами объекта мониторинга, 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**.

3. В верхней части страницы нажмите на кнопку **Создать**.

   Справа откроется панель **Создание тега**.

4. В раскрывающемся списке **Тип элемента** выберите значение **Актив**.

5. Если требуется, нажмите на кнопку **Выбрать значок** и в открывшемся окне выберите значок для актива.

   Вы можете загрузить значок для актива, нажав на кнопку **Загрузить значок**. Изображения любого формата, размер которых превышает 128 x 128 пикселей, будут уменьшены до указанного размера с сохранением соотношения сторон. Размер загружаемого изображения в формате SVG не должен превышать 200 КБ.

   Если требуется удалить значок актива, нажмите на него и в открывшемся окне нажмите на кнопку **Удалить**.

6. В раскрывающемся списке **Актив** выберите раздел дерева активов, в составе которого требуется создать актив.

7. В поле **Название** укажите имя актива.

8. В поле **Описание** укажите описание для актива.

9. 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.

10. Если вы выбрали один из типов активов, заданных в импортированном файле конфигурации, укажите значения для специальных параметров активов.

    Имена специальных параметров указываются на вкладке **directory_types** конфигурационного файла.

11. Нажмите на кнопку **Сохранить**.

Актив будет создан. Если требуется, вы можете изменить расположение актива в дереве.

Вы также можете создавать вложенные активы в дереве активов.

Чтобы создать актив с помощью дерева активов:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Активы**.

3. В дереве активов рядом с названием того раздела, в который требуется добавить актив, откройте вертикальное меню **...** и выберите пункт **Добавить актив**.

   Справа откроется панель **Создание актива**.

4. Если требуется, нажмите на кнопку **Выбрать значок** и в открывшемся окне выберите значок для актива.

Вы можете загрузить значок для актива, нажав на кнопку **Загрузить значок**. Изображения любого формата, размер которых превышает 128 x 128 пикселей, будут уменьшены до указанного размера с сохранением соотношения сторон. Размер загружаемого изображения в формате SVG не должен превышать 200 КБ.

Если требуется удалить значок актива, нажмите на него и в открывшемся окне нажмите на кнопку **Удалить**.

5. В поле **Название** укажите имя актива.
6. В поле **Описание** укажите описание для актива.
7. 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.
8. Если вы выбрали один из типов активов, заданных в импортированном файле конфигурации, укажите значения для специальных параметров активов.

   Имена специальных параметров указываются на вкладке **directory_types** конфигурационного файла.
9. Нажмите на кнопку **Сохранить**.

Актив будет создан. Если требуется, вы можете изменить расположение актива в дереве.

Изменение параметров актива в дереве активов

Управление активами и тегами доступно системным администраторам.

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 рядом с названием актива, параметры которого требуется изменить, откройте вертикальное меню **...** и выберите пункт **Изменить актив**.

   Справа откроется панель **Изменение актива**.
4. Если требуется изменить значок актива, нажмите на кнопку **Выбрать значок** и в открывшемся окне выберите значок для актива.

   Вы можете загрузить значок для актива, нажав на кнопку **Загрузить значок**. Изображения любого формата, размер которых превышает 128 x 128 пикселей, будут уменьшены до указанного размера с сохранением соотношения сторон. Размер загружаемого изображения в формате SVG не должен превышать 200 КБ.

   Если требуется удалить значок актива, нажмите на него и в открывшемся окне нажмите на кнопку **Удалить**.
5. В раскрывающемся списке **Актив** выберите раздел дерева активов, к которому вы хотите отнести актив.

Подразделы актива и их теги будут перемещены в новый актив.

6. В поле **Название** укажите новое имя для актива.

7. В поле **Описание** укажите новое описание для актива.

8. В раскрывающемся списке **Тип актива** выберите тип актива.

   Если вы загрузили конфигурацию тегов и активов в Kaspersky MLAD вы можете выбрать один из типов активов, заданных в файле конфигурации. Типы активов указываются на вкладке **directory_types** конфигурационного файла.

9. Если вы выбрали один из типов активов, заданных в импортированном файле конфигурации, укажите значения для специальных параметров актива.

   Имена специальных параметров указываются на вкладке **directory_types** конфигурационного файла.

10. Нажмите на кнопку **Сохранить**.

Актив будет изменен. Если требуется, вы можете изменить расположение актива в дереве.

Создание тега

Управление активами и тегами доступно системным администраторам.

В Kaspersky MLAD вы можете создавать новые теги для описания данных, поступающих от объекта мониторинга (исходные теги) или от службы Stream Processor.

Чтобы создать новый тег:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Активы**.

3. В верхней части страницы нажмите на кнопку **Создать**.

   Справа откроется панель **Создание тега**.

4. В раскрывающемся списке **Тип элемента** выберите **Тег**.

5. Если требуется, нажмите на кнопку **Выбрать значок** и в открывшемся окне выберите значок для тега.

   Вы можете загрузить значок для тега, нажав на кнопку **Загрузить значок**. Изображения любого формата, размер которых превышает 128 x 128 пикселей, будут уменьшены до указанного размера с сохранением соотношения сторон. Размер загружаемого изображения в формате SVG не должен превышать 200 КБ.

   Если требуется удалить значок тега, нажмите на него и в открывшемся окне нажмите на кнопку **Удалить**.

6. 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.

7. В поле **Название** укажите уникальное имя тега. Если требуется получать значения тега от внешней системы, укажите имя тега во внешней системе.

8. В поле **Описание** укажите описание тега.

9. Если требуется, в поле **Альтернативное название** укажите альтернативное имя тега.

10. В поле **ID** укажите уникальный числовой идентификатор тега.

11. В поле **Размерность** укажите единицы измерения для тега (например, % или мПа).

12. 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**.

13. В блоке **Пороги блокировки** в полях **Нижний** и **Верхний** укажите нижний и верхний пороги значений тега, при достижении которых требуется принять экстренные меры реагирования на АСУ ТП.

    Эти параметры требуются для корректной 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 графика тега, 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.

14. 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.

15. В блоке **Пороги достоверности измерений** в полях **Нижний** и **Верхний** укажите нижний и верхний пороги физически возможных значений тега.

16. В блоке **Границы отображения** в полях **Нижняя** и **Верхняя** укажите нижнюю и верхнюю границы отображения значений тега на графиках.

    Если значения тега будут выходить за указанные границы, то они не будут отображаться на графике тега. Допустимые границы отображения значений тега имеют приоритет над отображением порогов блокировки, даже если включена функция **Всегда показывать пороги блокировки**.

17. В поле **Устройство внешней системы** укажите имя устройства, созданного во внешней системе, для которого требуется получать теги.

18. В поле **Комментарий** введите краткий комментарий к тегу.

19. Если требуется добавить дополнительные горизонтальные пороговые линии для этого тега на графиках в разделах **Мониторинг** и **История**, выполните следующие действия:

    a. Нажмите на кнопку **Добавить линию**.

    b. В появившемся поле **Пороговое значение** укажите значение, которое требуется отображать на графиках.

    c. В поле **Цвет линии** выберите цвет, в котором будет отображаться пороговая линия на графиках.

    Дополнительные горизонтальные пороговые линии помогают визуально оценить колебания значений тега в определенных пределах. Вы можете добавить несколько дополнительных горизонтальных пороговых линий.

20. 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.

Добавление тега в актив

Управление активами и тегами доступно системным администраторам.

В Kaspersky MLAD вы можете добавлять теги в созданные активы.

Чтобы добавить тег в актив:

1. В нижнем левом углу страницы нажмите на кнопку .

   Вы перейдете в меню администратора.

2. Выберите раздел **Активы**.

3. В дереве активов рядом с разделом, в который требуется добавить тег, откройте вертикальное меню **...** и выберите пункт **Добавить тег**.

   Справа откроется панель **Создание тега**.

4. Если требуется, нажмите на кнопку **Выбрать значок** и в открывшемся окне выберите значок для тега.

   Вы можете загрузить значок для тега, нажав на кнопку **Загрузить значок**. Изображения любого формата, размер которых превышает 128 x 128 пикселей, будут уменьшены до указанного размера с сохранением соотношения сторон. Размер загружаемого изображения в формате SVG не должен превышать 200 КБ.

   Если требуется удалить значок тега, нажмите на него и в открывшемся окне нажмите на кнопку **Удалить**.

5. В поле **Название** укажите уникальное имя тега. Если требуется получать значения тега от внешней системы, укажите имя тега во внешней системе.

6. В поле **Описание** укажите описание тега.

7. Если требуется, в поле **Альтернативное название** укажите альтернативное имя тега.

8. В поле **ID** укажите уникальный числовой идентификатор тега.

9. В поле **Размерность** укажите единицы измерения для тега (например, % или мПа).

10. 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**.

11. В блоке **Пороги блокировки** в полях **Нижний** и **Верхний** укажите нижний и верхний пороги значений тега, при достижении которых требуется принять экстренные меры реагирования на АСУ ТП.

    Эти параметры требуются для корректной 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 графика тега, 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.

12. 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.

13. В блоке **Пороги достоверности измерений** в полях **Нижний** и **Верхний** укажите нижний и верхний пороги физически возможных значений тега.

14. В блоке **Границы отображения** в полях **Нижняя** и **Верхняя** укажите нижнюю и верхнюю границы отображения значений тега на графиках.

    Если значения тега будут выходить за указанные границы, то они не будут отображаться на графике тега. Допустимые границы отображения значений тега имеют приоритет над отображением порогов блокировки, даже если включена функция **Всегда показывать пороги блокировки**.

    В поле **Устройство внешней системы** укажите имя устройства, созданного во внешней системе, для которого требуется получать теги.

15. В поле **Комментарий** введите краткий комментарий к тегу.

16. Если требуется добавить дополнительные горизонтальные пороговые линии для этого тега на графиках в разделах **Мониторинг** и **История**, выполните следующие действия:

    a. Нажмите на кнопку **Добавить линию**.

    b. В появившемся поле **Пороговое значение** укажите значение, которое требуется отображать на графиках.

    c. В поле **Цвет линии** выберите цвет, в котором будет отображаться пороговая линия на графиках.

    Дополнительные горизонтальные пороговые линии помогают визуально оценить колебания значений тега в определенных пределах. Вы можете добавить несколько дополнительных горизонтальных пороговых линий.

17. 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

Управление активами и тегами доступно системным администраторам.

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**.

   В дереве активов рядом с названием того тега, который вы хотите изменить, откройте вертикальное меню **...** и выберите пункт **Изменить тег**.

   Вы можете отобразить или скрыть данные дерева активов с помощью значков плюс (⊞) и минус (⊟) слева от названий активов.

   Справа откроется панель **Изменение тега**. В верхней части открывшейся панели отображается количество ML-моделей, которые используют выбранный тег.

3. Если требуется изменить значок тега, нажмите на кнопку **Выбрать значок** и в открывшемся окне выберите значок для тега.

   Вы можете загрузить значок для тега, нажав на кнопку **Загрузить значок**. Изображения любого формата, размер которых превышает 128 x 128 пикселей, будут уменьшены до указанного размера с сохранением соотношения сторон. Размер загружаемого изображения в формате SVG не должен превышать 200 КБ.

   Если требуется удалить значок тега, нажмите на него и в открывшемся окне нажмите на кнопку **Удалить**.

4. В раскрывающемся списке **Актив** выберите новый актив, к которому вы хотите отнести выбранный тег.

   В поле **Название** укажите новое имя тега. Если требуется получать значения тега от внешней системы, укажите имя тега во внешней системе.

   Kaspersky MLAD периодически проверяет сведения о тегах, полученных от Kaspersky Industrial CyberSecurity for Networks. Если имя тега было изменено вручную, программа автоматически обновит имя тега в соответствии с именем тега в Kaspersky Industrial CyberSecurity for Networks после следующей проверки.

5. В поле **Описание** укажите новое описание тега.

6. Если требуется, в поле **Альтернативное название** укажите альтернативное имя тега.

7. В поле **Размерность** укажите новые единицы измерения для тега (например, % или мПа).

8. 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**.

9. В блоке **Пороги блокировки** в полях **Нижний** и **Верхний** укажите нижний и верхний пороги значений тега, при достижении которых требуется принять экстренные меры реагирования на АСУ ТП.

   Эти параметры требуются для корректной 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 графика тега, 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.

10. 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.

11. В блоке **Пороги достоверности измерений** в полях **Нижний** и **Верхний** укажите нижний и верхний пороги физически возможных значений тега.

12. В блоке **Границы отображения** в полях **Нижняя** и **Верхняя** укажите нижнюю и верхнюю границы отображения значений тега на графиках.

Если значения тега будут выходить за указанные границы, то они не будут отображаться на графике тега. Допустимые границы отображения значений тега имеют приоритет над отображением порогов блокировки, даже если включена функция **Всегда показывать пороги блокировки**.

В поле **Устройство внешней системы** укажите имя устройства, созданного во внешней системе, для которого требуется получать теги.

Kaspersky MLAD периодически проверяет сведения о тегах, полученных от Kaspersky Industrial CyberSecurity for Networks. Если информация об устройстве тега была изменена вручную, программа автоматически обновит сведения об устройстве в соответствии с именем устройства в Kaspersky Industrial CyberSecurity for Networks после следующей проверки.

13. В поле **Комментарий** введите краткий комментарий к тегу.

14. Если требуется добавить дополнительные горизонтальные пороговые линии для этого тега на графиках в разделах **Мониторинг** и **История**, выполните следующие действия:

    a. Нажмите на кнопку **Добавить линию**.

    b. В появившемся поле **Пороговое значение** укажите значение, которое требуется отображать на графиках.

    c. В поле **Цвет линии** выберите цвет, в котором требуется отображать пороговую линию на графиках в разделах **Мониторинг** и **История**.

    Дополнительные горизонтальные пороговые линии помогают визуально оценить колебания значений тега в определенных пределах. Вы можете добавить несколько дополнительных горизонтальных пороговых линий.

15. Нажмите на кнопку **Сохранить**.

Если требуется, вы можете изменить расположение тегов в дереве.

Перемещение активов и тегов

Управление активами и тегами доступно системным администраторам.

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 названиями активов и/или тегов, которые требуется переместить.

4. В верхней части страницы нажмите на кнопку **Переместить**.

   Справа откроется панель **Перемещение тегов**.

5. 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.

Вы также можете изменить расположение активов и тегов в дереве с помощью точек (⁞⁞) слева от названия нужного актива или тега. Для этого необходимо перетащить нужный актив или тег вверх или вниз в дереве, удерживая за точки (⁞⁞) слева от нужного актива или тега.

Удаление актива или тега

Управление активами и тегами доступно системным администраторам.

Вы можете удалять созданные ранее активы и/или теги из дерева активов, если выбранные теги или теги, относящиеся к выбранному активу, не используются ML-моделями.

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 установите флажок рядом с названием тега, который вы хотите удалить, и нажмите на кнопку **Удалить** в верхней части страницы.

   - В вертикальном меню **...** справа от нужного тега нажмите на кнопку **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 установите флажок рядом с названием актива, который вы хотите удалить, и нажмите на кнопку **Удалить** в верхней части страницы.

   - В вертикальном меню **...** справа от нужного актива нажмите на кнопку **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 названиями активов и/или тегов.

   Если требуется удалить один или несколько тегов из актива, разверните соответствующий раздел дерева активов, нажав на значок плюса (), и выберите нужные теги.

4. Нажмите на кнопку **Удалить** в верхней части страницы.

5. В открывшемся окне подтвердите удаление активов и/или тегов.

   Если выбранные активы и/или теги не используются ML-моделями, в открывшемся окне отображается значок галочки () напротив строки **Проверка связей тегов с загруженными моделями**. Выбранные теги будут удалены из Kaspersky MLAD безвозвратно.

   Если выбранные активы и/или теги используются ML-моделями, в открывшемся окне отображается значок крестика () напротив строки **Проверка связей тегов с загруженными моделями**. В таком случае вы не можете удалить выбранные активы и/или теги. Для удаления активов и/или тегов требуется удалить ML-модели, в которых они используются.

Проверка текущей структуры тегов

Управление активами и тегами доступно системным администраторам.

Kaspersky MLAD сохраняет теги, полученные от внешних устройств, в службе Time Series Database. При поступлении неизвестных тегов через коннектор KICS Connector программа также автоматически создает эти теги в разделе **kics** дерева 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.

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**.

3. В верхней части страницы нажмите на кнопку **Проверить теги**.

   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 названиями в формате **Tag <идентификатор тега>**.

4. 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, названия 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.

Управление активами и тегами доступно системным администраторам.

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**.

3. Нажмите на кнопку **Импорт**.

   Справа откроется панель **Импорт иерархической структуры**.

4. В поле **Импорт файла** добавьте файл в формате XLSX, содержащий необходимую конфигурацию активов и тегов иерархической структуры.

   Если требуется удалить файл конфигурации активов и тегов, нажмите на значок корзины ().

5. В раскрывающемся списке **Актив** выберите раздел дерева активов, в который требуется загрузить конфигурацию активов и тегов из файла.

6. 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.
   - **Перезаписать**. Kaspersky MLAD удалит ранее созданные и/или импортированные активы и теги из выбранного раздела и создаст новые активы и теги из файла конфигурации.

7. 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 активов, повторяющихся в разных разделах дерева активов, в режиме импорта **Добавить и обновить**. При этом загрузить теги с именами, соответствующими именам ранее созданных и/или загруженных тегов, невозможно.

8. 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

Управление активами и тегами доступно системным администраторам.

Вы можете сохранить структуру тегов в файл в формате XLSX для дальнейшего использования. Вместе со структурой тегов в файл будет сохранения структура активов иерархической структуры.

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**.

3. Нажмите на кнопку **Экспорт**.

   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 рекомендуется создать пресеты, которые включают в себя теги, соответствующие агрегатам установки. Если требуется, вы можете изменить уже существующие пресеты.

2. **Просмотр исторических данных**

   Перейдите в раздел **История**, чтобы просмотреть исторические данные технологических параметров, результаты их обработки Kaspersky MLAD – сформированные прогнозы и выделенные инциденты. Выберите необходимый пресет и укажите дату и интервал времени для просмотра данных. Вы можете просматривать исторические данные, используя навигацию.

3. **Мониторинг в онлайн-режиме**

   Для просмотра поступающих значений технологических параметров, их прогнозируемых значений и ошибок в онлайн-режиме, перейдите в раздел **Мониторинг**. Выберите необходимый пресет и интервал времени для отображения поступающих данных.

4. **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 необходимый пресет и укажите дату и интервал времени для просмотра данных. Вы можете просматривать данные, используя навигацию.

5. **Работа с инцидентами**

   Перейдите в раздел **Инциденты** и просмотрите информацию о зарегистрированных инцидентах. Проанализируйте инциденты и добавьте экспертные заключения или замечания, 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**.

6. **Работа с событиями и паттернами**

   Просмотрите события и паттерны, выявленные процессором событий в разделе **Процессор событий**. Для отслеживания определенных событий, паттернов или значений параметров событий создайте мониторы.

Просмотр сводных данных в разделе Информационная панель

В разделе **Информационная панель** представлена сводная информация о количестве тегов и событий, 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 тегов и событий. Вы можете включить или выключить отображение на графике поступающих тегов и событий, нажав на соответствующую легенду подписи данных, которая расположена под графиком. Левая шкала графика отображает диапазон количества тегов, поступающих в секунду. Правая шкала графика отображает диапазон количество событий, поступающих в секунду.

- **Последние инциденты** – таблица, содержащая **информацию о последних зарегистрированных инцидентах**.

  - **ID** – идентификатор зарегистрированного инцидента.
  - **Дата и время** – дата и время возникновения инцидента.
  - **Детектор** – название детектора, который зарегистрировал инцидент.
  - **Топ-тег** – название параметра технологического процесса, для которого зарегистрирован инцидент.

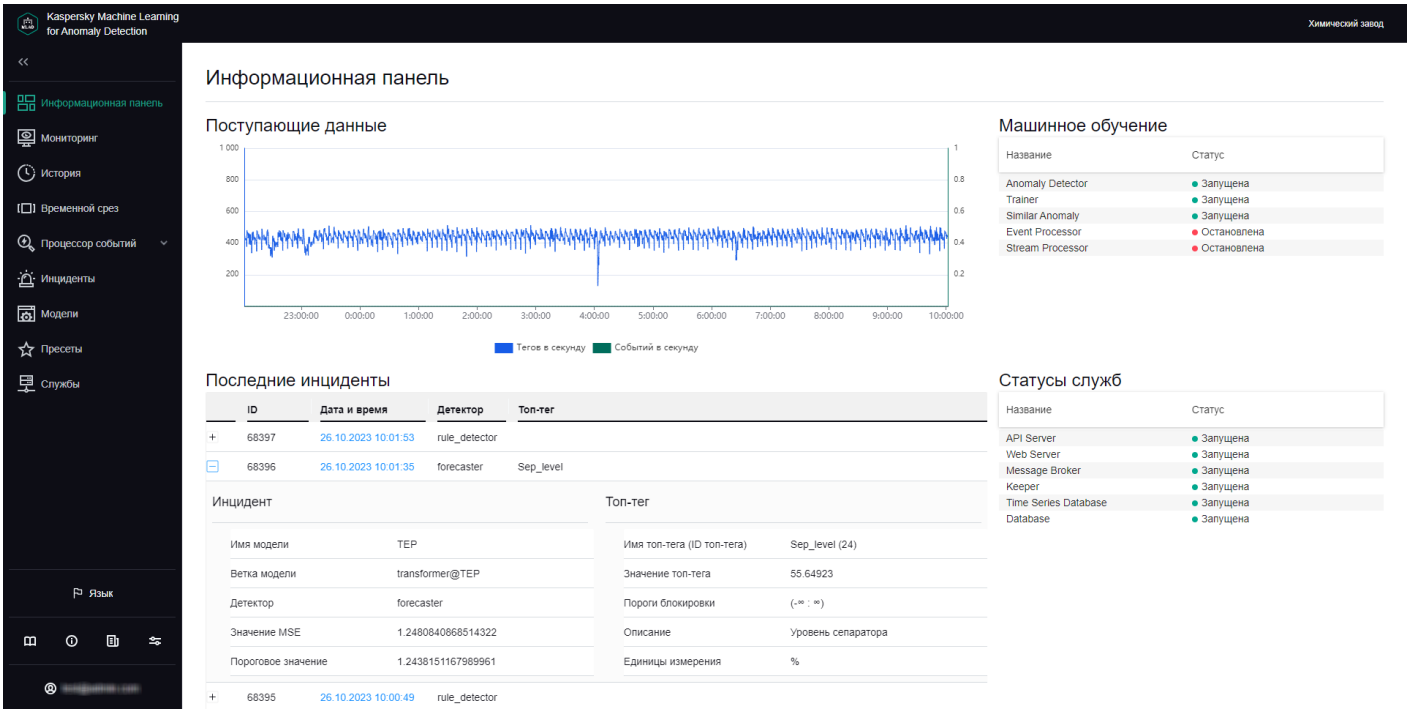
  При нажатии на значок плюса (+) около инцидента в таблице инцидентов раскрывается окно с техническими характеристиками выбранного инцидента и тега:

  - **Инцидент** – блок, содержащий информацию об инциденте:
    - **Имя модели** – название используемой ML-модели.
    - **Ветка модели** – название используемой ветки ML-модели.
    - **Детектор** – название детектора, который зарегистрировал инцидент.
    - **Значение MSE** – значение индивидуальной ошибки MSE.
    - **Пороговое значение** – пороговое значение MSE для используемой ветки ML-модели на момент регистрации инцидента.
  - **Топ-тег** – блок, содержащий информацию о теге, для которого зарегистрирован инцидент:
    - **Имя топ-тега (ID топ-тега)** – название и идентификатор тега, поведение которого привело к регистрации инцидента.
    - **Значение топ-тега** – зарегистрированное в момент инцидента значение топ-тега.
    - **Пороги блокировки** – пороги значений топ-тега, при достижении которых требуется принять экстренные меры реагирования на АСУ ТП.
    - **Описание** – описание топ-тега.
    - **Единицы измерения** – единицы измерения значений топ-тега.

- **Машинное обучение** – таблица, в которой отображается статус служб, используемых для работы и обучения ML-модели, а также имя активной ML-модели.

- **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 инцидента в таблице **Последние инциденты**. В разделе **История** отображается подробная информация о зарегистрированных Kaspersky MLAD инцидентах.



Раздел **Информационная панель**

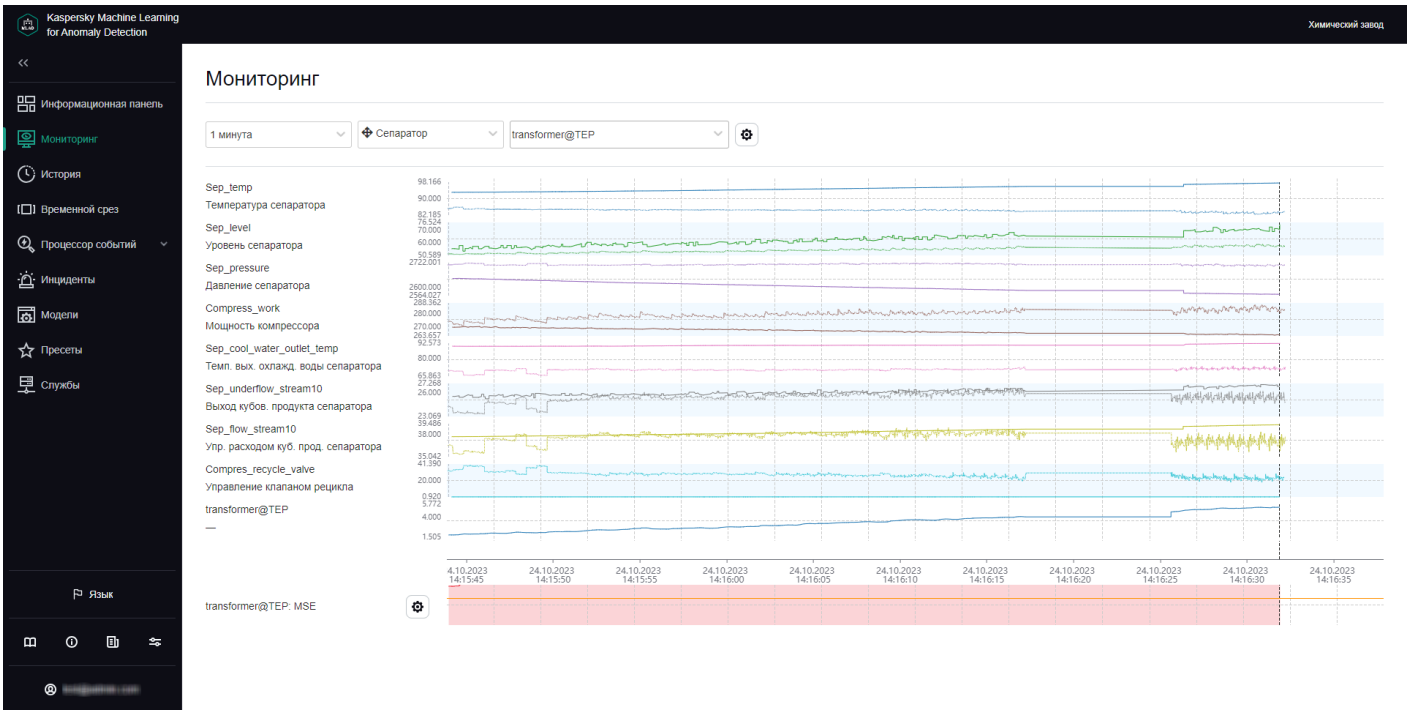
Просмотр поступающих данных в разделе Мониторинг

В разделе **Мониторинг** вы можете просматривать поступающие в реальном времени значения тегов, входящих в пресет и их прогнозируемые значения. В раскрывающемся списке вы можете выбрать необходимый пресет для просмотра данных по интересующим вас тегам. В список входят пресеты, которые можно создать в разделе **Пресеты**. Для каждого тега, входящего в выбранный пресет, поступающие значения отображаются в виде графика. Вы можете настроить отображение графиков, а также выбрать ветку определенной ML-модели, чтобы просмотреть результаты работы этой ветки: предсказанные детектором Forecaster значения тегов и их ошибки или значения, полученные в результате работы диагностических правил.

В нижней части страницы расположен блок, отображающий *суммарную среднеквадратичную ошибку MSE* (далее также "ошибка MSE" или "суммарная ошибка"), а также количество зарегистрированных инцидентов (цветные точки-индикаторы). Оранжевая линия отображает порог MSE, при превышении которого Kaspersky MLAD регистрирует инцидент.

В зависимости от выбранного масштаба времени и плотности инцидентов одна точка-индикатор может соответствовать одному или нескольким близко расположенным инцидентам, зарегистрированных одним или несколькими разными детекторами. Цвет точек-индикаторов соответствует цвету ветки ML-модели, с помощью которой был зарегистрирован инцидент. Для точек-индикаторов, которые соответствуют группе инцидентов, зарегистрированных разными ветками, а также для инцидентов, зарегистрированных детектором Limit Detector зарезервированы специальные цвета.

Для инцидентов, зарегистрированных детектором Rule Detector, значение ошибки MSE будет отсутствовать. При анализе таких инцидентов требуется обращать внимание на маркер срабатывания правила (цветная точка-индикатор) ниже графика ошибки MSE для выбранной ветки ML-модели.



Раздел **Мониторинг**

Просмотр данных для определенного пресета в разделе Мониторинг

Kaspersky MLAD позволяет выбирать пресеты, для которых отображаются данные, поступающие в реальном времени.

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.

Если требуется, вы можете изменить временной интервал отображения данных, настроить отображение графиков или выбрать определенную ветку ML-модели. Также вы можете изменить состав отображаемых тегов, изменив пресет.

Выбор определенной ветки ML-модели в разделе Мониторинг

В разделе **Мониторинг** вы можете просматривать поступающие в реальном времени значения тегов, входящих в пресет, их прогнозируемые значения и ошибки MSE.

Если для объекта мониторинга используется ML-модель, которая имеет несколько веток для обработки и предсказания данных, Kaspersky MLAD позволяет выбрать определенную ветку ML-модели для отображения результатов работы соответствующего элемента модели:

- Для ветки ML-модели, в основе которой лежит детектор Forecaster, результаты работы отображаются в виде предсказанных значений для отдельных тегов, индивидуальных ошибок предсказания отдельных тегов, а также общей ошибки MSE и точек-индикаторов инцидентов, зарегистрированных детектором.

- Для ветки ML-модели, в основе которой лежит детектор Rule Detector, результаты работы представлены в виде значений, полученных в результате работы диагностических правил, и точек-индикаторов инцидентов.

- Для детектора Limit Detector ветка 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 тегов.

Для отображения предсказанных значений тега на графиках в разделе **Мониторинг**, а также для вывода значений, полученных в результате работы диагностических правил, требуется настроить отображение графиков.

Чтобы просмотреть результаты работы определенной ветки ML-модели:

1. В основном меню выберите раздел **Мониторинг**.

2. На открывшейся странице в раскрывающемся списке **Ветка модели** установите флажки около нужных веток ML-модели.

   Имена выбранных веток отобразятся в поле.

   Ветки, которые относятся к используемой в текущий момент ML-модели, расположены в верхней части списка. В нижней части списка отображаются ветки других неиспользуемых в текущий момент ML-моделей, которые загружены в Kaspersky MLAD. Ветка ML-модели отображается в раскрывающемся списке только после того, как в Kaspersky MLAD появятся данные, полученные в результате ее работы.

   На графиках выбранного пресета отобразятся предсказанные значения тегов или значения, полученные в результате работы диагностических правил, в зависимости от типа детектора в выбранной ветке ML-модели.

   Если требуется скрыть отображение результатов работы выбранных ранее веток ML-модели, снимите флажки около этих веток (одна из веток должна остаться активной для отображения графиков в разделе **Мониторинг**).

3. Если требуется отображать ошибку MSE, которая получена в результате обработки данных определенной веткой ML-модели, выполните следующие действия:

   a. Нажмите на кнопку настройки , которая расположена под графиками тегов в левой части страницы.

   b. В появившейся справа панели **Параметры отображения графиков MSE** в раскрывающемся списке **Ветка модели** выберите ветку. Вы можете выбрать только одну ветку ML-модели из списка.

   c. Нажмите на кнопку **Закрыть**.

   На графике ошибки MSE отобразятся значения ошибки MSE для выбранной веткой ML-модели. В нижней части графика отображаются точки-индикаторы инцидентов, зарегистрированных выбранными ветками ML-модели. Если включен режим отображения индикаторов для всех тегов, то отображаются точки-индикаторы инцидентов, зарегистрированных всеми ветками ML-модели.

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 странице отобразятся графики заданного пресета для выбранного интервала времени.

Настройка параметров отображения графиков в разделе Мониторинг

Kaspersky MLAD позволяет настроить параметры отображения графиков пресетов в разделе **Мониторинг**.

Чтобы настроить параметры отображения графиков пресетов:

1. В основном меню выберите раздел **Мониторинг**.
2. На открывшейся странице нажмите на кнопку настройки , которая расположена в верхней части экрана.

   Справа появится панель **Параметры отображения графиков**.
3. В раскрывающемся списке **Высота графиков** выберите одно из следующих значений: 55 px, 110 px, 145 px, 190 px.

   По умолчанию параметр **Высота графиков** имеет значение 55 px.
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, с помощью переключателя **Отображать графики наблюдений в выбранном цвете** включите отображение графиков наблюдений тегов в определенном цвете и в поле **Цвет графиков наблюдений** выберите цвет.
6. Если требуется, с помощью переключателя **Отображать графики предсказаний в выбранном цвете** включите отображение графиков предсказаний тегов в определенном цвете и в поле **Цвет графиков предсказаний** выберите цвет.
7. Если требуется, с помощью переключателя **Имя и описание тега** включите отображение имени и описания тега на графиках.
8. Если требуется, с помощью переключателя **Предсказанное значение тега** включите отображение на графиках прогнозируемого значения тега и значений, полученных в результате работы диагностических правил.

9. Если требуется, с помощью переключателя **Персональная ошибка тега** включите отображение персональной ошибки тега на графиках.

10. Если требуется, с помощью переключателя **Отображать индикаторы для всех инцидентов** включите отображение точек-индикаторов инцидентов, зарегистрированных всеми ветками ML-модели.

    Если этот режим выключен, то будут отображаться только точки-индикаторы для инцидентов, которые были зарегистрированы выбранными ветками ML-модели.

11. Если требуется отображать установленные технические пределы для тега 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 режим выключен, то технические пределы будут отображаться, только если значение тега достигло соответствующего предела в отображаемой на экране области графика.

12. Если требуется, с помощью переключателя **Дополнительные пороговые линии** включите отображение дополнительных пороговых линий на графике.

13. Нажмите на кнопку **Закрыть** для возвращения к просмотру графиков в разделе **Мониторинг**.

Установленные параметры отображения графиков 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 прогнозов и регистрации инцидентов. Вы можете выбрать необходимый пресет в раскрывающемся списке. В список входят пресеты, которые можно создать в разделе **Пресеты**. Для каждого тега, входящего в выбранный пресет, поступающие значения отображаются в виде графика. Вы можете настроить отображение графиков, выбрать интервал времени для просмотра данных, а также выбрать ветку определенной ML-модели, чтобы просмотреть результаты работы этой ветки: предсказанные детектором Forecaster значения тегов и их ошибки или значения, полученные в результате работы диагностических правил.

В нижней части страницы расположен блок, отображающий *суммарную среднеквадратичную ошибку MSE* (далее также "ошибка MSE" или "суммарная ошибка"), а также количество зарегистрированных инцидентов (цветные точки-индикаторы). Оранжевая линия отображает порог MSE, при превышении которого Kaspersky MLAD регистрирует инцидент.

В зависимости от выбранного масштаба времени и плотности инцидентов одна точка-индикатор может соответствовать одному или нескольким близко расположенным инцидентам, зарегистрированным одним или несколькими разными детекторами. Цвет точек-индикаторов соответствует цвету ветки ML-модели, с помощью которой был зарегистрирован инцидент. Для точек-индикаторов, которые соответствуют группе инцидентов, зарегистрированных разными ветками, а также для инцидентов, зарегистрированных детектором Limit Detector зарезервированы специальные цвета.

Для инцидентов, зарегистрированных детектором Rule Detector, значение ошибки MSE будет отсутствовать. При анализе таких инцидентов требуется обращать внимание на маркер срабатывания правила (цветная точка-индикатор) ниже графика ошибки MSE для выбранной ветки ML-модели.

Раздел **История**

Просмотр исторических данных для определенного пресета

Kaspersky MLAD позволяет выбирать пользовательские пресеты, для которых отображаются исторические данные. Вы также можете просмотреть информацию о динамическом пресете Tags for event #N, если вы перешли в раздел **История** из раздела **Инциденты** нажатием на значение даты регистрации инцидента. Динамический пресет Tags for event #N содержит теги, оказавшие наибольшее влияние на формирование зарегистрированного 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.

Вы можете просматривать всю историю данных, используя навигацию по времени. Если необходимо, вы можете изменить дату и интервал времени. Также вы можете изменить состав тегов в пресете, создать новый пресет или выбрать определенную ветку ML-модели.

Выбор определенной ветки ML-модели в разделе История

В разделе **История** доступна история поступивших данных, результат их обработки Kaspersky MLAD с формированием прогнозов и регистрацией инцидентов.

Если для объекта мониторинга используется ML-модель, которая имеет несколько элементов для обработки данных, Kaspersky MLAD позволяет выбрать определенную ветку ML-модели для отображения результатов работы соответствующего элемента модели:

- Для ветки ML-модели, в основе которой лежит детектор Forecaster, результаты работы отображаются в виде предсказанных значений для отдельных тегов, индивидуальных ошибок предсказания отдельных тегов, а также общей ошибки MSE и точек-индикаторов инцидентов, зарегистрированных детектором.

- Для ветки ML-модели, в основе которой лежит детектор Rule Detector, результаты работы представлены в виде значений, полученных в результате работы диагностических правил, и точек-индикаторов инцидентов.

- Для детектора Limit Detector ветка 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 тегов.

Для отображения предсказанных значений тега на графиках в разделе **История**, а также для вывода значений, полученных в результате работы диагностических правил, требуется настроить отображение графиков.

Чтобы просмотреть результаты работы определенной ветки ML-модели:

1. В основном меню выберите раздел **История**.

2. На открывшейся странице в раскрывающемся списке **Ветка модели** установите флажки около нужных веток ML-модели.

   Имена выбранных веток отобразятся в поле.

   Ветки, которые относятся к используемой в текущий момент ML-модели, расположены в верхней части списка. В нижней части списка отображаются ветки других неиспользуемых в текущий момент ML-моделей, которые загружены в Kaspersky MLAD. Ветка ML-модели отображается в раскрывающемся списке только после того, как в Kaspersky MLAD появятся данные, полученные в результате ее работы.

   На графиках выбранного пресета отобразятся предсказанные значения тегов или значения, полученные в результате работы диагностических правил, в зависимости от типа детектора в выбранной ветке ML-модели.

   Если требуется скрыть отображение результатов работы выбранных ранее веток ML-модели, снимите флажки около этих веток (одна из веток должна остаться активной для отображения графиков в разделе **История**).

3. Если требуется отображать ошибку MSE, которая получена в результате обработки данных определенной веткой ML-модели, выполните следующие действия:

   a. Нажмите на кнопку настройки , которая расположена под графиками тегов в левой части страницы.

   b. В появившейся справа панели **Параметры отображения графиков MSE** в раскрывающемся списке **Ветка модели** выберите ветку. Вы можете выбрать только одну ветку ML-модели из списка.

   c. Нажмите на кнопку **Закрыть**.

   На графике ошибки MSE отобразятся значения ошибки MSE для выбранной ветки ML-модели.

В нижней части графика отображаются точки-индикаторы инцидентов, зарегистрированных выбранными ветками ML-модели. Если включен режим отображения индикаторов для всех тегов, то отображаются точки-индикаторы инцидентов, зарегистрированных всеми ветками ML-модели.

Выбор даты и интервала времени в разделе История

Kaspersky MLAD позволяет выбирать 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 значок календаря () и в открывшемся окне выберите дату и время, на которое 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 новые дату и время (точку) на графике, нажмите на значок местоположения (), который расположен слева от оси времени, и выберите на оси времени нужную точку.

   Выбранная точка станет новым центром графика. Вертикальная синяя пунктирная линия будет указывать на новые 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 значок выбора интервала (), который расположен слева от оси времени, выберите на оси времени нужный интервал и нажмите на . Если требуется еще раз изменить масштаб, повторите это действие.

На графиках заданного пресета отобразятся значения тегов 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 значков стрелки влево (<) и стрелки вправо (>), 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 графиков пресетов в разделе **История**.

Чтобы настроить параметры отображения графиков пресетов:

1. В основном меню выберите раздел **История**.
2. На открывшейся странице нажмите на кнопку настройки , которая расположена в верхней части экрана.

   Справа появится панель **Параметры отображения графиков**.
3. В раскрывающемся списке **Высота графиков** выберите одно из следующих значений: 55 px, 110 px, 145 px, 190 px.

   По умолчанию параметр **Высота графиков** имеет значение 55 px.
4. Если требуется, с помощью переключателя **Отображать графики наблюдений в выбранном цвете** включите отображение графиков наблюдений тегов в определенном цвете и в поле **Цвет графиков наблюдений** выберите цвет.
5. Если требуется, с помощью переключателя **Отображать графики предсказаний в выбранном цвете** включите отображение графиков предсказаний тегов в определенном цвете и в поле **Цвет графиков предсказаний** выберите цвет.
6. Если требуется, с помощью переключателя **Имя и описание тега** включите отображение имени и описания тега на графиках.
7. Если требуется, с помощью переключателя **Предсказанное значение тега** включите отображение на графиках прогнозируемого значения тега и значений, полученные в результате работы диагностических правил.

8. Если требуется, с помощью переключателя **Персональная ошибка тега** включите отображение персональной ошибки тега на графиках.

9. Если требуется, с помощью переключателя **Отображать индикаторы для всех инцидентов** включите отображение точек-индикаторов инцидентов, зарегистрированных всеми ветками ML-модели.

   Если этот режим выключен, то будут отображаться только точки-индикаторы для инцидентов, которые были зарегистрированы выбранными ветками ML-модели.

10. Если требуется отображать установленные технические пределы для тега 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 режим выключен, то технические пределы будут отображаться, только если значение тега достигло соответствующего предела в отображаемой на экране области графика.

11. Если требуется, с помощью переключателя **Дополнительные пороговые линии** включите отображение дополнительных пороговых линий на графике.

12. Нажмите на кнопку **Закрыть** для возвращения к просмотру графиков в разделе **История**.

Установленные параметры отображения графиков пресетов в разделе **История** будут применены.

Просмотр данных в разделе Временной срез

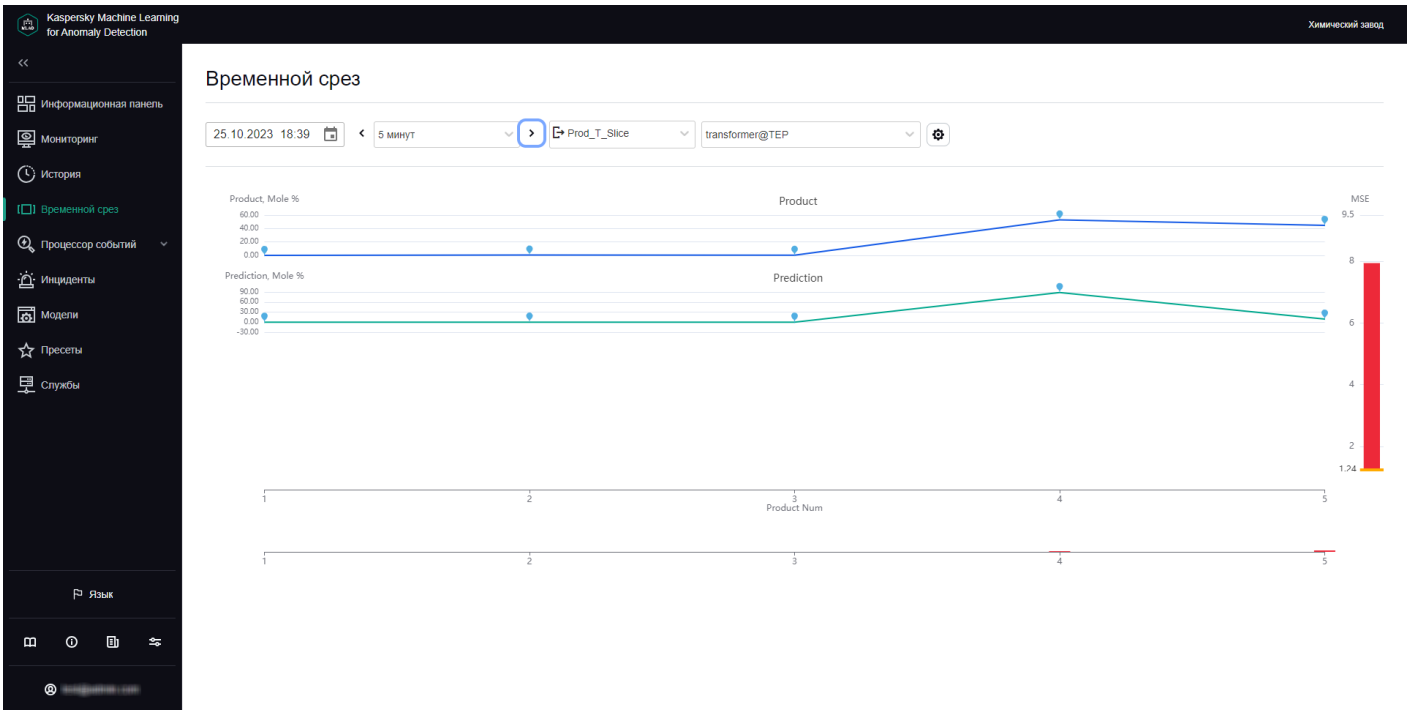
В разделе **Временной срез** вы можете просматривать значения технологических параметров, полученные от датчиков объекта мониторинга в один и тот же момент времени. Датчики должны быть однотипными (иметь одинаковую размерность) и расположены в пространстве линейно, например, датчики давления в трубе 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 MSE.

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 предсказываемых значениях тегов, индивидуальных ошибках предсказания, 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 персональные ошибки тегов пресета, полученные в результате обработки данных выбранным элементом ML-модели.



Раздел **Временной срез**

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 ветку ML-модели. Также вы можете изменить состав отображаемых тегов, изменив пресет.

Выбор определенной ветки ML-модели в разделе Временной срез

Если для объекта мониторинга используется ML-модель, которая имеет несколько веток для обработки и предсказания данных, Kaspersky MLAD позволяет выбрать определенную ветку ML-модели для отображения в разделе **Временной срез** персональных ошибок тегов, полученных в результате работы этой ветки.

Чтобы просмотреть персональные ошибки тега, полученные в результате обработки данных определенной веткой ML-модели:

1. В основном меню выберите раздел **Временной срез**.
2. На открывшейся странице в раскрывающемся списке **Ветка модели** выберите нужную ветку ML-модели.

   Имя выбранной ветки отобразится в поле.

На графиках тегов выбранного пресета отобразятся персональные ошибки тегов, полученные в результате обработки данных выбранной веткой ML-модели.

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 значок календаря (📅) и в открывшемся окне выберите дату и время, для которых требуется отображать данные на графиках.
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 значков стрелки влево (<) и стрелки вправо (>), 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 настройки , которая расположена в верхней части экрана.

   Справа появится панель **Параметры отображения графиков**.
3. В раскрывающемся списке **Высота графиков** выберите одно из следующих значений: 55 px, 110 px, 145 px, 190 px.

   По умолчанию параметр **Высота графиков** имеет значение 55 px.
4. Нажмите на кнопку **Закрыть** для возвращения к просмотру графиков.

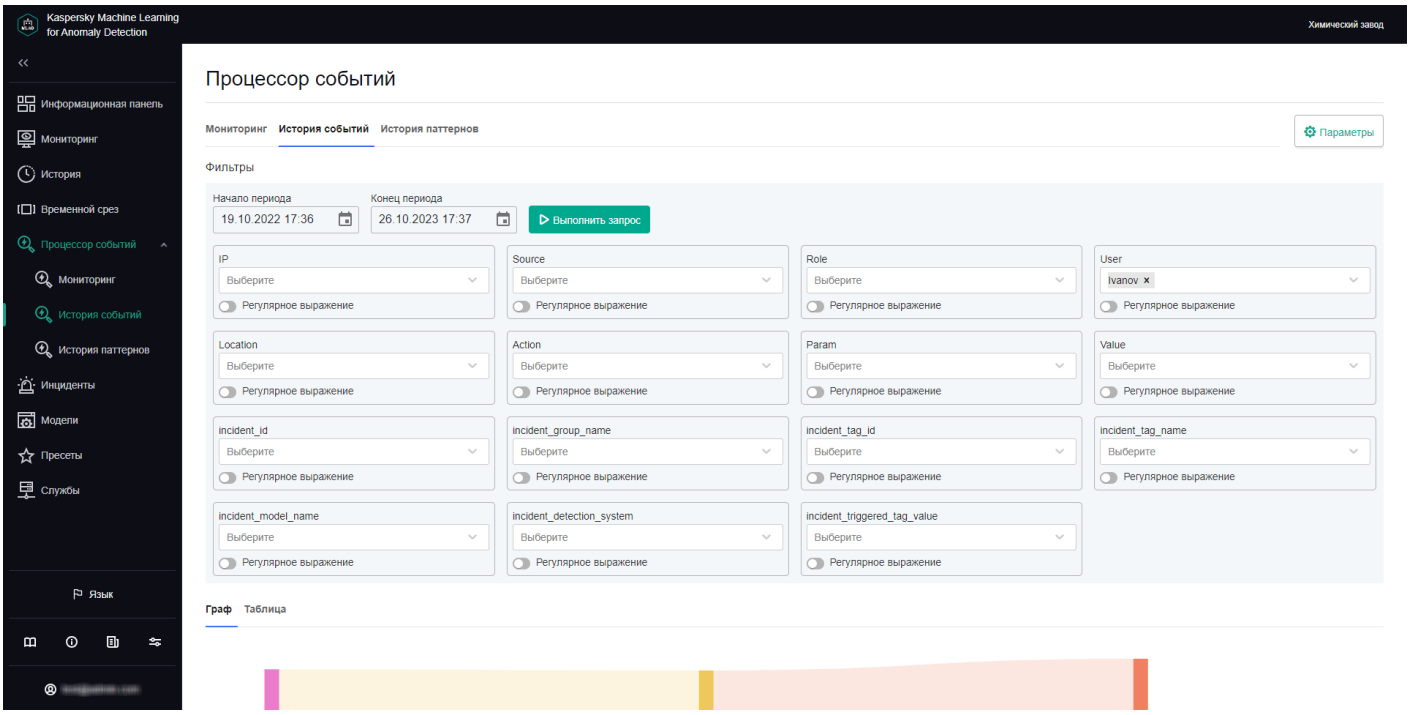
Установленные параметры отображения графиков будут применены.

Работа с событиями и паттернами

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 настраивать 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.

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**

Настройка параметров в разделе Процессор событий

Перед обработкой событий службой Event Processor требуется настроить параметры конфигурации внимания и отображение параметров событий.

Управление параметрами конфигурации внимания и отображением параметров событий доступно системным администраторам.

Большое количество направлений внимания может привести к замедлению работы основных служб Kaspersky MLAD (прием данных, обнаружение аномалий, работа веб-интерфейса). Для уточнения количества направлений внимания рекомендуется проконсультироваться со специалистом "Лаборатории Касперского" или сертифицированным интегратором.

Чтобы настроить параметры конфигурации внимания и отображение параметров событий:

1. В основном меню выберите раздел **Процессор событий** → **Мониторинг**.
2. На открывшейся странице нажмите на кнопку **Параметры**.

   Справа появится панель **Параметры процессора событий**.
3. В блоке **Настройка конфигурации внимания** для каждого параметра события, выполните одно из следующих действий:

   - Если требуется регистрировать паттерны по всем значениям параметра события, в раскрывающемся списке выберите **Все значения параметра**.
   - Если требуется регистрировать паттерны по конкретному значению параметра события, в раскрывающемся списке выберите значение параметра. Начните вводить нужное значение, чтобы все подходящие значения параметров отобразились в списке.

Если значение параметра отсутствует в списке, введите нужное значение и выберите **Создать значение: <значение параметра события>**.

- Если требуется регистрировать паттерны по шаблону значения параметра событий, включите переключатель **Регулярное выражение** для нужного параметра события, в раскрывающемся списке введите шаблон значения с помощью регулярного выражения и выберите **Регулярное выражение: <шаблон значения>**.

  Для поиска паттернов с помощью регулярных выражений вы можете использовать специальные символы регулярных выражений.

Каждое направление внимания задается значением параметра, которое должно присутствовать во всех событиях этого направления. При настройке направлений внимания вы можете указать определенные значения или шаблоны значений одного или нескольких параметров или задать направления внимания для всех возможных значений одного либо нескольких параметров.

4. Если требуется настроить отображение фильтров параметров событий в блоке **Фильтры** на вкладках **История событий** и **История паттернов**, в блоке **Настройка отображения фильтров параметров событий** установите флажки рядом с названиями нужных параметров событий.

   По умолчанию в блоке **Настройка отображения фильтров параметров событий** 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**, в процессор событий поступают события со следующими параметрами:

   - **incident_detection_system** – название детектора, который зарегистрировал инцидент.
   - **incident_model_name** – название используемой ML-модели.
   - **incident_tag_name** – имя тега, поведение которого привело к регистрации инцидента.
   - **incident_group_name** – название 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 нужный параметр события вверх или вниз в блоке **Настройка отображения фильтров параметров событий**, удерживая за название параметра события.

5. Нажмите на кнопку **Применить** для сохранения внесенных изменений.

Работа с мониторами

Управление мониторами доступно системным администраторам.

В разделе **Процессор событий** → **Мониторинг** вы можете создавать мониторы для отслеживания определенных событий, паттернов или значений параметров событий.

На вкладке **Мониторинг** отображаются все созданные в программе мониторы со следующей краткой информацией:

- Название монитора.
- **Порог монитора**.

  Количество активаций монитора на скользящем окне, при достижении которого программа отправляет оповещение об активации монитора во внешнюю систему.

- Скользящее окно, за время которого ведется учет количества активаций монитора.
- Количество активаций монитора на скользящем окне.

При необходимости вы можете просмотреть **подробную информацию о каждом мониторе**, нажав в таблице на кнопку **Информация**, которая расположена рядом с названием необходимого монитора.

- **ID монитора** – идентификатор просматриваемого монитора.
- **Количество активаций на скользящем окне** – количество зарегистрированных активаций монитора на скользящем окне.
- **Дата и время последней активации** – дата и время, когда монитор в последний раз был активирован.
- **Активирован** – тип элемента, который вызвал активацию монитора. Активация монитора может быть вызвана новым или существующим значением параметра события, событием, паттерном, а также другим монитором.
- **Подписка** – параметр, определяющий что отслеживает просматриваемый монитор: значения параметров событий, события или паттерны.
- **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** – количество активаций, которое должен зарегистрировать монитор на скользящем окне, прежде чем отправить во внешнюю систему оповещение об активации монитора с помощью коннектора CEF Connector.
- **Фильтры** – таблица, содержащая информацию о фильтрах для параметров событий, по которым текущий монитор отслеживает значения параметров событий, события и паттерны. Для каждого элемента отображаются следующие данные:
  - **Имя параметра** – названия параметров события, за значениями которых наблюдает просматриваемый монитор.
    Для каждого объекта мониторинга поступающие события и их параметры индивидуальны. Названия 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** – параметр, определяющий какие типы значений отслеживает просматриваемый монитор: определенные, новые или все значения.
  - **Назначение** – параметр, определяющий на каких параметрах событий сфокусировано внимание модели.
  - **Значения** – значения параметров события, за которыми наблюдает просматриваемый монитор.
- **Размер стека** – параметр, величина которого определяет количество последних активаций монитора, отображаемых в таблице **Стек активаций**.
- **Стек активаций** – таблица, содержащая информацию о последних активациях монитора:
  - **ID значения параметра** – идентификатор значения параметра события, обнаружение которого вызвало активацию монитора. Этот параметр отображается только при активации монитора значением параметра события.
  - **ID события** – идентификатор события, обнаружение которого вызвало активацию монитора. Этот параметр отображается только при активации монитора событием.

- **ID паттерна** – идентификатор паттерна, обнаружение которого привело к активации монитора. Этот параметр отображается только при активации монитора паттерном.

- **Системные параметры** – блок системных параметров, который содержит следующую информацию:

  - **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 при активации монитора событием или значением параметра события.

- **Дата и время активации** – дата и время активации монитора. Этот параметр отображается только при активации монитора паттерном.

- **Параметр события** – значение параметра события, поступившего от объекта мониторинга. Этот параметр отображается только при активации монитора значением параметра события.

- **Параметры события** – значения параметров события, поступившего от объекта мониторинга. Этот параметр отображается только при активации монитора событием.

- **События** – количество событий, входящих в состав паттерна, который вызвал активацию монитора. Этот параметр отображается только при активации монитора паттерном.

Вы можете просмотреть информацию о событиях, входящих в состав паттерна, нажав на количество событий в нужной строке таблицы. При нажатии на количество событий отображается информация об идентификаторах, системных параметрах и параметрах событий, входящих в состав выбранного паттерна.

На вкладке **Гистограмма** вы также можете посмотреть краткую статистику количества зарегистрированных активаций по каждому созданному монитору.

Создание монитора

Управление мониторами доступно системным администраторам.

Чтобы создать монитор:

1. В основном меню выберите раздел **Процессор событий → Мониторинг**.

2. Нажмите на кнопку **Создать монитор**.

   Справа появится панель **Создание монитора**.

3. В поле **Название** укажите имя монитора.

4. 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.

5. В поле **Порог** укажите количество активаций монитора на скользящем окне, после достижения которого монитор отправит оповещение во внешнюю систему.

6. В поле **Размер стека** укажите количество активаций монитора, которое требуется отображать при просмотре информации о мониторе.

7. В раскрывающемся списке **Тип подписки** выберите одно из следующих значений:

   - Если требуется обрабатывать данные по значениям параметров событий, выберите **Значения параметров**.
   - Если требуется обрабатывать данные по событиям, выберите **События**.
   - Если требуется обрабатывать данные по обнаруженным паттернам, выберите **Паттерны**.

8. Если требуется отслеживать новые события, паттерны или значения параметров событий, в блоке **Фильтры** включите переключатель **Только новые**.

9. Для фокусировки внимания модели на определенные направления развития событий, выполните одно из следующий действий:

   - Если вы выбрали **События** в раскрывающемся списке **Тип подписки**, выберите **Внимание** для нужного параметра события. Если требуется отслеживать события без указания направления внимания, снимите флажок **Внимание**.
   - Если вы выбрали **Паттерны** в раскрывающемся списке **Тип подписки**, установите флажок **Внимание** для нужного параметра события.

   Вы можете выбрать только одно направление внимания.

10. Для каждого параметра события, выполните одно из следующих действий:

    - Если требуется обрабатывать данные по всем значениям параметра события, в раскрывающемся списке выберите **Все значения параметра**.

      Этот пункт отображается, если вы указали направление внимания для текущего параметра события.

    - Если требуется обрабатывать данные только по новым значениям параметра события, в раскрывающемся списке выберите **Новые значения параметра**.

      Этот пункт отображается только при включенной функции **Только новые** для обработки данных по событиям.

    - Если требуется обрабатывать данные по конкретному значению параметра события, в раскрывающемся списке выберите значение параметра события. Начните вводить нужное значение, чтобы все подходящие значения параметров отобразились в списке.

Если значение параметра отсутствует в списке, введите нужное значение и выберите **Создать значение: <значение параметра события>**.

- Если требуется обрабатывать данные по шаблону значения параметра событий, включите переключатель **Регулярное выражение** для нужного параметра события, в раскрывающемся списке введите шаблон значения с помощью регулярного выражения и выберите **Регулярное выражение: <шаблон значения>**.

  Для поиска паттернов с помощью регулярных выражений используйте специальные символы регулярных выражений.

11. Нажмите на кнопку **Создать**.

Новый монитор будет создан и отобразится на вкладке **Мониторинг**.

Удаление монитора

Управление мониторами доступно системным администраторам.

Чтобы удалить монитор:

1. В основном меню выберите раздел **Процессор событий** → **Мониторинг**.
2. Нажмите на кнопку **Удалить** в ячейке того монитора, информацию о котором вы хотите удалить, и подтвердите свои действия.

Монитор будет удален.

Просмотр истории событий

Kaspersky MLAD позволяет просматривать события, которые поступили от внешних источников событий. Для просмотра событий требуется загрузить их в разделе **Процессор событий** → **История событий**.

Просмотр истории событий доступен системным администраторам.

Kaspersky MLAD 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.

Вы также можете просмотреть **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.
  - **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, поступивших от объекта мониторинга.

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 **Фильтры** выберите даты и время начала и окончания периода, за который вы хотите загрузить и просмотреть события, нажав на значок календаря (). Для настройки параметров событий выполните одно из следующих действий:
   - Если вы хотите загрузить события 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 загрузить события по шаблону значений, включите переключатель **Регулярное выражение** для нужных параметров события, в раскрывающихся списках введите шаблон значения с помощью регулярного выражения и выберите **Регулярное выражение: <шаблон значения>**.

     Для поиска с помощью регулярных выражений используйте специальные символы регулярных выражений.

   Для каждого объекта мониторинга количество и наименование параметров событий индивидуально.
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 найти и просмотреть структуру устойчиво повторяющихся и/или новых паттернов. Процессор событий формирует паттерны только по определенным направлениям, которые задаются в конфигурации внимания системным администратором.

Просмотр истории паттернов доступен системным администраторам.

Вы также можете просмотреть 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 **Фильтры** настройте следующие параметры отображения паттернов на странице:
   a. В поле **Начало периода** нажмите на значок календаря () и в открывшемся окне выберите дату и время начала периода, за который вы хотите просматривать паттерны.
   b. В поле **Конец периода** нажмите на значок календаря () и в открывшемся окне выберите дату и время окончания периода, за который вы хотите просматривать паттерны.
   c. 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.
   d. Для просмотра паттернов по определенному направлению внимания, выберите **Внимание** для нужного параметра события.

      Требуется выбрать одно из направлений внимания, заданных при настройке конфигурации внимания.
   e. 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, включите переключатель **Регулярное выражение** для нужных параметров события, в раскрывающихся списках введите шаблон значения с помощью регулярного выражения и выберите **Регулярное выражение: <шаблон значения>**.

Для поиска с помощью регулярных выражений используйте специальные символы регулярных выражений.

Для корректного выполнения запроса требуется ввести значения для параметра события, на котором сфокусировано внимание модели. Если в параметре события, на котором сфокусировано внимание, задано несколько значений параметра события, процессор событий сформирует паттерны для каждого значения параметра.

3. Нажмите на кнопку **Выполнить запрос**.

   В центральной части страницы отобразится таблица, которая содержит **данные о зарегистрированных паттернах**.

   - **ID паттерна** – идентификатор паттерна. Первая цифра идентификатора паттерна 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. Первая цифра идентификатора паттерна соответствует номеру слоя, на котором этот паттерн был обнаружен.
- **Количество событий** – количество событий, составляющих паттерн.
- **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.
- **Общее количество активаций** – количество обнаружений выбранного паттерна в потоке событий за заданный период.
- **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:
  - **<номер слоя> слой** – вкладки, позволяющие просматривать информацию о паттернах, входящих в состав выбранного паттерна на разных слоях его структуры. Вкладки отображаются, если вы выбрали паттерн, обнаруженного на четвертом слое и выше. Вы можете просматривать паттерны до второго уровня вложенности.
  - **ID паттерна** – идентификатор вложенного паттерна. Первая цифра идентификатора паттерна 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:

- **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 таблицу вложенных паттернов на определенном уровне вложенности, на вкладке **Паттерны** блока **Вложенные элементы** выберите нужный слой.

- Если требуется просмотреть события, составляющие паттерн на текущем уровне вложенности, нажмите на вкладку **События**.

Kaspersky MLAD отображает структуру паттерна с верхнего уровня вложенности.

Работа с инцидентами и группами инцидентов

В Kaspersky MLAD в составе ML-модели одновременно могут использоваться несколько типов детекторов, которые анализируют поступающие данные телеметрии и обнаруживают инциденты независимо друг от друга. Веб-интерфейс Kaspersky MLAD предоставляет возможность исследования обнаруженных инцидентов. В зависимости от типа детектора, зарегистрировавшего инцидент, информация об инциденте и методы его исследования могут отличаться.

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 замечание или экспертное заключение 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.

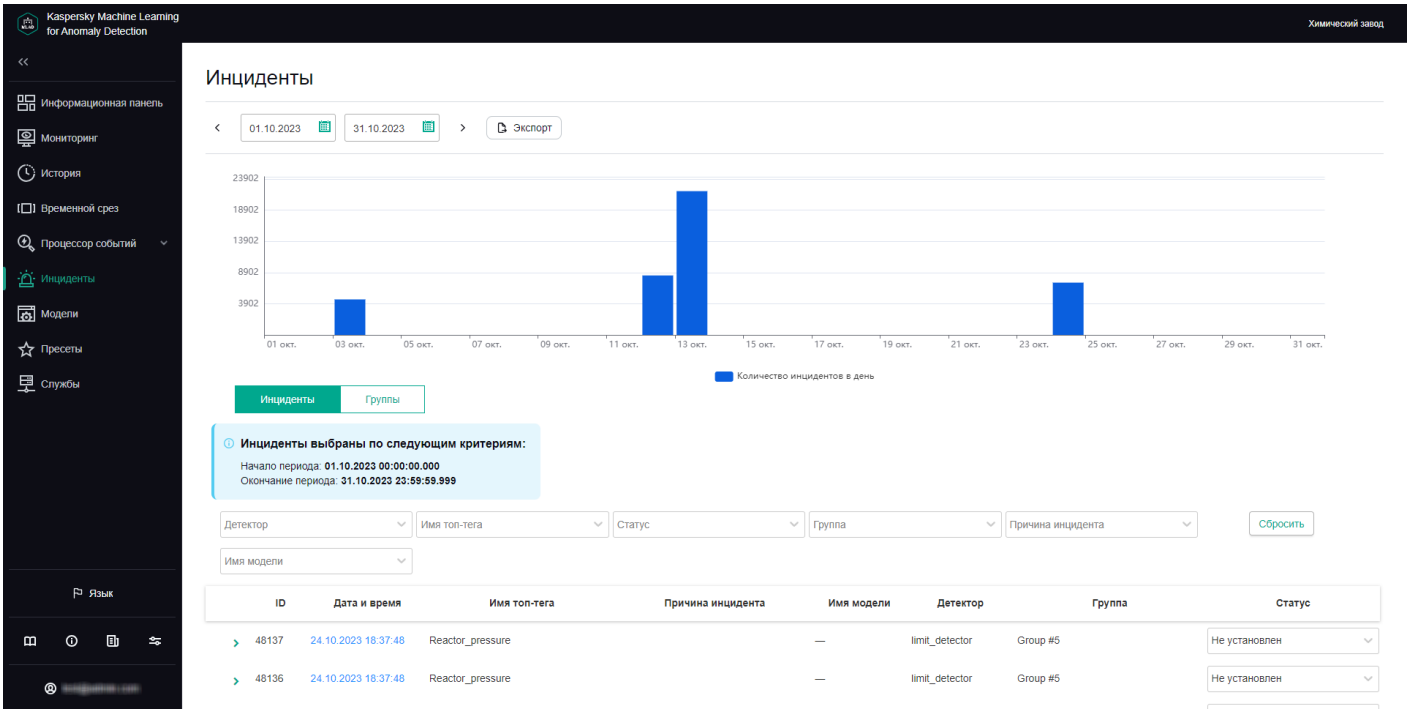
Диаграмма может отображать не более 60 столбцов. Если длительность заданного периода не превышает 60 дней, то инциденты на диаграмме сгруппированы по дням. Если длительность заданного периода составляет от 60 дней до 60 недель, то инциденты на диаграмме сгруппированы по неделям. В случае, когда длительность 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.



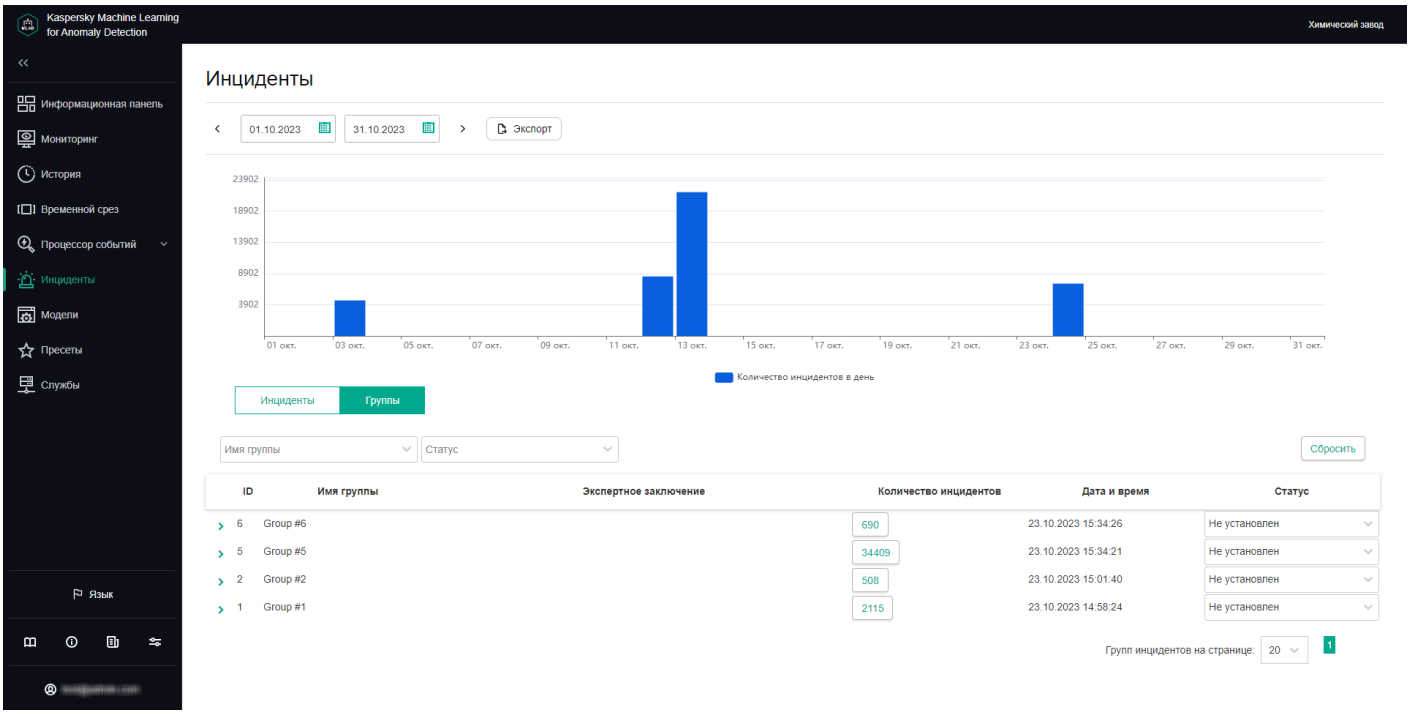
Вкладка **Инциденты**

Вы можете перейти в раздел **История**, нажав на дату и время инцидента.

Вкладка Группы

На вкладке **Группы** представлена таблица групп инцидентов. Kaspersky MLAD автоматически формирует группы похожих инцидентов.

Вы можете изменить имя группы, присвоенное автоматически, и установить статус инцидентов, которые входят в эту группу. Также вы можете указать экспертное заключение, содержащее, например, рекомендуемые действия при возникновении новых инцидентов в этой группе.



Вкладка **Группы**

Сценарий: анализ инцидентов

В этом разделе приводится последовательность действий, которые требуется выполнить при анализе зарегистрированных Kaspersky MLAD инцидентов.

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 регистрации, детекторе, который зарегистрировал инцидент, и экспертное заключение, если оно было добавлено. 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** нажмите на дату и время интересующего вас инцидента в таблице **Последние инциденты**. В открывшемся разделе **История** в нижней части страницы нажмите на точку-индикатор в блоке *ошибки MSE* для просмотра определенного инцидента. Откроется раздел **Инциденты**, в котором отобразятся только те инциденты, которые были зарегистрированы в период, представленный выбранной точкой-индикатором (период указан над таблицей инцидентов).

   - **Просмотр инцидентов в разделе Инциденты**

Если вам известны дата и время регистрации инцидента, выберите соответствующий инцидент в разделе **Инциденты**. Вы можете изменить интервал времени, в котором отображаются инциденты, используя столбчатую диаграмму или поле выбора даты в верхней части страницы.

- **Переход из уведомления об инциденте, поступившего по электронной почте**

  Если для вас было создано уведомление об инцидентах, при регистрации инцидента вы получите уведомление по электронной почте. Сообщение электронной почты содержит время начала инцидента, наиболее аномальный тег и ссылку для перехода в раздел **История** в веб-интерфейсе Kaspersky MLAD. Вы можете перейти по этой ссылке в раздел **История** в момент начала инцидента. В нижней части страницы раздела **История** нажмите на точку-индикатор в блоке ошибки MSE в соответствии с временем начала инцидента. Откроется раздел **Инциденты**, в котором отобразятся только те инциденты, которые были зарегистрированы в период, представленный выбранной точкой-индикатором (период указан над таблицей инцидентов).

Когда вы нашли запись об интересующем инциденте, нажмите на значок стрелки вправо (›) для просмотра подробной информации об инциденте.

2. **Просмотр информации о похожих инцидентах**

   При обнаружении двух и более похожих инцидентов Kaspersky MLAD автоматически объединяет их в группу. В таблице инцидентов в разделе **Инциденты** группа, к которой отнесен инцидент, отображается в столбце **Группа**. Если в этом столбце для выбранного инцидента ничего не указано, то Kaspersky MLAD к настоящему моменту не обнаружил для этого инцидента похожие.

   Для просмотра всех инцидентов группы выберите вкладку **Группы** и нажмите на значок стрелки вправо (›) рядом с нужной группой. В таблице отобразится информация об инцидентах, отнесенных к выбранной группе, а также экспертное заключение, если оно было добавлено. Ознакомьтесь с экспертными заключениями 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 детектора, который его зарегистрировал:

   - **Forecaster**. Нейросетевой элемент ML-модели регистрирует инциденты при обнаружении отклонений в поведении объекта мониторинга. Основываясь на информации, полученной при просмотре автоматически сформированного пресета Tags for event #N, 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 ошибки MSE, переместитесь назад по времени от момента достижения порога MSE и изучите поведение тегов в момент начала роста значений ошибки MSE.

   - **Rule Detector**. Для каждого инцидента, зарегистрированного элементов ML-модели на основе диагностического правила, автоматически формируется пресет Tags for event #N, в составе которого присутствует значение, полученное в результате работы диагностического правила и вызвавшее регистрацию инцидента.

   - **Limit Detector**. Для каждого инцидента, зарегистрированного детектором Limit Detector автоматически формируется пресет Tags for event #N, 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, экспертного заключения и замечания к инциденту или его группе**

Для каждого инцидента добавьте экспертное заключение или замечание, в которых вы можете указать, является ли инцидент аномалией. Экспертное заключение и замечание для инцидента отображаются только при просмотре определенного инцидента. Если требуется, вы можете указать статус и причину инцидента. Причина инцидента отображается в таблице инцидентов и при просмотре определенного инцидента. Вы также можете добавить или изменить статус и экспертное заключение для группы инцидентов.

Просмотр инцидентов

Чтобы просмотреть инциденты, зарегистрированные на конкретную дату:

1. В основном меню выберите раздел **Инциденты**.
2. В верхней части открывшейся страницы на столбчатой диаграмме нажмите на столбец диаграммы для нужной даты.
3. Если требуется, отфильтруйте инциденты по детектору, топ-тегу, статусу, группе или причине инцидентов, выбрав нужные значения в соответствующем раскрывающемся списке.

В таблице, расположенной в центральной области страницы, будут показаны инциденты, зарегистрированные в этот день 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 регистрации инцидента.

  Нажав на значение даты регистрации инцидента, вы перейдете в раздел **История**, где вы можете посмотреть информацию о пресете Tags for event #N, сформированного для зарегистрированного инцидента.
- **Имя топ-тега** – название параметра технологического процесса, для которого зафиксировано наибольшее отклонение от прогноза на момент регистрации инцидента.
- **Причина инцидента** – причина зарегистрированного инцидента, добавленная экспертом (технологом или специалистом АСУ ТП) по результатам анализа инцидента или заданная ML-моделью.
- **Имя модели** – имя ML-модели, элемент которой зарегистрировал инцидент.
- **Детектор** – название детектора, который определил аномалию и зарегистрировал инцидент: Forecaster, Limit Detector, Rule Detector, Stream Processor.
- **Группа** – название группы инцидентов, в которую входит зарегистрированный инцидент.

  Если обнаружены два или более похожих инцидента, то они объединяются в группу, которая создается автоматически с помощью службы Similar Anomaly. Вы можете просмотреть только те инциденты, которые входят в группу, выбрав название группы в раскрывающемся списке.
- **Статус** – статус зарегистрированного инцидента, указанный экспертом (технологом или специалистом АСУ ТП) по результатам анализа инцидента или заданный ML-моделью.

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.

Просмотр технических характеристик зарегистрированного инцидента

В разделе **Инциденты** вы можете просмотреть технические характеристики зарегистрированных инцидентов. Для этого нажмите на значок стрелки вправо (›) около нужного инцидента в таблице инцидентов. Для выбранного инцидента отобразятся следующие технические характеристики:

- **Инцидент** – блок, содержащий **информацию об инциденте**.
  - **Имя модели** – название используемой ML-модели.
  - **Ветка модели** – название ветки ML-модели. Отсутствует, если у ML-модели отсутствуют ветки.
  - **Детектор** – название детектора, который определил аномалию и зарегистрировал инцидент: Forecaster, Limit Detector, Rule Detector, Stream Processor.
  - **Значение MSE** – значение индивидуальной ошибки MSE.
  - **Пороговое значение** – пороговое значение MSE для используемой ветки ML-модели на момент регистрации инцидента.
- **Топ-тег** – блок, содержащий **информацию о теге**, для которого зарегистрирован инцидент.
  - **Имя топ-тега (ID топ-тега)** – название и идентификатор тега, поведение которого привело к регистрации инцидента.

    Если инцидент зафиксирован детектором Forecaster, отображается название наиболее аномального тега, который больше остальных повлиял на регистрацию инцидента. Для детектора Rule Detector в значении этого параметра отображается значение, полученное в результате работы диагностического правила. Для детектора 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** – пороги значений топ-тега, при достижении которых требуется принять экстренные меры реагирования на АСУ ТП.
  - **Описание** – описание топ-тега.
  - **Единицы измерения** – единицы 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 в Kaspersky MLAD 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.

- **Экспертное заключение** – поле для ввода экспертного заключения по анализу зарегистрированного инцидента. Это поле заполняет эксперт (технолог или специалист АСУ ТП).

- **Замечание** – поле для ввода комментария для выбранного инцидента. Если требуется, вы можете указать комментарий для инцидента.

Просмотр групп инцидентов

При обнаружении двух и более похожих инцидентов Kaspersky MLAD автоматически объединяет их в группу (с помощью службы Similar Anomaly). Это позволяет анализировать инциденты с учетом предыстории, а также использовать экспертные заключения, сделанные для аналогичных инцидентов. В таблице инцидентов в разделе **Инциденты** группа, к которой отнесен инцидент, отображается в столбце **Группа**. Если в этом столбце для инцидента ничего не указано, то Kaspersky MLAD к настоящему моменту не обнаружил для этого инцидента похожие. Инциденты могут быть перегруппированы, и при этом экспертные заключения, добавленные к этим инцидентам, мигрируют в новую группу. Имя группы присваивается автоматически – Group #N (N – порядковый номер группы). При необходимости вы можете изменить имя группы.

Чтобы просмотреть группы инцидентов,

в основном меню выберите раздел **Инциденты** и нажмите на **Группы**.

В таблице, расположенной в центральной части страницы, будут показаны все группы инцидентов для вашего объекта мониторинга.

Для каждой группы инцидентов в таблице, отображается следующая информация:

- **ID** – идентификатор группы инцидентов.

- **Имя группы** – название группы инцидентов.

- **Экспертное заключение** – заключение по анализу группы зарегистрированных инцидентов, добавленное 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**.

- **Дата и время** – дата и время создания группы инцидентов.

- **Статус** – статус зарегистрированных инцидентов в группе, указанный экспертом (технологом или специалистом АСУ ТП) по результатам анализа инцидентов.

  Вы можете установить статус группы инцидентов по результатам их анализа, 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.

Чтобы просмотреть подробную информацию о группе инцидентов:

1. Нажмите на значок стрелки вправо (>) около группы инцидентов.

   Отобразится список инцидентов, входящих в эту группу. Для каждого инцидента группы отображаются следующие технические характеристики:

   - **Дата инцидента** – дата и время регистрации инцидента.

     Вы можете перейти в раздел **История**, нажав на значение даты регистрации инцидента.

   - **Имя топ-тега** – название параметра технологического процесса, который оказал наибольшее влияние при возникновении инцидента.

   - **Значение топ-тега** – зарегистрированное значение тега, оказавшего наибольшее влияние при возникновении инцидента.

   - **Релевантные теги** – таблица, которая содержит идентификаторы тегов, оказавших влияние на определение похожих инцидентов и объединение таких инцидентов в группу.

2. Если требуется просмотреть степень влияния тега на формирование похожих инцидентов, нажмите на ячейку таблицы **Релевантные теги**, в которой содержится идентификатор нужного тега.

   Все ячейки таблицы, содержащие выбранный идентификатор тега, будут выделены зеленым цветом. Чем ближе к первому столбцу таблицы находятся выделенные зеленым цветом ячейки, содержащие идентификатор выбранного тега, тем большее влияние этот тег оказал на определение похожих инцидентов и объединение их в группу.

Также вы можете добавить статус и экспертное заключение для группы инцидентов.

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.

Исследование 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 было создано уведомление об инцидентах, вы можете перейти к инциденту по ссылке из уведомления электронной почты. Сообщение электронной почты содержит время начала инцидента, наиболее аномальный тег и ссылку для перехода в раздел **История** в веб-интерфейсе Kaspersky MLAD.

В разделе **История** Kaspersky MLAD отображает график тегов, полученных от объекта мониторинга, для которого зарегистрирован выбранный инцидент. На графике отображаются данные по пресету Tags for event #N (где N – идентификатор инцидента в разделе **Инциденты**), сформированному по дате и времени регистрации выбранного инцидента. В этот пресет входят теги, которые привели к регистрации инцидента. В зависимости от типа детектора, который зарегистрировал инцидент, это могут быть следующие теги:

- Теги, фактическое значение которых было признано ML-моделью наиболее аномальным, если инцидент был зарегистрирован детектором Forecaster.

- Теги, входящие в диагностическое правило, и значение, полученное в результате работы этого правила, если инцидент был зарегистрирован детектором Rule Detector.

- 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 регистрации инцидента на графике указывает вертикальная синяя пунктирная линия.

Пример графика тегов в разделе История

График тегов отображается в верхней части раздела **История**. В нижней части раздела **История** отображается график MSE.

График тегов в разделе **История**

2 Настройка параметров отображения данных на графике в разделе История

В разделе **История** вы можете включить отображение предсказанных значений тегов. Это позволяет оценить расхождение между фактическими и предсказанными значениями тегов. Также включенная функция отображения предсказанных значений позволяет просматривать значения, полученные в результате работы диагностических правил. Информация о теге (имя, числовой идентификатор, описание, единица измерения, время и значение тега) отображается при наведении указателя мыши на график тега. Также вы можете включить отображение имени и описания тега для каждого графика тега.

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 график тега отображался за более длительный период.

4. **Изменение вертикальных границ отображения данных в разделе История**

   Выбор вертикального масштаба каждого графика по умолчанию производится автоматически, исходя из минимального и максимального значений тега в отображаемой области. Вы можете контролировать масштаб графиков по шкале значений на вертикальной оси одним из следующих способов:

   - Если для тега установлены минимальное и максимальное допустимые значения (пороги блокировки), включите 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.

   - В свойствах тега установите допустимые границы отображения значений тега на графиках.

     Если значения тега будут выходить за указанные границы, то они не будут отображаться на графике тега. Допустимые границы отображения значений тега имеют приоритет над отображением порогов блокировки, даже если включена функция **Всегда показывать пороги блокировки**.

Добавление статуса, причины, экспертного заключения и замечания к инциденту или группе инцидентов

Kaspersky MLAD позволяет добавлять экспертное заключение или замечание к зарегистрированному инциденту.

Экспертное заключение, как правило, добавляет эксперт (технолог или специалист АСУ ТП), и оно может содержать анализ инцидента или рекомендации по устранению проблемы, на которую указывает выявленный инцидент. Экспертное заключение может быть добавлено как к инциденту, так и к группе инцидентов. При этом если сгруппированы инциденты, к которым ранее были добавлены экспертные заключения, то эти заключения отображаются и в группе (с привязкой к каждому конкретному инциденту). При перегруппировке инцидентов экспертное заключение для инцидента мигрирует вместе с инцидентом в новую группу.

Замечания предназначены для обсуждения между экспертами или операторами предпринятых по инциденту действий: анализ, расследование, исправление. В каждом замечании фиксируется информация о том, кто и когда его добавил.

Вы также можете добавить причину возникновения инцидента и статус инцидента, установленные экспертом по результатом анализа инцидента. 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.

Перед добавлением причины, статуса, замечания или экспертного заключения требуется провести анализ зарегистрированного инцидента.

Чтобы добавить экспертное заключение, статус, причину и замечание к инциденту:

1. В основном меню выберите раздел **Инциденты**.

2. При необходимости измените статус инцидента, выбрав в раскрывающемся списке **Статус** 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.

3. Для отображения подробных технических характеристик нажмите на значок стрелки вправо (›) около интересующего вас инцидента. В открывшейся области деталей вы можете выполнить следующие действия:

   - Если требуется добавить причину инцидента, в поле **Причина инцидента** выберите причину инцидента.

     При необходимости системный администратор может создать, изменить или удалить причины инцидентов.

   - Если требуется добавить экспертное заключение по анализу зарегистрированного инцидента, нажмите на значок **Изменить экспертное заключение** (), расположенную справа от поля **Экспертное заключение**, в появившемся поле введите заключение и нажмите на клавишу **ENTER**.

     Экспертное заключение будет добавлено к выбранному инциденту и отобразится в таблице инцидентов разделе **Инциденты**.

   - Если требуется добавить замечание к инциденту, в поле **Замечание** введите сообщение и нажмите на кнопку **Добавить замечание**.

     Вы можете указать сообщение длиной не более 512 символов.

Статус, причина, экспертное заключение и замечание будут добавлены к инциденту и будут доступны другим пользователям при просмотре этого инцидента.

При обнаружении двух и более похожих инцидентов Kaspersky MLAD автоматически объединяет их в группу. Имя группы присваивается также автоматически – Group #N (N – порядковый номер группы). Вы можете изменить название группы, а также изменить статус группы инцидентов и экспертное заключение, содержащее, например, рекомендации при анализе похожих инцидентов.

Чтобы добавить статус и экспертное заключение к группе инцидентов:

1. В основном меню выберите раздел **Инциденты** и нажмите на **Группы**.

2. При необходимости измените статус группы инцидентов, выбрав в раскрывающемся списке **Статус** один из следующих статусов: **Исследуется**, **Ожидается решение**, **Инструкции даны**, **Проблема закрыта**, **Причина неизвестна**, **Игнорировать** или **Ложное срабатывание**.

   При изменении статуса группы инцидентов Kaspersky MLAD изменяет статус инцидентов, входящих в эту группу. По умолчанию группе инцидентов присваивается статус **Не установлен**.

   Если требуется, системный администратор может создать, изменить или удалить статусы инцидентов.

3. В таблице групп инцидентов дважды нажмите на строку группы инцидентов.

   Откроется окно **Изменение группы**.

   Вы также можете перейти к изменению группы на вкладке **Инциденты**. Для этого выберите нужную группу в фильтре **Группа** и в блоке экспертного заключения для группы, отображающемся над таблицей инцидентов, нажмите на кнопку **Изменить**.

4. Если требуется изменить название группы инцидентов, в поле **Имя группы** введите новое название группы.

5. В поле **Экспертное заключение** введите текст экспертного заключения (например, рекомендации при анализе похожих инцидентов).

6. Нажмите на кнопку **Сохранить**.

Статус и экспертное заключение будут изменены для группы инцидентов и будут доступны для просмотра другим пользователям в таблице **Группы** в разделе **Инциденты**.

Экспорт инцидентов в файл

Вы можете сохранить в файл формата XLSX инциденты, зарегистрированные за определенный период в Kaspersky MLAD.

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.

ML-модели, шаблоны ML-моделей и разметки являются функциональными элементами иерархической структуры объекта мониторинга. Иерархическая структура отображается в виде дерева активов.

В Kaspersky MLAD ML-модели могут быть импортированы, созданы вручную, скопированы или созданы по шаблону. После добавления и обучения ML-модели в Kaspersky MLAD вы можете опубликовать ее. Вы также можете запустить исторический или потоковый инференс для обученной или опубликованной ML-модели, а также просмотреть граф потока данных в ML-модели.

В разделе **Модели** вы можете создавать разметки для формирования индикаторов обучения или индикаторов инференса. При необходимости вы можете изменять разметки и удалять их.

Сценарий: работа с ML-моделями

В этом разделе приводится последовательность действий, которые требуется выполнить при работе с ML-моделями.

Сценарий работы с ML-моделями состоит из следующих этапов:

1. **Добавление ML-модели**

   Вы можете добавить ML-модель в Kaspersky MLAD одним из следующих способов:

   - Загрузить ML-модель, созданную специалистами "Лаборатории Касперского" или сертифицированным интегратором в рамках *Услуги построения модели и внедрения Kaspersky MLAD*. После загрузки ML-

модели требуется ее активировать.

- Создать ML-модель вручную. Добавьте в созданную ML-модель нейросетевые элементы и/или элементы на основе диагностических правил.
- Создать ML-модель по шаблону. Предварительно создайте шаблон по нужной ML-модели. Если исходная ML-модель, по которой был создан шаблон, была создана вручную, вы можете добавить в новую ML-модель нейросетевые элементы и/или элементы на основе диагностических правил.
- Скопировать ранее добавленную ML-модель. При копировании ML-модели, которая была создана вручную или по шаблону на основе ML-модели, созданной вручную, вы можете добавить в скопированную ML-модель нейросетевые элементы и/или элементы на основе диагностических правил.

2. **Добавление разметок**

   Если требуется определить для ML-модели интервалы времени данных, на которых ML-модель может выполнять обучение или инференс, создайте разметки. Для формирования индикатора инференса укажите созданную разметку в параметрах соответствующей ML-модели.

3. **Обучение элементов ML-модели**

   Для проведения инференса ML-модель должна быть обучена. Для этого все нейросетевые элементы в составе ML-модели требуется предварительно обучить. Элементы на основе диагностических правил в составе ML-модели считаются обученными.

   ML-модель, загруженная 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 их обучения и переобучить нейросетевые элементы.

   Для формирования индикатора обучения укажите созданную разметку в параметрах обучения нейросетевого элемента.

4. **Подготовка ML-модели к публикации**

   После завершения обучения подготовьте ML-модель к публикации. ML-модель, подготовленная к публикации, недоступна для изменения.

5. **Публикация ML-модели**

   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. При необходимости системный администратор может создать роль, которой предоставлено право для публикации ML-моделей, и назначить ее нужному сотруднику.

6. **Запуск инференса ML-модели**

   Запустите инференс ML-модели. В процессе инференса ML-модель анализирует данные телеметрии и регистрирует инциденты.

   Инференс ML-модели может быть запущен как для опубликованной, так и для обученной ML-модели.

Работа с разметками

Этот раздел содержит информацию о работе с разметками.

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. Для формирования индикатора инференса вы можете выбрать ранее созданные разметки при создании или изменении параметров ML-модели. Для формирования индикатора обучения вы можете выбрать ранее созданные разметки при настройке параметров обучения нейросетевых элементов ML-модели.

Создание разметки

Вы можете использовать разметки для формирования индикаторов обучения или инференса ML-модели.

Чтобы создать разметку:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов рядом с названием актива, для которого требуется создать разметку, откройте вертикальное меню **...** и выберите пункт **Создать разметку**.

   Справа отобразится список параметров.
3. В поле **Название** укажите название 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 параметр **Интерпретировать невозможность оценки условия как выполнение правила** с помощью переключателя.

   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 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.

     Вы можете указать только начало или окончание однократного интервала.
   - **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.

   Вы можете добавить один или несколько временных интервалов.

9. Если требуется добавить критерии поведения тегов, выполните следующие действия:

a. В блоке параметров **Условия на теги** нажмите на кнопку **Условие**.

b. В раскрывающемся списке **Тег** выберите тег, для которого вы хотите добавить критерий поведения тега.

Если требуется исключить использование выбранного критерия поведения из добавляемого 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, в котором отсутствуют ступеньки с заданными параметрами.

c. 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.

d. В поле **Окно** укажите продолжительность интервала для анализа поведения тегов в шагах РИВС.

e. 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 минимальное количество выходов за пороговое значение в рамках отдельного окна в поле **Срабатывание**.
- 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 **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 параметр **Значение** не задан. Если значение параметра не задано, то любое повторяющееся значение тега вызывает срабатывание критерия.

- 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.

f. 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.

g. Если блок условий содержит более одного критерия поведения тегов, выберите один из следующих логических операторов между строками критериев:

- **AND**, если требуется отслеживать оба критерия в разметке.
- **OR**, если требуется отслеживать один из заданных критериев в разметке.

10. 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.

Предварительным условием называется блок условий, предшествующий темпоральному оператору. *Пост-условием* называется блок условий, следующий за темпоральным оператором.

Проверка блока предварительного условия проводится в текущем узле РИВС.

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 текущим узлом РИВС и первым будущим узлом РИВС, в котором будет выполняться проверка блока пост-условия (минимальный интервал ожидания).
- **до** – интервал между текущим узлом РИВС и последним будущим узлом РИВС, в котором будет выполняться проверка блока пост-условия (максимальный интервал ожидания).

Проверка блока 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 проверить выполнение критериев поведения тегов из блока пост-условия во всех узлах РИВС между минимальным и максимальным интервалом ожидания, выберите групповой

оператор **Все шаги**.

- Если требуется проверить выполнение критериев поведения тегов из блока 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 проверка блока предварительного условия в текущем узле РИВС дала отрицательный результат FALSE или неопределенный результат UNDEFINED, то это же значение будет результатом проверки блока пост-условия. Если проверка блока предварительного условия в текущем узле РИВС дала положительный результат TRUE, то проверка блока пост-условия проводится в каждом узле РИВС между минимальным и максимальным интервалом ожидания. Результат проверки определяется выполнением условия в зависимости от выбранного группового оператора (**Все шаги** или **Любой шаг**). 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.

11. Выберите один из следующих логических операторов между блоками разметки:

    - **AND**, если требуется отслеживать критерии поведения тегов в обоих блоках условий.
    - **OR**, если требуется отслеживать критерии поведения тегов только одного из блоков условий.

12. В правом верхнем углу окна 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.

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 появится панель с графиком разметки.
4. В раскрывающемся списке **Пресет** выберите необходимый пресет.
5. Если требуется, в поле **Разметки** выберите разметки для отображения интервалов данных.
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 значок **Новый центр графика** (), который расположен 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 значок **Новый интервал** (), который расположен слева от оси времени, выберите на оси времени нужный интервал и нажмите на кнопку **Применить**. Если требуется еще раз изменить масштаб, повторите это действие.

На графике отобразятся интервалы данных в цветах, заданных для выбранных разметок.

Изменение разметки

Вы можете изменить параметры разметки.

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. В поле **Название** укажите новое название разметки.
5. В поле **Описание** укажите новое описание разметки.
6. В поле **Шаг сетки (сек.)** укажите период РИВС в секундах в виде десятичной дроби для разметки.
7. В поле **Цвет разметки** выберите цвет, которым будут выделены интервалы данных, отобранные этой разметкой.

8. Если требуется, включите параметр **Интерпретировать невозможность оценки условия как выполнение правила** с помощью переключателя.

   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.

9. Если требуется изменить временные интервалы разметки в блоке параметров **Фильтрация по времени**, выполните следующие действия:

   a. 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.

        Вы можете указать только начало или окончание однократного интервала.

      - **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.

   b. Если требуется добавить интервал, нажмите на кнопку **Добавить интервал** и выполните шаг 9a.

   c. Если требуется удалить интервал, наведите курсор мыши на строку с нужным интервалом и нажмите на значок **Удалить интервал** (✕).

   Вы можете добавить один или несколько временных интервалов.

10. Если требуется изменить критерии поведения тегов, выполните следующие действия:

    a. В раскрывающемся списке **Тег** выберите тег, для которого вы хотите добавить критерий поведения тега.

       Если требуется исключить использование выбранного критерия поведения из добавляемого 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, в котором отсутствуют ступеньки с заданными параметрами.

    b. 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.

c. В поле **Окно** укажите количество шагов РИВС.

d. 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 минимальное количество выходов за пороговое значение в рамках отдельного окна в поле **Срабатывание**.

- 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 **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 параметр **Значение** не задан. Если значение параметра не задано, то любое повторяющееся значение тега вызывает срабатывание критерия.

- 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.

e. Если требуется добавить критерий поведения тегов в блок условий, нажмите на значок плюса в нижней части блока условий и повторите шаги с 10a по 10d.

f. Если блок условий содержит более одного критерия поведения тегов, выберите один из следующих логических операторов между строками критериев:

- **AND**, если требуется отслеживать оба критерия в разметке.

- **OR**, если требуется отслеживать один из заданных критериев в разметке.

g. Если требуется удалить критерий на поведение тегов из блока условий, наведите курсор мыши на строку с нужным критерием и нажмите на значок крестика (✕).

11. Если требуется изменить условия темпорального оператора **Пауза** и/или **Если далее**, выполните следующие действия:

a. В поле **Продолжительность (шаги)** укажите следующие интервалы ожидания:

- **от** – интервал между текущим узлом РИВС и первым будущим узлом РИВС, в котором будет выполняться проверка блока пост-условия (минимальный интервал ожидания).

- **до** – интервал между текущим узлом РИВС и последним будущим узлом РИВС, в котором будет выполняться проверка блока пост-условия (максимальный интервал ожидания).

Проверка блока пост-условия проводится в узлах РИВС между минимальным и максимальным интервалом ожидания.

b. В раскрывающемся списке **Проверить** выберите один из следующих групповых операторов:

- Если требуется проверить выполнение критериев поведения тегов из блока пост-условия во всех узлах РИВС между минимальным и максимальным интервалом ожидания, выберите групповой оператор **Все шаги**.

- Если требуется проверить выполнение критериев поведения тегов из блока 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 проверка блока предварительного условия в текущем узле РИВС дала отрицательный результат FALSE или неопределенный результат UNDEFINED, то это же значение будет результатом проверки блока пост-условия. Если проверка блока предварительного условия в текущем узле РИВС дала положительный результат TRUE, то проверка блока пост-условия проводится в каждом узле РИВС между минимальным и максимальным интервалом ожидания. Результат проверки определяется выполнением условия в зависимости от выбранного группового оператора (**Все шаги** или **Любой шаг**). 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:

- **AND**, если требуется отслеживать критерии поведения тегов в обоих блоках условий.

- **OR**, если требуется отслеживать критерии поведения тегов только одного из блоков условий.

13. В правом верхнем углу окна нажмите на кнопку **Сохранить**.

Удаление разметки

Вы можете удалить разметку, если она не используется для обучения или инференса какой-либо ML-модели.

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 окна нажмите на значок корзины (🗑).

4. В открывшемся окне подтвердите удаление разметки.

Работа с импортированными ML-моделями

Этот раздел содержит информацию о работе с импортированными ML-моделями и их элементами.

ML-модель может быть предоставлена специалистами "Лаборатории Касперского" или сертифицированным интегратором в рамках *Услуги построения модели и внедрения Kaspersky MLAD*. Такую ML-модель требуется загрузить в Kaspersky MLAD и активировать. Вы не можете создавать новые элементы для импортированной ML-модели, а также удалять уже существующие элементы.

ML-модель загружается в Kaspersky MLAD уже обученной. Если требуется, вы можете дополнительно обучить нейросетевые элементы в составе загруженной ML-модели перед ее публикацией и/или выполнением инференса.

Загрузка ML-модели

Если ML-модель была создана специалистами "Лаборатории Касперского" или сертифицированным интегратором, вы можете загрузить эту ML-модель в Kaspersky MLAD.

При загрузке ML-модели, размер которой превышает 1 ГБ, работа Kaspersky MLAD может замедлиться.

Загрузка ML-моделей доступна системным администраторами пользователям с правом **Загрузка моделей** из группы прав **Управление ML-моделями**.

Чтобы загрузить ML-модель:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов рядом с названием 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 загружена в Kaspersky MLAD. Новая ML-модель отобразится в группе **Модели** дерева активов. Группа **Модели** создается автоматически и отображается в составе выбранного раздела дерева активов. Группа **Модели** содержит подгруппы **Нейронные сети** и **Правила** для хранения элементов ML-модели на основе нейронных сетей и диагностических правил.

После загрузки ML-модели присваивается статус *Не активирована*. Требуется активировать ML-модель. При повторной загрузке ML-модели, которая ранее была активирована и затем удалена, повторная активация ML-модели не требуется.

Активация импортированной ML-модели

После загрузки 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 администраторами пользователям с правом **Активация моделей** из группы прав **Управление ML-моделями**.

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 окна.

ML-модель активирована. Ей будет присвоен статус *Обучена*. Для запуска анализа данных телеметрии от объекта мониторинга вы можете запустить инференс ML-модели.

Изменение параметров элемента импортированной ML-модели

Вы можете изменить некоторые параметры элемента импортированной ML-модели.

Изменение параметров элементов импортированных ML-моделей доступно системным администраторами пользователям с правом **Изменение черновиков моделей** из группы прав **Управление ML-моделями**.

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 окна нажмите на кнопку **Изменить**.
4. В поле **Название** укажите название элемента ML-модели.
5. В поле **Описание** укажите описание элемента ML-модели.
6. Если требуется, 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 раскрывающемся списке **Статус инцидента** выберите статус инцидента, который будет автоматически присвоен инцидентам, зарегистрированным элементом ML-модели.

d. В раскрывающемся списке **Причина инцидента** выберите причину инцидента, которая будет автоматически задана для инцидентов, зарегистрированных элементом ML-модели.

e. В поле **Цвет точек-индикаторов инцидентов** выберите цвет точек-индикаторов инцидентов, зарегистрированных элементом ML-модели, на графиках в разделах **Мониторинг** и **История**.

f. В поле **Порог регистрации инцидентов** укажите пороговое значение ошибки предсказания, при достижении которого происходит регистрация инцидента.

   > Значение порога регистрации инцидентов установлено по результатам обучения элемента импортированной ML-модели. Изменение этого параметра приведет к изменению чувствительности детектора.

g. В поле **Экспертное заключение** укажите экспертное заключение, которое будет автоматически создано для инцидентов, зарегистрированных элементом ML-модели.

7. В правом верхнем углу окна нажмите на кнопку **Сохранить**.

Работа с ML-моделями, созданными вручную

Этот раздел содержит информацию о работе с ML-моделями, созданными вручную и их элементами.

В случае создания ML-модели вручную вы можете добавлять элементы ML-моделей на основе нейронных сетей и/или диагностических правил, изменять и удалять их.

Для проведения инференса ML-модель должна быть обучена. Для этого все нейросетевые элементы в составе ML-модели требуется предварительно обучить. При необходимости вы можете просмотреть результаты обучения нейросетевых элементов. Элементы на основе диагностических правил считаются обученными.

Вы также можете запустить инференс после публикации ML-модели. После запуска инференса Kaspersky MLAD будет регистрировать инциденты.

Создание ML-модели

> Создание ML-моделей доступно системным администраторам и пользователям с правом **Создание моделей** из группы прав **Управление ML-моделями**.

Чтобы создать ML-модель:

1. В основном меню выберите раздел **Модели**.

2. В дереве активов рядом с названием актива, для которого вы хотите создать ML-модель, откройте вертикальное меню **...** и выберите пункт **Создать модель**.

   Справа отобразится список параметров.

3. В поле **Название** укажите название ML-модели.

   Вы можете указать название 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.

6. Если требуется просмотреть, какие данные будут отобраны разметками, нажмите на кнопку **На графике**.

   Разметки отобразятся в цветах, выбранных при их создании.

7. В правом верхнем углу окна 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. Группа **Модели** содержит подгруппы **Нейронные сети** и **Правила** для хранения элементов ML-модели на основе нейронных сетей и диагностических правил.

ML-модели будет присвоен статус *Черновик*.

Добавление нейросетевого элемента ML-модели

Добавление элементов ML-моделей доступно системным администраторам и пользователям с правом **Создание моделей** из группы прав **Управление ML-моделями**.

Чтобы добавить нейросетевой элемент ML-модели:

1. В основном меню выберите раздел **Модели**.

2. В дереве активов рядом с группой **Нейронные сети** в составе ML-модели, к которой вы хотите добавить нейросетевой элемент, откройте вертикальное меню **...** и выберите пункт **Создать элемент**.

   Справа отобразится список параметров.

3. В поле **Название** укажите название 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 **Шаг сетки (сек.)** укажите период РИВС для элемента в секундах в виде десятичной дроби.

d. В раскрывающемся списке **Статус инцидента** выберите статус инцидента, который будет автоматически присвоен инцидентам, зарегистрированным элементом ML-модели.

e. В раскрывающемся списке **Причина инцидента** выберите причину инцидента, которая будет автоматически задана для инцидентов, зарегистрированных элементом ML-модели.

f. В поле **Цвет точек-индикаторов инцидентов** выберите цвет точек-индикаторов инцидентов, зарегистрированных элементом ML-модели, на графиках в разделах **Мониторинг** и **История**.

g. В поле **Порог регистрации инцидентов** укажите пороговое значение ошибки предсказания, при достижении которого происходит регистрация инцидента.

h. В поле **Экспертное заключение** укажите экспертное заключение, которое будет автоматически создано для инцидентов, зарегистрированных элементом ML-модели.

6. Выберите одну из следующих архитектур нейросетевого элемента ML-модели: **Dense**, **RNN**, **CNN**, **TCN** или **Transformer**.

7. Если требуется задать параметры архитектуры нейросетевого элемента, а также степенной показатель и значение сглаживания суммарной ошибки предсказания, включите **Расширенные параметры нейронной сети** с помощью переключателя.

8. В блоке параметров **Основные параметры** выполните следующие действия:

a. В раскрывающемся списке **Входные теги** выберите один или несколько тегов, которые служат исходными данными для предсказания значений выходных тегов.

b. В раскрывающемся списке **Выходные теги** выберите один или несколько тегов, поведение которых предсказывается элементом модели.

c. Если включен режим расширенной настройки, в поле **Степенной показатель MSE** укажите степенной показатель суммарной ошибки предсказания в виде десятичной дроби.

d. Если включен режим расширенной настройки, в поле **Степень сглаживания** укажите значение сглаживания суммарной ошибки предсказания в виде десятичной дроби.

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 предсказывает выходные значения.

b. В поле **Смещение выходного окна** укажите количество шагов, на которое начало выходного окна будет смещено относительно начала входного окна.

c. В поле **Выходное окно (шаги)** укажите длину предсказания выходных тегов, вычисляемого на основании входных тегов на входном окне.

10. Если вы добавляете нейросетевой 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.

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`.

11. Если вы добавляете нейросетевой 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`.

12. Если вы добавляете нейросетевой 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 **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`.

    d. В поле **Количество нейронов на слоях декодирующего блока** укажите количество нейронов на слоях декодирующего блока.

13. Если вы добавляете нейросетевой 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 `0.1`.

    b. В поле **Размер фильтров** укажите размер фильтров элемента ML-модели.

По умолчанию этот параметр имеет значение `2`.

c. 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`.

d. 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**.

e. В поле **Количество кодирующих блоков** укажите количество кодирующих блоков.

По умолчанию этот параметр имеет значение `1`.

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.

14. Если вы добавляете нейросетевой 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.

15. В правом верхнем углу окна нажмите на кнопку **Сохранить**.

Новый элемент ML-модели отобразится в группе **Нейронные сети** в составе выбранной ML-модели в дереве активов.

ML-модели будет присвоен статус *Черновик*. Для запуска инференса ML-модели требуется обучить все ее нейросетевые элементы.

Изменение нейросетевого элемента ML-модели

Вы можете изменить параметры нейросетевого элемента ML-модели.

Изменение элементов ML-моделей доступно системным администраторам и пользователям с правом **Изменение черновиков моделей** из группы прав **Управление ML-моделями**.

Чтобы изменить нейросетевой элемент ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите нейросетевой элемент, который вы хотите изменить.

   Справа отобразится список параметров.
3. В правом верхнем углу окна нажмите на кнопку **Изменить**.
4. В поле **Название** укажите новое название элемента ML-модели.
5. В поле **Описание** укажите новое описание ML-модели.
6. Если требуется, 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 **Шаг сетки (сек.)** укажите период РИВС для элемента в секундах в виде десятичной дроби.
   d. В раскрывающемся списке **Статус инцидента** выберите статус инцидента, который будет автоматически присвоен инцидентам, зарегистрированным элементом ML-модели.
   e. В раскрывающемся списке **Причина инцидента** выберите причину инцидента, которая будет автоматически задана для инцидентов, зарегистрированных элементом ML-модели.
   f. В поле **Цвет точек-индикаторов инцидентов** выберите цвет точек-индикаторов инцидентов, зарегистрированных элементом ML-модели, на графиках в разделах **Мониторинг** и **История**.
   g. В поле **Порог регистрации инцидентов** укажите пороговое значение ошибки предсказания, при достижении которого происходит регистрация инцидента.
   h. В поле **Экспертное заключение** укажите экспертное заключение, которое будет автоматически создано для инцидентов, зарегистрированных элементом ML-модели.
7. Если требуется, измените архитектуру нейросетевого элемента.

   Kaspersky MLAD поддерживает следующие архитектуры нейросетевого элемента ML-модели: **Dense**, **RNN**, **CNN**, **TCN** или **Transformer**.
8. Если требуется изменить параметры архитектуры нейросетевого элемента, а также степенной показатель и значение сглаживания суммарной ошибки предсказания, включите **Расширенные параметры нейронной сети** с помощью переключателя.
9. Если требуется, в блоке параметров **Основные параметры** выполните следующие действия:

a. В раскрывающемся списке **Входные теги** выберите один или несколько тегов, которые служат исходными данными для предсказания значений выходных тегов.

b. В раскрывающемся списке **Выходные теги** выберите один или несколько тегов, поведение которых предсказывается элементом модели.

c. Если включен режим расширенной настройки, в поле **Степенной показатель MSE** укажите степенной показатель суммарной ошибки предсказания в виде десятичной дроби.

d. Если включен режим расширенной настройки, в поле **Степень сглаживания** укажите значение сглаживания суммарной ошибки предсказания в виде десятичной дроби.

10. Если требуется, 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 предсказывает выходные значения.

b. В поле **Смещение выходного окна** укажите количество шагов, на которое начало выходного окна будет смещено относительно начала входного окна.

c. В поле **Выходное окно (шаги)** укажите длину предсказания выходных тегов, вычисляемого на основании входных тегов на входном окне.

11. Если вы выбрали нейросетевой 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.

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`.

12. Если вы добавляете нейросетевой 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`.

13. Если вы выбрали нейросетевой элемент с CNN-архитектурой, в блоке параметров **Параметры архитектуры CNN** 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 **Размер окна выборки максимума (MaxPooling)** укажите размер окна выборки максимального значения через запятую без пробелов.

       По умолчанию этот параметр имеет значение `2,2,2`.

    d. В поле **Количество нейронов на слоях декодирующего блока** укажите количество нейронов на слоях декодирующего блока.

14. Если вы выбрали нейросетевой 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 `0.1`.

    b. В поле **Размер фильтров** укажите размеров фильтров элемента ML-модели.

       По умолчанию этот параметр имеет значение `2`.

    c. В поле **Расширения на слоях (dilations)** укажите экспоненциальные значения расширения выходных данных на слоях через запятую без пробелов.

       По умолчанию этот параметр имеет значение `1,2,4`.

    d. 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**.

    e. В поле **Количество кодирующих блоков** укажите количество кодирующих блоков.

       По умолчанию этот параметр имеет значение `1`.

    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.

15. Если вы выбрали нейросетевой 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.

16. В правом верхнем углу окна нажмите на кнопку **Сохранить**.

Добавление элемента ML-модели на основе диагностического правила

Добавление элементов ML-моделей доступно системным администраторам и пользователям с правом **Создание моделей** из группы прав **Управление ML-моделями**.

Чтобы добавить элемент ML-модели на основе диагностического правила:

1. В основном меню выберите раздел **Модели**.

2. В дереве активов рядом с группой **Правила** в составе ML-модели, к которой вы хотите добавить диагностическое правило, откройте вертикальное меню **...** и выберите пункт **Создать элемент**.

   Справа отобразится список параметров.

3. В поле **Название** укажите название 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 **Шаг сетки (сек.)** укажите период РИВС для элемента в секундах в виде десятичной дроби.

d. В раскрывающемся списке **Статус инцидента** выберите статус инцидента, который будет автоматически присвоен инцидентам, зарегистрированным элементом ML-модели.

e. В раскрывающемся списке **Причина инцидента** выберите причину инцидента, которая будет автоматически задана для инцидентов, зарегистрированных элементом ML-модели.

f. В поле **Цвет точек-индикаторов инцидентов** выберите цвет точек-индикаторов инцидентов, зарегистрированных элементом ML-модели, на графиках в разделах **Мониторинг** и **История**.

g. В поле **Экспертное заключение** укажите экспертное заключение, которое будет автоматически создано для инцидентов, зарегистрированных элементом ML-модели.

6. Если требуется, включите параметр **Интерпретировать невозможность оценки условия как выполнение правила** с помощью переключателя.

   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.

     Вы можете указать только начало или окончание однократного интервала.

   - **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, наведите курсор мыши на строку с нужным интервалом и нажмите на значок **Удалить интервал** (✕).

   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 критерии поведения тегов, выполните следующие действия:

   a. В блоке параметров **Условия на теги** нажмите на кнопку **Условие**.

   b. В раскрывающемся списке **Тег** выберите тег, для которого вы хотите добавить критерий поведения тега.

   Если требуется исключить использование выбранного критерия поведения из добавляемого 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, в котором отсутствуют ступеньки с заданными параметрами.

   c. 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.

d. В поле **Окно** укажите количество шагов РИВС.

e. 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 минимальное количество выходов за пороговое значение в рамках отдельного окна в поле **Срабатывание**.
- 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 **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 параметр **Значение** не задан. Если значение параметра не задано, то любое повторяющееся значение тега вызывает срабатывание критерия.
- 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.

f. 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.

g. Если блок условий содержит более одного критерия поведения тегов, выберите один из следующих логических операторов между строками критериев:

- **AND**, если требуется отслеживать оба критерия во время работы диагностического правила.
- **OR**, если требуется отслеживать один из заданных критериев во время работы диагностического правила.

9. 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.

Предварительным условием называется блок условий, предшествующий темпоральному оператору. *Пост-условием* называется блок условий, следующий за темпоральным оператором.

Проверка блока предварительного условия проводится в текущем узле РИВС.

b. В поле **Продолжительность (шаги)** укажите следующие интервалы ожидания:

- **от** – интервал между текущим узлом РИВС и первым будущим узлом РИВС, в котором будет выполняться проверка блока пост-условия (минимальный интервал ожидания).
- **до** – интервал между текущим узлом РИВС и последним будущим узлом РИВС, в котором будет выполняться проверка блока пост-условия (максимальный интервал ожидания).

Проверка блока 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 проверить выполнение критериев поведения тегов из блока пост-условия во всех узлах РИВС между минимальным и максимальным интервалом ожидания, выберите групповой оператор **Все шаги**.
- Если требуется проверить выполнение критериев поведения тегов из блока 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 проверка блока предварительного условия в текущем узле РИВС дала отрицательный результат FALSE или неопределенный результат UNDEFINED, то это же значение будет результатом проверки блока пост-условия.

Если проверка блока предварительного условия в текущем узле РИВС дала положительный результат TRUE, то проверка блока пост-условия проводится в каждом узле РИВС между минимальным и максимальным интервалом ожидания. Результат проверки определяется выполнением условия в зависимости от выбранного группового оператора (**Все шаги** или **Любой шаг**).

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.

10. Выберите один из следующих логических операторов между блоками правила:

- **AND**, если требуется отслеживать критерии поведения тегов в обоих блоках во время работы диагностического правила.

- **OR**, если требуется отслеживать критерии поведения тегов одного из блоков во время работы диагностического правила.

11. В правом верхнем углу окна нажмите на кнопку **Сохранить**.

    Новый элемент ML-модели отобразится в группе **Правила** в составе выбранной ML-модели в дереве активов.

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 нейросетевые элементы, перед запуском инференса их требуется обучить.

Изменение элемента ML-модели на основе диагностического правила

Вы можете изменить параметры элемента ML-модели на основе диагностического правила.

Изменение элементов ML-моделей доступно системным администраторам и пользователям с правом **Изменение черновиков моделей** из группы прав **Управление ML-моделями**.

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 окна нажмите на кнопку **Изменить**.
4. В поле **Название** укажите новое название диагностического правила.
5. В поле **Описание** укажите новое описание диагностического правила.
6. Если требуется, 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 **Шаг сетки (сек.)** укажите период РИВС для элемента в секундах.
   d. В раскрывающемся списке **Статус инцидента** выберите статус инцидента, который будет автоматически присвоен инцидентам, зарегистрированным элементом ML-модели.
   e. В раскрывающемся списке **Причина инцидента** выберите причину инцидента, которая будет автоматически задана для инцидентов, зарегистрированных элементом ML-модели.
   f. В поле **Цвет точек-индикаторов инцидентов** выберите цвет точек-индикаторов инцидентов, зарегистрированных элементом ML-модели, на графиках в разделах **Мониторинг** и **История**.

g. В поле **Экспертное заключение** укажите экспертное заключение, которое будет автоматически создано для инцидентов, зарегистрированных элементом ML-модели.

7. Если требуется, включите параметр **Интерпретировать невозможность оценки условия как выполнение правила** с помощью переключателя.

   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.

8. Если требуется, в блоке параметров **Фильтрация по времени** выполните следующие действия:

   a. 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.

        Вы можете указать только начало или окончание однократного интервала.

      - **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.

   b. Если требуется добавить еще один интервал, нажмите на кнопку **Добавить интервал** и выполните шаг 8a.

   c. Если требуется удалить интервал, наведите курсор мыши на строку с нужным интервалом и нажмите на значок **Удалить интервал** (✕).

   Вы можете добавить один или несколько временных интервалов. Если временной интервал не указан, то диагностическое правило применяется в каждом узле РИВС.

9. Если требуется изменить критерии поведения тегов, выполните следующие действия:

   a. В раскрывающемся списке **Тег** выберите тег, для которого вы хотите добавить критерий поведения тега.

      Если требуется исключить использование выбранного критерия поведения из добавляемого 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, в котором отсутствуют ступеньки с заданными параметрами.

   b. 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.

c. В поле **Окно** укажите количество шагов РИВС.

d. 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 минимальное количество выходов за пороговое значение в рамках отдельного окна в поле **Срабатывание**.

- 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 **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 параметр **Значение** не задан. Если значение параметра не задано, то любое повторяющееся значение тега вызывает срабатывание критерия.

- 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.

e. Если требуется добавить критерий поведения тегов в блок условий, нажмите на значок плюса в нижней части блока условий и повторите шаги с 9a по 9d.

f. Если блок условий содержит более одного критерия поведения тегов, выберите один из следующих логических операторов между строками критериев:

- **AND**, если требуется отслеживать оба критерия во время работы диагностического правила.

- **OR**, если требуется отслеживать один из заданных критериев во время работы диагностического правила.

10. Если требуется изменить темпоральный оператор:

a. В поле **Продолжительность (шаги)** укажите следующие интервалы ожидания:

- **от** – интервал между текущим узлом РИВС и первым будущим узлом РИВС, в котором будет выполняться проверка блока пост-условия (минимальный интервал ожидания).

- **до** – интервал между текущим узлом РИВС и последним будущим узлом РИВС, в котором будет выполняться проверка блока пост-условия (максимальный интервал ожидания).

Проверка блока пост-условия проводится в узлах РИВС между минимальным и максимальным интервалом ожидания.

b. В раскрывающемся списке **Проверить** выберите один из следующих групповых операторов:

- Если требуется проверить выполнение критериев поведения тегов из блока пост-условия во всех узлах РИВС между минимальным и максимальным интервалом ожидания, выберите групповой оператор **Все шаги**.

- Если требуется проверить выполнение критериев поведения тегов из блока 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 проверка блока предварительного условия в текущем узле РИВС дала отрицательный результат FALSE или неопределенный результат UNDEFINED, то это же значение будет результатом проверки блока пост-условия.

Если проверка блока предварительного условия в текущем узле РИВС дала положительный результат TRUE, то проверка блока пост-условия проводится в каждом узле РИВС между минимальным и максимальным интервалом ожидания. Результат проверки определяется выполнением условия в зависимости от выбранного группового оператора (**Все шаги** или **Любой шаг**).

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:

- **AND**, если требуется отслеживать критерии поведения тегов в обоих блоках во время работы диагностического правила.

- **OR**, если требуется отслеживать критерии поведения тегов одного из блоков во время работы диагностического правила.

12. В правом верхнем углу окна нажмите на кнопку **Сохранить**.

Удаление элемента ML-модели

При удалении элемента ML-модели Kaspersky MLAD также удаляет результаты работы выбранного элемента ML-модели.

Удаление элементов ML-моделей доступно системным администраторам и пользователям с правом **Удаление моделей** из группы прав **Управление ML-моделями**.

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 окна нажмите на значок корзины (🗑).
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**.

Вы можете создать ML-модель, скопировав ранее добавленную ML-модель. При копировании будет создана ML-модель, в которой состав элементов, параметры ML-модели и ее элементов, а также состояние обучения нейросетевых элементов будут идентичны составу элементов, параметрам ML-модели и ее элементов, состоянию обучения нейросетевых элементов ML-модели в момент ее копирования.

При копировании ML-модели, которая была создана вручную или по шаблону на основе ML-модели, созданной вручную, вы можете добавлять в скопированную ML-модель нейросетевые элементы и/или элементы на основе диагностических правил, изменять и удалять их.

При копировании 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 переобучить нейросетевые элементы скопированной ML-модели. Вы также можете запустить инференс ML-модели после ее публикации.

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 окна нажмите на значок **Копировать модель** (⧉).

   Справа появится панель **Копирование модели**.
4. В поле **Название** укажите название ML-модели.

   Вы можете указать название ML-модели длиной не более 100 символов.

   По умолчанию ML-модели присваивается название в формате `<название 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. Группа **Модели** содержит подгруппы **Нейронные сети** и **Правила** для хранения элементов ML-модели на основе нейронных сетей и диагностических правил.

Работа с шаблонами ML-моделей

Этот раздел содержит информацию о работе с шаблонами ML-моделей.

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, нейросетевые элементы 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 нейросетевые элементы. Вы также можете запустить инференс ML-модели, если она была опубликована.

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**.

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 в составе этой ML-модели есть нейросетевой элемент, для которого заданы входные и выходные теги, и/или элемент на основе диагностического правила, для которого сформированы условия правила.

Чтобы создать шаблон по ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов рядом с названием ML-модели, по которой вы хотите создать шаблон, откройте вертикальное меню **...** и выберите пункт **Создать шаблон**.

   Справа отобразится список параметров.
3. В поле **Название** укажите имя шаблона.

   Вы можете ввести не более 100 символов.

   По умолчанию шаблону присваивается название в формате `Шаблон_<название 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.

   Если теги, используемые в ML-модели, по которой вы создаете шаблон, были загружены или созданы в разделе **Активы** в меню администратора, их имена автоматически присваиваются тегам шаблона. Если тег, используемый в ML-модели, не обнаружен в Kaspersky MLAD, этому тегу присваивается имя по умолчанию в формате **Tag <ID тега модели>**.

   Вы можете указать имя тега шаблона, отличное от имен тегов в разделе **Активы** в меню администратора. Сопоставление тегов шаблона и тегов в разделе **Активы** происходит по идентификаторам тегов ML-модели, которые вы можете указать при создании ML-модели по шаблону.

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**.

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 окна нажмите на кнопку **Изменить**.
4. В поле **Название** укажите новое имя шаблона.

   Вы можете ввести не более 100 символов.

   По умолчанию шаблону присваивается название в формате `Шаблон_<название ML-модели>_<дата и время создания шаблона>`.

5. Если требуется изменить имена тегов шаблона, в столбце **Имя тега шаблона** укажите новые имена для нужных тегов.

   Вы можете указать имя тега шаблона, отличное от имен тегов в разделе **Активы** в меню администратора. Сопоставление тегов шаблона и тегов в разделе **Активы** происходит по идентификаторам тегов ML-модели, которые вы можете указать при создании ML-модели по шаблону.

6. 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**.

Вы можете создать новую ML-модель 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 названием 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** выберите имена тегов для каждого тега ML-модели, которые будут использоваться создаваемой ML-моделью.

   Сопоставление тегов шаблона и тегов в разделе **Активы** в меню администратора происходит по именам тегов ML-модели.
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. Группа **Модели** содержит подгруппы **Нейронные сети** и **Правила** для хранения элементов ML-модели на основе нейронных сетей и диагностических правил.

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**.

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 окна нажмите на значок корзины (🗑).
4. Подтвердите удаление шаблона ML-модели.

Выбранный шаблон ML-модели будет удален из Kaspersky MLAD.

Изменение параметров ML-модели

Вы можете изменить параметры ML-модели, созданной вручную, импортированной в Kaspersky MLAD, созданной по шаблону, а также скопированной ML-модели.

Изменение параметров ML-моделей доступно системным администраторам и пользователям с правом **Изменение черновиков моделей** из группы прав **Управление ML-моделями**.

Чтобы изменить параметры ML-модель:

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 окна нажмите на кнопку **Изменить**.
4. В поле **Название** укажите название ML-модели.

   Вы можете указать название ML-модели длиной не более 100 символов.
5. В поле **Описание** укажите описание ML-модели.
6. Если ML-модель не была импортирована в программу или создана на основе импортированной ML-модели, в блоке параметров **Индикатор инференса** выберите разметки для проведения инференса.
7. Если требуется просмотреть, какие данные отобраны разметками, нажмите на кнопку **На графике**.

   Разметки отобразятся в цветах, выбранных при их создании.
8. В правом верхнем углу окна нажмите на кнопку **Сохранить**.

Обучение нейросетевого элемента ML-модели

Kaspersky MLAD позволяет выполнить обучение нейросетевого элемента для ML-модели, созданной вручную, загруженной в Kaspersky MLAD, созданной по шаблону, а также для скопированной ML-модели.

Обучение элементов ML-моделей доступно системным администраторам и пользователям с правом **Обучение моделей** из группы прав **Управление ML-моделями**.

Чтобы обучить элемент ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите нейросетевой элемент, который вы хотите обучить.

   Справа отобразится список параметров.
3. Откройте вкладку **Обучение** и нажмите на кнопку **Изменить** в правом верхнем углу окна.

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.

6. Если требуется просмотреть, какие данные будут отобраны разметками, нажмите на кнопку **На графике**.

   Разметки отобразятся в указанных при создании цветах.

7. Если требуется, включите параметр **Расширенные параметры обучения** и выполните следующие действия:

   a. В поле **Максимальная продолжительность обучения (сек.)** укажите максимально время, которое сервер Kaspersky MLAD может затратить на обучение ML-модели в секундах.

   b. 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`.

   c. В поле **Максимальное количество эпох** укажите максимальное количество эпох для обучения ML-модели.

      По умолчанию этот параметр имеет значение `500`.

   d. 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`.

   e. 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`.

   f. В поле **Размер батча** укажите количество элементов выборки, которое требуется передать на обучение в рамках итерации.

      По умолчанию этот параметр имеет значение `16`.

   g. В поле **Количество блоков** укажите количество блоков, на которое требуется разбить набор данных для обучения ML-модели.

      По умолчанию этот параметр имеет значение `4`.

   h. В раскрывающемся списке **Режим инференса** выберите одно из следующих значений:

      - Если требуется загрузить все батчи в оперативную память, выберите **Быстрый инференс**.

        Этот режим инференса позволяет выполнить инференс быстрее.

      - Если требуется загружать в оперативную память по одному батчу данных, выберите **Экономия памяти**.

        Этот режим инференса позволяет выполнить инференс с минимальными затратами оперативной памяти, но медленнее, чем в режиме **Быстрый инференс**.

Выбранный режим инференса применяется только в процессе обучения нейросетевого элемента ML-модели.

i. В раскрывающемся списке **Режим обучения** выберите одно из следующих значений:

- Если требуется загрузить весь набор данных для обучения модели в оперативную память, выберите **Загрузить весь датасет 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 датасета**.
- 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.

j. 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**.

k. Если требуется учесть результаты предыдущего обучения при обучении ML-модели на новых данных, включите параметр **Инициализировать веса модели значениями из результатов предыдущего обучения**.

l. Если требуется перемешать данные для улучшения качества обучения ML-модели, включите параметр **Перемешать данные**.

8. В правом верхнем углу окна нажмите на кнопку **Сохранить**.

9. В информационном блоке, расположенном над параметрами обучения, нажмите на кнопку **Обучить элемент**.

В информационном блоке будет отображаться номер текущей эпохи обучения элемента ML-модели. После завершения обучения вы можете просмотреть результаты обучения элемента ML-модели на вкладке **Результаты обучения**.

После обучения всех нейросетевых элементов 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 нейросетевых элементов ML-модели.

Просмотр результатов обучения элементов ML-моделей доступно системным администраторам и пользователям с правом **Обучение моделей** из группы прав **Управление ML-моделями**.

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** отображаются следующие сведения о результатах обучения:

- Сообщение об успешном завершении обучения элемента ML-модели.

  Если требуется просмотреть параметры обучения элемента, указанные при его создании, нажмите на ссылку **Параметры обучения**.
- **Пользователь** – имя пользователя, который запустил обучение элемента ML-модели.
- **Общий интервал времени** – время, которое было потрачено сервером Kaspersky MLAD на обучение элемента ML-модели.
- **Начало обучения** – дата и время начала обучения элемента ML-модели службой Trainer.
- **Окончание обучения** – дата и время окончания обучения элемента ML-модели. Веса элемента ML-модели обновлены службой Trainer.
- **Продолжительность интервалов** – суммарная продолжительность интервалов времени данных с учетом разметок в обучающей выборке.
- **Число узлов РИВС** – количество узлов РИВС, входящих в обучающую выборку.
- **Ошибки обучения и валидации** – график, отображающий ошибки обучения и валидации в зависимости от эпохи обучения.
- **Прогноз обученной модели** – графики, отображающие прогнозы обученной модели для выходных тегов и общую ошибку предсказаний.

Подготовка ML-модели к публикации

После обучения ML-модели вы можете подготовить ее к публикации. ML-модель, подготовленная к публикации, будет недоступна для изменения.

Подготовка ML-модели к публикации доступно системным администраторам и пользователям с правом **Изменение черновиков моделей** из группы прав **Управление ML-моделями**.

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 ML-модели

Вы можете опубликовать ML-модель для регистрации инцидентов на рабочих данных от объекта мониторинга.

> Публикация ML-моделей доступна системным администраторам и пользователям с правом **Изменение черновиков моделей** из группы прав **Управление ML-моделями**.

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*.

После запуска инференса ML-модель будет регистрировать инциденты.

Запуск и остановка инференса ML-модели

Вы можете запускать и останавливать инференс ML-модели со статусами *Обучена* или *Опубликована* на исторических или вновь поступающих данных телеметрии.

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. В раскрывающемся списке **Вид инференса** выберите одно из следующих значений:

   - **Исторический** для запуска инференса ML-модели на исторических данных телеметрии. При выборе этого значения укажите интервал времени данных для работы ML-модели.

- **Потоковый** для выполнения инференса ML-модели на данных телеметрии, поступающих в режиме реального времени.

5. Нажмите на кнопку **Запустить**.

Если был запущен исторический инференс, Kaspersky MLAD добавит ML-модель в очередь на инференс.

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**.

Kaspersky MLAD остановит инференс для выбранной ML-модели.

Просмотр графа потока данных в ML-модели

Вы можете просматривать граф потока данных в ML-моделях.

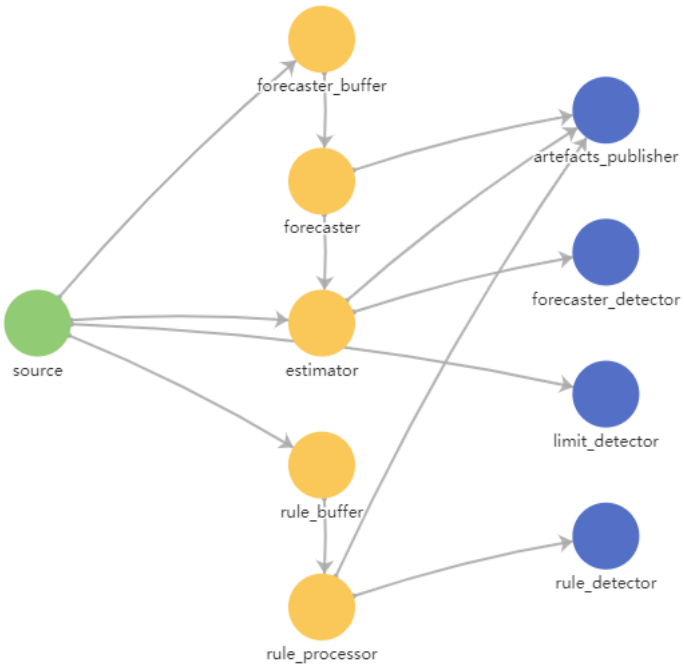
Чтобы просмотреть граф потоков данных в ML-модели:

1. В основном меню выберите раздел **Модели**.
2. В дереве активов выберите нейросетевой элемент, 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 ML-модели, наведите на него курсор мыши.

   Отобразится окно, в котором перечислены значения параметров выбранного элемента.



Граф потока данных в ML-модели

Удаление ML-модели

Вы можете удалить одну или несколько ML-моделей из Kaspersky MLAD.

После удаления ML-модели ее артефакты (например, предсказания, индивидуальные ошибки, ошибки предсказаний, 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**.

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 окна нажмите на значок корзины (🗑).
4. Подтвердите удаление ML-модели.

Выбранная ML-модель будет удалена из Kaspersky MLAD.

Управление пресетами

Пресет – это набор тегов, сформированный пользователем в произвольном порядке или созданный автоматически при регистрации инцидента. Набор тегов в составе пользовательского пресета может соответствовать определенному аспекту технологического процесса или участку объекта мониторинга.

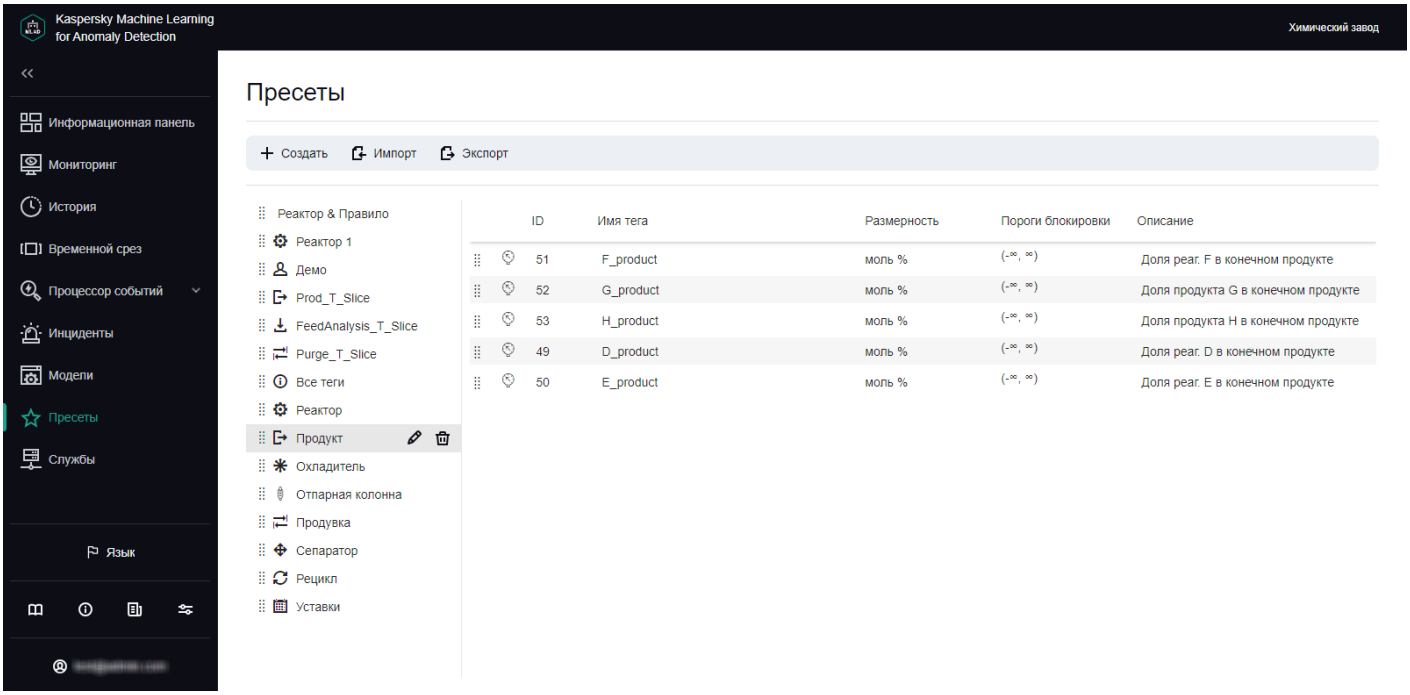
В разделе **Пресеты** в левой части окна расположен список доступных пользовательских пресетов, в правой части окна расположен список тегов, которые входят в состав выбранного в списке пресета.

Для просмотра получаемых данных на графиках в разделах **История** и **Мониторинг** вы можете загрузить конфигурацию пресетов в Kaspersky MLAD из JSON-файла. В рамках работ по внедрению Kaspersky MLAD может быть создана общая для всех пользователей конфигурация пресетов.

В разделе **Пресеты** вы также можете:

- Создавать необходимые пресеты, которые включают в себя теги, соответствующие агрегатам установки объекта мониторинга. Созданные вами пресеты будут отображаться только для вашей учетной записи.
- Изменять пресеты (добавлять, группировать или удалять теги).
- Удалять пресеты.
- Экспортировать пресеты в JSON-файл.

Вы также можете задать выражения с простыми арифметическими действиями (например, сложение, вычитание, умножение и деление) для расчета производных значений тегов.



Раздел **Пресеты**

Просмотр пресета

Вы можете просматривать пресеты, созданные или загруженные вами ранее в Kaspersky MLAD для вашего объекта мониторинга.

Чтобы просмотреть пресет:

1. В основном меню выберите раздел **Пресеты**.

   В левой части рабочей области отобразится список пресетов.

2. Нажмите на нужный пресет.

   В таблице справа отобразится список тегов, входящих в выбранный пресет. Для каждого тега в составе пресета представлена следующая информация:

   - **ID** – идентификатор тега.
   - **Имя тега** – название тега.
   - **Размерность** – единица измерения для тега.
   - **Пороги блокировки** – пороги блокировки, при достижении которых регистрируются инциденты, если включен детектор Limit Detector.
   - **Описание** – описание тега.

Если требуется, вы можете изменить пресет или создать новый пресет.

Создание нового пресета

В Kaspersky MLAD вы можете создавать новые пресеты.

При создании пресета вы можете указать выражение, по которому требуется рассчитывать значения тегов в составе пресета для отображения этих значений на графике в разделе **Временной срез**. Например, с помощью заданных выражений вы можете просмотреть персональные ошибки тегов, прогнозируемые значения тегов, а также значения тегов, полученные от датчиков объекта мониторинга, в один и тот же момент времени. Вы можете использовать следующие переменные в выражениях:

- *$tagValue* – полученное значение тега (по результатам наблюдения);
- *$tagError* – персональная 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.

Чтобы создать новый пресет:

1. В основном меню выберите раздел **Пресеты** и нажмите на кнопку **Создать**.

   Откроется окно **Создание пресета**.

2. В поле **Имя пресета** укажите имя пресета.

3. Если требуется, нажмите на кнопку **Выбрать значок** и в открывшемся окне выберите значок для пресета.

   По умолчанию пресету присваивается значок солнца (☼).

Вы можете загрузить значок для пресета, нажав на кнопку **Загрузить значок**. Изображения любого формата, размер которых превышает 128 x 128 пикселей, будут уменьшены до указанного размера с сохранением соотношения сторон. Размер загружаемого изображения в формате SVG не должен превышать 200 КБ.

Если требуется удалить значок пресета, нажмите на значок пресета и в открывшемся окне нажмите на кнопку **Удалить**.

4. Если требуется добавить выражение, по которому рассчитываются значения тегов для их отображения на графике в разделе **Временной срез**, выполните следующие действия:

   a. Включите переключатель **Настроить выражения для раздела Временной срез**.

   b. В поле **Подпись оси X** укажите подпись, которая отображается по оси абсцисс.

   c. Нажмите на кнопку **Добавить выражение** и в раскрывшемся блоке укажите следующие значения:

   - В поле **Имя выражения** введите имя выражения.
   - В поле **Подпись оси Y** введите подпись, которая отображается по оси ординат.
   - В поле **Выражение для расчета** введите выражение, по которому рассчитываются значения тегов.

     Вы можете задать выражения с простыми арифметическими действиями (например, сложение, вычитание, умножение и деление). Например, если с датчиков поступают значения температуры по Фаренгейту, для отображения на графике значений температуры по Цельсию вы можете указать следующее выражение:

     ```
     5/9 * ($tagValue - 32)
     ```

     Если требуется, вы можете добавить несколько выражений для раздела **Временной срез**.

   - В поле **Цвет графика** выберите цвет графика, который будет отображаться для пресета в разделе **Временной срез**.

   d. Если требуется удалить выражение в пресете для раздела **Временной срез**, нажмите на значок корзины ( ) в правом нижнем углу блока выражения.

5. Если требуется добавить теги, которые входят в состав другого пресета, выберите этот пресет в раскрывающемся списке **Копировать теги из выбранного пресета**.

6. Добавьте в пресет теги, установив флажки около нужных тегов в дереве активов ниже. Вы можете воспользоваться поиском, указав имя тега в поле **Поиск по имени тега**.

7. Если требуется удалить теги из пресета, в дереве активов снимите флажки около тех тегов, которые требуется удалить.

8. Нажмите на кнопку **Сохранить**.

Новый пресет отобразится в разделе **Пресеты** в списке пресетов слева и в раскрывающемся списке пресетов в разделах **История** и **Мониторинг**. Пресет, для которого выполнен пункт 4 этой инструкции, также отобразится в раскрывающемся списке пресетов в разделе **Временной срез**.

Если требуется, вы можете изменить расположение пресетов в списке пресетов. Для этого нужно перетащить пресет вверх или вниз списка, удерживая за точки слева (⣿) от его значка.

Изменение пресета

Вы можете изменять созданные или загруженные вами ранее пресеты.

Чтобы изменить пресет:

1. В основном меню выберите раздел **Пресеты**.

2. На открывшейся странице в списке пресетов слева выберите нужный пресет.

   В таблице справа отобразятся все теги, входящие в выбранный пресет.

   Если требуется, измените расположение тегов в таблице. Для этого нужно перетащить нужный тег вверх или вниз в дереве активов, удерживая за точки слева (⣿) от его значка.

3. Нажмите на кнопку **Изменить пресет** (🖉) рядом с выбранным пресетом.

   Откроется окно **Изменение пресета**.

4. Если требуется, в поле **Имя пресета** введите новое имя пресета.

   Вы также можете изменить имя пресета в списке пресетов. Для этого дважды нажмите на имя пресета, в открывшемся поле введите новое имя пресета и нажмите на клавишу **ENTER**.

5. Если требуется изменить значок пресета, нажмите на кнопку **Выбрать значок**, и в открывшемся окне выберите значок.

   Вы можете загрузить значок для пресета, нажав на кнопку **Загрузить значок**. Изображения любого формата, размер которых превышает 128 x 128 пикселей, будут уменьшены до указанного размера с сохранением соотношения сторон. Размер загружаемого изображения в формате SVG не должен превышать 200 КБ.

   Если требуется удалить значок пресета, нажмите на значок пресета и в открывшемся окне нажмите на кнопку **Удалить**.

6. Если требуется добавить выражение, по которому рассчитываются значения тегов для их отображения на графике в разделе **Временной срез** выполните следующие действия:

   a. Включите переключатель **Настроить выражения для раздела Временной срез**.

   b. В поле **Подпись оси X** укажите подпись, которая отображается по оси абсцисс.

   c. Нажмите на кнопку **Добавить выражение** и в раскрывшемся блоке укажите следующие значения:

   - В поле **Имя выражения** введите имя выражения.
   - В поле **Подпись оси Y** введите подпись, которая отображается по оси ординат.
   - В поле **Выражение для расчета** введите выражение, по которому рассчитываются значения тегов.

     Вы можете задать выражения с простыми арифметическими действиями (например, сложение, вычитание, умножение и деление). Например, если с датчиков поступают значения температуры по Фаренгейту, для отображения на графике значений температуры по Цельсию вы можете указать следующее выражение:

     ```
     5/9 * ($tagValue - 32)
     ```

     Если требуется, вы можете добавить несколько выражений для раздела **Временной срез**.

- В поле **Цвет графика** выберите цвет графика, который будет отображаться для пресета в разделе **Временной срез**.

d. Для удаления выражения в пресете для раздела **Временной срез** нажмите на значок корзины ( ) в правом нижнем углу блока выражения.

7. Если требуется, добавьте в пресет теги, установив флажки около нужных тегов в списке тегов ниже. Вы можете воспользоваться поиском, указав имя тега в поле **Поиск по имени тега**.

8. Если требуется, снимите флажки рядом с названиями тех тегов, которые нужно удалить из пресета.

9. Нажмите на кнопку **Сохранить**.

Измененный пресет обновится в списке пресетов в разделе **Пресеты** и в раскрывающемся списке пресетов в разделах **История** и **Мониторинг**. Измененный пресет, для которого выполнен пункт 6 этой инструкции, также отобразится в раскрывающемся списке пресетов в разделе **Временной срез**.

Если требуется, вы можете изменить расположение пресетов в списке пресетов. Для этого нужно перетащить пресет вверх или вниз списка, удерживая за точки слева (⣿) от его значка.

Удаление пресета

Вы можете удалять созданные или загруженные вами ранее пресеты.

Чтобы удалить пресет:

1. В основном меню выберите раздел **Пресеты**.

2. На открывшейся странице в списке пресетов слева выберите нужный пресет.

3. Нажмите на кнопку **Удалить пресет** (🗑) рядом с выбранным пресетом.

4. В открывшемся окне **Удаление пресета** нажмите на кнопку **Да**, чтобы подтвердить удаление пресета.

Пресет будет удален из списка пресетов.

Загрузка конфигурации пресетов из файла

Вы можете загрузить конфигурацию пресетов в Kaspersky MLAD из файла формата JSON.

Чтобы загрузить конфигурацию пресетов в Kaspersky MLAD:

1. В основном меню выберите раздел **Пресеты**.

2. В верхней части открывшейся страницы нажмите на кнопку **Импорт**.

3. Выберите файл формата JSON с конфигурацией пресетов на локальном диске.

Выбранный файл будет загружен в Kaspersky MLAD, новые пресеты отобразятся в списке пресетов.

Сохранение конфигурации 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 вами ранее в Kaspersky MLAD пресеты:

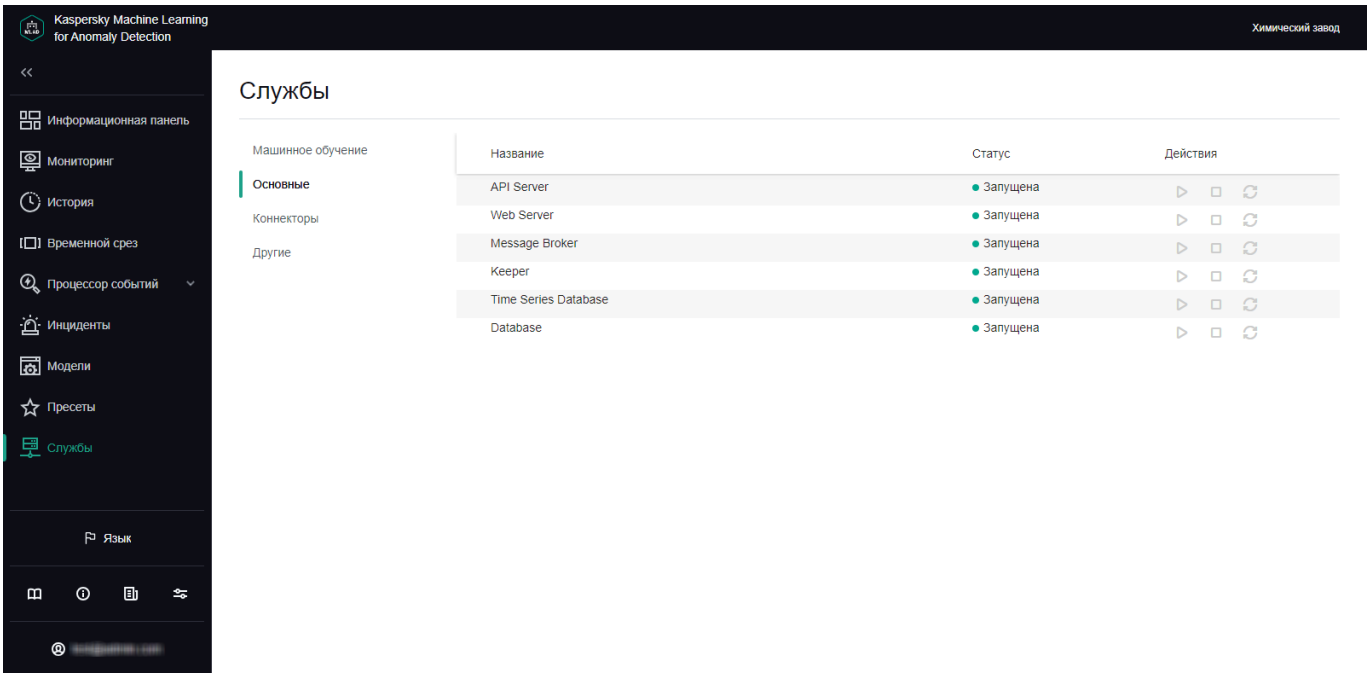
1. В основном меню выберите раздел **Пресеты**.
2. В верхней части открывшейся страницы нажмите на кнопку **Экспорт**.

Созданные и загруженные вами ранее в Kaspersky MLAD пресеты будут сохранены на локальном диске в файл формата JSON.

Управление службами

В разделе **Службы** отображается таблица, содержащая информацию о службах и их статусах. В веб-интерфейсе Kaspersky MLAD службы сгруппированы по функционалу, и для каждой службы отображается следующая информация:

- **Название** – название службы.
- **Статус** – текущий статус службы (*Запущена*, *Остановлена*, *Запускается*, *Недоступна*).
- **Действия** – доступные действия (запустить, остановить, перезапустить).



Раздел **Службы**

Просмотр статуса службы

Вы можете просмотреть статус службы, чтобы убедиться, что служба успешно запущена или остановлена.

Просмотр статуса службы 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 статус службы,

в основном меню выберите раздел **Службы**.

Откроется раздел **Службы**, в котором отображается таблица, содержащая перечисление всех доступных служб, их статусов, а также возможных действий (запуск, остановка и перезапуск).

Запуск, остановка и перезапуск служб

Kaspersky MLAD позволяет запускать, останавливать и перезапускать службы.

Запуск, остановка и перезапуск служб доступно системным администраторам и пользователям с правом **Управление статусами служб программы** из группы прав **Работа со службами программы**.

Чтобы запустить, остановить или перезапустить службу:

1. В основном меню выберите раздел **Службы**.
2. На открывшейся странице выберите один из следующих подразделов: **Машинное обучение**, **Основные**, **Коннекторы** или **Другие**.
3. Для нужной службы выполните одно из следующих действий:
   - Если вы хотите запустить службу, нажмите на кнопку **Запустить службу** (▷).
   - Если вы хотите остановить службу, нажмите на кнопку **Остановить службу** (□).
   - Если вы хотите перезапустить службу, нажмите на кнопку **Перезапустить службу** (↻).

   Новый статус службы отобразится в столбце **Статус**.

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 является доверенным. 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 является доверенным. Для использования доверенного сертификата вам нужно обратиться к квалифицированному техническому специалисту Заказчика, сотруднику "Лаборатории Касперского" или сертифицированному интегратору. Сотрудник может обновить сертификаты для подключения к Kaspersky MLAD через веб-интерфейс.

Вы можете временно использовать самоподписанный сертификат для подключения к Kaspersky MLAD (например, при тестовой 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.

Закончилось свободное пространство на жестком диске

Проблема

На жестком диске компьютера, на котором установлен Kaspersky MLAD, закончилось свободное пространство.

Решение

Для работы программы компьютер должен удовлетворять аппаратным и программным требованиям.

Чтобы программа работала корректно,

освободите на жестком диске компьютера достаточный объем пространства, соответствующий минимальным требованиям к объему свободного пространства.

Непредвиденная перезагрузка операционной системы

Проблема

Неожиданная перезагрузка компьютера с установленным Kaspersky MLAD.

Решение

Дождитесь окончания загрузки компьютера. После загрузки возможны следующие варианты состояния Kaspersky MLAD:

- Работоспособность Kaspersky MLAD восстановилась полностью.
- Работоспособность Kaspersky MLAD не восстановилась.

  Если неисправность сохраняется, обратитесь в Службу технической поддержки "Лаборатории Касперского".

Не удается подключиться к веб-интерфейсу Kaspersky MLAD

Проблема

При подключении к веб-интерфейсу Kaspersky MLAD после ввода корректного пароля отображается ошибка *Error! Invalid server error.*

Решение

Часто ошибка *Error! Invalid server error* возникает из-за того, что на сервере, на котором установлен Kaspersky MLAD, закончилось свободное пространство на жестком диске.

Чтобы восстановить корректную работу программы,

освободите на жестком диске сервера достаточный объем пространства, соответствующий минимальным требованиям к объему свободного пространства.

Если после освобождения пространства на жестком диске, не удается подключиться к веб-интерфейсу Kaspersky MLAD, требуется обратиться в Службу технической поддержки.

Не отображаются графики в разделах История и Мониторинг

Проблема

В разделах **История** и **Мониторинг** не отображаются графики.

Возможны следующие причины:

- Пресеты не импортированы в Kaspersky MLAD.
- Выбранный пресет не содержит теги.
- В разделе выбран **История** интервал времени, для которого отсутствуют данные.
- Коннектор, используемый для получения данных от объекта мониторинга, не запущен.
- Объект мониторинга отключен.

Решение

Убедитесь, что объект мониторинга включен. Включите коннектор, используемый для получения данных от объекта мониторинга. Импортируйте или создайте пресеты, содержащие теги. Для отображения данных на графике в разделе **История** выберите дату, интервал времени и пресет, содержащий теги. Для отображения данных в разделе **Мониторинг** выберите интервал времени и пресет, содержащий теги.

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 номер порта, по которому 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 может наблюдаться после изменения параметров службы Event Processor.

Решение

*Чтобы восстановить загрузку данных для просмотра истории событий и/или истории паттернов в разделе **Процессор событий**,*

рекомендуется подождать несколько минут. После перезапуска Kaspersky MLAD состояние службы Event Processor восстанавливается. Длительность процесса восстановления состояния при значительном объеме обработанных событий и зарегистрированных паттернов может занимать несколько минут. 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.

Неправильно обрабатываются данные в разделе Процессор событий

Проблема

Создается большое количество коротких паттернов.

Решение

Чтобы снизить количество регистрации коротких паттернов,

в параметрах службы Event Processor требуется увеличить длину эпизода.

Проблема

Приходит большое количество оповещений об активации монитора.

Решение

Чтобы снизить большое количество 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.

Не отображаются ранее созданные мониторы и заданные параметры конфигурации внимания в разделе Процессор событий

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 или файл в битовом формате. Если Kaspersky MLAD сохраняет состояние службы в таблицу базы данных, для сохранения созданных мониторов и заданных параметров конфигурации внимания рекомендуется не перезапускать службу Event Processor и не изменять ее параметры до обработки первого эпизода событий от объекта мониторинга. Если программа сохраняет состояние службы Event Processor в файл в битовом формате, для сохранения созданных мониторов и заданных параметров конфигурации внимания рекомендуется не перезапускать службу Event Processor и не изменять ее параметры до первого резервного копирования службы. Частота резервного копирования службы Event Processor зависит от значения параметра **Периодичность создания резервных копий компонента**.

Для получения событий требуется настроить параметры службы Event Processor и коннектора CEF Connector и запустить их. Если требуется обрабатывать зарегистрированные инциденты в качестве событий, требуется также настроить службу Anomaly Detector и коннектор, необходимый для получения данных телеметрии от объекта мониторинга, и запустить их. Перейдите в раздел **Информационная панель** и убедитесь, что события поступают в Kaspersky MLAD в онлайн-режиме.

Если неисправность сохраняется, обратитесь в Службу технической поддержки "Лаборатории Касперского".

Не отображается результат применения разметки

Проблема

В разделе **Модели** при просмотре графика разметок отсутствует окраска интервалов данных, которые должны быть отобраны разметкой.

Решение

Выбранный интервал времени может быть слишком коротким и может не содержать достаточного количества данных для принятия разметкой решения об отображении интервалов данных на графике. Укажите больший по продолжительности интервал времени для отображения данных на графике разметок в поле **Масштаб**.

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 выполнение некоторого числа эпох обучения.

Решение

Если обучение элемента ML-модели завершилось с ошибкой сразу после начала обучения, убедитесь, что по всем тегам в составе ML-модели есть данные в рамках интервала обучения, заданного в параметре **Интервал отбора данных**, с учетом применения разметок (индикатора обучения). Для этого при изменении параметров обучения нажмите на кнопку **На графике** и визуально проконтролируйте, что в рамках заданного интервала обучения отображаются отобранные разметками интервалы данных (как минимум один), и что в этих интервалах данных отображаются наблюдения для всех тегов, участвующих в обучении элемента ML-модели.

Если обучение элемента ML-модели завершилось с ошибкой после выполнения некоторого числа эпох, то выбранные для обучения данные могут не подходить для этого элемента ML-модели. В таком случае целевые метрики качества ML-модели не могут быть достигнуты. Просмотрите графики на вкладке **Результаты обучения** и выберите другой интервал для обучения элемента ML-модели.

Требуется изменить язык локализации Справки до подключения к программе

Проблема

Требуется изменить язык локализации Справки до подключения к веб-интерфейсу Kaspersky MLAD.

Решение

Чтобы изменить язык локализации Справки программы, не подключаясь к веб-интерфейсу 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. В верхнем правом углу открывшейся страницы ввода учетных данных нажмите на ссылку **Справка**.
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**/171583.htm);
   - en – если вы хотите открыть Справку на английском языке (например, https://<веб-адрес Kaspersky MLAD>/help/**en**/171583.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 логирования 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.

- Оповещения об активации мониторов службы Event Processor не сохраняются в базе данных Kaspersky MLAD.

- Рекомендуется сохранять состояние службы Event Processor в таблице базы данных. В случае сохранения состояния службы в файл в битовом формате, Kaspersky MLAD сохраняет состояние службы Event Processor согласно заданной периодичности создания резервной копии службы. Для сохранения и восстановления состояния службы Event Processor требуется некоторое время (до нескольких минут, если большой объем обрабатываемых данных). Перезапуск службы приведет к потере данных с момента последнего сохранения в файл в битовом формате.

- Служба Event Processor обрабатывает только категориальные данные. Все значения параметров события 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 направлений внимания.

- При большом потоке событий (около пяти тысяч событий в секунду) и большом разнообразии значений параметров событий работа службы Event Processor требует значительных вычислительных ресурсов.

- Служба Event Processor чувствительна к настройке ее параметров. Неправильно заданные параметры событий, размер и время формирования эпизодов, конфигурации внимания могут существенно снизить эффективность и производительность службы.

- 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.

- Kaspersky MLAD хранит всю историю полученных значений тегов, а также предсказанных 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.

- Служба Trainer поддерживает обучение только нейросетевых ML-моделей.

- Обновление программы с сохранением данных поддерживается только для версии Kaspersky MLAD 4.0.1-001 или выше. Для перехода от Kaspersky MLAD 3.0.0 к версии Kaspersky MLAD 4.0.1 и выше необходимо произвести новую установку Kaspersky MLAD и вручную импортировать данные из ранее установленной версии Kaspersky MLAD 3.0.0. Для получения подробной информации о переходе от Kaspersky MLAD 3.0.0 к Kaspersky MLAD версии 4.0.1 или выше рекомендуется обратиться в Службу технической поддержки "Лаборатории Касперского".

- Откат программы к предыдущей установленной версии поддерживается только для версии Kaspersky MLAD 4.0.1-001 или выше.

- Не группируются аномалии по однотипным тегам, относящимся к разным элементам ML-модели, если используется ML-модель, состоящая из нескольких однотипных элементов.
- При большом количестве одновременно запущенных ML-моделей (более 80) количество соединений с базой данных может быть исчерпано. При возникновении такой ситуации рекомендуется перезапустить Kaspersky MLAD.
- Отсутствует возможность использования элементов модели на основе детектора XGBoost.
- В дереве активов в разделе **Активы** не отображается значок, выбранный при создании или изменении тегов или активов.
- В разделе **Инциденты** в окне выбора периода для выбора доступны только те годы, за которые в Kaspersky MLAD есть данные.
- В разделах **История** и **Мониторинг** некорректно отображаются графики тегов, для которых указаны границы отображения по оси ординат, заданные при создании или изменении тега.
- В разделе **Модели** невозможно скопировать ML-модель, если в ее составе нет элементов или есть хотя бы один необученный нейросетевой элемент.
- В разделе **Модели** не всегда отображаются результаты обучения нейросетевого 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.

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 и 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.

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 в иерархической структуры в разделе **Активы** в меню администратора.

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.
- **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.
- **parent row** – номер строки, на которой описана 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.

- **tags** – вкладка, описывающая теги иерархической структуры с помощью следующих параметров:
  - **tag_id** – идентификатор тега. Идентификатор присваивается автоматически при экспорте первичных элементов иерархической структуры.
  - **tag_name** – уникальное имя тега.
  - **alternate_name** – уникальное альтернативное имя тега. Поле не обязательно для заполнения.
  - **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 блокировки, при достижении которого требуется принять экстренные меры реагирования на АСУ ТП. Поле не обязательно для заполнения.
- **red_max** – верхний порог блокировки, при достижении которого требуется принять экстренные меры реагирования на АСУ ТП. 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.
- **display_min** – нижняя граница отображения значений тега на графиках. Поле не обязательно для заполнения.
- **display_max** – верхняя граница отображения значений тега на графиках. Поле не обязательно для заполнения.
- **scale** – выражение, по которому требуется рассчитать значение тега из значения, переданного в Kaspersky MLAD. Вместо выражения вы можете указать конкретное число, на которое требуется умножить значение передаваемого тега. Если перерасчет значения тега не требуется, оставьте поле пустым.
- **comment** – комментарий к тегу.
- **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.

Ниже приведен пример файла в формате XLSX, который содержит описания активов и тегов и их конфигурацию.

Вкладка **directory_types**

directory_type_id	directory_type	parameter1_label	parameter2_label	parameter3_label	parameter4_
	Завод	Процесс	Регион		
	Агрегат	Производитель	Модель	Год изготовления	Ответственн
	Уставки				

Вкладка **directories**

directory_id	directory_type	directory_type row	directory_name	directory_info	parent	parent row	pa
	Завод	2	Химический завод	Tennessee Eastman Process			
	Агрегат	3	Реактор	Химический реактор	Химический завод	2	
	Уставки	4	Уставки	Уставки реактора	Химический завод; Реактор	3	

Вкладка **tags**

tag_id	tag_name	alternate_tag_name	tag_description	parent	parent_row	pa
	Reactor_pressure_setpoint		Уставка давления реактора	Химический завод; Реактор; Уставки	4	
	A_feed_stream1		Расход реагента A	Химический завод; Реактор	3	
	Нет отклика температуры реактора		Rule	Химический завод	2	

Пример JSON-файла, содержащего конфигурацию пресетов

Ниже приведен пример файла в формате JSON, который содержит описания пресетов.

Конфигурационный файл создается только квалифицированным сотрудником "Лаборатории Касперского". Конфигурация пресетов загружается пользователем в разделе **Пресеты**.

```
{
  "presets": [
    {
      "name": "Продукт",
      "tag_list": [
        51,
        52,
        53,
        49,
        50
      ],
      "evaluations": {
        "axis_x_name": "",
        "evaluations": []
      },
      "css_class": null,
      "icon": "logout-signout"
    },
...
    {
      "name": "Охладитель",
      "tag_list": [
        64
      ],
      "evaluations": {
        "axis_x_name": "",
        "evaluations": []
      },
      "css_class": null,
      "icon": "graph"
    }
  ]
}
```

Пример JSON-файла, содержащего конфигурацию параметров для службы Event Processor

Ниже приведен пример файла в формате JSON, который содержит конфигурацию параметров для службы Event Processor. Файл содержит описание параметров событий для процессора событий.

Конфигурационный файл создается только сотрудником "Лаборатории Касперского". Системный администратор загружает конфигурационный файл процессора событий при настройке параметров службы Event Processor.

```
{
    "timestamp_field": "TimeStamp",
    "timestamp_scale": "ms",
    "fields": [
        "User_Host",
```

```
        "User_Name",
        "Destination_Host",
        "Access_Result"
    ],
    "groupBy": [
        "User_Host",
        "User_Name",
        "Destination_Host",
        "Access_Result"
    ],
    "nodes": [
        {
            "name": "User_Name",
            "depth": 0,
            "tooltip": {
                "templates": [
                    "User: {{User_Name}}"
                ]
            }
        },
        {
            "name": "User_Host",
            "depth": 1,
            "tooltip": {
                "templates": [
                    "User host: {{User_Host}}"
                ]
            }
        },
        {
            "name": "Destination_Host",
            "depth": 2,
            "tooltip": {
                "templates": [
                    "Destination: {{Destination_Host}}"
                ]
            }
        }
    ],
    "links": [
        {
            "source": "User_Name",
            "target": "User_Host",
            "value": "interval_count",
            "tooltip": {
                "templates": [
                    "{{User_Name}} » {{User_Host}}",
                    "Count: {{interval_count}}"
                ]
            },
            "isGraphGroup": true
        },        {
            "source": "User_Host",
            "target": "Destination_Host",
            "value": "interval_count",
            "tooltip": {
                "templates": [
                    "{{User_Host}} » {{Destination_Host}}",
                    "DeviceEventClassID: {{Access_Result}}",
                    "Count: {{interval_count}}"
```

```
                ]
            }
        }
    ]
}
```

Просмотр журнала логирования Kaspersky MLAD

В Kaspersky MLAD используется система логирования Grafana для отслеживания состояния служб программы, а также для отслеживания событий информационной безопасности.

Отслеживание событий информационной безопасности Kaspersky MLAD в подсистеме логирования

В таблице ниже приведены типы событий ИБ, которые отслеживаются в Kaspersky MLAD.

Типы событий информационной безопасности

Идентификатор события информационной безопасности в системе логирования	Тип события информационной безопасности
`login`	Подключение и попытки подключения пользователей к Kaspersky MLAD
`access_control`	Проверка прав пользователей при выполнении действий в веб-интерфейсе Kaspersky MLAD
`logout`	Завершение подключения пользователей к Kaspersky MLAD
`service_control`	Запуск, остановка и перезапуск служб Kaspersky MLAD
`user_control`	Изменение учетных записей пользователей
`system_settings_control`	Изменение параметров Kaspersky MLAD
`model_control`	Создание, изменение и удаление моделей
`tag_control`	Импорт, создание, изменение и удаление тегов
`log_control`	Удаление логов событий ИБ из базы данных Kaspersky MLAD при превышении объема хранения логов или при истечении срока их хранения

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 логов событий ИБ.

- **8** – высокий.

  К этим событиям ИБ относятся записи об указании пользователями неправильных логина 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** – имя пользователя, действия которого привели к записи события ИБ.
- **ip_address** – IP-адрес компьютера, с которого пользователем было произведено действие, записанное в логи 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 логирования

Для обозначения служб Kaspersky MLAD, состояние которых отслеживается в подсистеме логирования, используются наименования соответствующих им контейнеров или образов в Docker. В качестве имени образа в большинстве случаев используется сокращенное название службы. Имя контейнера формируется по следующему шаблону:

`<директория программы>-<название образа>-#`,

где: # – номер контейнера Docker.

По умолчанию Kaspersky MLAD использует директорию `mlad-release-4.0.2-<номер установочной сборки>`.

В журнале логирования Kaspersky MLAD записи о состоянии служб программы хранятся только за последние 48 часов.

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-release-4.0.2-<номер установочной сборки>-anomaly_detector-1
Time Series Database	influxdb	mlad-release-4.0.2-<номер установочной сборки>-influxdb-1
Message Broker	kafka	mlad-release-4.0.2-<номер установочной сборки>-kafka-1
Keeper	keeper	mlad-release-4.0.2-<номер установочной сборки>-keeper-1
Logger	logger	mlad-release-4.0.2-<номер установочной сборки>-logger-1
Database	postgres	mlad-release-4.0.2-<номер установочной сборки>-postgres-1
Similar Anomaly	similar_anomaly	mlad-release-4.0.2-<номер установочной сборки>-similar_anomaly-1
Event Processor	event-processor	mlad-release-4.0.2-<номер установочной сборки>-event-processor-1
Stream Processor	stream-processor	mlad-release-4.0.2-<номер установочной сборки>-stream-processor-1
Trainer	trainer	mlad-release-4.0.2-<номер установочной сборки>-trainer-1
Web Server	nginx-ui	mlad-release-4.0.2-<номер установочной сборки>-nginx-ui-1
API Server	web-server	mlad-release-4.0.2-<номер установочной сборки>-web-server-1
Mail Notifier	postman	mlad-release-4.0.2-<номер установочной сборки>-postman-1
OPC UA Connector	opcua-connector	mlad-release-4.0.2-<номер установочной сборки>-opcua-connector-1
MQTT Connector	mqtt-connector	mlad-release-4.0.2-<номер установочной сборки>-mqtt-connector-1
AMQP Connector	amqp-connector	mlad-release-4.0.2-<номер установочной сборки>-amqp-connector-1
HTTP Connector	gate	mlad-release-4.0.2-<номер установочной сборки>-gate-1
KICS Connector	kics3-connector	mlad-release-4.0.2-<номер установочной сборки>-kics3-connector-1
CEF Connector	cef-connector	mlad-release-4.0.2-<номер установочной сборки>-cef-connector-1
WebSocket Connector	ws-connector	mlad-release-4.0.2-<номер установочной сборки>-ws-connector-1
	webstatic	mlad-release-4.0.2-<номер установочной сборки>-webstatic-1
	migrations	mlad-release-4.0.2-<номер установочной сборки>-migrations-1

Для служб Time Series Database, Message Broker, Logger, Database, Web Server, а также образов webstatic и migrations используется уровень логирования **Инфо**. Уровни логирования для остальных служб Kaspersky MLAD задаются системным администратором при настройке параметров программы.

Сценарий: просмотр логов событий информационной безопасности

Перед началом работы с подсистемой логирования рекомендуется ознакомиться с руководством пользователя системы Grafana.

Объем и время хранения записей событий ИБ задаются при настройке параметров безопасности.

Запись логов событий информационной безопасности в базу данных Kaspersky MLAD ведется автоматически. Если требуется, системный администратор может указать параметры внешней системы, в которую требуется отправлять логи событий ИБ.

Сценарий просмотра логов событий информационной безопасности состоит из следующих этапов:

1. **Переход в подсистему логирования**

   Перейдите в систему логирования нажатием на кнопку . Откроется интерфейс Grafana, в котором требуется указать логин и пароль пользователя Kaspersky MLAD.

   Доступно только системным администраторам и пользователям с правом **Работа с логами программы**.

2. **Переход в раздел с логами событий информационной безопасности**

   Перейдите в раздел **Security audit**.

3. **Анализ логов событий информационной безопасности**

   Проанализируйте записи логов событий ИБ за выбранный период. Вы можете выполнить фильтрацию по параметрам логов событий ИБ. Для этого в столбце с нужным параметром логов нажмите на значок фильтрации (), установите флажки около нужных критериев фильтрации и нажмите на кнопку **Ok**. Для сброса критериев фильтрации снимите нужные флажки и нажмите на кнопку **Ok**.

4. **Экспорт логов событий информационной безопасности**

   Для выгрузки в текстовый файл логов событий ИБ за выбранный период, в разделе **Security audit** в раскрывающемся списке **Security audit** над таблицей логов 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 логирования рекомендуется ознакомиться с руководством пользователя системы Grafana.

При первом подключении к подсистеме логирования 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 логирования**

   Перейдите в систему логирования нажатием на кнопку . Откроется интерфейс Grafana, в котором требуется указать логин и пароль пользователя Kaspersky MLAD.

   > Доступно только системным администраторам и пользователям с правом **Работа с логами программы**.

2. **Анализ основных метрик Kaspersky MLAD**

   В разделе **Summary docker metrics** 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. Изменяется в процентах.
   - *RAM usage* – история использования контейнером оперативной памяти. Изменяется в байтах.
   - *Disk usage* – история нагрузки контейнера на дисковую подсистему (операции записи и чтения). Изменяется в байтах.
   - *Network usage* – история задействования контейнером сетевых ресурсов. Изменяется в байтах в секунду.

Сценарий: просмотр метрик и логов контейнера

> Перед началом работы с подсистемой логирования рекомендуется ознакомиться с руководством пользователя системы Grafana.

> В журнале логирования Kaspersky MLAD хранятся записи только за последние 48 часов.

В этом подразделе приводится последовательность действий, которые требуется выполнить для оценки работоспособности и просмотра логов определенного контейнера из комплекта поставки Kaspersky MLAD.

Сценарий оценки работоспособности и просмотра логов определенного контейнера состоит из следующих этапов:

1. **Переход в подсистему логирования**

   Перейдите в систему логирования нажатием на кнопку . Откроется интерфейс Grafana, в котором требуется указать логин и пароль пользователя Kaspersky MLAD.

   > Доступно только системным администраторам и пользователям с правом **Работа с логами программы**.

2. **Переход в раздел с метриками и логами контейнера**

   Перейдите в раздел **Service detailed monitoring** и выберите нужный контейнер из раскрывающегося списка **Container**.

3. **Анализ метрик контейнера**

   Проанализируйте графики метрик Kaspersky MLAD для выбранного контейнера за необходимый период, которые отображаются в разделе **Service detailed monitoring**.

   В разделе **Service detailed monitoring** представлены следующие метрики:

   - *Memory* – история использования контейнером оперативной памяти. Изменяется в байтах.
   - *CPU* – история загрузки центрального процессора контейнером. Изменяется в процентах.
   - *File system* – история нагрузки контейнера на дисковую подсистему (операции записи и чтения). Изменяется в байтах.
   - *Network* – история задействования контейнером сетевых ресурсов. Изменяется в байтах в секунду.

4. **Анализ логов контейнера**

   Проанализируйте записи логов контейнера за выбранный период, которые отображаются под информационной панелью с метриками. Вы можете выполнить поиск по записям логов 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**.

5. **Экспорт логов контейнера**

   Для выгрузки в текстовый файл логов контейнера за выбранный период, в разделе **Service detailed monitoring** в раскрывающемся списке **Service log** выберите **Inspect** → **Data** и в открывшейся панели нажмите на кнопку **Download CSV**.

Специальные символы регулярных выражений

Для поиска событий, паттернов и значений параметров событий в разделе **Процессор событий** вы можете использовать регулярные выражения. Kaspersky MLAD поддерживает использование следующих специальных символов в регулярных выражений:

- `^` – Соответствует началу значения параметра. Например, `^A` означает, что поиск в параметре события будет осуществляться по значениям, начинающимся с символа A.
- `$` – Соответствует концу значения параметра. Например, `A$` означает, что поиск в параметре события будет осуществляться по значениям, заканчивающимся на символ A.
- `.` – Соответствует одному любому символу.
- `|` – Разделяет допустимые варианты символов или совокупности символов в значении параметра. Например, `к(о|и)т` соответствует как значению параметра `кот`, так и `кит`.
- `\` – Символ, указывающий на то, что следующий символ является обычным символом в значении параметра, а не специальным. Вы можете использовать символ `\` для поиска специальных символов в значении параметра. Например, `\.` описывает точку в значении параметра, 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 в значениях параметров событий вы можете использовать следующие специальные символы:

- `?` – Символ, определяющий, что предшествующее выражение может встречаться в значении параметра ноль или один раз.

- `*` – Символ, определяющий, что предшествующее выражение может встречаться в значении параметра ноль или более раз.

- `+` – Символ, определяющий, что предшествующее выражение может встречаться в значении параметра 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 значении параметра ровно `n` раз.

  - `{m,n}` – Выражение, предшествующее фигурным скобкам, встречается в значении параметра от `m` до `n` раз включительно.

  - `{m,}` – Выражение. предшествующее фигурным скобкам, встречается в значении параметра не менее `m` раз.

  - `{,n}` – Выражение, предшествующее фигурным скобкам, встречается в значении параметра 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.

Глоссарий

ML-модель

Алгоритм, основанный на методах машинного обучения, задачей которого является анализ телеметрии объекта мониторинга и обнаружение аномалий.

Актив

Раздел иерархической структуры, представляющий, например, завод, цех или отдельный агрегат объекта мониторинга.

Аномалия

Нештатное, не ожидаемое и не предусмотренное производственным процессом отклонение в поведении объекта мониторинга.

АСУ ТП

Аббревиатура от "автоматизированная система управления технологическим процессом". Группа технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях.

Ветка ML-модели

Определяет способ расчета предсказанного значения тега, персональной ошибки тега и ошибки MSE. Для сложной модели в расчете могут участвовать несколько элементов ML-модели, которые имеют различный состав тегов и параметров расчета ошибки.

Внимание

Специальная конфигурация процессора событий, которую требуется настроить для отслеживания событий и паттернов по отдельным подмножествам истории событий (направлениям внимания). Направление внимания определяется значением параметра событий, которое должно присутствовать во всех событиях этого направления. Процессор событий выявляет события и паттерны только по тем направлениям внимания, которые заданы в конфигурации внимания.

Градиентный бустинг

Техника машинного обучения для задач классификации и регрессии, которая строит модель предсказания в форме ансамбля предсказывающих моделей, обычно деревьев решений (XGBoost).

Детектор

Компонент в составе ML-модели, который определяет аномалию и регистрирует инциденты.

Иерархическая структура объекта мониторинга

Способ организации данных объекта мониторинга в виде дерева, конечные узлы которого соответствуют исходным тегам и/или тегам, обработанными службой Stream Processor.

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 детектором аномалий 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 скользящий временной интервал, число последовательных обнаружений, фильтры на значения параметров событий, а также условие на обнаружение новых событий, паттернов или значений параметров событий.

Паттерн

Последовательность событий или других паттернов, на которые разбивается поток событий от объекта мониторинга.

Пресет

Набор тегов, сформированный пользователем в произвольном порядке или созданный автоматически при регистрации инцидента. Набор тегов в составе пользовательского пресета может соответствовать определенному аспекту технологического процесса или участку объекта мониторинга.

Равноинтервальная временная сетка (РИВС)

Бесконечная последовательность моментов времени, следующих друг за другом через равные интервалы, к которой приводится поток поступающих данных телеметрии.

Разметка

Набор интервалов времени, заданных для тегов, что позволяет формировать индикаторы обучения и инференса ML-модели.

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, описывающих изменение состояния объекта мониторинга по заранее заданному перечню параметров, с указанием момента времени, когда произошло изменение.

Тег

Переменная, которая содержит значение какого-либо параметра технологического процесса (например, температуры).

Топ-тег

Параметр технологического процесса, для которого зафиксировано наибольшее отклонение от прогноза на момент регистрации 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 приложение отправляет через системы доставки сообщений (например, по электронной почте) на указанные адреса.

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 – товарный знак Google LLC.

TensorFlow и любые связанные с ним обозначения являются товарными знаками Google LLC.

Intel, Core и Xeon – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Microsoft и Excel являются товарными знаками группы компаний Microsoft.

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.