MLAD PoC Guide

> Настоящий документ описывает общий порядок проведения пилотных проектов программного продукта Kaspersky Machine Learning for Anomaly Detection (далее - MLAD).

> В частных случаях порядок пилотного проекта может быть адаптирован или изменён по договоренности между участниками пилотного проекта..

???????? ??????? ? ??????????

MLAD – Machine Learning for Anomaly detection
API – программный интерфейс приложения
ПМИ – программа и методика испытаний
ML – машинное обучение (machine learning)
Инференс – использование обученной модели ML на новых данных

????????? ????????? ???????

В пилотном проекте могут принимать участие следующие организации:

- **Заказчик** - организация, в инфраструктуре или с использованием данных которой устанавливается решение MLAD в рамках пилотного проекта.
- **Исполнитель** – организация, ответственная за проведение пилотного проекта в инфраструктуре или на данных Заказчика.
- **Вендор** - АО «Лаборатория Касперского». Со стороны Вендора в пилотном проекте принимают участие следующие сотрудники:

Инженер предпродажной поддержки
Сотрудник, представляющий техническую экспертизу по решению MLAD, техническую поддержку инженеров внедрения со стороны Партнёра или Дистрибутора (при наличии), а также осуществляющий внедрение программных компонентов MLAD в рамках пилотного проекта в случае отсутствия Партнёра и Дистрибутора

Архитектор

Сотрудник, представляющий техническую экспертизу по решению MLAD и других программных продуктов Вендора, а также организовывающий взаимодействие с участниками пилотного проекта со стороны Вендора (организация встреч, совещаний и иных взаимодействий в рамках пилотного проекта и внедрения программных продуктов Вендора)

Менеджер по развитию бизнеса MLAD

Сотрудник, предоставляющий консультацию по всем иным вопросам, касающимся пилотного проекта и внедрения программных компонентов MLAD в промышленной инфраструктуре Заказчика, за исключением технических вопросов

Менеджер по работе с ключевыми клиентами

Сотрудник, отвечающий за управление взаимоотношениями с Заказчиком

Также к пилотному проекту ПРИ НЕОБХОДИМОСТИ могут быть привлечены **Партнер** и **Дистрибутор**

Партнёр

Организация, которая участвует в пилотном проекте в роли инженера внедрения, разработчика документации и/или предоставляет необходимое оборудование. Со стороны Партнёра участие в пилотном проекте принимает инженер внедрения - Сотрудник Партнёра, отвечающий за развертывание MLAD в тестовой среде на объекте Заказчика. Необходимость участия Партнёра в пилотном проекте определяется Заказчиком. Партнер определяется Заказчиком.

Дистрибутор

Организация, которая участвует в роли инженера внедрения, разработчика документации и/или предоставляет необходимое оборудование. Со стороны Дистрибутора участие в пилотном проекте принимает инженер внедрения - Сотрудник Дистрибутора, отвечающий за развертывание MLAD в тестовой среде на объекте Заказчика. Дистрибутор участвует в пилотном проекте совместно с Партнёром или при отсутствии Партнёра. Необходимость участия Дистрибутора в пилотном проекте определяется Заказчиком.

???????? ??????? Kaspersky MLAD

Kaspersky Machine Learning for Anomaly Detection (MLAD) — это программный продукт, предназначенный для выявления аномалий в работе промышленного оборудования.

MLAD предназначен для одновременного наблюдения за большим количеством параметров телеметрии и автоматического анализа данных с целью:

- выявления отклонений в работе промышленных объектов до того, как эти отклонения станут представлять угрозу для производства;
- повышения эффективности технологического процесса, продления срока службы оборудования и снижения затрат не техническое обслуживание и ремонт;
- выявления нетипичных действий сотрудников и программного обеспечения, выявления подозрительной активности;
- решения специфических аналитических задач, таких как аналитический контроль и предиктивный анализ.

Документация на ПО MLAD доступна по ссылке: https://help.kaspersky.com.

?????? ??????????? ?????????? ???????

Пилотный проект с использованием программного продукта Kaspersky MLAD может быть проведен в двух различных форматах по договоренности с Заказчиком:

Пилотный проект формата офлайн – проводится в офисе Исполнителя. Данные для обучения и проведения инференса предоставляются Заказчиком. Развертывание MLAD в инфраструктуре Заказчика не производится.

Пилотный проект формата онлайн – проводится Исполнителем с развертыванием Kaspersky MLAD в инфраструктуре Заказчика, с непосредственным подключением программного продукта к источнику данных. Данные для обучения предоставляются Заказчиком, в то время как инференс проводится на потоковых данных, получаемых их источника данных. Аппаратное и программное обеспечение для развертывания Kaspersky MLAD предоставляется Заказчиком (или другим участником пилотного проекта – по договоренности). Требования к программно-аппаратному обеспечению приведены в документации на ПО MLAD (https://help.kaspersky.com).

????? ??????????? ?????????? ???????

В таблице ниже приведены этапы пилотного проекта и их задачи.

Этап	Задачи этапа

Предварительный этап	До начала проведения пилотного проекта Участники ознакомились с возможностями программного продукта Kaspersky MLAD и определили: 1. Цель проведения пилотного проекта. 2. Задачи, решаемые в рамках проведения пилотного проекта и критерии оценки успешности пилотного проекта. 3. Технологический процесс или единицы оборудования для проведения пилотного проекта. 4. Сроки проведения пилотного проекта. 5. Формат проведения пилотного проекта (онлайн/офлайн). 6. Для онлайн-формата – возможность удаленного подключения к инфраструктуре заказчика для разворачивания Kaspersky MLAD и его настройки. 7. Для онлайн-формата – протокол/API для подключения Kaspersky MLAD к источнику данных. 8. Участника пилотного проекта, ответственного за предоставление программно-аппаратного обеспечения для развертывания Kaspersky MLAD.
Установочная встреча участников пилотного проекта	• Определение круга лиц, участвующих в пилотном проекте. • Определение участника пилотного проекта со стороны Исполнителя, ответственного за развертывание программного продукта MLAD в тестовой среде, обработку данных, создание и обучение моделей и подготовку отчета. • Определение участника пилотного проекта со стороны Заказчика, ответственного за взаимодействие с представителем Исполнителя в процессе проведения пилотного проекта, в т.ч. по вопросам передачи данных, обеспечения доступов, выделения аппаратного обеспечения и т.д. • Определение формата взаимодействия участников пилотного проекта: группа в одном из мессенджеров, электронная почта, др.

Сбор исходных данных	• Определение Заказчиком (с привлечением остальных участниками пилотного проекта) перечня параметров процесса, релевантных для решения поставленных задач пилотного проекта. *На данном этапе требуется привлечение со стороны Заказчика инженера-технолога или иного специалиста, который сможет на схемах/мнемокадрах АРМ объяснить технологический процесс, показать, какие теги являются ключевыми, как происходит регулирование техпроцесса, как быстро меняется процесс. Здесь же необходимо уточнить детали, связанные с решаемой задачей. Например, если решается задача аналитического контроля, то необходимо выяснить, в какое время берутся пробы, сколько делается анализ, как часто оператор регулирует параметры и т.д.* • Предоставление Заказчиком массива исторических данных по соответствующим параметрам процесса, требуемых для создания, обучения и работы предиктивных моделей Kaspersky MLAD, в формате CSV или в формате Excel-таблиц. *Таблица должна содержать метки времени, имя тега и его значение. Отдельно для каждого тега должно быть предоставлено описание, размерность (опционально) и пороговые значения (опционально). Предоставленная для обучения выборка исторических данных должна охватывать нормальный режим работы оборудования. Количество точек информации в предоставленных данных и их дискретность зависит от инертности выбранного для пилотного проекта технологического процесса. За ориентир можно взять историю за 2 месяца с частотой дискретизации в 1 минуту.* • При проведении пилота в формате офлайн Заказчик также предоставляет выборку исторических данных, предназначенную для проведения инференса. Данная выборка должна позволить верифицировать результат работы предиктивных моделей Kaspersky MLAD. К примеру, это может быть выборка, содержащая аномалию, которую должен выявить Kaspersky MLAD в соответствии с поставленными задачами пилотного проекта. • Анализ, обработка и верификация предоставленных исторических данных Исполнителем. Подготовка данных для последующей загрузки в Kaspersky MLAD. • При проведении пилота в формате онлайн оптимальным способом является первоначальная установка, настройка, импорт данных, создание и обучение моделей в Kaspersky MLAD на локальном компьютере, после чего резервную копию настроенной локальной инсталляции можно развернуть на объекте.

Подготовка инфраструктуры Заказчика к развертыванию тестовой среды (при проведении пилота в формате онлайн)	• Предоставление ответственной стороной программно-аппаратного обеспечения (далее Сервер) для разворачивания Kaspersky MLAD в инфраструктуре заказчика. Проверка того, что выбранное для проведения пилота оборудование удовлетворяет требованиям к аппаратному и программному обеспечению для установки программных компонентов Kaspersky MLAD. • Предоставление Исполнителю всех доступов к инфраструктуре Заказчика, необходимых для разворачивания и настройки Kaspersky MLAD. • Обеспечение сетевого доступа от Сервера Kaspersky MLAD до источника данных для получения потоковых данных.
Развертывание тестовой среды (при проведении пилота в формате онлайн)	• Предоставление тестовых (NFR) лицензий на срок не менее одного, но не более трех месяцев в объеме, необходимом для реализации тестовой среды. Данные лицензии используются только для целей пилотного проекта. • Установка программных компонентов Kaspersky MLAD на предоставленный Сервер в инфраструктуре Заказчика (преднастроенная резервная копия или новая инсталляция). *Если разворачивается уже преднастроенная инсталляция, то после данного шага можно переходить непосредственно к настройке коннектора и подключению к источнику данных.* • Создание перечня активов в Kaspersky MLAD в соответствии с перечнем тегов процесса, предоставленным Заказчиком. • Загрузка исторических данных в Kaspersky MLAD. • Создание необходимых разметок и моделей в Kaspersky MLAD. • Обучение созданных моделей на обучающей выборке исторических данных, верификация результатов обучения. • Создание и настройка коннектора в Kaspersky MLAD для подключения к источнику данных. Проверка работоспособности.

Развертывание тестовой среды (при проведении пилота в формате офлайн)	• Предоставление тестовых (NFR) лицензий на срок не менее одного, но не более трех месяцев в объеме, необходимом для реализации тестовой среды. Данные лицензии используются только для целей пилотного проекта. • Установка программных компонентов Kaspersky MLAD в инфраструктуре Исполнителя. • Создание перечня активов в Kaspersky MLAD в соответствии с перечнем тегов процесса, предоставленным Заказчиком. • Загрузка исторических данных в Kaspersky MLAD. • Создание необходимых разметок и моделей в Kaspersky MLAD. • Обучение созданных моделей на обучающей выборке исторических данных, верификация результатов обучения.
Проведение испытаний (при проведении пилота в формате онлайн)	• Запуск обученных моделей на потоковый инференс. • Накопление прогнозируемых данных в объеме, достаточном для демонстрации решения поставленных задач пилотного проекта. • Демонстрация результатов работы предиктивных моделей и решения поставленных задач пилотного проекта Заказчику. • Оформление результатов прохождения испытаний в виде итогового отчета. В случае возникновения у Заказчика замечаний к работе программных компонентов Kaspersky MLAD или прохождению испытаний, это также фиксируется в отчете.
Проведение испытаний (при проведении пилота в формате офлайн)	• Запуск обученных моделей на исторический инференс с использованием тестовой выборки исторических данных, предоставленных Заказчиком. • Демонстрация результатов работы предиктивных моделей и решения поставленных задач пилотного проекта Заказчику. • Оформление результатов прохождения испытаний в виде итогового отчета. В случае возникновения у Заказчика замечаний к работе программных компонентов Kaspersky MLAD или прохождению испытаний, это также фиксируется в отчете.

Решение проблем, возникших в ходе развертывания тестовой среды и проведения испытаний	Для устранения ошибок и сбоев в работе программных компонентов Kaspersky MLAD во время пилотного проекта Исполнитель предоставляет подробное описание проблемы Инженеру предпродажной поддержки Вендора. если Инженер предпродажной поддержки Вендора не может помочь с решением возникшей проблемы, то Инженер внедрения заводит кейс на портале поддержки Вендора (https://companyaccount.kaspersky.com/) и далее следует инструкциям инженеров технической поддержки в части сбора дополнительной информации об ошибке или сбое и выполнения действий в тестовой среде по их устранению.
Пилотная эксплуатация (при необходимости)	После развертывания тестовой среды, настройки программных компонентов Kaspersky MLAD и завершения испытаний по желанию Заказчика, продукт может остаться в пилотной эксплуатации до окончания срока действия ключей, выпущенных под пилотный проект. Если у Заказчика есть необходимость увеличить срок действия опытной эксплуатации, это обсуждается отдельно с Менеджером по развитию бизнеса Kaspersky MLAD Вендора.
Оценка результатов пилотного проекта	• Организация сессии для оценки результатов пилотного проекта. • Определение степени успешности пилотного проекта в соответствии поставленными целями и задачами. • Согласование дальнейших шагов после завершения пилотного проекта.
Сбор обратной связи	Сбор Инженером предпродажной поддержки Вендора обратной связи от других участников пилотного проекта о вопросах, касающихся программных компонентов Kaspersky MLAD: • процедура развертывания, • полнота документации, • неудобства и проблемы эксплуатации, • необходимость внедрения дополнительного функционала; • иные вопросы на усмотрение участников пилотного проекта. Передача обратной связи также может осуществляться и на более ранних этапах пилотного проекта в формате. Формат передачи обратной связи определяется по договоренности.

???????? ????????? ? ??????

В дополнение к перечисленным в документе материалам, могут быть полезны следующие ресурсы:

- https://mlad.kaspersky.com – сайт Kaspersky Machine Learning for Anomaly Detection;
- https://www.kaspersky.ru/enterprise-security/industrial-cybersecurity – сайт, посвященный KICS;
- https://www.kaspersky.ru/enterprise-security/industrial-cybersecurity#certification – список сертификаций KICS;
- https://ics-cert.kaspersky.ru – сайт Kaspersky ICS CERT;
- https://os.kaspersky.ru – сайт Kaspersky OS;
- https://box.kaspersky.com/f/9a924f698b56405a93ce/ – обзор функциональности решения KICS for Networks;
- https://www.kaspersky.ru/enterprise-security/industrial-cybersecurity/certification – сертификаты совместимости программных компонентов KICS с решениями промышленных вендоров;
- https://support.kaspersky.ru/corporate/lifecycle – жизненный цикл программных продуктов АО «Лаборатория Касперского»;
- https://support.kaspersky.ru/common/certificates – сертификаты ФСТЭК и ФСБ на программные продукты АО «Лаборатория Касперского»;
- https://regulhub.kaspersky.ru – регуляторный хаб;
- https://support.kaspersky.com/help – онлайн справка по продуктам;
- https://locator.kaspersky.com – сертифицированные Партнёры;
- https://box.kaspersky.com/d/1290ec9a671c4599bc58/ – ссылка на презентацию по решению KICS.

Revision #5
Created 19 February 2026 08:17:35 by Эльдар Юсуфов
Updated 19 February 2026 08:44:28 by Эльдар Юсуфов