Kaspersky®
Machine Learning
for Anomaly Detection

Kaspersky MLAD

Опыт импортозамещения системы раннего обнаружения аномалий для ГТУ ТЭЦ

Азат Шайхутдинов
Лаборатория Касперского

https://mlad.kaspersky.ru
mlad@kaspersky.ru

Экосистема кибербезопасности

Конвергенция IT-OT

Промышленный XDR

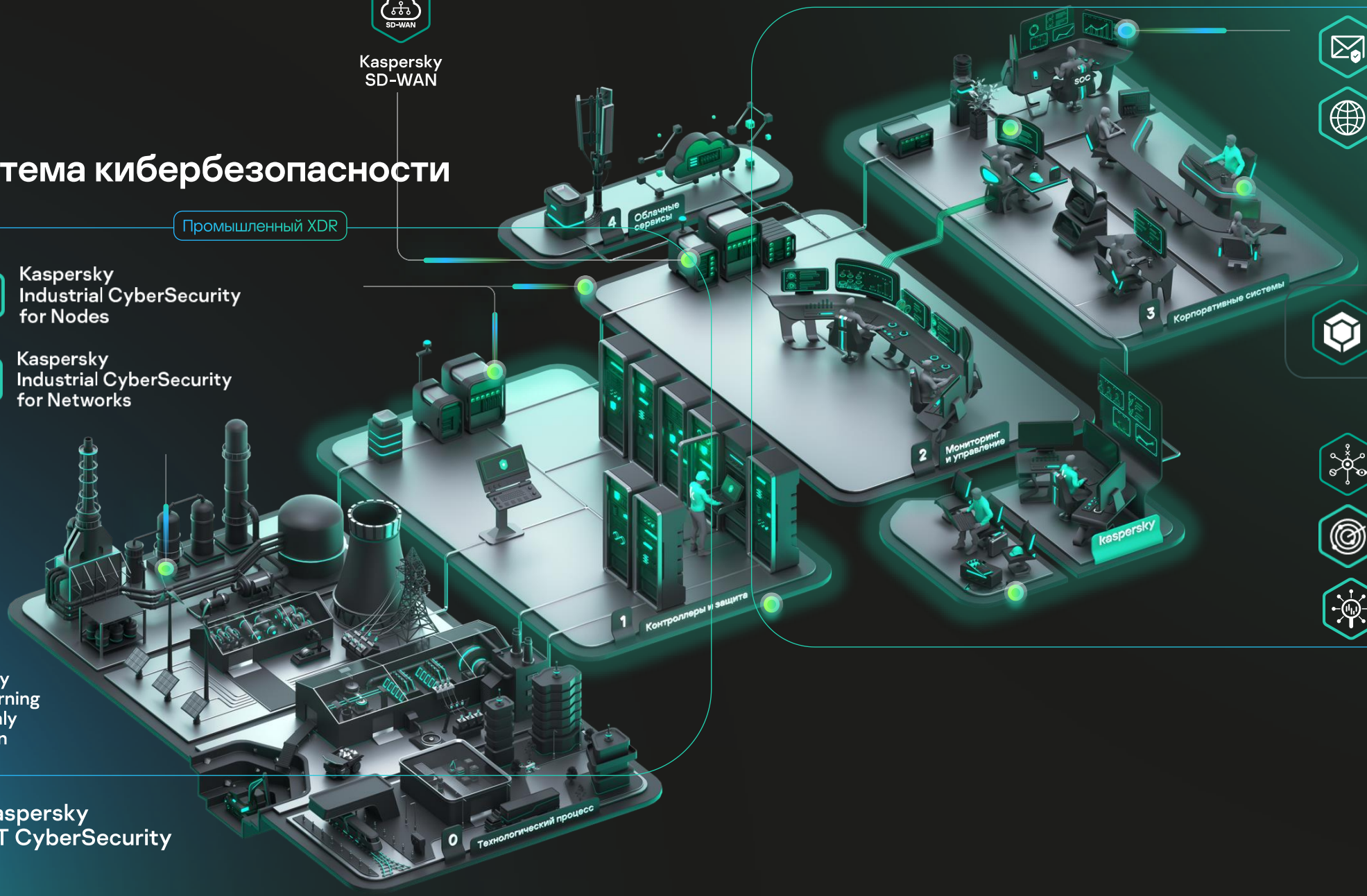
Kaspersky SD-WAN

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

Kaspersky Machine Learning for Anomaly Detection

Kaspersky OT CyberSecurity



Kaspersky Security для почтовых серверов

Kaspersky Security для интернет-шлюзов

Kaspersky Security для бизнеса

Kaspersky EDR Expert

Kaspersky Anti Targeted Attack

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Symphony XDR

Проектный опыт с вендорами АСУ ТП

Платформа Kaspersky Industrial CyberSecurity имеет сертификаты совместимости с более чем 50 решениями поставщиков АСУ ТП. «Лаборатория Касперского» регулярно проводит тестирование на совместимость, осуществляет интеграцию решений и продуктов, предлагает отлаженные и проверенные временем инструменты для защиты промышленных систем.

- **123 сертифицированных систем от 67 поставщиков АСУ ТП**
- **2 национальных и международных сертификатов**

ОАО «АГАТ – системы управления»
- АГАТ-2000

ООО НПП «ЭКРА»
- EKRASCADA
- EKRASMS
- EKRASMS-SP
- EKRASCADA 2.12

АО «ЭлеСи»
- SCADA Infinity
- Integrity SCADA

ООО «НТК ИНТЕРФЕЙС»
- ОИК-ДИСПЕТЧЕР НТ

ООО НПФ «КРУГ»
- SCADA КРУГ-2000

ООО «Прософт-Системы»
- ПТК ARIS MC/MD/MT
- Программный комплекс «ARIS SCADA»
- Устройство противоаварийной автоматики энергоузла

Hangzhou HollySys Automation
- HOLLiAS MACS

Schneider Electric
- Citect SCADA
- Clear SCADA
- Unity Pro engineering software
- EMCS-PACiS (SCADA system EcoSUI)
- PACiS Software
- SEPAM Relay Protection Devices
- MiCOM P series
- MiCOM C264/C264C Bay Computer Unit
- MiCOM H35V2 Switch
- ConneXium Switch
- Foxboro (Foxboro Evo)
- EcoStruxure Hybrid

Common Criteria ISO/IEC 15408
- Kaspersky Security Center 13

ARC Informatique
- PcVue

Сертификаты совместимости с промышленными вендорами
https://www.kaspersky.ru/enterprise-security/industrial-cybersecurity/certification

Сертификаты ФСТЭК и ФСБ
https://www.kaspersky.ru/enterprise-security/industrial-cybersecurity/certification

Наши клиенты в Энергетике – публичные истории успеха

https://www.kaspersky.ru/enterprise-security/industrial-cybersecurity#stories

СМОЛЕНСКАЯ АЭС
РОСАТОМ

Энергетика

«Лаборатория Касперского» обеспечивает кибербезопасность Смоленской АЭС

КУРСКАЯ АЭС
РОСАТОМ

Энергетика

Комплексный подход к защите Курской АЭС

РОССЕТИ
СЕВЕРО-ЗАПАД

Энергетика

Объекты «Россети Северо-Запад» защищены от современных киберугроз

ОБЪЕДИНЕННАЯ ЭНЕРГЕТИЧЕСКАЯ КОМПАНИЯ

Энергетика

«ДиалогНаука» внедрила систему ИБ в АСУ ТП «Объединенной энергетической компании»

Сетевая Компания

Энергетика

«Лаборатория Касперского» реализует проект по защите объектов промышленной инфраструктуры АО «Сетевая компания»

ИНТЕР РАО
ЭЛЕКТРОГЕНЕРАЦИЯ

Энергетика

Объекты ПАО «Интер РАО» защищены от современных киберугроз

ТГК-2
ТЕРРИТОРИАЛЬНАЯ ГЕНЕРИРУЮЩАЯ КОМПАНИЯ №2

Энергетика

«ТГК-2» защищает промышленную сеть с помощью Kaspersky Industrial CyberSecurity

ТАТЭНЕРГО

Энергетика

Kaspersky Industrial CyberSecurity for Nodes защитит критическую инфраструктуру ТЭЦ и ГЭС АО «Татэнерго»

Шулбі ГЭС
Шульбинская ГЭС

Энергетика

Шульбинская ГЭС сотрудничает с «Лабораторией Касперского»

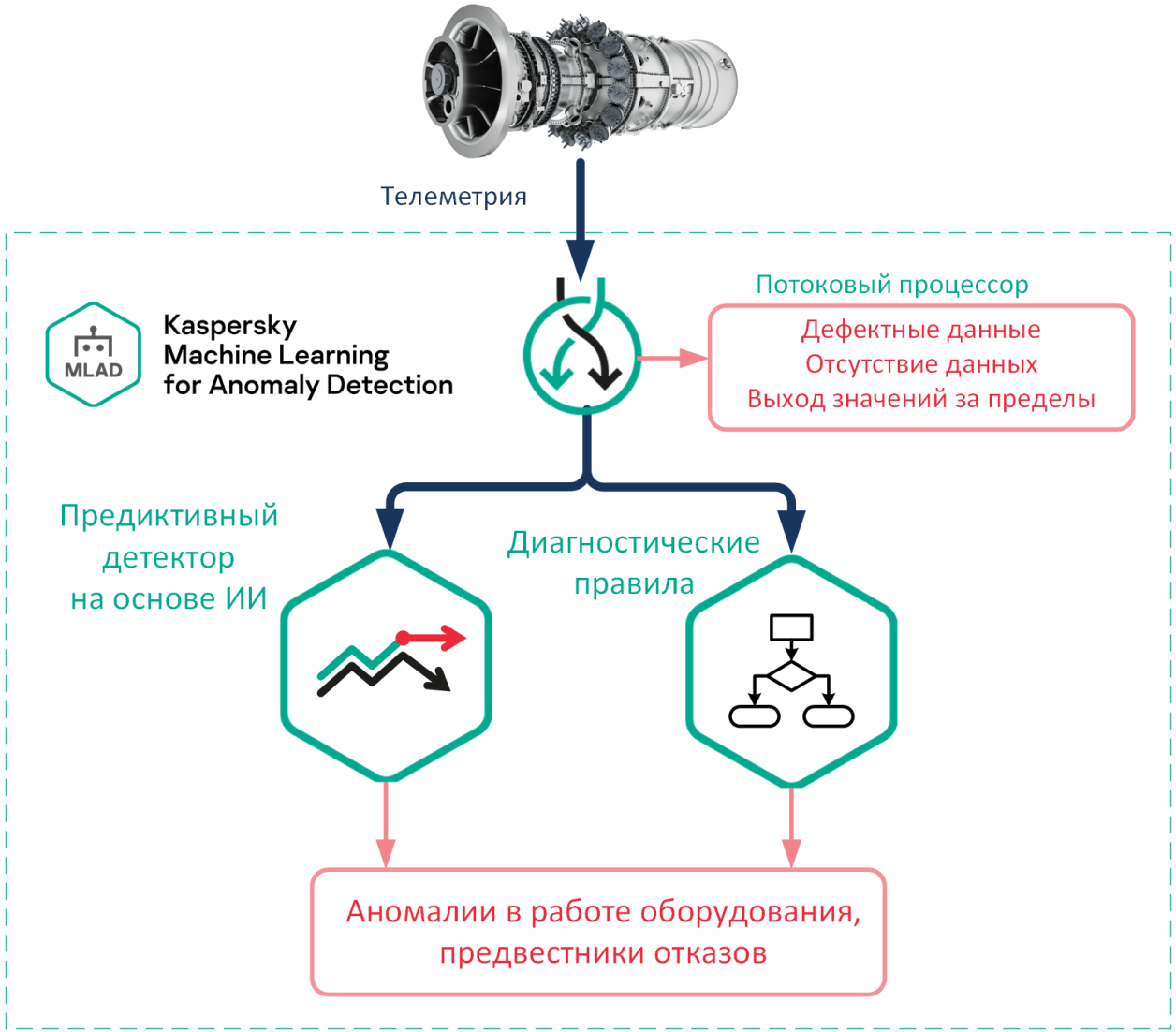
alperia

Энергетика

Компания Alperia выбрала Kaspersky Industrial CyberSecurity for Nodes для защиты своих систем удаленного управления

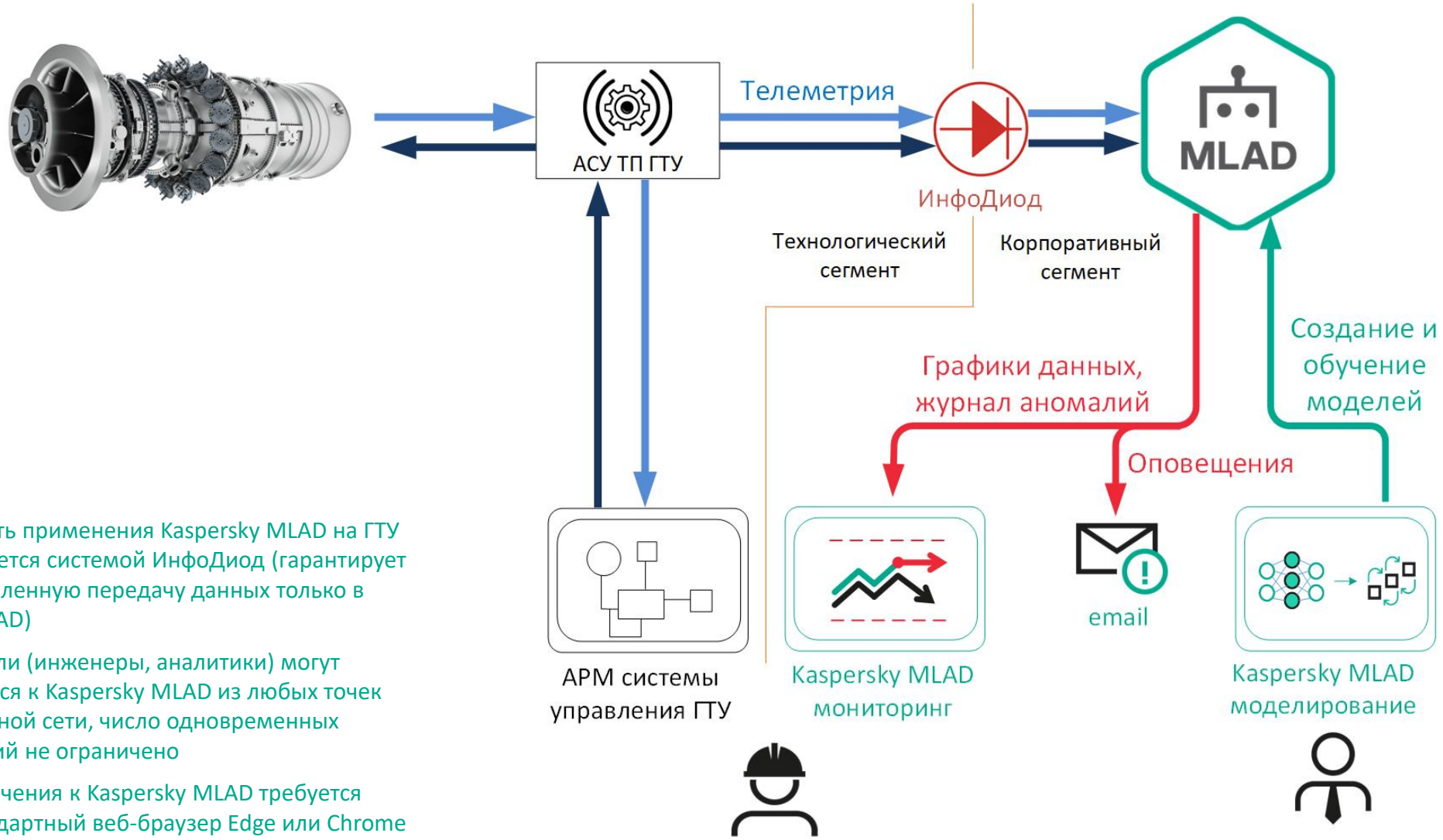
Kaspersky MLAD

Предиктивная аналитика на базе искусственного интеллекта



- **Раннее** обнаружение потенциально опасных отклонений в работе оборудования или ошибок персонала
- **Предотвращение** незапланированных остановов
- **Повышение** эффективности работы установки
- **Продление** межремонтных интервалов
- Возможность применения как **искусственного интеллекта**, так и **диагностических правил**
- Встроенный **конструктор моделей**
- Анализируем – находим – извещаем **без вмешательства** в контур управления
- Зарегистрировано в Реестре **российского ПО** под №16939

Схема развертывания Kaspersky MLAD



- Безопасность применения Kaspersky MLAD на ГТУ обеспечивается системой ИнфоДиод (гарантирует однонаправленную передачу данных только в сторону MLAD)
- Пользователи (инженеры, аналитики) могут подключаться к Kaspersky MLAD из любых точек корпоративной сети, число одновременных подключений не ограничено
- Для подключения к Kaspersky MLAD требуется только стандартный веб-браузер Edge или Chrome

Использование Kaspersky MLAD

Kaspersky®
Machine Learning
for Anomaly Detection

Внедрение на ТЭЦ

Цель: Повышение механической готовности технологического оборудования газотурбинной установки (ГТУ) ТЭЦ путем обнаружения в данных телеметрии признаков начала деградации оборудования, указывающих на вероятное возникновение отказа в будущем, или ошибочных действий персонала.

Задачи проекта

- Развертывание на ГТУ отечественного решения Kaspersky MLAD (импортозамещение системы Predix от General Electric + дополнительные возможности).
- Создание и оценка предиктивных / диагностических моделей для ГТУ в Kaspersky MLAD.
- Предоставление возможности для специалистов ГТУ самостоятельно создавать / изменять предиктивные модели.

Kaspersky®
Machine Learning
for Anomaly Detection

Предварительные результаты

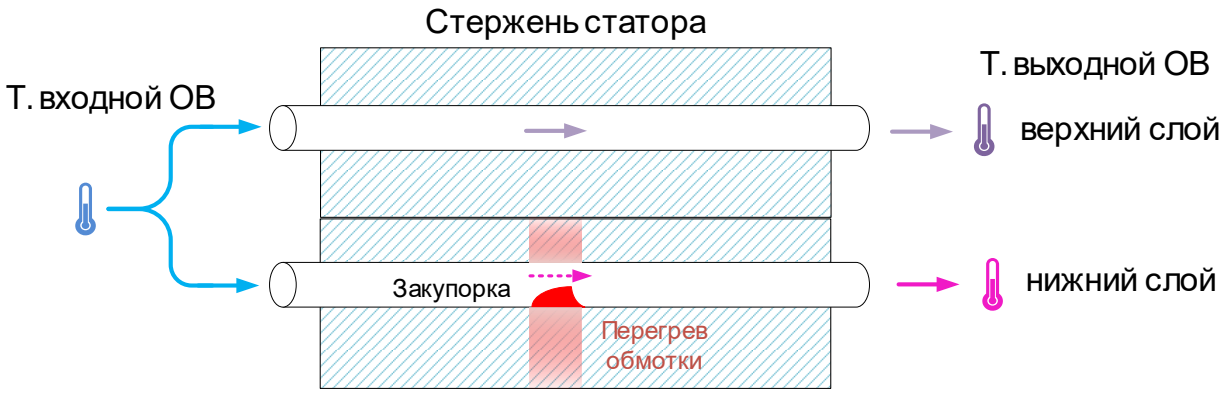
- Отобрано ок. **5000** тегов телеметрии ГТУ для анализа в Kaspersky MLAD.
- Декодирован и загружен в MLAD архив исторических данных за 3 года. Всего около **5 миллиардов** индивидуальных значений.
- Kaspersky MLAD анализирует поток телеметрии ГТУ в реальном времени. Всего около **1700** индивидуальных значений в секунду.
- Совместно со специалистами ТЭЦ созданы, обучены и поставлены в работу предиктивные модели для основных компонентов ГТУ. Работа по созданию моделей продолжается.
- Kaspersky MLAD выявил деградацию критического оборудования, не обнаруженную другими средствами и персоналом. Приняты надлежащие меры по диагностике, запланирован ремонт.

Kaspersky®
Machine Learning
for Anomaly Detection

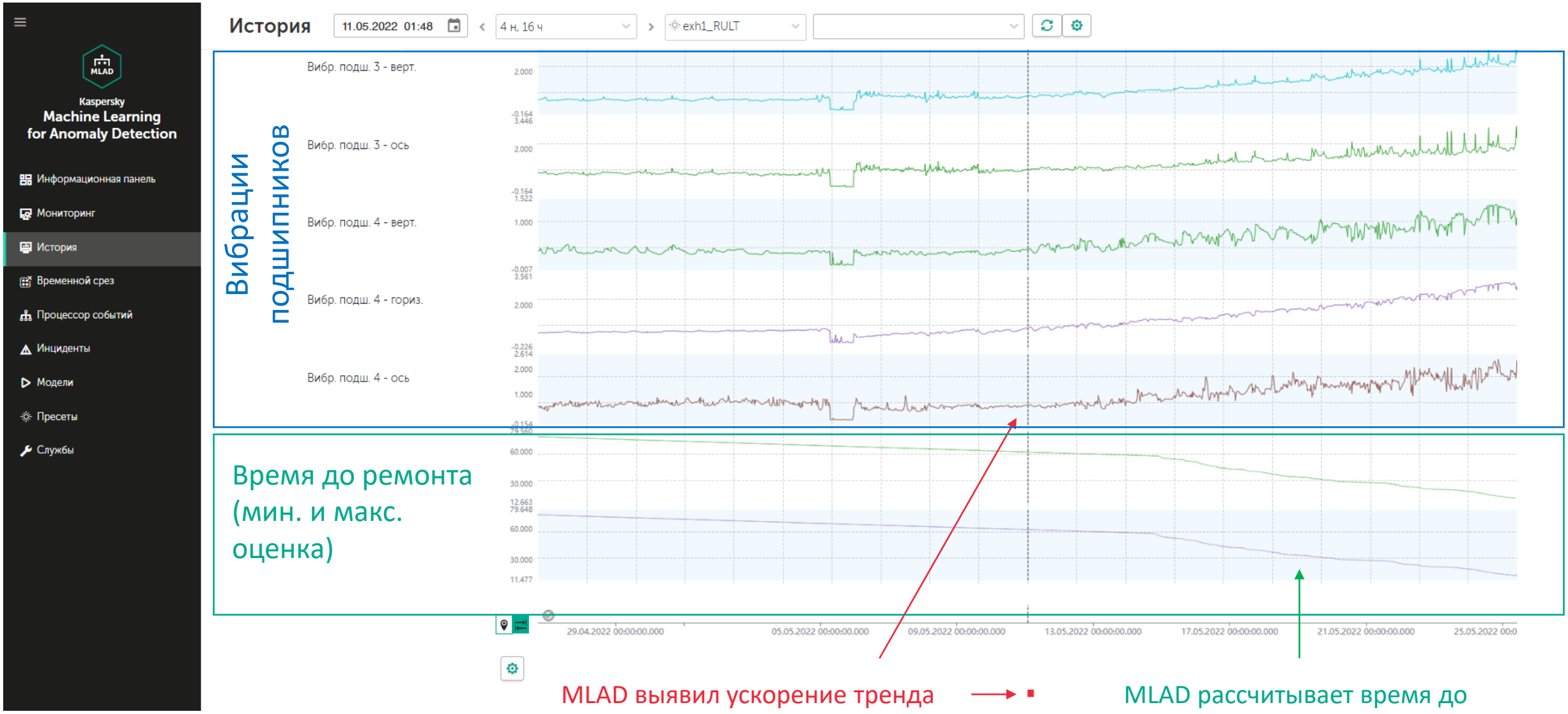
Пример: Ранее выявление перегрева турбогенератора

Традиционный контроль не видит проблемы:
значение температур воды не превышает заданный порог

Kaspersky MLAD обнаруживает проблему:
поведение одной из температур аномально, так как его динамика не объясняется влиянием прочих известных факторов



Пример: Оценка остатка срока службы подшипника



Итоги проекта

- ✓ Выявление признаков развивающихся дефектов и нештатных ситуаций в работе ГТУ **без необходимости привлечения производителя и отправки данных за периметр**
- ✓ Возможность **сфокусировать** предиктивные детекторы на конкретные проблемные точки/процессы ГТУ
- ✓ Возможность использовать **экспертизу собственных** специалистов при создании и корректировке моделей
- ✓ **Инновационный подход** к анализу данных с применением искусственного интеллекта.
- ✓ **Удобный и наглядный** доступ к графикам данным (в том числе исторических), инструменты анализа данных

MLAD

Kaspersky®
Machine Learning
for Anomaly Detection

kaspersky

AZAT.SHAYKHUTDINOV@KASPERSKY.COM
89179200078
https://mlad.kaspersky.ru
mlad@kaspersky.ru