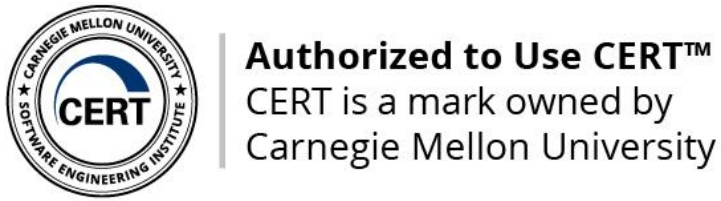
kaspersky

Kaspersky Industrial CyberSecurity
Стратегический подход к промышленной кибербезопасности

Содержание

Kaspersky ICS CERT



Глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Прогнозы на 2021

Случайные заражения

- Заражения будут становиться менее случайными или иметь неслучайные продолжения. Появление новых нестандартных сценариев атак на АСУ ТП и полевые устройства, а также неожиданные схемы их монетизации
- Вероятность повторения сценария наподобие WannaCry в самом ближайшем будущем (снятие с поддержки Windows 7 и Server 2008, утечка исходных кодов Windows XP)

Атаки вымогателей

- Вымогатели становятся все более технологически оснащенными и изощренными
- Получат развитие идеи, реализованные в Snake. Направленность шифровальщиков на АСУ ТП
- Атаки замаскированные под атаки вымогателей, но с совсем иными целями, как это уже было с ExPetr

APT

- Кибератаки, включая атаки на промышленные предприятия, будут использоваться как инструмент военных действий наряду с беспилотниками и информационными атаками через СМИ
- Появление новых акторов, в том числе атакующих организации, относящиеся к различным промышленным секторам
- Не исключено, что в 2021 году мы увидим продолжение серии Stuxnet — Black Energy — Industroyer — Triton.

Последствия COVID-19

- Ограничение возможности проведения работ «на месте» замедлило темпы усиления защиты периметра
- Увеличене масштаба распространения вредоносного ПО и усугубление последствий киберинцидентов (причина - удаленка)
- Ухудшение экономической обстановки – пополнение рядов хакеров, подкуп работников предприятий.

Kaspersky Industrial CyberSecurity

СЕРВИСЫ

Обучение и программы повышения осведомленности

- Kaspersky® Security Awareness
- Kaspersky® Security Trainings

Экспертные сервисы и данные об угрозах

- Kaspersky® Security Assessment
- Kaspersky® Incident Response
- Kaspersky® Threat Intelligence

РЕШЕНИЯ

Защита промышленных компьютеров

- KICS for Nodes

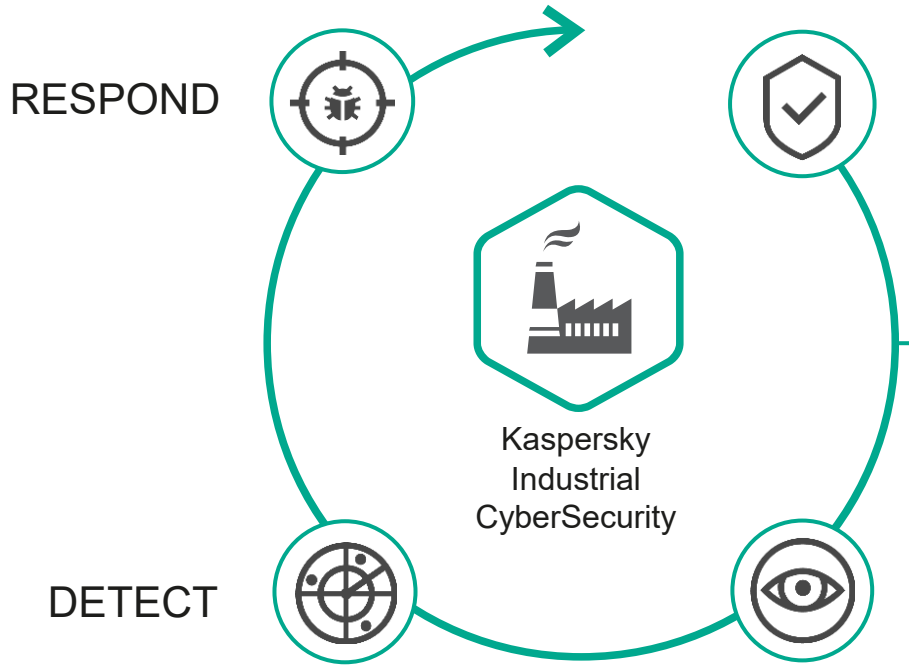
Обнаружение аномалий и угроз в промышленной сети

- KICS for Networks

Централизованное управление безопасностью

- Kaspersky Security Center

Kaspersky Industrial Cybersecurity



400+ проектов
21 страна

РОССИЯ

30 000+
Промышленных АРМ/серверов
под защитой KICS for Nodes

200+
Промышленных сетей
под защитой KICS for Networks

Kaspersky Industrial Cybersecurity. Сертификация ФСТЭК РФ, ФСБ

ФСТЭК: Nodes - «АВ3» уровня 3-В

Networks – «СОВ» С-4

ФСБ: СОА класса Г

Kaspersky Industrial Cybersecurity. Партнерства с вендорами АСУ ТП

EMERSON

Schneider Electric

SIEMENS

YOKOGAWA

Honeywell

Ресурсы

ИСТОРИИ УСПЕХА | СЕРТИФИКАТЫ СОВМЕСТИМОСТИ | ОБЗОР РЕШЕНИЯ

Развитие безопасных сред требует совместных усилий. Именно поэтому «Лаборатория Касперского» все больше взаимодействует с производителями систем промышленной автоматизации. Мы предлагаем наши тесты на сертфикацию и интероперабельность, готовим модели возможного взаимодействия, а также интегрируем наши продукты и решения.

«Лаборатория Касперского» предлагает надежные и проверенные инструменты, которые помогают построить защищенную и гибкую промышленную среду. Наша экспертиза позволяет производителям встраивать передовое защитное решение, полностью сочетающееся с требованиями и рекомендациями регуляторов. Результат этого — интегрированное решение, которое полезно не только для защиты конечных пользователей, но и для каждого участника цепи поставок.

ARC Informatique
- PcVue

Aveva
- Wonderware SP2017
- Wonderware System Platform

B&R
- РСУ Апрол

Siemens
- PCS 7 V8.2 SP1, V9.0
- SPPA T3000
- WinCC Open Architecture 3.14
- WinCC Open Architecture 3.15
- WinCC Open Architecture 3.16 P006

TÜV Austria Services
- Сертификация соответствия IEC 62443

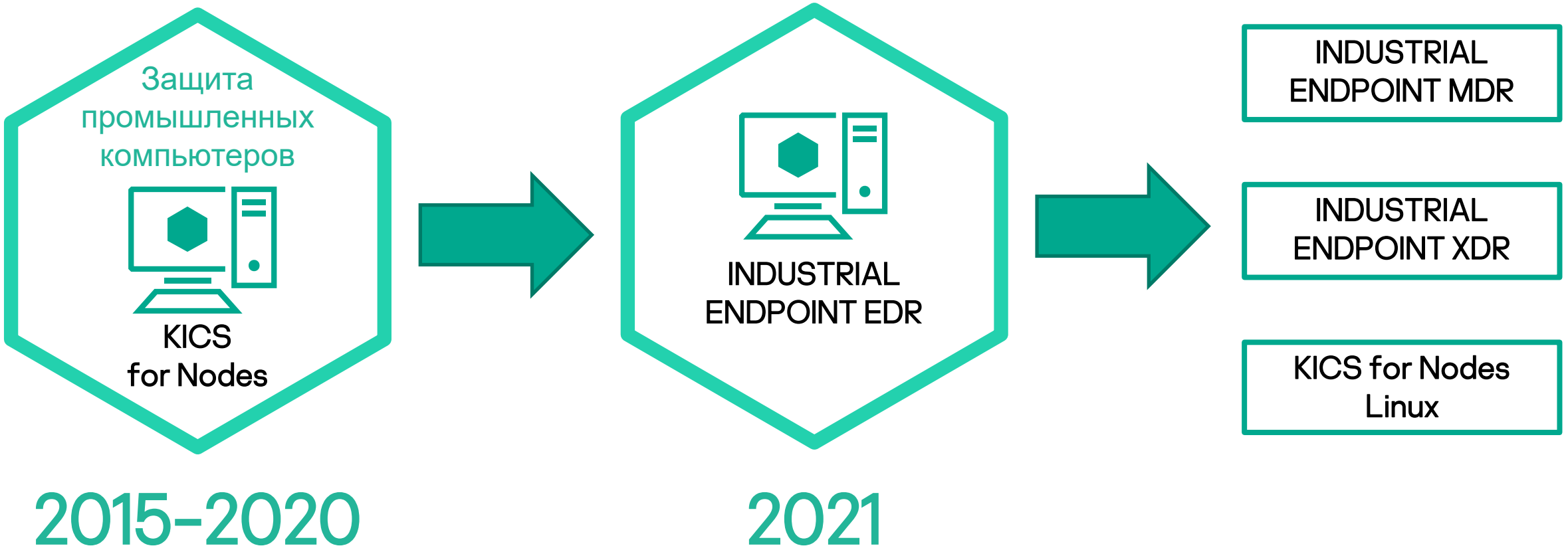
Монитор Электрик
- СК-11 (ver. 11.5.2)

НПП «Вибробит»
- Вибробит Web.Net.Monitoring

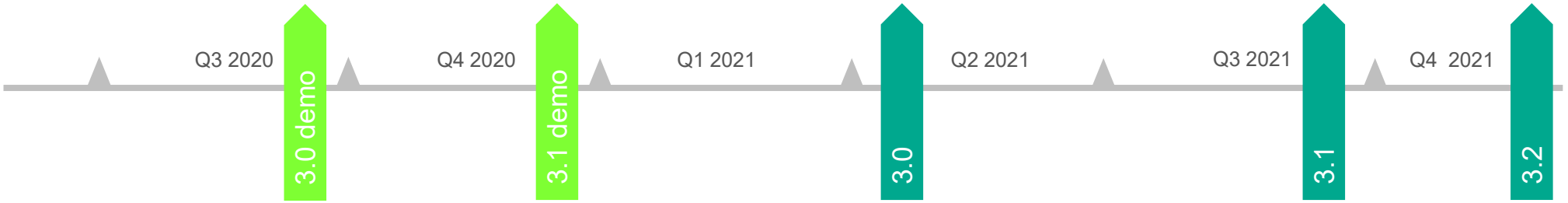
НПП ИТ
- «ВАКС» «Стандартный»

Kaspersky Industrial Cybersecurity. Технологические партнерства

Kaspersky Industrial Cybersecurity. Развитие KICS for Nodes



Kaspersky Industrial Cybersecurity. Развитие KICS for Networks



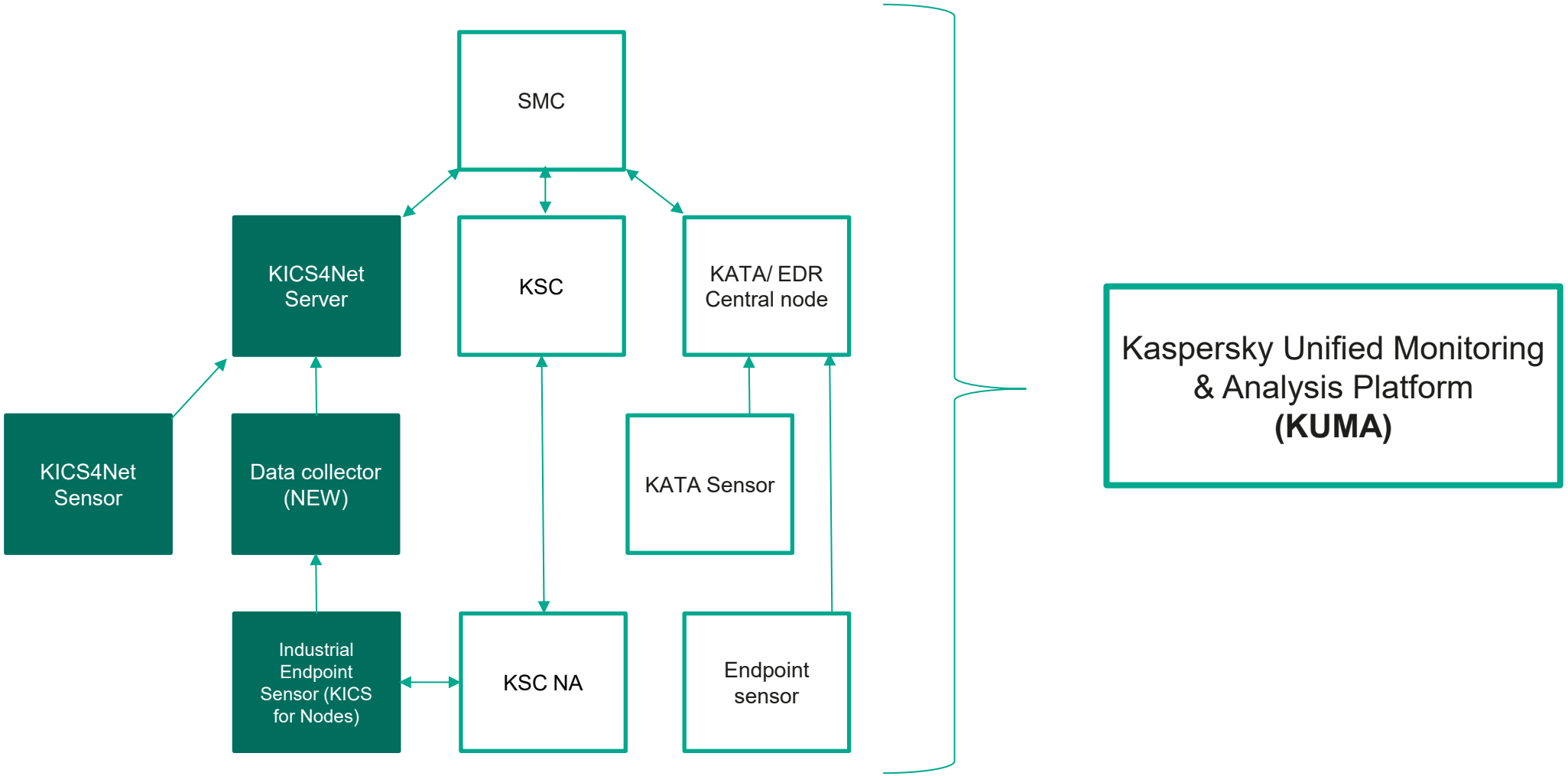
KICS for Networks 3.0:

- Мониторинг уязвимостей с формированием рекомендаций по устранению
- Полнофункциональная веб-консоль

KICS for Networks 3.1:

- Централизованное управление распределенной инфраструктурой серверов KICS for Networks
- Интеграция KICS for Nodes и KICS for Networks (EDR сценарии, обмен информацией об ассетах)
- Скоринг рисков

Kaspersky Industrial Cybersecurity. Кросс-продуктовая интеграция



Оценка авторитетных агентств

KICS был отмечен авторитетными аналитическими агентствами:

- Gartner
- Forrester
- ARC Advisory
- Bloomberg NEF

https://kas.pr/kics-gartner

KICS 2015-2021
Истории успеха

ТАНЕКО

«Этот проект наглядно продемонстрировал возможность использования подобных решений на промышленных объектах. ТАНЕКО планирует и далее расширять своё сотрудничество с «Лабораторией Касперского» в области защиты индустриальных сетей.» - Марат Гильмутдинов, Начальник отдела АСУ ТП, ТАНЕКО

Производитель нефти

Основанная в 2005 году, входит в состав группы «Татнефть», которая оценивается в 15 миллиардов долларов

Использует промышленные системы управления, чтобы обеспечить технологическое преимущество над конкурентами и минимизировать производственные затраты

Растущий уровень автоматизации производства и использование технологий, изначально разработанных для корпоративных сетей, в своей промышленной инфраструктуре подвергли компанию риску кибератак.

Защищена непрерывность производственного процесса

Обнаружены аномалии и несанкционированные попытки перенастроить контроллеры

Отслеживаются технологические процессы и автоматически обнаруживаются отклонения процесса от нормального поведения с технологией MLAD

Системы обнаружения аномалий, анализа отклонений и автоматического раннего предупреждения

AGC

«За 2 года использования Kaspersky Industrial CyberSecurity мы оценили индивидуальный подход „Лаборатории Касперского“ и динамичное развитие ее решения. В отношении сотрудничества этой компании также нет равных: мы всегда можем рассчитывать на эффективную командную работу и консультативную помощь» – Ян Хоубен, директор завода AGC Glass Germany GmbH

Производственный сектор

- Год основания: 2003
- Клиенты: BMW, Volkswagen, Mercedes, Volvo, Opel
- Использует решение Kaspersky Industrial CyberSecurity с 2016 года

«Лаборатория Касперского» обеспечила интеграцию KICS с платформой Tomorrow Connect. Это открыло целый ряд новых полезных возможностей:

• телеметрические данные производства и статус киберзащиты отображаются на панели управления директора завода в режиме реального времени;

• KICS выявляет нарушения технологических процессов с помощью технологии DPI, что помогает избежать ошибок на производстве и гарантировать качество продукции.

НЛМК

«Внедрение современных интеллектуальных систем автоматического управления на производстве увеличивает риски потенциальных кибератак, которые могут повлиять на технологический процесс. Для их предотвращения на НЛМК мы внедряем комплексную эшелонированную защиту на уровне инфраструктуры систем автоматизации.» - Сергей Слаута, директор дирекции по автоматизации технологических процессов НЛМК

Производитель стали

Крупнейший металлургический завод в России

Основано в 1931

Работает в России, Европе и США.

Защищено

Промышленные системы управления в цехе динамной стали защищены от кибератак

Модернизирована инфраструктура автоматизации благодаря объединению вычислительных ресурсов АСУ ТП в нескольких территориально распределенных центрах обработки данных.

Внедрена не только возможность киберзащиты конечных узлов АСУ ТП, но и обнаружения нештатных ситуаций и вторжений в промышленные сети при помощи технологий пассивного мониторинга.

АО «Сетевая компания»

«АО «Сетевая компания» реализует комплекс эффективных организационно-технических мер направленных на обеспечение приемлемого уровня информационной безопасности своих объектов во избежание нарушения или остановки своих критических процессов. В связи с этим, мы обратились к специалистам «Лаборатории Касперского» с целью оказания содействия по повышению защищенности предприятия от киберугроз» - Зыков Сергей, , начальник центра кибербезопасности АО «Сетевая компания»

Электроэнергетика

Входит в десятку самых крупных электросетевых компаний России.

Защищено

В результате реализации проекта **более 150 серверов и рабочих станций** технологического контура АО «Сетевая компания» защищены с применением KICS for Nodes, а мониторинг ключевых сегментов технологической сети обеспечивают **10 серверов KICS for Network**.

Реализованный комплексный подход к защите критической инфраструктуры позволил значительно снизить риск нарушения критических процессов и обеспечить высокий уровень кибербезопасности на объектах АО «Сетевая компания».

МосГаз

«Уверены, что этот совместный проект послужит основой для тесного многолетнего сотрудничества. Модернизация системы кибербезопасности АСУ ТП АО «МОСГАЗ» будет продолжаться» – Александр Кузин, заместитель начальника управления информатизации АО «МОСГАЗ»

Транспортировка природного газа по газораспределительным сетям Москвы

Основано в 1865

Ежегодная отгрузка 23 миллиардов кубометров природного газа

7500 километров газораспределительных сетей

Защищены промышленные узлы и сети

Более 500 газораспределительных станций с KICS for Network

- Всего ~600 ПЛК Siemens
- До 20 клапанов в каждом ПЛК

Группа из 7 централизованных SCADA-серверов с KICS for Nodes

Kaspersky Industrial Cybersecurity Conference 2021

Kaspersky

https://ics.kaspersky.ru/conference/

Познякевич Александр
Менеджер по развитию бизнеса
Kaspersky Industrial Cybersecurity

Alexander.Poznyakevich@kaspersky.com
Tel: +7 (903) 527 65 88
www.kaspersky.com

kaspersky