



KAMAZ

**Промышленная
инфраструктура
автомобильного
завода «КАМАЗ»
под защитой
«Лаборатории
Касперского»**

kaspersky АКТИВИРУЙ
БУДУЩЕЕ



**Kaspersky
Industrial
CyberSecurity**



Автомобильное производство

- Год основания: 1969
- Объем продукции составляет 45% всего российского рынка тяжелых грузовых автомобилей
- За время работы завода выпущено более 2 240 000 грузовых автомобилей

«Наша компания проводит полную интеграцию цифровых систем проектирования, производственных процессов и управления оборудованием, поэтому одним из наших главных приоритетов стало обеспечение необходимого уровня информационной безопасности, в связи с чем мы обратились к специалистам “Лаборатории Касперского”»

Шостак Юрий Григорьевич,
директор ЦИКТ ПАО
“КАМАЗ”

Группа компаний «КАМАЗ» – крупнейшая автомобильная корпорация Российской Федерации. ПАО «КАМАЗ» входит в число двадцати ведущих мировых производителей тяжелых грузовых автомобилей и находится на 16-м месте по объемам производства тяжелых грузовиков полной массой более 16 тонн. Производственные мощности составляют 71 тыс. автомобилей в год.

Единый производственный комплекс группы организаций ПАО «КАМАЗ» охватывает весь технологический цикл производства грузовых автомобилей – от разработки, изготовления, сборки автотехники и автокомпонентов до сбыта готовой продукции и сервисного сопровождения. В состав технологической цепочки входит несколько крупных заводов: литейный и кузнечный заводы, завод двигателей, прессово-рамный завод, автомобильный завод, ремонтно-инструментальный завод, Индустриальный парк «Мастер». Всего в технологической цепочке ПАО «КАМАЗ» занято 32,7 тыс. человек.

Главной целью ПАО «КАМАЗ» в области качества является создание конкурентоспособной продукции и сервиса, удовлетворяющих требованиям и ожиданиям потребителей и обеспечивающих стабильное финансовое положение компании. Группа компаний выпускает грузовую технику широкого спектра: грузовые автомобили (более 60 моделей, свыше 1500 комплектаций), прицепы, автобусы, двигатели, силовые агрегаты, городские развозные грузовики и электробусы.

Задача

ПАО «КАМАЗ» уделяет особое внимание цифровой трансформации производства, цифровые технологии активно внедряются в работу всех блоков предприятия. Однако изменения, связанные с цифровой трансформацией предприятия, повышают риски проникновения вредоносного ПО на конечные автоматизированные рабочие места (АРМ), а также на серверы технологического сегмента и анализа сетевого трафика в технологических сегментах АСУ ТП.

В связи с существующими глобальными угрозами информационной безопасности руководство ПАО «КАМАЗ» приняло решение повысить уровень защищенности технологических процессов на автомобильном заводе, заводе двигателей и прессово-рамном заводе. Для предприятий с таким крупносерийным и стандартизированным производством главным приоритетом является сохранение непрерывности и доступности технологических процессов, поскольку в случае задержки или полной остановки производства компания может понести значительные убытки, – Гиззатов Рамиль Маратович, директор ДИР ЦИТ ООО «Центр обслуживания бизнеса»



Решение



Незначительное влияние на защищаемые устройства

Kaspersky Industrial CyberSecurity не оказывает влияния на непрерывность технологических процессов и позволяет минимизировать потребление вычислительных ресурсов.



Высокая совместимость

Решение совместимо с программными и аппаратными компонентами промышленных систем автоматизации, таких как SCADA, ПЛК и PCU.



Контроль среды

Kaspersky Industrial CyberSecurity обеспечивает применение политики запуска приложений и доступа к съемным устройствам, а также осуществляет пассивный мониторинг сетевого трафика АСУ ТП.

На основе данных сравнительного анализа представленных на рынке продуктов для обеспечения информационной безопасности промышленной инфраструктуры, руководством ПАО «КАМАЗ» было выбрано решение Kaspersky Industrial CyberSecurity (KICS):

KICS for Nodes – средство защиты инженерных рабочих станций, станций диспетчеров, серверов SCADA. Продукт обеспечивает контроль запуска приложений (whitelisting), контроль целостности файлов, контроль периферийных устройств, обнаружение и блокирование вредоносного ПО. KICS for Nodes позволяет минимизировать потребление ресурсов. Модульная архитектура продукта позволяет устанавливать только необходимые защитные компоненты, при этом они могут быть сконфигурированы и для предотвращения угроз, и только для их обнаружения.

KICS for Networks – продукт для пассивной инвентаризации устройств и сетевых коммуникаций в промышленной сети, а также пассивного мониторинга атак и аномалий в трафике промышленной сети с инспекцией промышленных протоколов (DPI) для контроля команд и технологических параметров процесса. KICS for Networks выявляет аномалии и вторжения в АСУ ТП на ранних этапах и обеспечивает необходимые контрмеры для предотвращения ущерба технологическим процессам. Возможности продукта не зависят от используемого промышленного модуля, поэтому клиенты не ограничены в выборе поставщиков для своей инфраструктуры. Интерфейс KICS for Networks включает панель управления, данные которой обновляются в режиме реального времени, и карту сети, что позволяет удобно работать с устройствами предприятия и отслеживать события безопасности.

Результаты

«Kaspersky Industrial CyberSecurity имеет оптимизированный набор компонентов защиты по сравнению с другими решениями, а также обеспечивает сниженную нагрузку на вычислительные ресурсы, благодаря чему наши технологические процессы остаются непрерывными»

Халфин Марат, начальник отдела управления корпоративными сервисами ЦИКТ ПАО «КАМАЗ»

Комплексный подход к промышленной безопасности обеспечил высокий уровень киберзащиты на производственных объектах ПАО «КАМАЗ», снизив риск нарушения критически важных процессов. Продукты «Лаборатории Касперского» обеспечили безопасность электронных блоков, панелей, систем управления и навигации.

Решение "Лаборатории Касперского", выбранное для защиты промышленной среды, уникально тем, что позволяет выявлять аномалии в режиме реального времени, но при этом имеет незначительное влияние на защищаемые устройства, – Кузнецов Вадим Петрович, главный специалист ДИР ЦИТ ООО «Центр обслуживания бизнеса»



**Kaspersky
Industrial
CyberSecurity**

Kaspersky Industrial CyberSecurity – это набор технологий и сервисов, созданных для защиты различных уровней промышленной инфраструктуры и других элементов предприятия, в том числе серверов SCADA, операторских панелей, инженерных рабочих станций, ПЛК, сетевых соединений и даже самих инженеров. При этом решение не влияет на непрерывность технологических процессов.

Узнайте больше на: www.kaspersky.ru/ics

www.kaspersky.ru
#ИстиннаяБезопасность

© АО «Лаборатория Касперского», 2021.
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.



"Компания года" по версии Frost and Sullivan в сфере промышленной кибербезопасности (АСУ ТП) – 2020



Победитель платиновой награды VDC Research 2020 в категории "Промышленная безопасность"