Решения для бизнеса

Нефть под защитой: «Лаборатория Касперского» реализовала проект промышленной безопасности на Павлодарском нефтехимическом заводе

ҚазМұнайГаз
ПАВЛОДАР МҰНАЙ-ХИМИЯ ЗАУЫТЫ

https://www.pnhz.kz/

ПНХЗ

Павлодарский нефтехимический завод (ТОО «ПНХЗ») – крупнейшее предприятие на северо-востоке Казахстана по переработке нефти и производству нефтепродуктов.

Нефтепереработка

- Введен в эксплуатацию в 1978 году
- Входит в АО «Национальная компания «КазМунайГаз»
- Имеет сбалансированную мощность 5,1 млн тонн нефти в год

Павлодарский нефтехимический завод (ТОО «ПНХЗ») – одно из трех ключевых нефтяных предприятий Республики Казахстан.

ПНХЗ выпускает широкую линейку нефтепродуктов. Среди них автомобильные бензины различных марок: АИ-80, АИ-92, АИ-95, АИ-98, дизельное топливо, нефтяное топливо (мазут), углеводородные сжиженные газы, вакуумный газойль, техническая сера, битумы нескольких сортов (строительный, дорожный, кровельный), нефтяной кокс.

Приоритет для ПНХЗ сегодня – обеспечение производства моторных топлив, соответствующих экологическим классам К4, К5, в необходимом для нужд страны объеме, увеличение технического ресурса завода, вывод его на двухгодичный межремонтный цикл, выпуск авиатоплива нового для предприятия международного стандарта Jet A.

Проблематика

Защищенность промышленных объектов – одна из самых горячо обсуждаемых тем в Казахстане. Во втором полугодии 2016 года Казахстан занял 7-е место в мире по количеству атакованных промышленных компьютеров.

Одним из ключевых приоритетов деятельности ПНХЗ является обеспечение промышленной кибербезопасности и повышение надежности автоматизации предприятия.

Увеличение степени автоматизации, а также активное проникновение технологий, разработанных для бизнес-структур, в промышленную инфраструктуру, значительно повышает риски, связанные с кибератаками на промышленные объекты.

В настоящее время защищенность промышленных объектов – одна из самых горячо обсуждаемых тем в Казахстане. И это неслучайно: по данным отчета ICS CERT «Лаборатории Касперского», во втором полугодии 2016 года Казахстан занял седьмое место в мире по количеству атакованных промышленных компьютеров. В первом полугодии 2017 года атакам подверглись 45,9% систем промышленной автоматизации в Казахстане.

Таким образом, перед заводом в полной мере стояла задача обеспечить промышленную безопасность с точки зрения киберугроз.

Безопасность

Мониторинг системных команд программируемых логических контроллеров (ПЛК) защищает от кибератак, направленных на ключевые объекты АСУ ТП.

Контроль

Обнаружение несанкционированных устройств позволяет осуществлять контроль целостности промышленной сети.

Управление рисками

Внедрение комплексного решения по киберзащите промышленных сред помогает усовершенствовать систему управления рисками на предприятии.

Решение

Выбранное на ПНХЗ решение Kaspersky Industrial CyberSecurity – набор технологий и сервисов для защиты ключевых уровней промышленных систем, включая серверы SCADA, операторские панели, инженерные рабочие станции, ПЛК и сетевые соединения.

Для обеспечения кибербезопасности своей инфраструктуры ПНХЗ выбрал не только решение по защите конечных узлов из портфолио Kaspersky Industrial CyberSecurity, но и защиту на уровне промышленной сети, а также тренинг для персонала. Такой комплексный подход обеспечивает надежную защиту всех компонентов производственной среды – от рабочих мест до серверов и ПЛК. Это помогает сохранить непрерывность и стабильность технологических процессов.

Решение Kaspersky Industrial CyberSecurity разработано специально для защиты критически важных инфраструктур и промышленного оборудования. Решение использует широкий ряд технологий борьбы с угрозами, таких как защита от вредоносных программ, создание белых списков и поиск аномалий в промышленных протоколах. Кроме того, оно обеспечивает контроль доступа к устройствам, благодаря чему клиенты могут отслеживать подключения к портативным устройствам хранения данных и периферийным устройствам.

«Повседневные возможности защиты бизнеса, предлагаемые «Лабораторией Касперского» дополнены технологиями, разработанными специально для промышленных сред: такими как проверка целостности и семантический мониторинг команд управления процессами. Кроме того, Kaspersky Industrial CyberSecurity может работать в специальном режиме мониторинга, позволяющем обнаруживать кибератаки, операционные ошибки сотрудников и аномалии в промышленных сетях», – комментирует Татьяна Пятина, отвечающая за развитие бизнеса «Лаборатории Касперского» в Казахстане.

«Перед “Лабораторией Касперского” стояла задача обеспечить кибербезопасность индустриальных АРМ-операторов и SCADA-сервера, а также контроля целостности технологической сети и контроля ключевых параметров технологического процесса. Кроме этого, решение не должно было требовать изменения конфигурации АСУ ТП и оказывать влияния на технологический процесс. Поставленная задача была успешно выполнена»

Семен Тихоненко,
главный специалист по защите информации ТОО «ПНХЗ»

Результаты

Внедрение экспертами «Лаборатории Касперского» решений из портфолио Kaspersky Industrial CyberSecurity совместно с проведением профильного тренинга позволило сформировать на ПНХЗ системный подход к обеспечению промышленной кибербезопасности и обеспечить надежную защиту от киберугроз.

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