



**Решение Kaspersky Industrial CyberSecurity
«Лаборатории Касперского» прошло испытания
в промышленной инфраструктуре НЛМК**



НЛМК

Новолипецкий металлургический комбинат (НЛМК) – основная производственная площадка международной Группы НЛМК, одной из самых эффективных металлургических компаний мира с вертикально-интегрированной моделью бизнеса и активами в России, Европе и США.



Черная металлургия

- Основан в 1934 году
- Входит в Группу НЛМК
- Липецк, Россия
- Доля в российском производстве стали: **18%**
- Производственная мощность: **более 13 млн тонн стали в год**

Благодаря самообеспеченности основным сырьем, энергоресурсами, а также высокой технологической оснащенности, Группа НЛМК является лидером российской металлургии и единственной компанией из России, которая входит в двадчатку крупнейших производителей стали в мире. Мощности Группы по производству стали превышают 17 млн тонн в год.

В Липецке выпускают около 80% всей стальной продукции Группы НЛМК. Производство включает все технологические процессы: от переработки сырья до выпуска металлопродукции высоких переделов. Она используется в различных отраслях – от строительства и машиностроения до энергетического оборудования и оффшорных ветровых установок.

Задача

«Лаборатория Касперского» совместно с Новолипецким металлургическим комбинатом приступила к реализации пилотного проекта по созданию эффективной защиты промышленных информационных систем от кибератак в цехе динамной стали.

В ходе реализации проекта НЛМК была поставлена задача создать современную инфраструктуру автоматизации с объединением вычислительных ресурсов автоматизированных систем управления (АСУ ТП) в нескольких территориально распределенных центрах обработки данных. Такой подход повышает надежность АСУ ТП и сокращает издержки на ее поддержку. При этом, такая архитектура позволяет сформировать четкий сетевой периметр и организовать безопасную передачу данных из систем автоматизации в корпоративные сети, таким образом повысив устойчивость промышленных информационных систем к кибератакам.

«Проект по защите инфраструктуры НЛМК стал для нас ценным и уникальным опытом. Использование виртуализации на верхнем уровне АСУ ТП поставило сразу несколько интересных технических задач, с которыми эксперты «Лаборатории Касперского» успешно справились. Такие вызовы безусловно оказывают положительное влияние на развитие нашего решения, и мы всегда готовы пойти им навстречу»

Георгий Шебулдаев,
руководитель направления Kaspersky
Industrial CyberSecurity в России



Неинтрузивное решение

Решение Kaspersky Industrial CyberSecurity не влияет на непрерывность технологических процессов.



Реальные сценарии атак

Технологии Kaspersky Industrial CyberSecurity разработаны на основе реальных сценариев киберфизических атак на различные отрасли промышленности.



Управление рисками

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

Решение

Для обеспечения кибербезопасности внутри защищенного периметра, на площадке НЛМК было использовано решение Kaspersky Industrial CyberSecurity, разработанное «Лабораторией Касперского», которое включает набор технологий и сервисов для защиты различных уровней промышленной инфраструктуры, в том числе серверов визуализации процессов, инженерных рабочих станций и программируемых логических контроллеров.

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

«Для нас проект по защите инфраструктуры НЛМК стал ценным и уникальным опытом. Использование виртуализации на верхнем уровне АСУ ТП поставило сразу несколько интересных технических задач, – **говорит Георгий Шебулдаев, руководитель направления Kaspersky Industrial CyberSecurity в России.** – К примеру, размещение нескольких виртуальных серверов на одном физическом гипервизоре накладывает дополнительные требования по обеспечению безопасности и балансированию нагрузки. Так при одновременном запуске антивирусного сканирования на нескольких виртуальных серверах увеличение общей нагрузки на дисковую подсистему может повлиять на работу остальных виртуальных машин и, в конечном итоге, на технологический процесс. Эксперты «Лаборатории Касперского» успешно справились с задачами, продиктованными не типичной для промышленного заказчика инфраструктурой».

В настоящее время все компоненты решения Kaspersky Industrial CyberSecurity успешно опробованы и находятся на пользовательском тестировании в цехе.

«Сотрудничество
НЛМК и «Лаборатории
Касперского»
не ограничивается
пилотными
и коммерческими
внедрениями, а скорее
является перспективным
технологическим
партнерством»

Сергей Слаута,
директор Дирекции
по автоматизации технологических
процессов ПАО «НЛМК»

Результаты

«Внедрение современных интеллектуальных систем автоматического управления на производстве увеличивает риски потенциальных кибератак, которые могут повлиять на технологический процесс. Для их предотвращения на Новолипецком комбинате мы внедряем комплексную эшелонированную защиту на уровне инфраструктуры систем автоматизации, – **подчеркнул Сергей Слаута, директор дирекции по автоматизации технологических процессов НЛМК.** – Решение Kaspersky Industrial CyberSecurity учитывает реальные потребности нашего предприятия и отвечает основным требованиям по обеспечению кибербезопасности технологических процессов. Уверен, что сотрудничество Группы НЛМК и «Лаборатории Касперского» не ограничится пилотным проектом, а станет началом перспективного технологического партнерства».



**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», 2018. Все права защищены. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.