

ТГК-2 выбрала решения «Лаборатории Касперского»

для построения комплексной
XDR-защиты

kaspersky активируй
будущее



5000

сотрудников компании

> 2 700 000

человек проживает в городах
деятельности компании



Одна из 14 территориальных
генерирующих компаний
(ТГК) России.

ПАО «Территориальная генерирующая компания № 2» (ТГК-2)

ТГК-2 — одна из крупнейших теплоэнергетических компаний Северо-Западного и Центрального округов России, внедрила решение класса SIEM — Kaspersky Unified Monitoring and Analysis Platform (KUMA). Эта система обеспечивает сбор, анализ и корреляцию событий информационной безопасности и призвана объединить решения, обеспечивающие безопасность промышленного и корпоративного сегментов, в комплексную систему безопасности предприятия.

Включает крупнейшие
генерирующие предприятия
пяти регионов: Архангельской,
Вологодской, Костромской,
Новгородской и Ярославской
областей.

В Ярославле, Костроме
и Архангельске за ТГК-2
закреплён статус единой
теплоснабжающей
организации (ЕТО).

к

История сотрудничества ТГК-2 с «Лабораторией Касперского» насчитывает почти 15 лет. Началась она практически с момента основания теплоэнергетической компании. Первым продуктом, внедрённым на предприятии, стал Kaspersky Endpoint Security для бизнеса. Затем постепенно на ТГК-2 развернули и другие решения:

- Kaspersky Industrial CyberSecurity for Networks — для мониторинга промышленных сетей АСУ ТП;
- Kaspersky Industrial CyberSecurity for Nodes — для защиты конечных узлов промышленной среды;
- Kaspersky Automated Security Awareness Platform (KASAP) — онлайн-платформу для обучения сотрудников основам киберграмотности.

Предыстория

До развёртывания KUMA в ТГК-2 пользовались иностранным решением класса SIEM. После того как производитель покинул Россию, перед ИБ-специалистами компании встала острая необходимость поиска равнозначной замены из отечественных решений.

Решение должно было одновременно не уступать продуктам лидеров мирового рынка по функциональности, лёгкости масштабирования и помогать в соответствии с требованиями регуляторов. В результате оценки функциональных возможностей и пилотирования было выбрано решение от «Лаборатории Касперского», которое оправдало все ожидания ещё в ходе пилотного проекта. KUMA легко устанавливается и интегрируется с другими защитными решениями «Лаборатории Касперского» и продуктами сторонних вендоров как в корпоративном, так и в промышленном сегментах ТГК-2. Это позволяет развернуть единую XDR-платформу на всех объектах предприятия. Центральный элемент KUMA собирает и анализирует данные и предоставляет ИБ-специалистам ТГК-2 полную картину происходящего и инструменты для оперативного реагирования на инциденты.



**Kaspersky
Unified Monitoring
and Analysis Platform**

Ключевые

преимущества KUMA

- Высокая производительность и низкие системные требования
- Лёгкая масштабируемость и отказоустойчивость
- В основе — современная микросервисная архитектура
- Интеграция из «коробки» с решениями «Лаборатории Касперского» и продуктами сторонних поставщиков с возможностью реагирования при обнаружении инцидента
- Помощь в соответствии требованиям регуляторов
- Интегрированный модуль ГосСОПКА для обмена данными с НКЦКИ
- Дорожная карта и чёткие планы развития в соответствии с мировыми трендами в области разработки SIEM-систем

Александр Суворов

Начальник отдела информационной безопасности ПАО «ТГК-2»

Марина Усова

Руководитель управления корпоративных продаж «Лаборатории Касперского»

Решение

Kaspersky Unified Monitoring and Analysis Platform (KUMA) — высокопроизводительная SIEM-система отечественного производства.

Платформа обеспечивает централизованный сбор, анализ и корреляцию событий безопасности из различных источников данных. Полученная информация позволяет ИБ-специалистам ТГК-2 быть в центре событий: своевременно выявлять потенциальные угрозы и реагировать на них. KUMA объединяет продукты «Лаборатории Касперского» и других вендоров в единую ИБ-систему и является ключевым компонентом для реализации комплексного подхода к информационной безопасности. Это решение позволяет предприятиям топливно-энергетического комплекса защитить себя от актуальных киберугроз как в корпоративном, так и в промышленном сегментах.

Результат и отзывы

Специалисты «Лаборатории Касперского» помогли оперативно развернуть Kaspersky Unified Monitoring and Analysis Platform на ТГК-2, доказав её эффективность и лёгкость масштабирования. В результате ТГК-2 удалось заместить импортный продукт и создать комплексную систему класса XDR на базе уже внедрённых решений «Лаборатории Касперского» для защиты промышленных объектов и корпоративных сетей.



В разумные сроки нам удалось заменить импортную SIEM-систему на решение отечественного производителя — нашего многолетнего партнера. По своим техническим возможностям KUMA не уступает продуктам мировых лидеров SIEM, быстро разворачивается, легко масштабируется и управляется из единой консоли. Особенно ценно, что внедрение KUMA позволило выйти на новый уровень защиты сложной инфраструктуры ТГК-2 и сделать уверенный шаг в сторону комплексной безопасности.



ТГК-2 — одно из первых промышленных предприятий в России, которое осознало важность комплексного подхода к информационной безопасности и внедрило решение KUMA для защиты промышленных объектов и корпоративных сетей. В свою очередь, KUMA — это центральный элемент платформы XDR (Extended Detection and Response), в рамках которой решения «Лаборатории Касперского» и продукты сторонних поставщиков взаимодействуют между собой и способны обеспечить топовый уровень безопасности компаний, а также предоставить высококласный инструментарий для работы внутренних ИБ-команд.

Расширение сотрудничества

В 2025 году безопасность инфраструктуры ТГК-2 усилили решения **Kaspersky Anti Targeted Attack** с модулем **NDR** и **Kaspersky EDR Expert**. Их внедрение обеспечит функционал для быстрого обнаружения угроз, непрерывного мониторинга и сбора данных в режиме реального времени.

Встроенный модуль NDR расширит возможности КАТА в части сетевых угроз, что позволит проводить глубокий анализ сетевого трафика, выявлять атаки с помощью правил детектирования, индикаторов компрометации и ретроспективного анализа.



**Kaspersky
Anti Targeted
Attack**

Преимущества КАТА с NDR

- Построение карты сети без SPAN
- Коннекторы для настраиваемого реагирования на сетевых устройствах
- Возможность использования детектов на узлах для формирования комплексных инцидентов, включающих сетевые и узловые алерты



**Kaspersky
Endpoint Detection
and Response
Expert**

Преимущества KEDR Expert

- Централизованное реагирование на инциденты
- Повышение эффективности анализа угроз и реагирования на инциденты
- Устранение брешей в системе безопасности и быстрое обнаружение сложных угроз и целевых атак
- Сокращение трудозатрат на процесс обработки сложных инцидентов на уровне конечных точек



**Kaspersky
Unified Monitoring
and Analysis
Platform**

[Подробнее](#)



**Kaspersky
Anti Targeted
Attack**

[Подробнее](#)



**Kaspersky
Endpoint Detection
and Response
Expert**

[Подробнее](#)

www.kaspersky.ru

© 2025, АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки
обслуживания являются собственностью
их правообладателей.

#kaspersky
#активируйбудущее