Объекты «Россети Северо-Запад» защищены от современных киберугроз

РОССЕТИ СЕВЕРО-ЗАПАД

ПАО «МРСК Северо-Запада»

2021

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Industrial CyberSecurity

Объекты «Россети Северо-Запад» защищены от современных киберугроз

mrsksevzap.ru

Передача и распределение электроэнергии

Крупнейшая сетевая организация на Северо-Западе России

Дочернее общество ПАО «Россети»

Основано в 2004 году

Компания «Россети Северо-Запад» (ПАО «МРСК Северо-Запада») – основной оператор, оказывающий услуги по передаче электроэнергии и присоединению к электросетям в Архангельской, Вологодской, Мурманской, Новгородской, Псковской областях, Республике Карелия и Республике Коми. Территория обслуживания компании – 1,4 млн кв. км с населением около 5,8 млн человек. Общая протяженность воздушных и кабельных линий электропередачи составляет 177,8 тыс. км. Количество подстанций напряжением 35 кВ и выше, состоящих на балансе, – 1180 штук, установленная мощность силовых трансформаторов подстанций – 19,52 тыс. МВА.

В рамках задач, поставленных Энергетической стратегией России перед электроэнергетикой, «Россети Северо-Запад» видит свою миссию в обеспечении качественного и бесперебойного энергоснабжения с применением современных инновационных технологий.

Задача и приоритеты компании

В качестве основных стратегических приоритетов компания «Россети Северо-Запад» выделяет обеспечение надежного и безопасного энергоснабжения потребителей, сокращение потерь электроэнергии, а также цифровую трансформацию деятельности. Однако цифровая трансформация повышает риски реализации кибератак в отношении информационной инфраструктуры предприятия, что может привести к перебоям в работе электростанций, потере электроэнергии и росту несчастных случаев. В связи с этим «Россети Северо-Запад» уделяет особое внимание обеспечению кибербезопасности своих объектов. Руководство компании поставило задачу внедрить решение, которое обеспечит защищенность объектов электроэнергетики всех типов киберугроз, а также выполнение требований законодательства по защите значимых объектов критической информационной инфраструктуры.

Решение

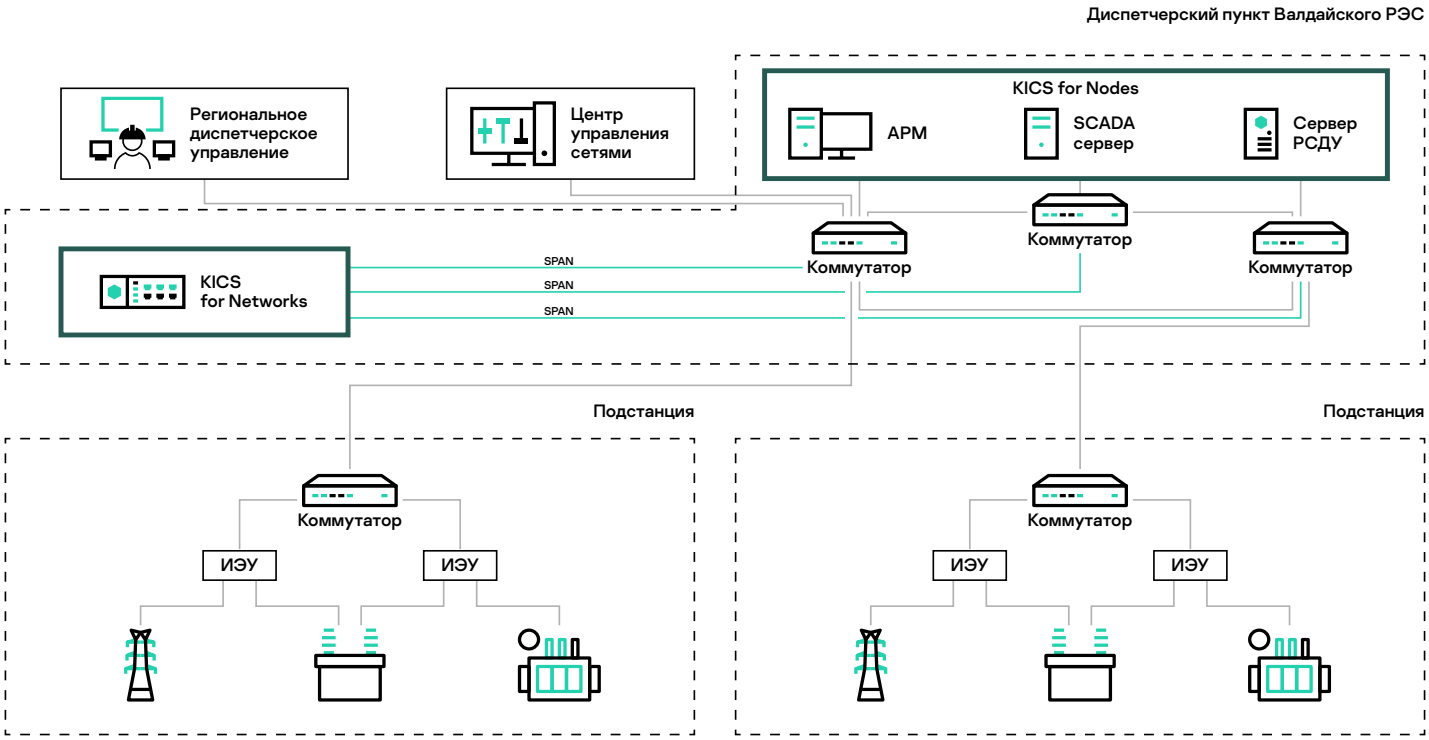
В качестве решения специалисты «Россети Северо-Запад» выбрали продукт Kaspersky Industrial CyberSecurity (KICS). В середине 2020 года было проведено полномасштабное пилотное внедрение продукта в Валдайском районе электрических сетей (РЭС), который является наиболее передовым и цифровизированным РЭС в МРСК Северо-Запада.

KICS for Networks – это решение, позволяющее реализовать сценарии инвентаризации устройств и сетевых коммуникаций, пассивного выявления атак и аномалий в трафике промышленной сети, а также инспекции промышленных протоколов для контроля команд и параметров технологического процесса. KICS for Networks выявляет аномалии и вторжения в АСУ ТП на ранних этапах и обеспечивает необходимые контрмеры для предотвращения ущерба технологическому оборудованию. Возможности продукта не зависят от используемой аппаратной платформы, поэтому клиенты не ограничены в выборе поставщиков для своей инфраструктуры. Интерфейс KICS for Networks включает консоль управления, данные которой обновляются в режиме реального времени, и карту сети, что позволяет удобно работать с устройствами предприятия и отслеживать события безопасности.

KICS for Nodes – это средство комплексной защиты узлов промышленной сети от различных типов киберугроз, которые могут быть вызваны человеческим фактором, вредоносным ПО, целевыми атаками и диверсиями. Продукт совместим с программными и аппаратными компонентами промышленных систем автоматизации.

Преимущества решения

- ✓ **Обнаружение устройств**: пассивная идентификация и учет устройств в промышленной сети
- ✓ **Deep Packet inspection (DPI)**: анализ телеметрии технологических процессов практически в режиме реального времени
- ✓ **Контроль целостности сети**: обнаружение несанкционированных хостов и потоков в сети
- ✓ **Система обнаружения вторжений**: оповещение о вредоносной активности в сети
- ✓ **Контроль команд**: проверка команд, передаваемых по промышленным протоколам
- ✓ **Поддержка внешних систем**: обнаружение угроз внешними системами благодаря интеграции через API
- ✓ **Использование машинного обучения для обнаружения аномалий (MLAD)**: выявление аномалий в цифровых и физических процессах с помощью телеметрии в режиме реального времени и обработки исторических данных (рекуррентная нейронная сеть)
- ✓ **Обнаружение уязвимостей**: обновляемая база уязвимостей промышленного оборудования



«Сотрудничество «Россети Северо-Запад» и «Лаборатории Касперского» не ограничивается пилотным внедрением KICS for Networks в Валдайском РЭС – мы планируем защитить и другие объекты электроэнергетики при помощи Kaspersky Industrial CyberSecurity»

Кирилл Паничкин,
начальник отдела информационной безопасности департамента безопасности «Россети Северо-Запад»

Результаты

Пилотное внедрение Kaspersky Industrial CyberSecurity было завершено успешно: специалисты «Россети Северо-Запад» убедились в том, что продукт эффективно выполняет заявленные функции, обеспечивает выполнение требований законодательства и стабильность технологического процесса в МРСК Северо-Запада. Пробная эксплуатация KICS for Networks позволила принять решение о внедрении продукта и дальнейшем масштабировании проекта с установкой KICS for Networks на других РЭС и подстанциях в течение следующих нескольких лет, а также провести внедрение продукта KICS for Nodes с целью обеспечения защиты АРМ и серверов АСУ ТП предприятия.

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

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

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