



«Лаборатория Касперского» реализует проект по защите объектов промышленной инфраструктуры АО «Сетевая компания»



Миссия АО «Сетевая компания» — обеспечение надежного, качественного и доступного электроснабжения потребителей, создание условий для эффективной деятельности предприятий и организаций, комфортной и безопасной жизнедеятельности населения в целях динамичного социально-экономического развития Республики Татарстан.

«АО «Сетевая компания» реализует комплекс эффективных организационно-технических мер направленных на обеспечение приемлемого уровня информационной безопасности своих объектов во избежание нарушения или остановки своих критических процессов. В связи с этим, мы обратились к специалистам «Лаборатории Касперского» с целью оказания содействия по повышению защищенности предприятия от киберугроз.»

Зыков Сергей, начальник центра кибербезопасности АО «Сетевая компания»

АО «Сетевая компания» входит в десятку самых крупных электросетевых компаний России. Компания занимает лидирующие позиции по показателю общей протяженности эксплуатируемых воздушных и кабельных линий, а также по количеству подстанций, трансформаторных подстанций и распределительных пунктов.

На данный момент в филиалах АО «Сетевая компания» находится в эксплуатации 381 подстанция 35–500 кВ установленной мощностью 18871,3 МВА, в работе на ПС 35–500 кВ находится 755 силовых трансформаторов (автотрансформаторов) 35–500 кВ. Общая протяженность воздушных линий 35–500 кВ по трассе составляет 10444,8 км, кабельных линий 35–220 кВ – 129,4 км. Филиалами АО «Сетевая компания» эксплуатируется 23670,3 км воздушных линий 6(10) кВ, 26973,1 км воздушных линий 0,38 кВ, 20063 ТП и РП 6(10) кВ, 5319,1 км кабельных линий 6(10) кВ и 4999 км кабельных линий 0,38 кВ.

Кроме того, АО «Сетевая компания» является единственной в России территориальной сетевой организацией, которой принадлежат объекты электросетевого хозяйства уровней напряжения от 0,4 кВ до 500 кВ.

В качестве своей миссии АО «Сетевая компания» выделяет обеспечение надежного, качественного и доступного электроснабжения. Компания создает подходящие условия для эффективной деятельности предприятий и организаций, комфортной и безопасной жизнедеятельности населения в целях динамичного социально-экономического развития Республики Татарстан.

Техническая политика АО «Сетевая компания» определяется необходимостью достижения надежности электроснабжения потребителей качественной электроэнергией, снижения издержек на эксплуатацию, удовлетворения спроса на услуги по передаче электрической энергии и присоединению потребителей. Компания внедряет современные технологии и оборудование для обеспечения максимальной эффективности и надежности действующих активов.

Задача

Являясь одной из крупнейших электросетевых компаний в российской электроэнергетике и управляя стратегически важным сектором Республики Татарстан, АО «Сетевая компания» придает большое значение вопросам безопасности объектов критической информационной инфраструктуры (далее ОКИИ).

В связи с этим, компания поставила перед собой задачу – в рамках выполнения проекта по реконструкции программно-технического комплекса автоматизированной системы диспетчерского управления Центра управления сетями и систем телемеханики филиалов АО «Сетевая компания» спроектировать и реализовать подсистемы безопасности (ПИБ), направленные на нейтрализацию угроз безопасности и обеспечивающие устойчивое функционирование системы при проведении компьютерных атак.



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 РСУ.



Контроль среды

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

Решение

В качестве основных критериев при выборе средств защиты информации, создаваемых ПИБ, были выделены следующие:

- качество и полнота реализации функций защиты;
- присутствие в реестре отечественного программного обеспечения;
- наличие сертификатов ФСТЭК и ФСБ РФ;
- успешное прохождение испытаний на совместимость с оборудованием и программным обеспечением, входящим в состав проектируемых систем;
- удобство и простота эксплуатации, интеграционные возможности со смежными компонентами подсистемы ИБ.

По результатам сравнительного анализа представленных на рынке средств защиты информации, а также проведения пилотного внедрения на одном из действующих объектов компании было принято решение о включении в состав создаваемых ПИБ продуктов семейства Kaspersky Industrial CyberSecurity (KICS):

- KICS for Nodes – для защиты инженерных рабочих станций, станций диспетчеров, серверов SCADA. Средство защиты обеспечивает контроль запуска приложений (whitelisting), контроль целостности файлов, контроль периферийных устройств, обнаружение и блокирование вредоносного ПО.
- KICS for Networks – 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.

«С помощью продуктов Лаборатории Касперского удалось решить задачи, которые мы ставили перед собой при реализации проекта. Полученный опыт позволит нам в будущем тиражировать данные решения и на других площадках компании.»

Курбангалиев Тимур, заместитель Генерального директора по информационным технологиям АО «Сетевая компания»

«Особенностью проекта являлась необходимость мониторинга трафика специфических протоколов с огромного количества технологических устройств, и в этом нам помог режим "обучения", реализованный в продукте, который значительно ускорил создание схемы информационных потоков системы», – Павлюкевич Дмитрий, заместитель начальника центра кибербезопасности АО «Сетевая компания»

Результаты

В результате реализации проекта более 150 серверов и рабочих станций технологического контура АО «Сетевая компания» защищены с применением KICS for Nodes, а мониторинг ключевых сегментов технологической сети обеспечивают 10 серверов KICS for Network.

Реализованный комплексный подход к защите критической инфраструктуры позволил значительно снизить риск нарушения критических процессов и обеспечить высокий уровень кибербезопасности на объектах АО «Сетевая компания».



**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.



Frost and Sullivan recognizes Kaspersky with the 2020 Global Company of the Year Award



Kaspersky is recognized as the 2020 Winner of VDC Research's Platinum Award for Industrial IoT Vendors in the Industrial Cybersecurity category.