Kaspersky OT CyberSecurity

Отраслевые решения
для операторов систем
энергоснабжения,
электростанций и ЖКХ

kaspersky

Краткий обзор

Отрасль Энергетики & ЖКХ имеет важное значение для общества. Она играет ключевую роль в стимулировании экономического роста, повышении качества жизни людей и развитии новых технологий. Электроэнергия – это важнейший ресурс, который обеспечивает работу целого ряда ключевых отраслей экономики:

Бытовое потребление и «умные» города
(уличное освещение, системы отопления, вентиляции и системы управления дорожным движением и т. п.)

Транспорт
(электромобили, зарядные станции)

Производственный сектор

Отрасль играет важную роль в достижении нулевого уровня выбросов в соответствии с целями Парижского соглашения (ООН). Она способствует электрификации других отраслей экономики и стимулирует переход на возобновляемые источники энергии.

Тенденция перехода к чистой энергии требует развития надежных и эффективных «умных» энергосетей.

~x2

объем мировых инвестиций в чистую энергию по сравнению с инвестициями в ископаемое топливо[1]

(1)Отчет Международного энергетического агентства «World Energy Investment 2024»

Цели цифровизации

Цифровизация способствует устойчивому развитию отрасли, а цифровые решения помогают ее участникам достигать стратегических целей:

- Повышение безопасности и эффективности использования активов
- Стимулирование глобальной декарбонизации и электрификации
- Ускоренное развертывание инфраструктуры возобновляемой энергетики
- Повышение надёжности и устойчивости энергосистемы

Основные сценарии использования цифровых решений в отрасли

- **Устройства интернета вещей в энергетике (IoE)**
  Обеспечение комплексной автоматизации для мониторинга и управления энергосетями в режиме реального времени
- **Энергетическое облако (Energy Cloud)**
  Аналитика в режиме реального времени, масштабируемая инфраструктура, удаленное управление и интеграция новых технологий
- **Цифровые двойники объектов энергетики**
  Симуляция различных режимов работы энергосети, прогнозирование, мониторинг в режиме реального времени и диагностика оборудования
- **Интеллектуальные энергосети на базе машинного обучения (ML) и ИИ**
  Оптимизация, предиктивное обслуживание и мониторинг состояния оборудования
- **Роботизация**
  Обследование электростанций с помощью роботизированных систем и дронов, контроль за растительностью

Цифровая трансформация отрасли неизбежно влечет за собой риски безопасности.

Энергосистемы будут испытывать всё большую потребность в безопасных системах автоматизации.

21,4%

Доля компьютеров АСУ энергетической отрасли в России, на которых были заблокированы вредоносные объекты во втором квартале 2025 года[2]

(2) Отчёт ICS CERT «Ландшафт угроз для систем промышленной автоматизации. Второй квартал 2025»

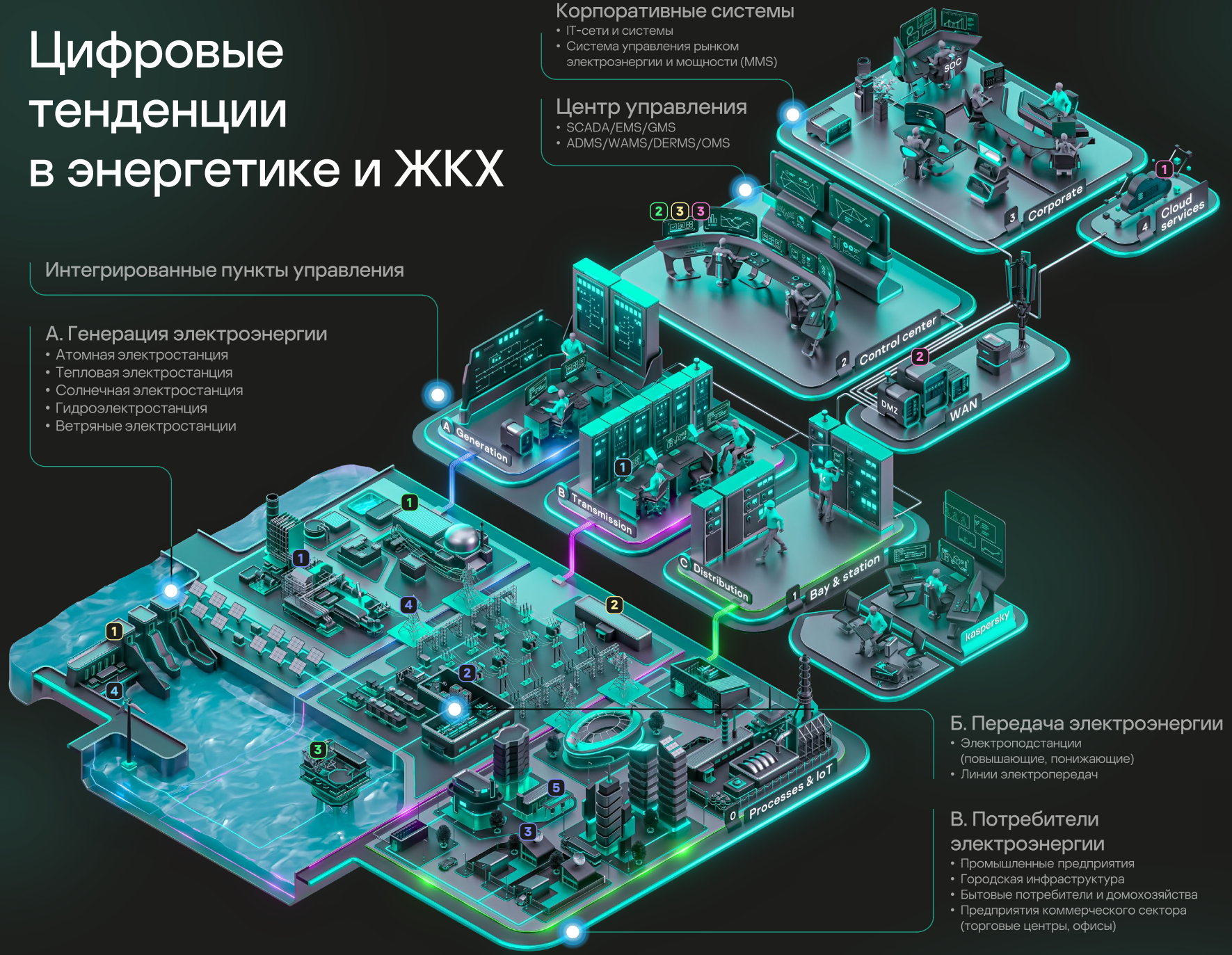
Цифровые тенденции в энергетике и ЖКХ

Корпоративные системы
- IT-сети и системы
- Система управления рынком электроэнергии и мощности (MMS)

Центр управления
- SCADA/EMS/GMS
- ADMS/WAMS/DERMS/OMS

Интегрированные пункты управления

А. Генерация электроэнергии
- Атомная электростанция
- Тепловая электростанция
- Солнечная электростанция
- Гидроэлектростанция
- Ветряные электростанции



Б. Передача электроэнергии
- Электроподстанции (повышающие, понижающие)
- Линии электропередач

В. Потребители электроэнергии
- Промышленные предприятия
- Городская инфраструктура
- Бытовые потребители и домохозяйства
- Предприятия коммерческого сектора (торговые центры, офисы)

IoE
1. «Умные» счетчики электроэнергии и тепла
2. Мониторинг состояния основного оборудования
3. Управление распределенными энергоресурсами (DER)
4. Мониторинг состояния линий передачи и распределения энергии (T&D)
5. Мониторинг зарядных станций и подключенных автомобилей

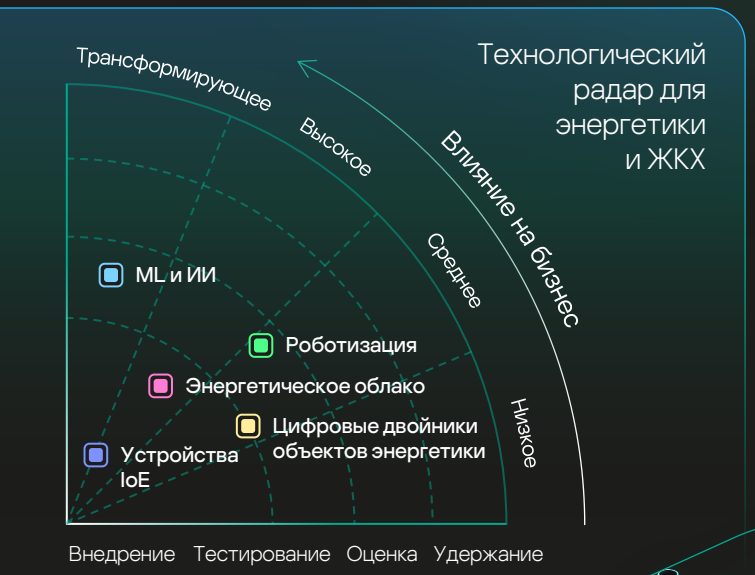
Энергетическое облако
1. Предиктивный анализ поставок с учетом погодных условий и других данных
2. Глобальные сети (WAN), обеспечивающие связь в режиме реального времени между OT-системами, датчиками и центрами управления энергосетями
3. Сетевые информационные системы (NIS), предоставляющие операторам распределительных сетей маршрутизацию и сетевую топологию

Цифровые двойники объектов энергетики
1. Управление производительностью активов, мониторинг оборудования и анализ первопричин
2. Картографирование рисков для выявления областей с высокой концентрацией рисков и предотвращения каскадных сбоев
3. Симуляция накопления энергии для оптимизации планов поставки и анализа пиковых нагрузок

ML и ИИ
1. Балансировка энергосети за счет динамической настройки потоков энергии, минимизации потерь и предотвращения перегрузки
2. Оптимизация реактивной мощности и контроль напряжения для предотвращения перебоев в питании
3. Анализ данных, поступающих с «умных» приборов учета, для повышения коммерческой прибыли и выравнивания пикового спроса
4. Прогнозирование погодных условий для регулировки положения лопастей ветряных электростанций

Роботизация
1. Оборудованные сенсорами дроны для аэрофотосъемки
2. Автоматизация инспекционных работ для выявления потенциальных проблем («горячие точки», утечки, повреждения ЛЭП и т. д.)
3. Подводная инспекция морских ветряных электростанций

Проблемы кибербезопасности в энергетике



Цифровая трансформация отрасли ведет к появлению ряда проблем кибербезопасности

1. Устаревшие цифровые устройства релейной защиты и автоматики.
2. Увеличение количества уязвимых узлов
3. Уязвимые сервисы удаленного доступа и синхронизации времени
4. Недостаточная сегментация IT- и OT-сетей
5. Требования к безопасности объектов критически важной инфраструктуры

Устаревшие цифровые устройства релейной защиты и автоматики

Энергетическое облако | ML и ИИ

Энергетическое облако

Данные клиентов и контроль доступа

SCADA для управления несколькими объектами

Цифровой двойник электростанции

Контроллер микросетей

Оптимизатор распределения

Пример генерации электроэнергии

Центральный человеко-машинный интерфейс (HMI)

Центральная сеть

Магистраль приложений

Сервер безопасности

Центральные серверы

Сервер приложений

Терминальный сервер

Маршрутизатор

WAN

Маршрутизатор

Внешний уровень

Магистраль приложений

Сервер приложений

Сервер безопасности

Прикладной уровень

Уровень автоматизации

Магистраль автоматизации

Управление турбиной

Управление подземным трубопроводом

Управление котельной установкой

Электрическая часть

Сторонняя система

Уровень автоматизации

Попытка интеграции устаревших систем с современными технологиями, такими как ML, AI и облачные решения, влечет за собой ряд серьезных проблем. Проблемы совместимости могут возникнуть, если устаревшие системы плохо взаимодействуют с новыми технологиями. Ограниченная совместимость может нарушить работу и снизить эффективность, которую обеспечивают современные решения. В частности, устаревшие системы не всегда эффективно коммуницируют с облачными платформами или инструментами автоматизации с поддержкой AI.

Устаревшее оборудование в настоящее время составляет

65%

генерирующего оборудования в России составляет оборудование, введённое в эксплуатацию в советские годы[1]

(1) Генеральная схема размещения объектов электроэнергетики до 2042 года

Характеристики предложения

Чем может помочь «Лаборатория Касперского»

Kaspersky Industrial CyberSecurity

- Непрерывный мониторинг промышленных сетей на наличие неразрешенных взаимодействий и кибератак
- Технологии обнаружения и реагирования на конечных точках
- Регулярный аудит безопасности

Kaspersky Machine Learning for Anomaly Detection

- Прогнозирует отказы технологических процессов, используя алгоритмы машинного обучения
- Выявляет киберугрозы для устаревших систем релейной защиты

Вспомогательные сервисы

Kaspersky ICS Threat Intelligence

- Комплексный анализ с целью оценки рисков и уровня безопасности сетевых промышленных инфраструктур

Увеличение количества уязвимых узлов

IoE

Электростанция

Центральный человеко-машинный интерфейс (HMI)

Подстанции компьютер

Шлюз

WAN

Центр управления

Пример цифровой подстанции

Станционная шина

ПО

ПО

Ячейка распредели-тельного устройства

Защита ИЭУ

Защита ИЭУ

Управление ИЭУ

Управление ИЭУ

Защита ИЭУ

Защита ИЭУ

Шина процесса

ПО

ПО

Процессы и IoT

Интеллектуаль-ное электронное устройство (ИЭУ)

Основной модуль

Датчик IoT

Выключатель

Трансформатор тока/напряжения

Интеллектуаль-ное электронное устройство (ИЭУ)

Основные часы

Датчик IoT

Выключатель

Антенна

Интеграция роботов и устройств IoT в работу подстанций создает больше точек входа для кибератак, поскольку любое незащищенное устройство является потенциальной мишенью.

Управление разнообразными подключенными устройствами и установка патчей – сложная задача. Любое нарушение безопасности может привести к цепной реакции во всех системах и широкомасштабному сбою.

Характеристики предложения

Чем может помочь «Лаборатория Касперского»

Kaspersky Industrial CyberSecurity

- Видимость внутри сети и выявление сетевых аномалий
- Глубокий анализ трафика (DPI) в промышленных коммуникациях с использованием алгоритмов машинного обучения
- Подробный аудит системы
- Анализ уязвимостей устройств в технологической сети

Kaspersky Machine Learning for Anomaly Detection

- Выявление аномального поведения оборудования и нарушений технологического процесса в следствие реализации киберугроз

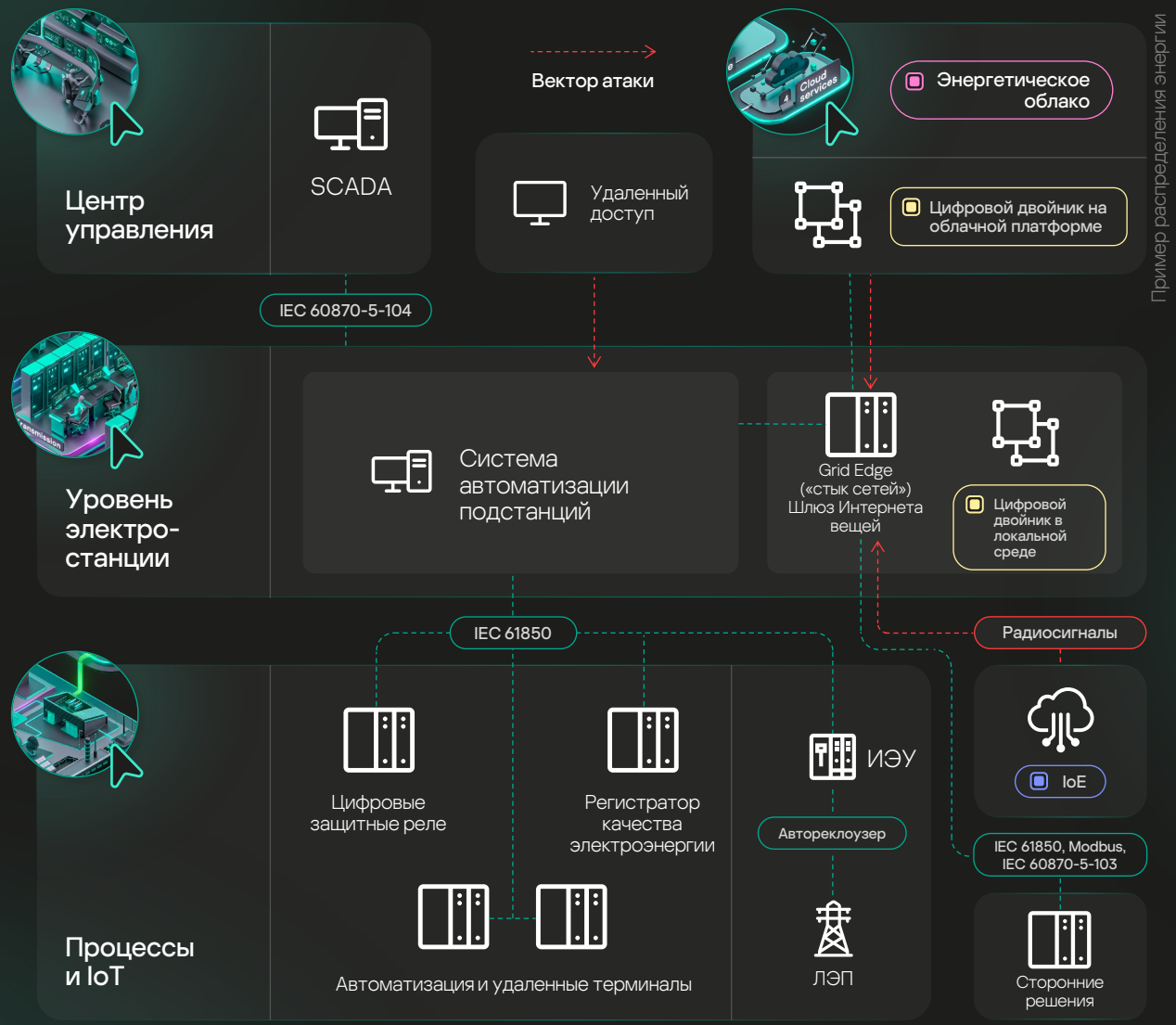
Вспомогательные сервисы

Managed Detection and Response

- Активный поиск угроз и расследование инцидентов
- Мониторинг безопасности

Уязвимость подключений и сервисов синхронизации времени

IoE · Энергетическое облако · Цифровые двойники объектов энергетики



Интеграция таких технологий, как IoE, цифровые двойники и облачные сервисы, в работу электроподстанций увеличивает риск кибератак из-за уязвимости подключений. В результате злоумышленники могут получить доступ к системам SCADA и сетям управления. Кроме того, крайне важно поддерживать высокоточную синхронизацию времени для защитных реле и устройств синхронизированных векторных изменений (УСВИ), поскольку любая ошибка может привести к сбоям в работе энергосети.

Характеристики предложения

Чем может помочь «Лаборатория Касперского»

Kaspersky Industrial CyberSecurity for Networks

- Обнаружение в сетевом трафике попыток эксплуатации уязвимостей

Kaspersky Thin Client

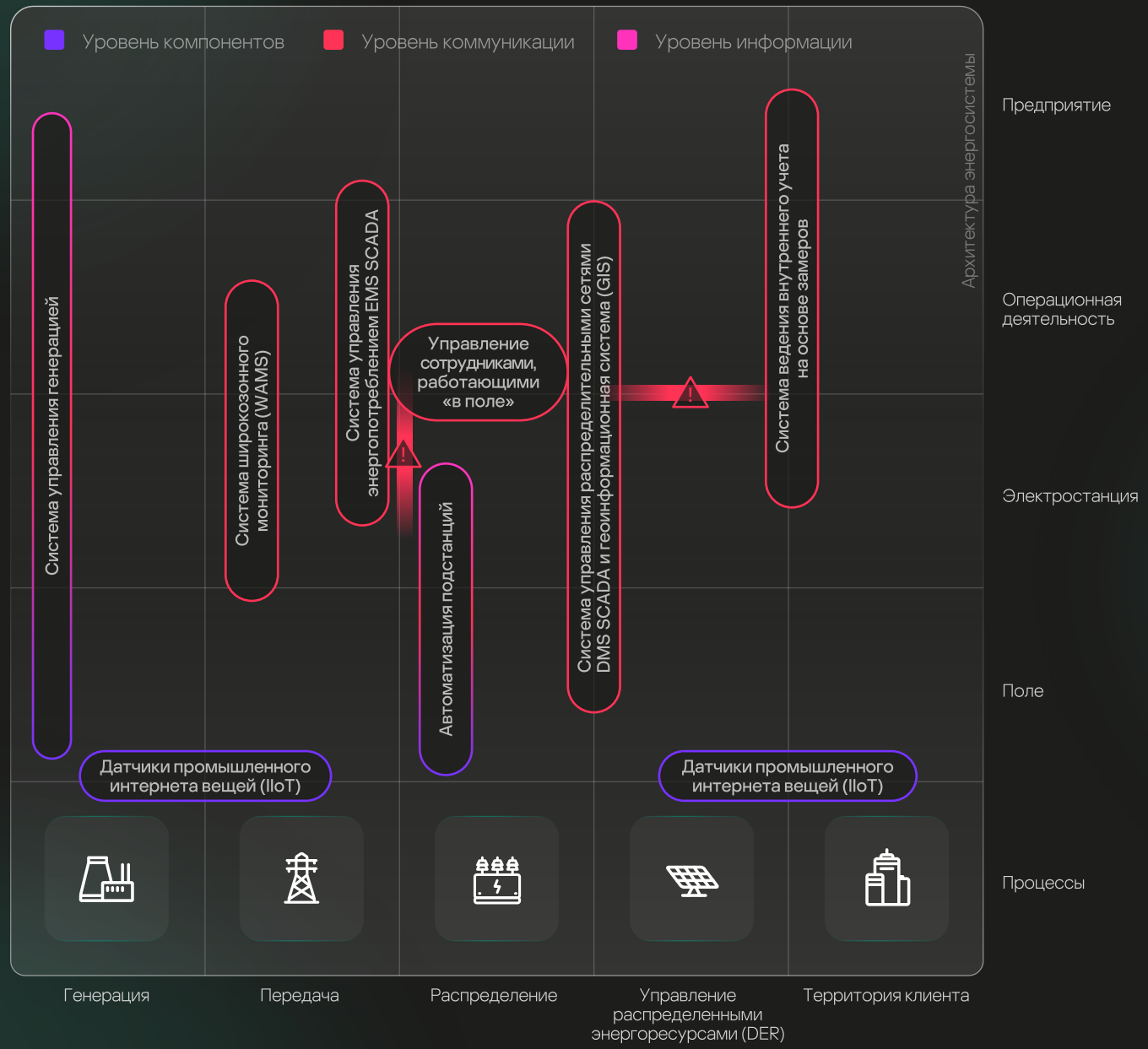
- Удаленное подключение и инженерная поддержка силами сотрудников и подрядных организаций
- Централизованный мониторинг и управление всеми событиями инфраструктуры тонких клиентов

Kaspersky Industrial CyberSecurity for Nodes

- Защита конечных узлов от эксплойтов

Недостаточная сегментация IT- и OT-сетей

IoE



Недостаточная сегментация сетей в энергосистемах, особенно при использовании цифровых двойников, может привести к появлению серьезных уязвимостей. При ненадлежащей сегментации сетей использование цифровых двойников, которые по определению являются взаимосвязанными, может увеличить риск распространения кибератак из IT-систем на критически важную OT-инфраструктуру. Это может нарушить процессы распределения энергии и привести к широкомасштабным отключениям электроэнергии.

Характеристики предложения

Чем может помочь «Лаборатория Касперского»

Kaspersky Industrial CyberSecurity

- Анализ сетевого трафика для выявления аномалий и угроз
- Защита рабочих мест, обнаружение и реагирование
- Сегментация сетей и соблюдение правил пользования

Kaspersky SD-WAN

- Мониторинг распределенной сети в режиме реального времени
- Видимость внутри сети
- Централизованное управление сетью и обеспечение ее безопасности

Kaspersky NGFW

- Контроль сетевых соединений
- Защита от сетевых угроз
- Контроль веб-трафика

Вспомогательные сервисы

Kaspersky ICS Security Assessment

- Выявление нарушений безопасности сетевой архитектуры
- Предоставление практических рекомендаций по ликвидации последствий
- Внутреннее тестирование на проникновение

Требования к безопасности объектов критически важной инфраструктуры

Чем может помочь «Лаборатория Касперского»

Решения «Лаборатории Касперского» служат для защиты электростанций, подстанций, энергосетей и других элементов энергосистемы, позволяя обеспечивать бесперебойную работу критически важных объектов промышленности и ЖКХ в соответствии с нашей политикой глубинной защиты.

Kaspersky Industrial CyberSecurity

Решения для энергосетей, соответствующие **стандартам** ISA/IEC 62443, ISO/IEC 27001

Kaspersky Security Awareness и экспертные тренинги

позволяют развить у сотрудников навыки кибербезопасности и повысить устойчивость бизнеса к инцидентам, связанным с человеческим фактором.

Узнайте все требования регуляторов к вашему бизнесу и получите рекомендации по их выполнению.

> 150

систем от более чем 50 поставщиков

Протестировано на совместимость:

Schneider Electric, SIEMENS, GE, Mitsubishi, CHINT, ProSoft Systems, EKRA, Valmet

Киберустойчивость с OT-платформой «Лаборатории Касперского»

Инвентаризация активов

Инвентаризация сетевых ресурсов

- Проведение инвентаризации всех программных и аппаратных ресурсов в составе OT-инфраструктуры
- Создание подробного перечня для планирования стратегии кибербезопасности

Инвентаризация рабочих мест

- Создание каталога аппаратных и программных компонентов рабочих мест
- Регулярное обновление каталога для выявления критически важных ресурсов и уязвимостей

Оценка рисков

Разработка политик

- Разработка комплекса политик и процедур
- Использование анализа рисков и последствий для установления уровней кибербезопасности и определения необходимых средств контроля

Базовая защита

Повышение надежности операционной системы

- Безопасная настройка систем и регулярная установка исправлений и обновлений
- Введение дополнительных мер контроля
- Защита от эксплойтов и проверка съемных устройств

Контроль приложений

- Ограничение использования неавторизованных приложений для поддержания целостности системы

Защита рабочих мест

- Внедрение решений для борьбы с вредоносным ПО для защиты устройств в АСУ ТП и OT-средах

Передовые средства обнаружения угроз

Видимость внутри сети

- Мониторинг сетевого трафика для выявления аномалий и понимания моделей атак

Обнаружение угроз и аномалий

- Использование машинного обучения и глубокого анализа трафика (DPI) для выявления сетевых вторжений и аномалий
- Использование технологии EDR для мониторинга телеметрии OT-хостов

Аудит безопасности и соответствие нормативным требованиям

Аудиты безопасности

- Регулярные сканирования на предмет уязвимостей и аудиты на соответствие нормативным требованиям

Контроль конфигураций

- Проведение подробных системных аудитов и контроль конфигураций

Обеспечение соответствия внешним требованиям

- Обеспечение соответствия нормативным требованиям и отраслевым стандартам

Сегментация сетей

Предотвращение вторжений

- Расширение возможностей обнаружения и предотвращения атак за счет интеграции с имеющимся сетевым оборудованием

Ограничение потока данных

- Использование SD-WAN и VLAN для оптимизации потока данных и сегментации сети
- Контроль безопасности даже на удаленных и небольших объектах

Контроль за IIoT

- Обеспечение прозрачных мер контроля безопасности с помощью современных безопасных по умолчанию шлюзов и протоколов для устройств IoT

Удаленный доступ

- Использование тонких клиентов и защищенных шлюзов для контроля удаленного доступа

Отлаженные процессы обеспечения безопасности

Аналитические данные об угрозах для промышленных SOC

- Использование получаемых в режиме реального времени данных об угрозах для защиты от вредоносных программ, фишинга и эксплойтов

Консультирование по вопросам SOC

- Привлечение экспертов для расширения возможностей SOC по борьбе с комплексными угрозами

Обнаружение угроз и реагирование на них в конвергентных IT/OT-средах

- Интеграция систем безопасности для IT- и OT-сред с целью унификации механизмов обнаружения угроз и реагирования на них

Защита силами экспертов

- Использование управляемых служб обнаружения и реагирования для непрерывного мониторинга и квалифицированной обработки инцидентов

Отказоустойчивость и готовность

Обучение специалистов

- Проведение специализированных тренингов по кибербезопасности для сотрудников для эффективного устранения неисправностей и их последствий

Тренинги для повышения осведомленности о киберугрозах

- Регулярные тренинги для повышения общей отказоустойчивости систем и готовности к кибератакам среди всех сотрудников

Анализ производительности активов

- Использование инструментов и методологий для анализа производительности активов, обеспечения надежности и выявления потенциальных отказов

Узнайте больше о комплексном подходе «Лаборатории Касперского» к обеспечению кибербезопасности на всех уровнях

Достижения «Лаборатории Касперского» в сфере энергетики и ЖКХ

10+
лет
активного опыта работы в отрасли

80+
проектов
реализовано в атомной, тепловой, гидроэнергетике и других отраслях, включая энергетику возобновляемых источников

40+
предприятий энергетики и ЖКХ
уже используют защитные решения «Лаборатории Касперского»

60,000+
лицензий
выдано клиентам из энергетической отрасли

Kaspersky OT CyberSecurity предоставляет комплексную защиту промышленной инфраструктуры энергетических компаний на всех уровнях

Почему предприятия энергетики и ЖКХ выбирают решения «Лаборатории Касперского»

Обеспечение совместимости и соответствия нормативным требованиям

- Решения проверены на совместимость с продуктами ведущих производителей промышленных систем автоматизации
- Надежные меры кибербезопасности полностью соответствуют многочисленным отраслевым стандартам и требованиям регуляторов

Создание масштабируемой архитектуры

- Повышение прозрачности в системе АСУ ТП с учетом специфических нужд предприятий энергетической отрасли
- Поддержка как современных, так и устаревших систем с защитой всех компонентов АСУ ТП

Интеграция в надежную платформу

- Решение от единого поставщика для комплексной защиты в рамках целостной платформы
- Интеграция корпоративной и OT-среды в единую защищенную инфраструктуру со сквозной системой безопасности

Успешно реализованные проекты в сфере энергетики и ЖКХ

Проекты «Лаборатории Касперского» только за последние десять лет:

Предоставление услуг кибербезопасности для **компании – производителя электроэнергии**, которая является 4-й по величине в мире, а ее гидроэнергетический комплекс входит в первую пятерку по установленной мощности

Реализация защитных решений для крупнейшего национального поставщика электроэнергии, обеспечивающего **17% всей электроэнергии в стране**

Реализация проекта по защите промышленной инфраструктуры для **компании, входящей в пятерку ведущих мировых производителей возобновляемой энергии**, в состав которой входит более 600 генерирующих объектов

СМОЛЕНСКАЯ АЭС РОСАТОМ

Крупнейшее предприятие в топливно-энергетическом балансе региона

Защитные решения «Лаборатории Касперского» обеспечили быстрое обнаружение и реагирование на потенциальные угрозы, а также улучшение процессов мониторинга и аналитики в области кибербезопасности и технологического процесса.

3 000 МВт установленная мощность

>3 000 чел. трудятся на станции

РОССЕТИ СЕВЕРО-ЗАПАД

Крупнейшая сетевая организация на Северо-Западе России

После интеграции Kaspersky Unified Monitoring and Analysis Platform в корпоративный сегмент «Россети Северо-Запад» осуществили трансформацию, избавившись от необходимости администрирования множества систем. Теперь все операции осуществляются через удобный веб-интерфейс KUMA.

1,4 млн км² территория обслуживания компании

19 670 МВА мощность силовых трансформаторов подстанций

ТАТЭНЕРГО

Региональная энергетическая компания России

Решения «Лаборатории Касперского» защищают автоматизированные системы управления технологическим процессом «Татэнерго», обеспечивая непрерывность технологических и бизнес-процессов.

Более 5 тыс. сотрудников

5 427 МВт установленная мощность

ИНТЕР РАО

Одна из крупнейших в России электроэнергетических компаний

Kaspersky Industrial CyberSecurity имеет более 80 сертификатов совместимости с решениями АСУ ТП.

31 000 МВт совокупная мощность электростанций

Более 48 тыс. сотрудников

www.kaspersky.ru

Управляйте своей безопасностью вместе с решениями «Лаборатории Касперского» и станьте ее партнером

Получите презентации спикеров Kaspersky Industrial Cybersecurity Conference 2025

Подробнее

#kaspersky
#активируйбудущее