Кибербезопасный обогрев стрелок: сотрудничество «Лаборатории Касперского» и «РЖД»

kaspersky KasperskyOS РЖД НИИАС

«СМАРТ. Обогрев стрелок» — важный шаг на пути к цифровой железной дороге будущего. Умная система помогает автоматизировать процессы железнодорожной инфраструктуры и значительно повысить их надежность и эффективность. Мы гордимся, что стали частью этого передового проекта с Kaspersky IoT Infrastructure Security — одним из первых решений на базе KasperskyOS для транспортной инфраструктуры, которое защищает системы от кибератак, обеспечивая их бесперебойную работу. Мы продолжаем развивать технологии для высокоавтоматизированных и беспилотных транспортных средств»

Григорий Сизов,
директор по развитию бизнеса KasperskyOS

«Российские железные дороги» решают задачу ресурсосбережения путевого хозяйства Центральной дирекции инфраструктуры (филиал ОАО «РЖД»). Чтобы снизить затраты на электроэнергию, АО «НИИАС», ведущим отраслевым институтом ОАО «РЖД», был разработан передовой проект «**СМАРТ. Обогрев стрелок**». Он позволяет оптимизировать работу электрообогрева стрелочных переводов путем автоматизации процессов и самостоятельной адаптации к параметрам среды.

Создание подобного проекта было бы невозможно без комплексной киберзащиты. Успешная атака на «СМАРТ. Обогрев стрелок» может не просто нарушить работу системы, но и поставить под угрозу информационную и физическую безопасность инфраструктуры. Защитить ее на всех уровнях помогли технологии «Лаборатории Касперского», в том числе специальное решение на основе KasperskyOS, Kaspersky IoT Infrastructure Security для безопасного и функционального интернета вещей.

Задача

На большей части сети ОАО «РЖД» управление электрообогревом стрелочных переводов осуществляется в ручном режиме.

У существующих систем обогрева стрелочных переводов есть недостатки:

- избыточное включение без учета реальных угроз обледенения или выпадения осадков;
- несвоевременное выключение.

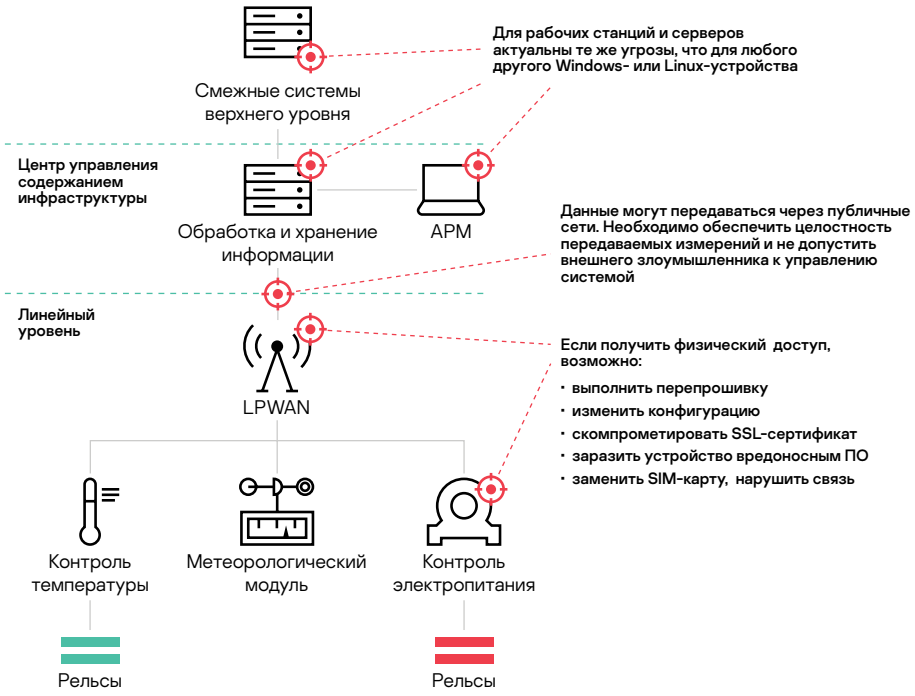
«СМАРТ. Обогрев стрелок» помогает устранить указанные проблемы благодаря адаптивному управлению, основанному на мониторинге температуры рельсов, метеоусловий, состояния устройств электропитания. Автоматическая онлайн-обработка этих параметров позволит оптимизировать работу обогрева, а решения «Лаборатории Касперского» комплексно защитят инфраструктуру и не позволят злоумышленникам эксплуатировать ее уязвимости.

«Современные железные дороги — сложный технологический комплекс, предъявляющий повышенные требования к информационной безопасности. Использование передовых технологий киберзащиты «Лаборатории Касперского» позволяет ускорить внедрение в холдинге ОАО «РЖД» инноваций, обеспечивающих новые уровни качества, скорости и безопасности железнодорожных перевозок»

Илья Николаев,
начальник Центра телекоммуникационных систем и промышленного интернета АО «НИИАС» — Ростовский филиал

Важность киберзащиты

Развитие автоматизации и цифровизации инфраструктуры «РЖД» значительно повышает риски кибератак на ее объекты. Каналы передачи данных, облачные платформы, устройства интернета вещей больше всего привлекают внимание злоумышленников.



Векторы угроз для систем обогрева рельсов

Внутренние угрозы

Несанкционированные подключения к системе «СМАРТ. Обогрев стрелок» могут привести к заражению автоматизированного рабочего места вредоносным ПО и, как следствие, к нарушению его работы. В частности, злоумышленники могут:

- воздействовать на ММК (метеорологический модуль контроля), МКЭ (модуль контроля электропитания), МКТР (модуль контроля температуры рельса), МС (модуль связи LPWAN), чтобы нарушить целостность передаваемых данных;
- вывести из строя систему «СМАРТ. Обогрев стрелок» или ее отдельные элементы.

Внешние угрозы

Цифровые инфраструктуры, подключенные к интернету, особенно подвержены атакам извне. Для системы «СМАРТ. Обогрев стрелок» наиболее актуальны следующие угрозы:

- компрометация и, как результат, вывод из строя системы или отдельных ее элементов;
- удаленное воздействие на ММК, МКЭ, МКТР, МС с целью нарушить целостность передаваемых данных;
- перехват и изменение информации, передаваемой через публичные сети.

Проблемы (угрозы), возникающие при администрировании и обеспечении работоспособности системы

- Сложность мониторинга IoT-инфраструктуры (отсутствие полной картины в режиме реального времени)
- Долгое время реагирования на инциденты ИБ (запоздалое обнаружение/ оповещение о проблеме)
- Сложность обеспечения работоспособности и управления (отсутствие единой системы управления, отчетности, реагирования на инциденты)

Последствия кибератак на систему «СМАРТ. Обогрев стрелок»

- Потеря возможности мониторинга IoT-инфраструктуры (получение некорректных данных от МКЭ, МКТР, ММК)
- Нарушение работы ММК, МКЭ, МКТР, МС:
  - невозможность управляющего воздействия;
  - получение некорректных данных от МКЭ, МКТР, ММК. Выработка некорректного управляющего воздействия;
  - выход из строя системы электрообогрева стрелочных переводов.

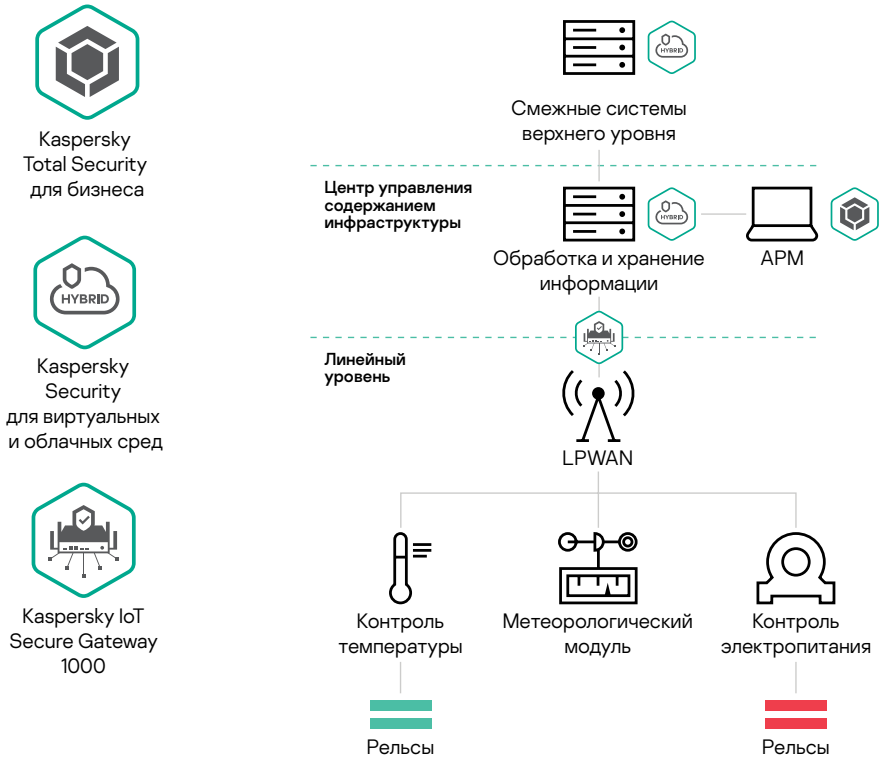
Существующие проблемы работы с инцидентами ИБ

- Нет возможности обнаружить опасное воздействие до появления очевидных негативных последствий (материального ущерба)
- Долгое время реагирования на инциденты ИБ
- Отсутствие единой системы управления и работы с инцидентами ИБ
- Отсутствие отчетности по инцидентам ИБ

Решение

Для кибербезопасности системы обогрева стрелок на всех уровнях архитектуры необходим комплексный подход:

Уровни	Функции	Продукты и решения «Лаборатории Касперского»
Уровень управления (модуль обработки и хранения информации)	Антивирусная защита	Kaspersky Security для виртуальных и облачных сред Kaspersky Total Security для бизнеса
Канал передачи данных	Защита данных, передаваемых в облако, путем шифрования трафика (TLS-MQTT) Защита от внешних угроз (Firewall/IPS)	Kaspersky IoT Secure Gateway 1000
	DDoS (недоступность канала)	Kaspersky DDoS Protection
Линейный уровень	Обнаружение неавторизованных устройств Запрет посторонних взаимодействий (Firewall) Защита шлюза от взлома: · Проверка прошивки шлюза при загрузке (Secure Boot) · Проверка обновлений (Secure Update) · Запрет неавторизованных взаимодействий на уровне кибериммунной операционной системы (KasperskyOS)	Kaspersky IoT Secure Gateway 1000



Комплексный подход «Лаборатории Касперского» к киберзащите «СМАРТ. Обогрев стрелок»

Средства защиты

Kaspersky IoT Secure Gateway (KISG) 1000 — программно-аппаратный комплекс на базе операционной системы KasperskyOS. Шлюз обладает кибериммунитетом – «врожденной» защитой от кибератак. Это значит, что он будет выполнять свои критичные функции даже в агрессивной среде. KISG 1000 защищает данные, формирует события безопасности в IoT-инфраструктуре, позволяет управлять подключенными устройствами по протоколу MQTT поверх TLS и помогает строить безопасные системы интернета вещей. Централизованное администрирование событиями шлюза ведется через платформу Kaspersky Security Center.

Kaspersky Security для виртуальных и облачных сред — решение для защиты виртуальных машин и систем (как локальных, так и размещенных в центрах обработки данных или в публичных облаках).

Kaspersky Total Security для бизнеса — решение для защиты конечных устройств (рабочих станций и серверов), а также других узлов корпоративной сети (почтовых серверов, интернет-шлюзов).

Результат

Разработки «Лаборатории Касперского» обеспечили кибербезопасность системы «СМАРТ. Обогрев стрелок» на всех уровнях, а также сделали ее прозрачной и управляемой.

Уровни	Векторы угроз	Продукты и решения «Лаборатории Касперского»
Облако	DDoS (недоступность системы)	Kaspersky DDoS Protection (сервис)
	Компрометация (взлом, получение доступа, изменение конфигураций, подмена/утечка данных)	Kaspersky Security для виртуальных и облачных сред
Канал передачи данных	Компрометация (Man-in-the-middle, получение доступа к данным, подмена данных)	Шифрование трафика (MQTT) обеспечивает безопасность подключения и передачи данных (Kaspersky IoT Secure Gateway 1000)
	DDoS (недоступность канала)	Kaspersky DDoS Protection
Шлюз	Компрометация шлюза — сетевая или локальная атака/физический доступ (взлом, получение доступа, изменение конфигураций ПО, подмена/утечка данных)	IDS/IPS, Secure Boot, Secure Update; невозможность выполнять неавторизованные действия и влиять на выполнение критических функций системы (Kaspersky IoT Secure Gateway 1000 и технологии KasperskyOS)
Внутренняя IoT-сеть (внутренний нарушитель)	Нарушение структурной целостности сети (несанкционированные новые подключения к сети)	Network Discovery — обнаружение нарушителя и оповещение о подключении неавторизованного устройства/пользователя (Kaspersky IoT Secure Gateway 1000)
Облачная платформа (внешний нарушитель)	Обнаружение и компрометация системы «СМАРТ. Обогрев стрелок»	Kaspersky Security для виртуальных и облачных сред

Процессы администрирования и обеспечения работоспособности системы	Сложность мониторинга IoT-инфраструктуры и долгое время реагирования на инциденты ИБ (нельзя обнаружить опасное воздействие до появления физического ущерба; отсутствие полной картины в режиме реального времени; запоздалое обнаружение/ оповещение о проблеме)	Множество возможностей оповещения: передача событий безопасности в Kaspersky Security Center, облачные платформы, SIEM-системы; push-уведомления на устройства
	Обеспечение работоспособности и управление системой безопасности (отсутствие единой системы управления, отчетности, реагирования на инциденты)	Единая система управления кибербезопасностью с централизованной системой отчетности, журналирования и уведомлений (Kaspersky Security Center)

«Лаборатория Касперского» - международная компания, работающая в сфере информационной безопасности и цифровой приватности с 1997 года. Глубокие экспертные знания и многолетний опыт лежат в основе защитных решений и сервисов нового поколения, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и рядовых пользователей.

Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты конечных устройств, а также ряд специализированных решений и сервисов для борьбы со сложными и постоянно эволюционирующими киберугрозами. Кроме того, компания развивает направление по созданию кибериммунных решений на базе собственной операционной системы KasperskyOS. Такие решения обладают встроенной защитой от подавляющего большинства угроз – как существующих, так и еще неизвестных.

Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 240 тысяч корпоративных клиентов во всем мире.

Открытое акционерное общество «Российские железные дороги» — это современный транспортно-логистический комплекс, имеющий стратегическое значение для России. Компания является важнейшим связующим звеном в единой экономической системе страны и обеспечивает бесперебойную хозяйственную деятельность промышленных предприятий, доступные пассажирские и грузовые перевозки для миллионов граждан.

Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи (АО «НИИАС») — дочернее предприятие ОАО «РЖД». Оно занимается разработкой и внедрением на железнодорожном транспорте передовых цифровых решений. Среди главных направлений деятельности Института — комплексные интеллектуальные системы управления, автоматизации и диагностики, беспилотный подвижной состав, роботизация технических средств, кибербезопасность.

KasperskyOS

Kaspersky
IoT Infrastructure
Security

Подробнее на os.kaspersky.ru

www.kaspersky.ru