МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
Минтранс России

Транспортный университет

ВИШ | ControlSphere

Ожидаемые сроки исполнения:

один

Заказчик

ООО «ЖелдорЦТИ»

2025

Контекст

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
Минтранс России

Транспортный университет

Транспортный комплекс. Интернет вещей

Проблема

Что за проблема: кто пытается достичь какую цель и что мешает?

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
Минтранс России

Транспортный университет

Кто?

Операторы телекоммуникационных сетей Специалисты по безопасности

Что хочет?

Операторы телекоммуникационных сетей: Они сталкиваются с проблемами, связанными с разрушениями, вандализмом и возгораниями на своих объектах. Эти инциденты могут привести к значительным финансовым потерям и ухудшению качества услуг. Специалисты по безопасности: Они несут ответственность за защиту объектов и инфраструктуры. Нехватка эффективных инструментов мониторинга и реагирования может привести к недостаточной защите и увеличению рисков.

Что мешает?

Совместимость систем: Интеграция новой системы с устаревшими существующими решениями может быть сложной и затратной. Технические неисправности: Проблемы с работой датчиков и сенсоров могут привести к ложным срабатываниям или пропуску реальных инцидентов Неинформированность о новых угрозах: Быстро меняющаяся природа угроз (например, новые виды вандализма или кибератак) требует постоянного обновления знаний и технологий

Какие есть способы решения и почему они не подходят?

Системы мониторинга на базе IoT: Системы умного города: Внедрение датчиков и устройств, которые собирают данные о состоянии объектов инфраструктуры, таких как освещение, транспорт и телекоммуникационные сети. Например, системы, использующие датчики для мониторинга состояния кабелей и оборудования на базовых станциях. Системы видеонаблюдения: CCTV-системы: Установка камер видеонаблюдения на ключевых объектах телекоммуникационной инфраструктуры, которые позволяют в реальном времени отслеживать ситуацию и фиксировать инциденты. Примеры включают системы от компаний, таких как Hikvision и Dahua. Системы контроля доступа: Биометрические системы: Использование биометрических технологий (например, отпечатков пальцев или распознавания лиц) для контроля доступа к критически важным объектам и оборудованию. Такие системы могут быть разработаны как местными, так и международными компаниями. Системы управления инцидентами: Системы SCADA: Используются для мониторинга и управления телекоммуникационными сетями и инфраструктурой. Они позволяют отслеживать состояние оборудования, выявлять неисправности и управлять процессами в реальном времени. Платформы для аналитики больших данных: Системы предиктивной аналитики: Используются для анализа данных о трафике, производительности сетей и потенциальных угрозах. Примеры таких платформ могут включать решения от компаний, таких как SAS или IBM. Системы обнаружения вторжений (IDS): Системы кибербезопасности: Применяются для защиты телекоммуникационных сетей от кибератак. Эти системы способны обнаруживать и реагировать на подозрительную активность в сетях, например, решения от компании Cisco или Check Point. Платформы для управления проектами и ресурсами: Системы ERP и CRM: Используются для управления проектами, ресурсами и взаимодействия с клиентами. Примеры включают SAP и 1С, которые могут быть адаптированы для нужд телекоммуникационных компаний. Государственные инициативы: Система "Безопасный город": Программа, направленная на создание комплексной системы безопасности в городах, включающая видеонаблюдение, системы оповещения и мониторинга.