Основные тенденции строительства и эксплуатации ЦОДов

Внедрение IoT и периферийных вычислений заставляет переосмыслить подходы к организации инженерной инфрастркутуры

Алексей Соловьев
Технический директор
IT Division Schneider Electric

Life Is On Schneider Electric

Основные векторы развития

Взгляд со стороны инженерной платформы

- Цифровизация и автоматизация процессов повышает производительность и эффективность производства
- Облачные технологии, периферийные вычисления и IoT меняют ИТ-архитектуру компании
- При внедрении ИТ-решений нужно опираться на надежную инфраструктуру
- Служба эксплуатации – основа надежности ЦОДа

3 основных типа ЦОДов,
каждый из которых является критически важным

1

Централизованный ЦОД
Коммерческий/корпоративный

2

Региональные серверные

3

Локальные узлы связи
(или микро-ЦОДы)

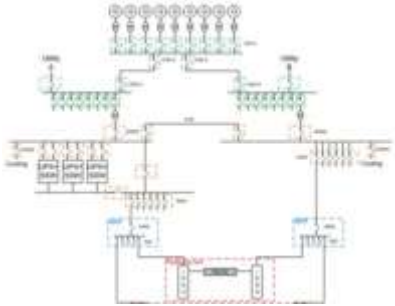
Лучшие существующие практики, применяемые в коммерческих и корпоративных центрах обработки данных...

Биометрические замки на дверях

Кабины-КПП

Охрана

Запираемые стойки организованные в ряды



Резервирование критически важных систем

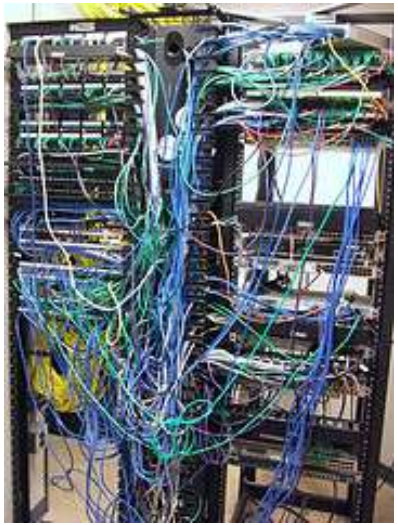
Постоянный контроль

...редко встречаются на периферии...

Нередко в удаленных филиалах и офисах отсутствуют выделенные помещения для серверных и коммутационных узлов или они выглядят так:

незащищённые стойки

отсутствие контроля доступа



отсутствие резервирования

кабельная организация низкого качества

отсутствие специализарованного охлаждения

Облачные вычисления сейчас уменьшают до нескольких стоек то, что раньше было локальным центром обработки данных мощностью сотни кВт

или
даже...

Устойчивость и работоспособность «того, что осталось» следует рассматривать так же, как и основной дата-центр

Life Is On Schneider Electric

Современные представления о доступности фокусируются на отдельных объектах

Если сосредоточиться на доступности только централизованного ЦОДа уровня Tier 3...

Централизованный ЦОД

Доступность = **99,98 %**

Простой = **1,6 часов/год**

А если принять во внимание точку зрения пользователя периферийного ЦОДа…

$$Доступность_{системы} = Доступность_1 \times Доступность_2$$

Доступность облачного ЦОДа Tier 3 = 99,98 %

Доступность периферийного ЦОДа Tier 1 = 99,67 %

Доступность = 99,98 % × 99,67 % = **99,65 %**

Простой = **30,7 часов/год**

Наше понимание «неисправности» нуждается в развитии

Текущая парадигма

Неисправность определяется как нарушение работы ИТ-оборудования в одном ЦОДе.

- Фокус на централизованных ЦОДах
- Сбой в случае воздействия на ИТ-оборудование в стойке
- Не охватывает филиалы/удаленные площадки или рабочих/бизнес-процессы

Новая парадигма

Неисправность понимается как прерывание работы пользователя, включая потерю связи в локальных микро-ЦОДах

- Фокус на гибридной среде и производительности системы
- Сбой в случае воздействия на пользователя
- Критическое влияние количества пользователей и их функций

Нам необходимо переосмыслить подход к надежности архитектуры локальных ЦОДов и сосредоточиться на безопасности, дублировании/резервировании и управлении

Рекомендации по улучшению периферийной инфраструктуры

- Физическая защита
- Мониторинг (DCIM), дистанционный контроль, управление и автоматизация
- Резервные системы питания и охлаждения
- Параллельное обслуживание
- Резервирование каналов связи
- Оптимизация работы систем охлаждения

Если нет выделенной серверной

Пример микро-ЦОДа
в корпусе SmartBunker CX

Резюме:

1. Надежность связи на периферии более важна при использовании облачных архитектур
2. Устойчивость и эксплуатацию оставшегося «периферийного» оборудования в гибридной архитектуре следует рассматривать так же, как и устойчивость традиционного корпоративного ЦОДа
3. Необходима более полная оценка доступности, ориентированная на измерение надежности подключения к облаку в этой распределенной среде

WP256: почему облачные вычисления требуют переосмысления отказоустойчивости на периферии

Life Is On | Schneider Electric