Life Is On Schneider Electric

Почему облачные вычисления требуют переосмысления отказоустойчивости на периферии

Информационная статья 256

Редакция 0

Кевин Браун и Венди Торелл

Аннотация

Отмечается быстрый рост использования компаниями облачных вычислений. Более сильная зависимость от областей применения, основанных на облачных вычислениях, означает, что компаниям нужно переосмыслить уровень резервирования оборудования, формирующего локальную физическую инфраструктуру (питание, охлаждение, передача данных) для периферийных вычислений. В данной статье мы рассмотрим современные практики организации инженерной инфраструктуры, предложим методы анализа необходимой отказоустойчивости, а также опишем лучшие варианты использования, обеспечивающие надежный доступ сотрудников к наиболее важным для бизнеса приложениям.

Введение

Развитие «Интернета вещей», растущий объем трафика передаваемых данных и областей применения «облачных» решений являются основными технологическими тенденциями, меняющими представление о ЦОДе.

Крупные и гигантские «облачные» ЦОДы сегодня размещают в себе множество важных для бизнеса приложений, в прошлом располагавшихся внутри компании. Однако не все приложения переносятся в «облако», и причины для этого разные, в том числе государственные отраслевые нормы регулирования, корпоративная политика, пропиетарные приложения, фактор задержки передачи данных и т.д.

В результате формируется то, что мы называем в данной статье «гибридной средой для ЦОДа». Другими словами, это среда, совмещающая (1) централизованные «облачные» ЦОДы, (2) средние и крупные региональные ЦОДы и (3) локальные малые ЦОДы. См. **рис. 1**. Локальный центр обработки данных мощностью 1 МВт, который раньше находился на территории филиала компании, сейчас может состоять из пары стоек ИТ-оборудования, на которых работают важные приложения и/или обеспечена связь с «облаком». Снижение количества возложенных функций и мощности локального ЦОДа вовсе не означает снижения важности. Чаще всего то, что компаниииоставляют внутри, является самым важным.

В данной статье описаны наиболее распространенные практики использования трех типов ЦОДов, перечисленных выше, описано, как изменились ожидания в направлении доступа к оборудованию, предложен метод оценки необходимого уровня отказоустойчивости для периферийных (локальных) ЦОДов для обеспечения достижения целей развития бизнеса, а также описаны лучшие практики применения микро-центров обработки данных на периферии.

Рис. 1
Три типа ЦОДа. В статье акцент ставится на периферийные ЦОДы

Типы ЦОДов

Централизованная «облачная» система была изначально создана для определенных типов приложений (например, почты, платежей, социальных сетей). Данные приложения не зависели так сильно от времени. Однако с переносом важных приложений в «облако» стало очевидным, что необходимо решать вопросы задержки передачи данных, ограничения пропускной способности, безопасности и прочих нормативных требований. Например, использование автомобилей с функцией автоматического управления. Для успешной реализации данного решения необходимы существенные объемы вычислений, поэтому вопрос задержки передачи данных критичен, иначе она может привести к авариям. Еще одним примером жизненно важного применения «облачных» технологий является здравоохранение: датчики, собирающие данные с пациентов, или хирургические инструменты, передающие хирургам данные о ходе операции в реальном времени. Очевидной стала необходимость переноса вычислений ближе к месту использования.

Распределение данных, требовательных к пропускной способности канала, является еще одной областью применения, где перенос данных ближе к месту использования имеет свои преимущества. Благодаря ему сокращаются расходы на поддержание пропускной способности, повышается качество потокового вещания.

У некоторых предприятий часто возникает потребность (или желание) поддерживать работу некоторых важных для бизнеса приложений на месте. Это позволяет лучше контролировать работу наряду с соблюдением государственных отраслевых норм регулирования и требований доступа к данным. Иногда данные приложения дублируются в «облаке» с резервными целями.

Далее в информационной статье Schneider Electric 226 Движущие факторы и преимущества периферийных вычислений объясняются особенности данных приложений, ведущие нас к созданию экосистемы, включающей в себя региональные и локальные ЦОДы. В данном разделе описан каждый из этих типов ЦОДов, описаны типичные для каждого из них практики работы с физической инфраструктурой.

Централизованный ЦОД

Крупные централизованные ЦОДы мощностью несколько мегаватт, являясь частью «облачной» системы или собственностью предприятия, часто рассматриваются как системы для решения критически важных задач, поэтому при их создании особое внимание обращается на доступ к данным. Существует ряд признанных практик, используемых уже много лет для обеспечения надежной защиты данных в дата-центре. Работа оборудования и сотрудников ИТ-компаний на данных площадках направлена на обеспечение непрерывной и эффективной работы всех систем 24 часа в сутки 7 дней в неделю. Кроме того, такие дата-центры часто спроектированы и иногда сертифицированы согласно стандартам Uptime Institute Tier 3 или Tier 4. Операторы коммерческих ЦОДов и «облачных» сервисов часто используют эти особенности дизайна, обеспечивающие высокую степень доступа, как выигрышные моменты при продаже услуг.

Распространенные лучшие практики включают в себя:

- **Резервирование критических систем:** наиболее важные системы питания и охлаждения спроектированы с учетом резервирования (часто 2N) для избежания простоев вследствие неисправности или технического обслуживания;
- **Высокий уровень физической безопасности:** распространенными стали биометрические датчики на дверях, кабины КПП, видеонаблюдение и круглосуточная охрана, которые обеспечивают безопасность систем и доступ только авторизованного персонала;
- **Организованные в ряды стойки:** помимо структурированного расположения стоек, упорядочено положение сетевых проводов и проводов питания для уменьшения возможности человеческой ошибки, например, вытаскивания не того провода, подключения обоих источников питания к одной линии питания и т. п. Организовано распределение воздуха, установлены панели-заглушки в неиспользованные юниты и щеточные уплотнители в технологические отверстия и т.д. для исключения возникновения точек перегрева;
- **Мониторинг:** установлены датчики и измерительные приборы для того, чтобы система управления инфраструктурой ЦОДа (DCIM) и система управления зданием (BMS) могли осуществлять контроль, управление и оптимизацию всех систем ЦОДа.

На **рис. 2** показаны методы обеспечения безопасности, наиболее распространенные в данных центрах обработки данных.

Рис. 2
Наиболее распространенные методы обеспечения безопасности в централизованных «облачных» и коммерческих ЦОДах


Биометрические датчики


Кабины КПП


Охрана

Региональный ЦОД

Региональные ЦОДы располагаются ближе к конечным точкам (то есть там, где данные генерируются и используются), они меньше по размеру, чем крупные централизованные дата-центры. Как описывалось выше, данные ЦОДы направлены на перенос приложений, чувствительных к задержке передачи данных или показателям пропускной способности, ближе к месту использования. Их расположение стратегически направлено на обработку больших объемов данных. Такие площадки можно сравнить с «мостиком» между центральными и локальными ЦОДами на местах.

Как и крупные централизованные ЦОДы, региональные обычно спроектированы с учетом обеспечения безопасности и доступа к данным. Дизайн подобных объектов часто соответствует стандартам Uptime Institute Tier 3. Иногда при их создании могут быть использованы решения высокой заводской готовности, и в качестве отправной точки могут использоваться базовые варианты дизайна (см. пример на **рис. 3**).

Рис. 3
Пример базового варианта дизайна в качестве начальной точки строительства централизованного или регионального ЦОДа

Локальный ЦОД

Локальный ЦОД – это центр сбора и обработки данных, расположенный в том же месте что и его пользователи. Существует большое количество терминов, используемых для описания данного типа ЦОДа (например, **центр обработки данных, расположенный внутри компании**, или **микро-ЦОД**). Локальные дата-центры могут варьироваться по мощности от 1–2 МВт до небольших 10–20 кВт. Учитывая тенденцию все увеличивающегося числа бизнес-приложений, перенесенных в «облако» или на площадки коммерческих ЦОДов, размер локального дата-центра становится все меньше, и иногда он может состоять из пары стоек, расположенных в небольшой комнате или корпусе.

Во многих из таких современных уменьшенных ЦОДах особенности дизайна часто соответствуют стандарту Uptime Institute Tier 1, при котором мало учитывается резервирование и доступ к данным. Частыми недостатками таких малых локальных ЦОДов являются:

- **Низкий уровень безопасности:** помещения часто не имеют защиты, стойки открыты (не имеют дверей);
- **Не упорядоченны стойки:** об организации проводов задумываются в последнюю очередь, что приводит к их запутыванию, проблемам с вентиляцией внутри стоек, увеличению числа человеческих ошибок во время добавления/ передвижения/ изменения компонентов. См. **рис. 4**;
- **Отсутствие резервирования:** системы питания (ИБП, система распределения питания) часто имеют конфигурацию N, что уменьшает их доступность и способность поддерживать работоспособность центра во время технического обслуживания;
- **Отсутствие специальной системы охлаждения:** в малых помещениях и шкафах часто используется общая система пассивной вентиляции, в результате чего возможен перегрев оборудования;
- **Отсутствие DCIM:** помещения часто остаются без присмотра, не закрепляются за обслуживающим персоналом или не контролируются программным обеспечением, которое бы управляло оборудованием и обеспечивало бесперебойную работу ЦОДа.

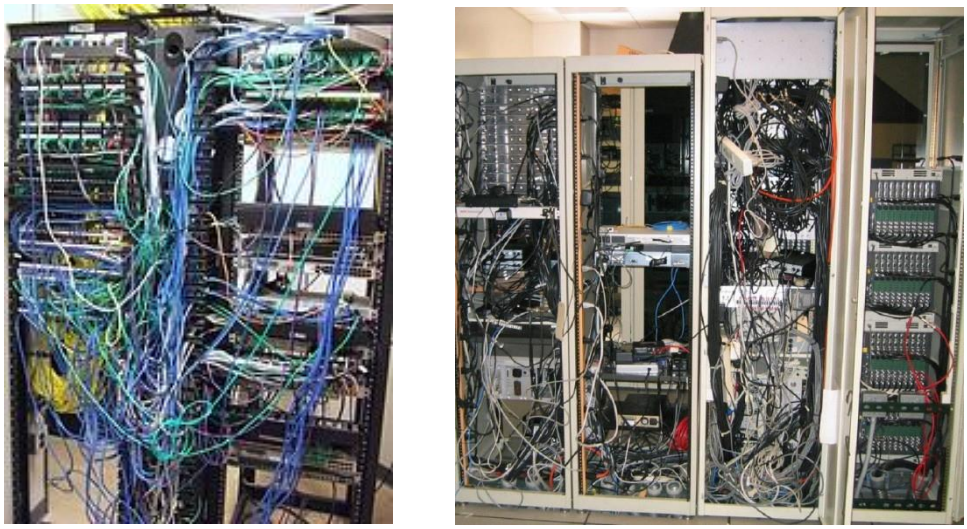

Рис. 4
Примеры малых локальных ЦОДов с плохой системой организации проводов и низким уровнем безопасности

Часто такое происходит из-за того, что предприятия, переходя в «облако» или на внешнее размещение, уделяют недостаточного внимания оставшимся стойкам. Вместо этого большее значение придается доступу к крупным ЦОДам. В такой логике есть недостатки, так как часто оставшиеся стойки по уровню важности выполняемых задач одинаковы или даже более важны, чем «облачные» ресурсы.

Рассмотрим, что обычно остается внутри компании: (1) пропиетарные, важные для компании приложения и (2) сетевое оборудование для подключения к «облаку». Каковы последствия для продуктивности бизнеса при возникновении проблем с доступом к приложениям? Если предположить, что в компании остается работать то же количество сотрудников, что и раньше, при этом количество стоек сократилось до пары штук, логично, что **возрастает важность работы с ресурсами на каждую стойку**. Локально расположенное оборудование имеет особую важность для обеспечения связи с повседневными бизнес-приложениями. С учетом того, что все больше и больше ресурсов переходит в «облако», невозможность подключения к таким ресурсам снижает продуктивность сотрудников.

Все это свидетельствует о необходимости изменения принципов проектирования подобных малых локальных ЦОДов. Нельзя концентрироваться только на централизованных и региональных дата-центрах, необходимо также уделять внимание и локальным площадкам, поскольку именно они на сегодняшний день являются более слабым компонентом сети. Далее будут описаны лучшие практики, которые необходимо использовать на данных площадках для обеспечения высокопродуктивного и имеющего развитую сетевую структуру бизнеса.

Более развитые показатели доступа к данным

При анализе данной гибридной среды, в которой все компоненты взаимосвязаны, возникает важный вопрос: должны ли мы пересмотреть наш взгляд на критичность и резервирование? Инструменты, которые мы используем в современной отрасли проектировки дата-центров, направлены на то, как сделать отдельный ЦОД максимально надежным. Мы учитываем стандарты Uptime Institute при проектировании конкретных площадок таким образом, чтобы достичь необходимого уровня доступности (9s). Неисправность обычно определяется как нарушение работы ИТ-оборудования в конкретном ЦОДе.

Инструменты и показатели не учитывают зависимость от количества ЦОДов, количества пользователей, на которых повлияла данная неисправность, критичность функций, на которые повлияла данная неисправность, или отказоустойчивость приложения (ПО). Мы считаем, что все это важно для движения вперед.

Изменение ожидаемого уровня доступа

Ожидания современных рабочих и рабочих старшего поколения различаются. По мере роста возраста рабочего, все больший перевес идет в сторону миллениалов, а вместе с ними меняются и ожидания. Поколение миллениалов росло с мыслью о том, чтобы быть «всегда на связи, всегда онлайн», то есть они ожидали, что все приборы и устройства никогда не выключаются. Устойчивость к нарушениям работы сервисов существенно ниже. Технологии представляют большую важность для них в повседневной жизни, включая работу.

Фактически 82 % миллениалов считают, что уровень применяемых технологий на рабочем месте влияет на их решение о выборе нового места работы[1].

Если предположить, что данная тенденция будет только расти, чрезвычайно важно найти более универсальные пути мониторинга отказоустойчивости ЦОДа, благодаря которым мы сможем получить необходимые представления и сделать правильные изменения при их проектировании. Как учит старая поговорка: «Не оценив ситуацию, нельзя ею управлять». Необходимо развитие факторов отказоустойчивости, чтобы соответствовать требованиям современного бизнеса.

Альтернативная точка зрения

Альтернативная точка зрения на доступ к данным может привести к иной стратегии развития. В **таблице 1** показано сравнение текущей (старой) и новой парадигмы, которое, как нам кажется, важно для принятия нужных решений.

Таблица 1
Изменение парадигмы, приводящее к нарушениям работы ЦОДа

Старая парадигма	Новая парадигма
Фокус на централизованных ЦОДах	Фокус на гибридной среде
Сбой в случае воздействия на ИТ-оборудование на стойке	Сбой в случае воздействия на пользователя
Не охватывает удаленные площадки или рабочих/функции	Критическое влияние количества рабочих и функций

Приведем в качестве примера коммунальные предприятия (энергоснабжение) и то, как они смотрят на доступность сервисов. Они не только следят за своими станциями и высоковольтными линиями (метафорически их «центральным ЦОДом»). Они подрезают ветки деревьев, ремонтируют трансформаторные подстанции и, наконец, измеряют успешность в зависимости от качества поставляемого электричества пользователям (то есть их «периферийные ЦОДы»). Отрасли проектирования дата-центров необходимо двигаться к описанной модели, в которой периферийная часть так же важна (если не важнее), как и центральная часть.

Уровень доступа двух систем с учетом того, что ваш бизнес зависит от доступа к обеим системам, вычисляется по формуле:

$$Доступность_{системы} = Доступность_1 * Доступность_2$$

Начнем с того, что представим пользователя, который зависит от доступности и продуктивности локального и центрального ЦОДов. Для расчета доступа ЦОДа в этом аспекте используется данная формула. Если, например, доступ к центральной площадке – 99,98 % (ЦОД 3 уровня, 1,6 часа простоя), доступ к локальной плоащдке – 99,67% (ЦОД уровня 1, 28,8 часа простоя), общее время простоя с точки зрения пользователя составит 99,98 %*99,67 % или 99,65 % (30,7 часа простоя).

Если взглянуть на это с точки зрения директора по информационным технологиям, как можно оценить воздействие на всю экосистему ЦОДа на продуктивность бизнеса и наличие связей внутри системы? Не каждый ЦОД зависит от работы остальных площадок, обеспечивающих работу персонала.

[1] http://www.dell.com/learn/us/en/uscorp1/press-releases/2016-07-18-future-workforce-study-provides-key-insights (дата последнего доступа: 31.10.2016)

Например, офис дочернего отделения компании в Лондоне не зависит от такого же офиса в Калифорнии, но они оба могут зависеть от центрального ЦОДа в Нью-Йорке.

Не все дата-центры имеют одинаковое воздействие на бизнес. Фактором является количество затронутых рабочих. Например, локальный ЦОД на 1000 человек может рассматриваться как более важный, чем ЦОД на 10 человек. В **таблице 2** показан простой в человеко-часах в модели экосистемы, включающей один центральный ЦОД Tier 3 и 10 локальных ЦОД Tier 1, каждый из которых обслуживает 100 рабочих. Из данной таблицы ясно, что общий объем простоя зависит от количества дата-центров Tier 1. Чем больше количество периферийных площадок Tier 1, тем меньше количество часов без отказа на площадках.

Таблица 2

Доступ 10 периферийных ЦОДов и 1 центрального, включая затронутых рабочих

Доступ к ЦОДу						
Описание	**Доступ**	**Простой (часов)**	**Кол-во площадок**	**Кол-во рабочих на площадку**	**Общее кол-во рабочих затронутых**	**Человеко-часы простоя в год**
Tier 1, периферийные ЦОДы	99,67 %	28,82	10	100	1000	28820
Tier 3, центральный ЦОД	99,98 %	1,58	1	0	1000	1580
				Общее кол-во человеко-часов времени простоя в год		30400
					Доступ	99,65 %

В таблице представлен простой сценарий с 2 уровнями дата-центров, в которых 1000 человек были затронуты обеими уровнями. С увеличением количества ЦОДов, причем каждый их них имеет разный уровень доступности и количество затронутых рабочих мест, посчитать эффективность становится намного сложнее. Кроме того, данная формула не является полной, так как из нее исключен рейтинг выполняемой бизнес-функции каждой площадки. Площадка, выполняющая функцию службы поддержки клиентов или производства, скорее всего будет более важной, чем площадка, состоящая из административного персонала, который может работать дистанционно в случае «отказа» сети.

Анализ критичности

Качественный анализ критичности является признанным методом оценки рисков и выбора корректирующих действий (также имеет название «анализ характера, последствий и критичности отказов» (FMECA)). Данный метод часто упоминается в опубликованных материалах по технике обеспечения надежности. Данный анализ включает коэффициент интенсивности последствий отказов и категории приоритета уровня риска (RPN). RPN основывается на 3 факторах: (1) интенсивность отказа, (2) вероятность возникновения и (3) обнаружение отказа[2].

Мы считаем, что лучшим подходом к общей оценке всех площадок является использование карт показателей, как показано в примере в **таблице 3**. Это поможет директорам по информационным технологиям и руководителям ЦОДа выявить наиболее важные площадки, которые нужно усовершенствовать. Карта показателей включает информацию по доступности и сопутствующему времени простоя каждой площадки в гибридной среде ЦОДа (идеальные показатели) и, что важнее всего, уровень важности каждой площадки. Для получения подробной информации о научных методах оценки критичности см. **сноску**[2]. В случае с ЦОДом интенсивность последствий отказа каждой площадки зависит от:

- количества затронутых рабочих мест;
- выполняемой функции.

Часто для оценки используется шкала от 1 до 5, где 1 – это наименьшее воздействие на бизнес в случае сбоя в работе площадки, а 5 – это наибольшее воздействие. Несмотря на качественный характер данной системы оценки, она обеспечивает систематический подход при анализе всех площадок в экосистеме бизнес-ЦОДа. Обратите внимание на то, что различные типы бизнеса будут по-разному рассматривать приведенные здесь значения. Самым важным является последовательный метод оценки всех площадок.

[2] http://www.weibull.com/hotwire/issue46/relbasics46.htm (дата последнего доступа: 31.10.2016)

В данном примере показаны 5 дата-центров, образующих воображаемую экосистему. Ежегодное время простоя каждого из них умножается на установленную величину «интенсивности последствий отказа» для получения взвешенного значения.

Исходя из этого можно просто отсортировать площадки по этому значению, где самое большое значение означает наибольшую приоритетность для улучшений. Также можно посчитать процент от значения для каждой площадки (как показано в примере – «воздействие сайта на значение»), площадки с высоким процентом имеют самый высокий уровень приоритетности.

Таблица 3

Пример карты показателей для оценки приоритетности ЦОДов с точки зрения улучшений

Карта показателей ЦОДа					
Название площадки	**Доступность**	**Ежегодное время простоя (часов)**	**Интенсивность последствий отказов (1–5)***	**Значение (взвешенное с учетом важности)**	**Воздействие площадки на RPN**
1	99,98 %	1,752	2	3,5	0,4 %
2	99,20 %	70,08	4	280,3	30,0 %
3	99,60 %	35,04	1	35,0	3,7 %
4	98,60 %	122,64	5	613,2	**65,5 %**
5	99,98 %	1,752	2	3,5	0,4 %
			Общее значение важности:	*935,6*	

Данный процесс основан на методе последовательной шаговой мультипликации. Как только уровень доступа к площадке 4 в примере будет улучшен, новая площадка поднимется в начало списка как самая важная. В течение данного непрерывного цикла улучшений будет улучшено качество наиболее сильно затронутых площадок.

Используя подходящий метод отчетности, можно будет явно выделить моменты, требующие улучшения, чтобы обеспечить наибольшую продуктивность и экономический эффект. **В большинстве случаев после выполнения данного метода становится ясно, что периферийные ЦОД, часто имеющие более низкий уровень доступности, оказывают наибольшее влияние на бизнес.**

Лучшие практики на периферии

При использовании правильных метрик и методов становится ясно, что необходимо переосмысление структуры периферийных систем ЦОДа. Стандартные практики работы со структурой периферийных центров (как было описано ранее) не соответствуют особенностям данных площадок с точки зрения важности для успешности бизнеса. Улучшения необходимы в следующих областях:

- физическая безопасность;
- управление (УИЦОД), рабочие практики, дистанционный контроль;
- резервные системы питания и охлаждения;
- резервирование каналов связи.

В следующих разделах будут описаны базовые лучшие практики развертывания периферийных вычислительных систем. В информационной статье 174 от Schneider Electric *Практические советы по развертыванию малых серверных и микро-центров обработки данных* подробно рассматриваются методы реального улучшения систем питания, охлаждения, стоек, физической безопасности и управления в малых серверных и офисах дочерних предприятий компаний с ИТ-нагрузкой до 10 кВт.

Безопасная рабочая среда

Малые локальные ЦОДы часто разворачиваются в помещении с открытым доступом (например, в офисе, где находится несколько отделов). Часто для стоек нет выделенного места, поэтому они остаются открытыми и незащищенными. Это порождает риски для нарушения безопасности вследствие осознанных или неосознанных действий.

Лучшими практиками для снижения данных рисков являются:

- перенос оборудования в закрывающееся помещение или корпус (-а);
- обеспечение биометрического или прочих видов контроля доступа;
- в случае неблагоприятных условий размещения – защита оборудования в корпусе, защищающем от пожаров, наводнений, влажности, вандализма или воздействий электромагнитного излучения;
- разворачивание системы круглосуточной защиты и контроля окружающей среды, а также системы видеонаблюдения.

Примеры защищенных корпусов показаны на **рис. 5**. Данные варианты часто поставляются в собранном виде, включая все необходимые компоненты инженерной инфраструктуры.

Рис. 5
Примеры микро-центров обработки данных от Schneider Electric

Управление ЦОДом

Процедуры управления и эксплуатации часто отличаются на разных периферийных площадках (если такие процедуры определены). Управление сотнями или тысячами периферийных площадок может быть затратным с точки зрения финансов и времени, так же уровень доступности на многих площадках зависит от смежного использования инфраструктуры на объекте (например, генераторы, коммутационные устройства, система охлаждения).

Лучшими практиками для снижения данных рисков являются:

- анализ текущих методов и систем управления;
- объединение всей инфраструктуры на площадках в единой системе мониторинга;
- развертывание системы дистанционного контроля при ограниченных ресурсах. См. информационную статью 237 Цифровой дистанционный контроль и его влияние на изменения в принципах эксплуатации и обслуживания ЦОДа, чтобы узнать больше о том, как дистанционный контроль может помочь сократить время простоя.

Питание и охлаждение

Инфраструктура систем питания и охлаждения (например, ИБП и кондиционеры) обычно разворачиваются на периферийных площадках, где отсутствует резервирование. Это приводит к единичным отказам, а также к невозможности обслуживания систем без остановки работы ЦОДа. В некоторых случаях в помещениях отсутствует специальная система охлаждения, что приводит к перегреву оборудования. Часть инженерных систем часто используются несколькими компаниями внутри одного здания, поэтому уровень доступа к ЦОДу зависит от уровня доступа к этим совместно используемым ресурсам.

Лучшими практиками для снижения данных рисков являются:

- измерение температуры и влажности для понимания необходимого уровня охлаждения (то есть пассивное охлаждение, активное охлаждени, или специальная система охлаждения);
- Задуматься о необходимости резервных линий питания для обеспечения возможности параллельного обслуживания на наиболее важных площадках;
- обеспечение работы наиболее важных цепей от резервного генератора.

На **рис. 6** показан пример микро-ЦОДа Tier 3, поставляемый в корпусе 42U с предварительно установленными и интегрированными резервными ИБП и системой распределения питания.

Рис. 6
Пример одностоечного микро-центра обработки данных со встроенной функцией резервирования

Связность сети

Как было описано ранее, подключение к «облаку» является важным фактором работы периферийных площадок. Однако часто бывает, что связь с Интернетом реализуется только одним провайдером. Это обстоятельство создает единую точку отказа. Беспорядок в кабельном хозяйстве также может стоть причиной человеческих ошибок.

Лучшими практиками для снижения данных рисков являются:

- подключение резервного канала передачи данных;
- разводка сетевых проводов при помощи средств кабельной организации (каналы для прокладки проводов, кабельные организаторы, фиксаторы и т. д.);
- маркировка и цветовая дифференциация проводов для избежания человеческих ошибок.

Заключение

Развитие «облачных» технологий приводит все больше и больше компаний к мысли о создании гибридных сред для «облачных» и локальных ЦОДов (на периферии). Несмотря на то, что количество «оставшегося» оборудования уменьшается, важность его даже увеличивается. Причины:

- с учетом того, что все больше приложений переходит в «облако», подключенность к «облаку» становится более важным фактором для работы бизнеса;
- формируется культура рабочих, которые привязаны к «онлайн» технологиям и не допускают простоя сервисов.

К сожалению, сегодня дизайн большинства периферийных ЦОДов имеет изъяны, что приводит к дорогостоящим простоям. Необходим систематический подход к оценке уровня доступности ЦОДа в гибридной среде для того, чтобы обеспечить наибольшую экономическую эффективность инвестиций там, где это нужно.

Представленная в статье концепция использования карт показателей позволяет руководителям и менеджерам целостное представление рабочей среды с учетом числа людей и бизнес-функций каждого ЦОДа. Данный метод помогает выявить наиболее важные площадки, требующие инвестиций.

Микро-ЦОД высокой заводской готовности представляют собой наиболее простой способ обеспечения безопасной, наиболее доступной инженерной среды на периферии. Лучшие практики, такие как использование резервных ИБП и защищенных стоек, системы организации кабелей и воздушных потоков, удаленный мониторинг и резервные канала передачи данных, обеспечивают необходимый уровень доступности на наиболее важных площадках.

Об авторах

Кевин Браун – технический директор подразделения IT Division компании Schneider Electric. Кевин имеет степень бакалавра технических наук в Корнелльском университете. Ранее Кевин занимал должность директора по рыночному управлению в компании Airxchange (производитель систем и компонентов кондиционирования с регенерацией электроэнергии в отрасли производства систем вентиляции, кондиционирования и обогрева). До объединения с Airxchange Кевин занимал многочисленные руководящие должности в Schneider Electric, в том числе должности директора группы по развитию ПО и старшего вице-президента по решениям для ЦОДов.

Венди Торелл – старший аналитик-исследователь в научном центре ЦОД Schneider Electric. В ее обязанности входит исследование лучших практик по разработке и эксплуатации дата-центров, публикация информационных документов и статей, разработка инструментов TradeOff Tools для помощи клиентам в оптимизации уровня доступа, эффективности и расходов в их ЦОДе. Она также занимается консультированием клиентов по научным концепциям доступности и практикам проектирования, чтобы помочь им добиться требуемых рабочих характеристик ЦОДа. Является выпускницей Юнион колледжа (г. Скенектади, Нью-Йорк), имеет степень бакалавра в области инженерной механики, а также закончила Род-Айлендский университет со степенью магистра бизнес-администрирования. Венди является дипломированным инженером по надежности согласно Американскому обществу по

Информационные материалы

Экономический эффект микроцентров обработки данных
Информационная статья 223

Движущие факторы и преимущества периферийных вычислений
Информационная статья 226

Цифровой дистанционный контроль и его влияние на изменения в принципах эксплуатации и обслуживания ЦОД
Информационная статья 237

Смотреть все статьи
whitepapers.apc.com

Смотреть все инструменты TradeOff Tools™
tools.apc.com

Обратная связь

Для отзывов и комментариев относительно содержания данной статьи:

Научный центр ЦОД:

dcsc@schneider-electric.com

Если вы являетесь клиентом и у вас есть вопросы по вашему проекту ЦОДа,

свяжитесь с вашим региональным представителем Schneider Electric на сайте

www.apc.com/support/contact/index.cfm