ЦОД для промышленных предприятий: о чем стоит задуматься?

В.А. Цыганков (Компания «Энвижн Груп»)

Традиционно центры обработки данных (ЦОД) создают организации либо из сферы ИТ – разработчики ПО, сервис-провайдеры, Internet-магазины, либо из сферы массового обслуживания – телеком-операторы, банки и страховые компании, платежные системы, торговые сети и т.д. Но повсеместная автоматизация приводит к тому, что практически любое крупное промышленное предприятие вынуждено обрабатывать и хранить огромные объемы информации. Рассмотрены нюансы, о которых следует задуматься, если предприятие «доросло» до необходимости арендовать ЦОД или построить собственный.

Ключевые слова: центры обработки данных, надежность, отказоустойчивость, системы хранения данных, энергоэффективность.

ЦОД или не ЦОД?

Для начала нужно определиться, нужен ли предприятию собственный дата-центр. По оценкам некоторых экспертов, ЦОД начинается с 25 серверов, при этом размещенными на них информационными системами пользуются не менее 30% сотрудников. При более низких показателях достаточно серверной комнаты.

Если же цифры соответствуют ситуации, то следует задуматься о важных требованиях: нужно помещение площадью не менее 90 м^2, оснащенное системами кондиционирования для поддержания температуры не выше 20°С. Кроме того, сотрудники ИТ-департамента и службы охраны должны обеспечивать информационную и физическую безопасность дата-центра.

В случае невозможности выделить помещение и специалистов можно воспользоваться услугами коммерческого ЦОД: арендовать готовые к работе серверы (с установленными ОС и защитным ПО) или только стойки для размещения в них собственного вычислительного или коммутационного оборудования [1].

Яркий пример промышленного ЦОД — суперкомпьютер концерна BMW, который рассчитывает аэродинамику новых автомобилей и анализирует результаты краш-тестов. Изначально он размещался в Германии, но в 2012 г. компания перенесла вычислительные мощности в коммерческий ЦОД Verne Global в Исландии, недалеко от г. Рейкьявика. Комплекс примечателен грамотным использованием природных ресурсов: для кондиционирования применяется естественная вентиляция — холодный воздух и ветер, а для энергоснабжения — гидроэлектростанции и геотермальные источники — гейзеры. Все это помогает не только экономить, но и снизить вредное воздействие на окружающую среду: благодаря «переезду» BMW избавилась от ежегодного выброса в атмосферу 3570 тонн углекислого газа.

Что главное в ЦОД?

Ключевое требование к ЦОД — надежность или отказоустойчивость. Для измерения этого абстрактного понятия используется количественный показатель — процент доступности. Он отражает максимально допустимое время, которое ЦОД может простаивать за год с минимальным ущербом для деятельности предприятия.

В международной практике дата-центры оцениваются по американскому стандарту TIA-942 или стандарту, разработанному Uptime Institute. Несмотря на некоторые отличия, в целом документы схожи и по набору параметров проводят разделение на четыре класса надежности — от Tier I до Tier IV (таблица).

Классы надежности дата-центров

Параметры	Tier I	Tier II	Tier III	Tier IV
Доступность, %	99,671	99,749	99,982	99,995
Допустимый простой, ч/год	28,8	22	1,6	0,4
Максимальная мощность, Вт/м^2	До 320	До 530	До 1615	От 1615
Тип здания	Многоцелевое		Выделенное	

Классификацию можно укрупнить: для проведения профилактических и планово-ремонтных работ на уровнях Tier I и Tier II требуется остановка ЦОД, для Tier III и Tier IV благодаря использованию резервных систем жизнеобеспечения она не нужна.

Базовым критерием для обеспечения надежности в упомянутых стандартах считается именно избыточность инженерной инфраструктуры — наличие в системах энергоснабжения, кондиционирования (охлаждения) и пожаротушения дублирующих элементов, которые поддерживают рабочее состояние комплекса при выходе из строя или техническом обслуживании основных.

Очевидно, что избыточность необходима и другим составляющим ЦОД — вычислительной и телеком-

муникационной инфраструктурам: о какой надежности может идти речь, если сломается сервер или коммутатор, а запасного оборудования нет? Кроме того, для защиты ИТ-систем от киберугроз необходимо специализированное ПО и аппаратно-программные комплексы: антивирусы, межсетевые экраны, системы обнаружения вторжений (IPS) и предотвращения утечек информации (DLP), а также системы резервного копирования и восстановления данных.

Пример из практики. В 2014 г. «Энвижн Груп» модернизировала дата-центр ОАО «Интер РАО». Заказчик решил повысить производительность вычислительного комплекса и при этом сохранить высокий уровень доступности всех сервисов. Аудит показал, что необходимо внести изменения во все критические инженерные системы: установить дополнительные распределительные щиты, аккумуляторные батареи, прецизионные кондиционеры и другое оборудование, а также применить конструкторские решения — произвести компоновку блоков воздухообмена и организовать в машинном зале так называемый холодный коридор. Сложность проекта заключалась в том, что все операции пришлось выполнять в «горячем» режиме — без остановки ЦОД, хотя он и не был на это рассчитан.

Другой важный момент проекта — обеспечить полное резервирование всех компонентов инженерных систем, «вписать» новое оборудование в имеющиеся помещения.

Думать о будущем… и о мелочах

Во избежание трудностей вроде описанных выше следует еще на стадии проектирования предусмотреть перспективы масштабирования, наращивания мощности ЦОД. Конечно, создание запаса для любого материального актива «тянет карман» — увеличивает бюджет строительства (если решено создавать собственный ЦОД; в случае аренды все заботы о масштабировании ложатся на плечи владельца ЦОД). Но, во-первых, затраты на «дельту» невелики по сравнению со стоимостью всего ЦОД, во-вторых, они являются инвестициями в динамичное развитие компании.

И все же будущее — это продолжение настоящего, поэтому отталкиваться следует от текущих задач и потребностей. Набор эксплуатируемых информационных систем, число пользователей и массивы регулярно генерируемых данных определяют параметры как ИТ-инфраструктуры — число и мощность серверов, объем систем хранения данных (СХД), так и телеком-инфраструктуры — производительность коммутаторов и маршрутизаторов, пропускную способность каналов.

Совокупность ИТ- и телеком-оборудования позволяет рассчитать необходимое число стоек — серверных и коммутационных шкафов, а также полезную площадь машинного зала (с учетом коридоров, требуемых для доступа обслуживающего персонала и циркуляции воздуха).

Наконец, для поддержания ИКТ-решений нужна инженерная инфраструктура — системы пожаротушения, охлаждения и энергоснабжения. Им в свою очередь тоже требуется пространство — как скрытое (под фальшполом в машинном зале), так и явное, например, помещения для систем бесперебойного питания и дизель-генераторных установок. Таким образом, можно оценить общую площадь ЦОД.

Пример из практики. В 2012 г. «Энвижн Груп» по заказу ОАО «Ростелеком» построила в г. Сочи центр информационных технологий для организации и проведения Олимпиады-2014. Комплекс мощностью 2 МВт занял помещение площадью 2 тыс. м^2, на которых разместились основной ЦОД и 400 рабочих мест для специализированных служб круглосуточной технической поддержки, обучения, тестирования, контроля сети, управления спортивными ИТ-системами и т. д.

Фокус на эффективности: укрощаем «аппетит»

Проектируя ЦОД, следует уделить внимание показателю энергоэффективности (Power Usage Effectiveness, PUE), который отражает отношение мощности всего ЦОД к мощности ИТ-оборудования. На первый взгляд оценить его довольно просто. Но в реальности тривиальная формула оборачивается уравнением со многими неизвестными.

Во-первых, надо учитывать местные климатические особенности — колебания температуры, давления и влажности, от которых зависит нагрузка на инженерную инфраструктуру, особенно на системы охлаждения и кондиционирования. Во-вторых, нагрузка на вычислительное оборудование также сильно варьируется даже в течение одного дня, не говоря уже о более длительных промежутках времени: нужно помнить о выходных, праздниках, отчетных периодах и других нюансах производственных и бизнес-процессов. В-третьих, существует множество различных методик измерения энергопотребления: на уровне розеток, блоков питания, стоек, отдельных устройств и т. д.

Эти и другие, еще более специфичные детали говорят о том, что даже после кропотливой работы расчетный показатель будет лишь приблизительно характеризовать энергоэффективность будущего ЦОД. Реальный показатель PUE можно вычислить лишь по итогам регулярных измерений в действующем дата-центре на протяжении не менее 1 года.

В идеале PUE должно стремиться к единице. На практике очень хорошим считается даже показатель, равный 1,2...1,5. Супертехнологичный ЦОД Facebook в США достигает уровня 1,08. Но каких усилий это стоит компании?

Здравый смысл подсказывает, что нужно искать «золотую середину». С одной стороны, приложить усилия для минимизации PUE: использовать энергоэффективное оборудование, современные строительные материалы и «зеленые» технологии, например, солнечные батареи для собственного производства электричества. Все это позволяет заботиться как об экологической обстановке, так и о бюджете пред-

приятия — чем ниже энергопотребление, тем лучше. С другой стороны, соизмерять затраты, направленные на «стремление к единице», и выгоду, которую впоследствии можно будет получить.

Фокус на эффективности: повышаем производительность

Разумеется, ИКТ-инфраструктура тоже должна быть эффективной. Среди технологий, способствующих повышению производительности, следует выделить виртуализацию. По экспертным оценкам, полезная загрузка обычного сервера составляет всего 20...30% от его реальных возможностей, а благодаря виртуализации можно добиться загрузки до 90%. Выгода очевидна: физический парк ИТ-оборудования сократится в 3...4 раза.

Дополнительный эффект дает виртуализация рабочих мест (Virtual Desktop Infrastructure, VDI). Сконцентрировав все информационные системы и необходимые для повседневной деятельности данные на серверах, можно пересадить сотрудников с «классических» десктопов на более легкую технику: бухгалтеров и других офисных работников — на терминалы, а «полевых» инженеров — и вовсе на планшеты.

Виртуализация упрощает и работу с телеком-оборудованием. Так, концепция программно-конфигурируемых сетей (Software Defined Networking, SDN) подразумевает управление всей инфраструктурой передачи данных в ЦОД как единым целым, абстрагируясь от специфики каждого отдельно взятого коммутатора или маршрутизатора. Такой подход превращает принципиально разные сети (LAN и SAN) в конвергентную среду передачи любого вида трафика (IP, FCoE, iSCSI) между серверами, СХД и виртуальными приложениями.

Пример из практики. В 2013 г. «Энвижн Груп» построила для компании «МТС Украина» ЦОД мощностью 3 МВт, нацеленный на виртуализацию вычислительных ресурсов. В компании было создано частное облако, и доля виртуализации систем достигла 75%. Такая инфраструктура значительно ускорила обслуживание клиентов и ввод новых услуг, а также обеспечила усиленную защиту абонентских данных: информация хранится удаленно на сервере и защищена от переноса и копирования. Кроме того, появилась возможность быстро создавать новые рабочие места с централизованным управлением.

Фокус на эффективности: все под контролем

Многие промышленные предприятия привыкли контролировать производственные процессы с помощью автоматизированных систем диспетчеризации и управления (АСДУ) на базе SCADA [2]. Но возможности решений этого класса гораздо шире: их инструментарий легко приспосабливается и к управлению сложным «организмом» ЦОД. В современной ИТ-терминологии соответствующие платформы называют системами управления инфраструктурой ЦОД (Data Center Infrastructure Management, DCIM). Казалось бы, наименование условное, но оно помогает избежать путаницы с «классическими» АСДУ, которые в данном случае выступают источниками информации для ЦОД.

Полноценная DCIM-система позволяет контролировать не только инженерную, но и ИТ-инфраструктуру — серверы, стойки, каналы передачи данных, а иногда и некоторые сервисы. Например, большинство таких решений интегрируются с продуктами VMware и благодаря этому управляют виртуальными машинами и загрузкой серверов. Кроме того, DCIM может не только агрегировать данные из SCADA и BMS, но и частично заменить их, так как поддерживают различные «полевые» протоколы — SNMP, BacNet, ModBus и т. д.

Сильная сторона систем диспетчеризации — наглядность: современные мультимедиа-решения предоставляют оператору 3D-модель ЦОД с максимальной детализацией вплоть до каждой отдельной единицы оборудования и конкретного кабеля, а также объемные графики температуры по помещениям. Благодаря такой визуализации проще не только обслуживать инфраструктуру, но и проводить масштабирование — размещать новые серверы и стойки с учетом минимальных затрат на их жизнеобеспечение, то есть с максимальной эффективностью.

Перечисленные возможности дают ощутимый экономический эффект: использование инструментария АСДУ/DCIM снижает затраты на эксплуатацию и техническое обслуживание ЦОД в среднем на 30%.

Пример из практики. В 2014 г. «Энвижн Груп» построила для телеком-оператора МТС новый ЦОД мощностью 2,2 МВт. Комплекс оснащен инструментами для управления ИТ-инфраструктурой: системой сбора и анализа информации в реальном времени на базе решения SYSTIMAX iPatch, а также средствами диспетчеризации на базе ПО Iconics.

Новый ЦОД был призван повысить качество управления сетью и предоставления новых коммерческих сервисов. Инновационные решения — online-диагностика оборудования, контроль достаточности ресурсов и проактивная система выявления неисправностей — позволили расширить спектр предоставляемых услуг и обеспечить их максимальную доступность сервисов для клиентов.

Кому доверить дата-центр?

Даже краткий обзор нюансов, связанных со строительством и обслуживанием дата-центра, заставляет вернуться к вопросу, озвученному в самом начале: вам действительно нужен собственный ЦОД? Если ответ по-прежнему утвердительный, остается дать еще один совет: привлечь к созданию и эксплуатации сложного технологического комплекса надежного партнера.

Выполнение соответствующих работ — от проектирования до технической поддержки — разумно

доверить крупной ИТ-компании с опытом в этой сфере деятельности. Желательно, чтобы в команде, отвечающей за разработку и функционирование ЦОД, присутствовал хотя бы один сертифицированный специалист — например, со статусом Accredited Tier Designer (ATD) или Accredited Tier Specialist (ATS) от вышеупомянутого Uptime Institute. Международная сертификация повышает вероятность того, что ЦОД будет построен в соответствии с требованиями международных отраслевых стандартов, а значит, будет иметь высокий уровень надежности и эффективности.

Список литературы

1. *Жилкина Н.* Дата-центр на аутсорсинг: рынок на подъеме // Компьютерра. 2013. март. http://www.computerra.ru/cio/2722.
2. *Ицкович Э.Л.* Современные SCADA-программы разных производителей: их свойства и отличия, важные для потенциальных заказчиков // Автоматизация в промышленности. 2007. №4.

Цыганков Вячеслав Анатольевич *– эксперт компании "Энвижн Груп".*
Контактный телефон (495) 641-12-12.
Http:// www.nvg.ru

ИТ-инфраструктура предприятия: особенности, тренды, опасности в кризис и не только

И.И. Батов, А.В. Переведенцев (Компания Техносерв)

Построение и оптимизация ИТ-инфраструктуры, удовлетворяющей бизнес-процессам организации – сложная и многогранная задача. Рассмотрены современные инновационные подходы, применяемые при создании ЦОД: виртуализация задач, систем хранения данных и инфраструктуры сетей передачи данных, а также организационные вопросы – кибербезопасность, аудит инженерной инфраструктуры предприятия, создание модульных ЦОД, использование аутсорсинговых ЦОД.

Ключевые слова: центр обработки данных, кибербезопасность, виртуализация, инженерная инфраструктура, аутсорсинг.

Свой или чужой ЦОД: кому и что выбрать?

Информационные системы играют важную роль в деятельности предприятий, повышая эффективность и поддержку бизнес–процессов. Перед предприятиями, потребности которых в обработке информации неуклонно растут, лежат два пути. Первый — установка своего оборудования или информационной системы в коммерческом центре обработки данных (ЦОД). Этот вариант дает возможность воспользоваться «всеми благами» готовой инфраструктуры ЦОД, предлагающих свои ресурсы в аренду. Второй вариант — создание собственного корпоративного ЦОД.

Компании, которые выбирают вариант ЦОД на аутсорсинг — это предприятия, бизнес которых не находится в прямой зависимости от непрерывного функционирования ИТ-систем. Возможна ситуация, когда компания — аутсорсер является родственной или дочерней компанией заказчика услуг (это позволит контролировать работу ЦОД, сделать ее более прозрачной). Многие компании отдают на аутсорсинг часть задач, которые не являются критичными или конфиденциальными.

Почему же ряд предприятий не доверяют аутсорсинговым ЦОД критичные задачи?

Прежде всего, это различный уровень зрелости. Компании, предлагающие ЦОД на аутсорсинг, достаточно молоды. Как правило, они не обеспечивают соглашение об уровне предоставления услуги (Service Level Agreement SLA) высокого уровня, удовлетворяющего заказчика.

Остается еще ряд проблем: возможные утечка информации, потеря контроля над собственными ресурсами, проблемы у компании-аутсорсера (например, банкротство), а также непредсказуемые последствия при аварийной остановке ЦОД (нет контроля над инфраструктурой ЦОД).

Построить ЦОД в кризис

Понимая минусы аутсорсинговой модели, рассмотрим вариант создания собственного ЦОД. Сформулируем задачу предельно конкретно: как построить «бюджетную» инфраструктуру, но при этом обеспечить базу для стабильного функционирования ЦОД на протяжении многих лет?

В текущих экономических условиях в создании ЦОД заинтересованы крупные организации энергетического сектора для получения технологического фундамента и расширения бизнеса, операторы связи, компании, ориентирующиеся при создании ЦОД на эксплуатацию его в коммерческих целях, и, конечно, промышленный сектор, наращивающий затраты на ИТ-услуги ввиду усиления долевого участия государства и роста экспортных продаж вооружения. Впрочем, компании, которые будут строить ЦОД в ближайшие годы можно разделить на два сектора: компании с государственным участием и компании со стабильно развивающимся спросом (например, Internet и телеком-компании).

На первых этапах при строительстве ЦОД необходимо выяснить, насколько глубоко бизнес-процессы компании зависят от ИТ-решений (зависимость бизнеса от информационных систем). Эта информация