Строим ЦОД. Часть 1

© Фото: Евгений Вирцер
Директор компании "Инсистемс" Евгений Вирцер учит читателей Digit.ru строить безопасные центры обработки данных - ЦОД. И начинает с выбора площадки.
28/04/201119:33
Автор: Евгений Вирцер
Ключевые слова: ЦОД

Будем исходить из того, что состав оборудования и программного обеспечения определен. Задача состоит в том, чтобы построить надежный, безопасный ЦОД.

Во-первых, строительные конструкции здания или будущего серверного помещения должны соответствовать требованиям нормативов по несущей способности перекрытий, пределу огнестойкости и т.д. Во-вторых, нужно учесть, что к площадке, на которой планируется строить ЦОД, должны быть подведены необходимые внешние коммуникации - электроснабжение требуемой категории, каналы связи и т.д. В-третьих, внутри здания или помещения должна быть построена отказоустойчивая инженерная инфраструктура.

Цена вопроса зависит от исходного состояния площадки. Наиболее дорогостоящие работы - обеспечение дополнительной электроэнергией, включая реконструкцию существующей электроустановки здания. Стоимость инженерной инфраструктуры если и меняется из-за особенностей площадки, то, как правило, незначительно.

Правильно, чтобы строительство ЦОД опиралось на известные методики управления проектами. Но у нас в стране так поступают только тогда, когда строительство - инвестиционный проект. Большинство владельцев ЦОДов, особенно если речь идет о корпоративном центре обработки данных или серверной комнате, приступает к делу без лишних раздумий: на этом этаже у нас есть свободное помещение, значит, здесь и будем строить. Проектно-изыскательские работы обычно не проводятся, экономия видится заказчику очевидной - площадь уже арендована либо находится в собственности, ЦОД или серверная располагаются здесь же, поди плохо.

О том, пригодно ли это помещение, и легко ли будет его оборудовать инженерными системами, мало кто думает. Понятно, почему. Корпоративный ЦОД - вообще продукт долгой эволюции. Сначала хватало одного сервера, потом оборудовали серверную, потом ее расширили, потом расширили еще разок, но больше расширить не могут - и тут-то решают строить ЦОД. Вопрос, где его строить, обсуждается редко. Конечно, в том же здании и хорошо бы на смежной площади.

Часто случается, что из-за дефицита площадей в офисных зданиях местом строительства будущего ЦОДа выбирают, скажем, столовую или другое помещение, не слишком пригодное для установки серверов. В практике "Инсистемс" был даже случай, когда нам пришлось перестраивать под серверное помещение… санузел. Такие проекты исполнителю интересны нетривиальностью, но заказчику, надо признать, обходятся недешево. Скажем, если к помещению подведена вода (а в случае с санузлом, как вы понимаете, так оно и было), эти коммуникации необходимо полностью перенести, иначе ЦОД будет под постоянной угрозой затопления.

В тех случаях, когда ЦОД размещается на втором или более высоком этаже, нужно в обязательном порядке проводить исследование несущей способности конструкций. В общем-то, такое исследование следует провести, даже когда речь идет о первом этаже или подвале - несущая способность фундамента тоже может оказаться недостаточной, особенно в зданиях старой постройки. Если не организовать такую превентивную проверку, есть риск обрушения перекрытий и стен. Серверы, системы охлаждения и резервного питания весят много больше мебели.

Причем исследование лучше провести даже тогда, когда есть результаты более ранних изысканий. Если по документам десяти- пятнадцатилетней давности стена помещения, где планируется строить ЦОД, должна выдержать необходимый вес, это еще не значит, что и правда выдержит. Под нагрузкой в стене может образовываться трещина, и тогда придется укреплять конструкцию в экстренном порядке, да еще и в помещении, куда уже завезли оборудование. Получится несколько дороже, чем могло бы быть.

Нужно также учитывать специфику строительства ЦОД. Скажем, необходимо будет просверлить в стенах каналы достаточно большого диаметра для прокладки кабелей. Если не изучить особенности здания или помещения заранее, из-за этого не исключено ощутимое проседание перекрытий. Придется домкратами возвращать их на место и усиливать металлическими конструкциями.

Для России такие ситуации типичны: заказчики у нас очень не любят платить за проектно-изыскательские работы, хотя именно с них начинается безопасность ЦОД.

О других рисках - в другой раз.

Строим ЦОД. Часть 2

Как правильно выбрать площадку для строительства ЦОД, мы уже выяснили. Теперь поговорим о самом строительстве инженерных систем, обеспечивающих безопасность ЦОД. Речь об энергетической и климатической защите, защите от пожара, затопления и несанкционированного доступа.

Энергетические системы – приоритет номер один. Необходимо не только подвести

необходимую мощность, но также позаботиться об энергообеспечении в экстренных ситуациях: предусмотреть дополнительные вводы, установить резервные генераторы, ИБП.

Наиболее проблемная ситуация при строительстве ЦОДа в действующем офисе – недостаток мощностей. Затраты на подключение одной и той же дополнительной мощности могут различаться в разы. Сравнительно экономичный вариант, когда поблизости есть действующая подстанция с резервом мощности – остается проложить кабель. Но дело может дойти и до того, что владельцу будущего ЦОДа придется за свой счет реконструировать, а то и строить новую трансформаторную подстанцию. Важно помнить о том, что помимо входной мощности необходимо обеспечить защиту ЦОДа от электромагнитного излучения, которое может привести к сбоям в работе оборудования и повреждению данных.

Не исключено, что после детальной оценки энергетических рисков и сопутствующих расходов логичнее будет перенести строительство на другую территорию, где мощности можно подвести за более разумную плату.

Что касается средств пожаротушения, то тут для ЦОДов и серверных помещений предусмотрены весьма жесткие нормативы. Помещение должно быть оборудовано системой автоматического газового пожаротушения – использование воды недопустимо, она повредит оборудование и данные. Использование таких систем обязывает проводить дополнительные мероприятия. Во-первых, требуется предусмотреть сброс избыточного давления, создающегося при выпуске газового огнетушащего вещества. Во-вторых, помещение должно быть оборудовано системой газоудаления. В-третьих, нужны правила эвакуации персонала и противогазы для него.

Мы уже упоминали о том, что в помещении не должно быть транзитных коммуникаций (отопление, водопровод, канализация). Но для серверных помещений существуют требования к уровню влажности воздуха, так что вода в некоторых количествах все же нужна, и нужна постоянно. От риска внешнего затопления можно защититься с помощью гидроизоляции на этапе строительной подготовки, но дополнительно необходимо установить датчики протечки – они защитят оборудование, если, например, лопнет труба, подающая воду для обеспечения необходимой влажности воздуха.

Отдельная система – климатическая. Именно она больше всего отличается от стандартного оборудования, применяющегося в большинстве помещений. Если мы говорим об обычных офисных площадях, то их нужно отапливать или охлаждать в зависимости от сезонных изменений температуры. Специфика ЦОДа в том, что серверы требуют постоянного, круглосуточного охлаждения и отвода тепла, даже если центр обработки данных находится за полярным кругом. Это сложная инженерная задача, понадобится специальное оборудование, которое – об этом тоже нельзя забывать – требует значительной электрической мощности.

В заключение отметим, что порой приходится не только защищать ЦОД от внешних рисков, но и ограждать прочие помещения от воздействия "агрессивных" серверов. В ходе одного из наших проектов заказчик потребовал дополнительную шумоизоляцию для серверного помещения: в соседней комнате проводились заседания совета директоров, которым мешали посторонние звуки.

Следующая тема – материалы, которые следует использовать для строительства ЦОД.

Строим ЦОД. Часть 3. Из чего: бетон против "конструктора"

При создании центра обработки данных у заказчика есть два способа обеспечить физическую безопасность на этапе строительства. Первый - использование типовых строительных материалов и конструкций: бетонные или кирпичные стены, металлическое усиление несущих перекрытий, стандартная гидроизоляция потолка и стен. Проблема в том, что эти материалы обеспечивают лишь частичное соответствие требованиям, предъявляемым к современному ЦОД. Кирпич и бетон, к примеру, обладают отличной огнестойкостью, но при пожаре выделяют горячий пар. В считанные минуты температура и влажность в помещении достигают значений, при которых серверы гарантированно "гибнут", а информация на дисках полностью уничтожается.

Второй путь - использование специальных материалов. На сегодняшний день на рынке представлено множество разновидностей "защитных оболочек" для ЦОД. По сути, это многослойная "одежда" помещения, обеспечивающая защиту от всех внешних угроз - затопления, пожара, электромагнитного излучения и несанкционированного доступа. Кроме того, эти конструкции за счет продуманной и более компактной структуры позволяют значительно увеличить объем рабочего пространства ЦОД и строить серверные помещения внутри уже возведенных стен. Еще одна особенность таких оболочек - они намного легче типовых бетонных перекрытий или кирпичных стен, а значит, требования к несущей способности основной конструкции здания заметно снижаются. Да и само строительство (независимо от того, ведется оно "с нуля" на свободной площадке или внутри функционирующего здания) обойдется дешевле и будет проведено быстрее.

В наших проектах до недавнего времени использовались модульные конструкции зарубежного производства, но при всех их преимуществах у них сохранялся один существенный недостаток - высокая стоимость. Поэтому мы разработали собственный модуль безопасности, сертифицировали его на соответствие всем нормам, в том числе и международным, действующим для конструкций для строительства ЦОД.

Надо сказать, что условия для испытаний "конструктора" создаются достаточно жесткие, особенно в части пожарной безопасности. Проверка на огнестойкость проводится в печи, где создается постоянная температура на уровне 1000-1100 градусов по Цельсию. Наш модуль безопасности в таких условиях показал 90-минутную огнестойкость - значительно дольше, чем предусмотрено нормативами. При этом на протяжении часа температура в помещении не поднималась выше 50 градусов, а влажность оставалась на уровне 75%. При таких температурно-влажностных условиях целостность данных не подвергается угрозе в течение времени, которого достаточно для тушения даже сильного пожара.

Понятно, что после таких пиковых нагрузок, если они возникнут в реальности, "одежду" для ЦОДа придется демонтировать и возводить снова. Однако нужно учитывать, что серверное оборудование и информация остаются в безопасности. А двухслойная гидроизоляция - внешняя и внутренняя - гарантирует, что аппаратура не будет повреждена водой и другими жидкостями при тушении огня. Если бы подобный пожар возник в бетонном здании, то с дорогостоящим оборудованием пришлось бы распрощаться навсегда, а полная потеря данных, возможно, оказалась бы фатальной для бизнеса.

Таким образом, строительный материал напрямую влияет на степень защищенности ЦОДа в аварийных ситуациях, и грамотный подход к выбору способен сэкономить существенные средства, а также гарантировать: даже пожар и потоп не отнимут у компании ни байта важной информации.

На этом мы заканчиваем свой небольшой цикл статей об инженерной безопасности центров обработки данных, однако готовы продолжить тему, если у читателей digit.ru появятся вопросы, на которые мы сможем ответить.