



Игорь Анисимов/
директор департамента
инженерных систем «Энвижн Груп»/
ATD #115/

Если ничто другое не помогает,
прочтите, наконец, инструкцию!
Из законов Мерфи

ЦОД: игра по правилам



Первый вопрос часто задают проектировщики, получая в работу исходные данные, которые противоречат требованиям технического задания. Второй обращают к себе заказчики, когда в результате самообразования начинают понимать, что же они построили в ходе проекта по созданию ЦОД. Третий относится к самой идее создания ЦОД.

Попробуем рассмотреть сложившуюся ситуацию и вернуть обсуждение из философских категорий в техническую плоскость.

Классификация надежности

Начнем с небольшого экскурса в историю. В 1993 году в США был основан The Uptime Institute

С каждым годом в России и за рубежом задачи создания инженерной инфраструктуры центров обработки данных становятся сложнее и интереснее. Все чаще приходится отмечать, что вопросы, возникающие перед архитектором ЦОД, из области чисто технической перемещаются в философскую: «Кто виноват?», «Что делать?», «Быть или не быть?».

(UTI), который на сегодня является интеллектуальным лидером в области повышения надежности и бесперебойной доступности (uptime) центров обработки данных. Институт проводит обучение специалистов с последующей сертификацией, осуществляет консалтинг, организует семинары и конференции, а также проводит независимые исследования и разрабатывает стандарты надежности ЦОД. В октябре 2009 года UTI вошел в состав консалтинговой компании The 451 Group, с полным сохранением бренда, персонала и программ института. Сегодня Uptime Institute признан мировым ИТ-сообществом как независимый аудитор соответствия ЦОД требованиям отказоустойчивости.

С момента своего основания и до наших дней сотрудники

Uptime Institute собрали и обработали данные более чем о 4 тысячах происшествий в ЦОД, расположенных по всему миру. Эти данные легли в основу Tier Classification — системы определения рейтингов надежности ЦОД по уровням отказоустойчивости (Tier I — Tier IV). Классификация Tier фактически стала международным стандартом, когда была включена в виде приложения в состав американского стандарта построения ЦОД TIA/EIA-942, который де-факто применяется во всем мире. TIA/EIA-942 представляет собой детальное описание требований к инженерной инфраструктуре ЦОД и содержит внушительный набор практических рекомендаций по ее реализации.

Написанная в терминах, понятных бизнесу, классификация отказоустойчивости центров обработки данных Tier I — Tier IV стала справочным пособием для руководителей, принимающих решения о строительстве дата-центров. Построение и сертификация ЦОД, соответствующего заданному уровню Tier, является гарантией того, что все работы выполнены с надлежащим качеством и обеспечена заданная надежность.

Согласно Tier Classification принято различать четыре уровня надежности (см. таблицу).

Tier I — первый, базовый уровень надежности ЦОД (коэффициент доступности — 99,67%). На данном уровне инженерная инфраструктура дата-центра создается без требований по резервированию. Необходимо одно: чтобы дата-центр имел собственные,

автономные системы инженерного обеспечения. В противном случае его нельзя будет отнести к дата-центрам — это будет всего лишь часть инфраструктуры здания. Обратите внимание: наличие системы гарантированного электроснабжения — дизель-генератора — предполагается уже в базовом варианте.

На первом уровне допускаются простои (два обслуживания по 12 часов, плюс одна-две поломки — в среднем 28,8 часа

простоев в год) — как по причине сбоев в работе элементов ЦОД, так и для плановых регламентных работ.

Tier II (коэффициент доступности ЦОД — 99,75%) накладывает дополнительные ограничения: все активные элементы систем должны быть зарезервированы по схеме 2N, N+1, N+2 и т. д., где N (сокращение от англ. need) — минимально необходимое число ресурсов. Соответственно, любая внезапная поломка активного элемента не приведет к мгновенной остановке вычислительных систем. Тем не менее и на данном уровне модель работы ЦОД допускает возможность его плановых и неплановых остановок (три обслуживания за 2 года, плюс одна поломка в год — в среднем 22 часа простоев в год).

Дата-центр с уровнем надежности Tier III (коэффициент доступности — 99,98%) функционирует по принципу обслуживания без остановки. Согласно TIA/EIA-942, ЦОД уровня Tier III должен обеспечивать резервирование всех инженерных подсистем. Это означает, что все вычислительные системы инфраструктуры ЦОД должны продолжать работать непрерывно, и при этом сохраняется возможность проведения модернизации и плановых ремонтно-профилактических работ без остановки сервисов. На данном уровне допускается 4 часа на восстановление после поломки за два с половиной года, что соответствует 1,6 часа простоев в среднем в год. Эта возможность обеспечивается за счет резервирования активных и пассивных компонентов инфраструктуры, что означает наличие

как основных, так и резервных систем распределения электропитания, охлаждения, СКС и т. д. Переход от Tier II к Tier III — серьезный качественный сдвиг в организации ЦОД.

Четвертый уровень надежности дата-центра — Tier IV — предполагает создание действительно полностью отказоустойчивого ЦОД (коэффициент доступности — 99,99%). Такая схема позволяет выполнить любые плановые и внеплановые работы без прерывания функционирования дата-центра и гарантированно защищает от его остановки по причине умышленной или случайной поломки любого элемента инженерной инфраструктуры. Допустимым считается 4 часа на восстановление после поломки за 5 лет, что соответствует в среднем 0,8 часа простоев в год. На этом уровне обеспечивается наиболее надежная защита от сбоев: система инженерного обеспечения устойчива к отказам и способна автоматически локализовать их. Помимо резервирования активных и пассивных элементов, топология системы предполагает, что отказ любого элемента не приводит к снижению уровня резервирования.

На практике оказывается, что для соблюдения этих требований в проектах создания ЦОД необходимо решать еще много промежуточных вопросов. В курсе обучения Uptime Institute «Accredited Tier Designer», проводимом три раза в год, как раз подробно рассматриваются все без исключения вопросы применения требований UTI к каждой из инженерных подсистем.

Если задача поставлена шире и речь идет не о создании инженерной инфраструктуры отдельного ЦОД, а о построении информационной системы корпорации, то Uptime Institute рассматривает дополнительные критерии к эксплуатационной готовности ЦОД, которую определяют пять факторов:

- > характеристики площадки для ЦОД (угрозы природных и техногенных катастроф, доступность и качество внешних инженерных сетей, квалификация и наличие обслуживающего персонала);
- > характеристики здания (состояние конструкций и инженерных систем);
- > возможность дальнейшего развития ЦОД;
- > инвестиционная эффективность (энергоэффективность, рост или потеря стоимости со временем, соответствие задачам бизнеса);
- > управление и эксплуатация (уровень подготовки персонала, уровень кооперации службы ИТ и службы эксплуатации ЦОД).

В соответствии с этими критериями вводятся три уровня эксплуатационной готовности: «А», «В» и «С».

Комплексный анализ отказоустойчивости информационной системы компании — сложная и многокомпонентная задача. По нашему

мнению, именно в целях предоставления этой услуги произошло объединение Uptime Institute и The 451 Group.

■ В таблице приведены базовые требования к ЦОД по системе классификации UTI.



Какой уровень отказоустойчивости предпочесть?

Перед владельцами коммерческих дата-центров, как и перед организациями, создающими ЦОД для собственных нужд, встает серьезный вопрос: на какой уровень надежности ориентироваться? Очевидно, что универсальных рецептов ответа на этот вопрос нет: многое зависит от конкретных условий и требований заказчика.

Здесь в качестве отправной точки необходимо взять время простоев вычислительных систем, допустимых для данной организации. Например, для образовательного учреждения или фирмы с обычным режимом работы вполне допустимы ночные простои. Для такой организации повышать отказоустойчивость систем ЦОД до уровня Tier III имеет смысл лишь в том случае, когда она стремится к достижению высочайшего уровня репутации в национальном или глобальном масштабе.

Требование	Tier I	Tier II	Tier III	Tier IV
Резервирование активных систем инженерного обеспечения	N	N+1	N+1	N после любого отказа
Распределительные системы	1	1	1 — активный 1 — запасной	2 одновременно активных
Возможность обслуживания без отключения полезной нагрузки — Concurrently Maintainable	нет	нет	да	да
Устойчивость к отказам Fault Tolerant	нет	нет	нет	да
Топологическое разделение — Compartmentalization	нет	нет	нет	да
Непрерывное охлаждение	возможно	возможно	возможно	обязательно
Автоматическая локализация сбоев и переключение на резервное оборудование	возможно	возможно	возможно	обязательно



Для транснациональных компаний, чей бизнес расположен в нескольких часовых поясах, а информационные ресурсы централизованы, остановка информационных систем может повлечь серьезные убытки. Следовательно, им необходим ЦОД с высоким уровнем надежности. Обеспечить его можно двумя способами. Если архитектура информационных ресурсов предполагает резервирование информационных систем с топологическим разделением основной и резервной системы (например, в наличии имеется два или более ЦОД с дублирующими функциями), то требования к резервированию и надежности инженерной инфраструктуры могут быть несколько снижены, но при этом не ниже, чем уровень резервирования и надежности вычислительных систем. При создании в организации единственного ЦОД имеет смысл сразу ориентироваться на более высокий уровень надежности.

Построение и сертификация ЦОД, соответствующего заданному уровню Tier, гарантирует надлежащее качество работы и обеспечивает заданную надежность.

Эти же рекомендации можно адресовать и госструктурам, для которых бесперебойность услуг регламентируется законодательством.

Для компаний, чей бизнес базируется на собственной ИТ-инфраструктуре — например, Yandex, Google, Amazon, E-Bay, — необходимо как физическое, так и логическое резервирование и зеркалирование данных, а следовательно, и создание отказоустойчивых ЦОД. На сегодняшний день эти компании являются флагманами в разработке и применении новых технологий инженерного обеспечения ЦОД.

Как получить «знак качества»

Сегодня «Энвижн Груп» предлагает своим заказчикам как разработку технических требований к ЦОД, так и организацию работ по сертификации ЦОД в Uptime Institute.

Процесс сертификации предполагает два этапа. На первом осуществляется сертификация проектной документации Uptime Institute, для чего проводится проверка чертежей и технических решений. По ее результатам проект регистрируется как сертифицированный на соответствие заданному уровню Tier.

На втором этапе проходит сертификация построенного ЦОД, определяется уровень его надежности. Эти работы проводят специалисты Uptime Institute непосредственно на объекте. Они проверяют, насколько созданный дата-центр соответствует проекту, и по собственной методике проводят тестирование всех его подсистем.

Если результат оказывается удовлетворительным, дата-центр регистрируется как сертифицированный объект и в качестве подтверждения получает соответствующий лейбл.

Если процесс создания ЦОД состоит из нескольких этапов или пусковых комплексов, то необходимо помнить, что сертификат будет выдан на те комплексы, которые на момент сертификации были введены в эксплуатацию. Таким образом, сертификация ЦОД, состоящего из нескольких очередей, — предмет отдельной проработки.

На рисунке (см. на стр. 61) можно видеть, как выглядят сертификационные знаки UTI (Computersite Engineering — второе название Uptime Institute Professional Service, подразделения, непосредственно проводящего сертификацию).

Стоимость услуг Uptime Institute сравнима со стоимостью проектирования небольшого ЦОД. Но эти затраты, особенно в случае создания крупных объектов, оправданы. В ходе сертификации компания получает филигранный консалтинг высокого уровня, гарантию обеспечения отказоустойчивости ЦОД и внятные перспективы его развития.

Нужна ли нам сертификация?

Такой вопрос возникает у многих владельцев ЦОД. Действительно, есть ли смысл затевать процедуру сертификации дата-центра, тратить на нее время и деньги? Что дает владельцам ЦОД и арендаторам наличие сертификата?

Прежде всего сертификат гарантирует соответствие дата-центра определенному уровню Tier. По официальным оценкам экспертов, в России подавляющее большинство коммерческих дата-центров соответствует категории надежности Tier II, а ряд ЦОД декларирует свой уровень как Tier III. Увы, приходится констатировать, что это

излишне оптимистичный взгляд на вещи. В реальности уровень многих корпоративных и коммерческих ЦОД, как показано выше, можно охарактеризовать как «ни два ни полтора».

На отечественном рынке ЦОД широкое распространение полу-

чила интересная комбинация требований к различным системам инженерного обеспечения, в рамках которой системы кондиционирования, как правило, выполняются по требованиям к Tier II, а системы электроснабжения — по Tier III. При этом воодушевленный заказчик и не менее воодушевленный подрядчик, находясь в состоянии эйфории от успешно завершеного строительства, хором утверждают, что построили ЦОД уровня Tier III, хотя на самом деле это не так.

Однако это наиболее благоприятный вариант. Существуют, к сожалению, и более серьезные отклонения от правил построения ЦОД в соответствии с классификацией UTI.

Так, например, система гарантированного электроснабжения может базироваться на одном дизель-генераторе (Tier I), а система бесперебойного электроснабжения — иметь резервирование 2(N+1). При этом заказчик искренне считает, что он построил ЦОД Tier III, за исключением самой малости. Обратите внимание: эта «малость» на самом деле дает ошибку на целых два уровня — ведь надежность определяется по самому слабому элементу инфраструктуры. В результате в 18 раз увеличивается возможное время простоя ЦОД!

Еще один пример распространенных заблуждений — когда заказчики в ТЗ требуют, чтобы вычислительные системы ЦОД были отнесены к электроприемникам первой особой категории электроснабжения. Поскольку в России это самая высокая категория, то делается заключение, что такого требования достаточно, чтобы система электроснабжения соответствовала Tier III или Tier IV. Мы знаем, что данное заключение в общем случае неверно, и, чтобы соответство-

вать, например, Tier IV, необходимо выполнить ряд серьезных дополнительных требований по резервированию путей распределения электропитания и дизель-генераторных установок (ДГУ), по физическому разделению основного и резервного оборудования, а также построить системы мониторинга и диспетчеризации, позволяющие локализовать любую неисправность в автоматическом режиме.

Да, отключения электроэнергии у нас случаются крайне редко. Но случаются. Все мы помним блекаут в Москве в конце мая 2005 года, когда из-за перегрузки линий электропередачи произошла системная авария, и за ней последовала лавина потери напряжения в сети с отключением сотен тысяч потребителей в Москве, Московской области и ряде прилегающих районов. Поэтому нельзя уходить в допущения — это самообман! И рано или поздно такой подход неизбежно приведет к реальным потерям в бизнесе.

С другой стороны, в нашей практике бывали случаи, когда, создавая систему гарантированного электроснабжения на основе ДГУ, заказчик не доверял ее работе и требовал от систем бесперебойного электроснабжения работы в течение 30–60 минут для возможности корректного «шатдауна» вычислительных систем. Понятно, что за этим скрывается опасение некачественного технического сопровождения ДГУ, приводящего к невозможности их запуска в критический момент аварии. Случаи качественно построенных инженерных систем, вышедших из строя по причине отсутствия или недостаточного качества техобслуживания, все еще нередки.

Как мы видим, в большинстве случаев заказчик волей-неволей пытается обмануть самого себя. Причина в том, что в глубине души он полагает: если и произойдет серьезная авария на внешних сетях, то либо она не продлится долго, и ресурсов систем инженерного обеспечения будет достаточно для поддержания ЦОД на этот период, либо даже в случае остановки ЦОД потери можно будет списать на форс-мажорные обстоятельства. Это означает, что в действительности простои ЦОД не столь критичны для деятельности организации, как об этом говорится, когда формулируются требования ТЗ на ЦОД, а в ряде случаев говорит о том, что конкретный руководитель не боится ответственности за последствия своих действий.

Есть и еще одна простая причина создания ЦОД с непрозрачным уровнем отказоустойчивости — традиционная надежда на авось. Заказчик сознательно идет на некоторые отклонения от стандарта, полагая, что вероятность наступления критической ситуации ничтожно мала. При этом расчет этой самой вероятности ведется чисто гипотетически.

Другая распространенная ситуация — присваивание определенного уровня отказоустойчивости «авансом». Например, коммерческий дата-центр, декларируя уровень Tier II или Tier III, спроектировал для своей системы холодоснабжения основной и резервный чиллеры. Однако по причине перерасхода бюджета проекта закупил и ввел в эксплуатацию только один из них. Второй чиллер планируется к закупке из бюджета поступлений от арендных платежей, и под него даже приготовлена площадка и проложены коммуникации. Но в данный момент очевидно, что такой ЦОД не соответствует Tier II — даже при том условии, что все остальные системы могут быть выполнены по требованиям Tier III. Стоит ли о такой «мелочи» сообщать клиентам? Не уверен, что последние, будь они предупреждены, полностью разрешили бы оптимизм арендодателя: ведь ни о каком серьезном уровне отказоустойчивости в его дата-центре на данный момент речи не идет. Декларация, что ЦОД имеет уровень Tier III, при реальном Tier I является банальным обманом.



В последнее время наблюдается устойчивая тенденция к увеличению потребности в независимом аудите проектов и функционирующих ЦОД.

При всем вышеизложенном нередко можно наблюдать ситуацию, особенно в корпоративном секторе, где действуют отраслевые стандарты, когда заказчик обоснованно требует выполнения различных подсистем ЦОД с различными требованиями к отказоустойчивости. В этом случае сертификация не принесет ничего позитивного.

Но достаточно уже о заказчиках. Как быть с подрядчиками, которые убеждают, что могут построить ЦОД любого уровня, а результат не выдерживает критики?

Проблема не только в недостаточной квалификации исполнителей, но и в том, что если хотя бы одна из подсистем ЦОД не соответствует заданному уровню надежности, то и уровень надежности ЦОД будет определяться по этому «слабому звену». В этом коренное отличие строительства ЦОД от обычного понятия «стройки». Отсюда и требование к наличию профессиональной команды проектировщиков и опыту строительства аналогичных объектов. Если какая-то из систем спроектирована неправильно, то для исправления оплошности придется сломать добрую половину ЦОД. Между тем договор с подрядчиками иногда не отражает ничего, кроме финансовых условий.

Как уберечь себя от попадания в такую ситуацию? Значит ли это, что, принимая решение об аренде, необходимо самому воочию убедиться в наличии всех компонентов систем инженерного обеспечения и их согласованной работы? Потратить время собственных

специалистов или, за неимением сотрудников нужной квалификации, привлечь (оплатить) сторонних экспертов?

Ответ на вопрос очевиден уже в названии этой главы: избавить арендатора от долгой и затратной процедуры проверки может наличие у коммерческого ЦОД сертификата Uptime Institute. Независимая сертификация — гарантия высокого уровня предоставления услуг. Риски некачественного монтажа также велики, поэтому независимый аудит является своего рода гарантией заказчика.

Сертификация выгодна и самим коммерческим дата-центрам, причем не только с точки зрения выстраивания прозрачных взаимоотношений с арендаторами. Класс отказоустойчивости коммерческого ЦОД определяет основную часть стоимости его услуг: клиенты платят за надежность.

Это в большой степени относится и к корпоративным дата-центрам. Репутация любой компании неразрывно связана с понятием



надежности. Отказоустойчивый корпоративный ЦОД — одна из гарантий надежности и бесперебойности работы компании. Процесс осознания ЦОД как важного актива организации уже начался: так, например, Сбербанк РФ заложил в свою концепцию развития ИТ создание сертифицированного по Uptime дата-центра, и сейчас проект находится в начальной стадии реализации.

О пользе и вреде плюсов

Для того чтобы строить ЦОД «по правилам», рассмотрим еще одну разновидность отклонений от стандарта — внесение в инфраструктуру дата-центра элементов, категория отказоустойчивости которых превышает общий уровень. В результате возникает, например, такая своеобразная «вариация на тему», как Tier III+. О ней стоит поговорить отдельно.

В последнее время в технических заданиях на проектирование центров обработки данных, в рекламных буклетах и выступлениях представителей коммерческих ЦОД все чаще упоминается подобный «плюсовый» уровень надежности. Между тем никаких промежуточных уровней в системе классификации отказоустойчивости центров обработки данных Uptime Institute не предусмотрено. Возникает резонный вопрос: что вызвало к жизни Tier III+ и стоит ли все-без рассматривать его как ориентир?

Прежде всего разберемся с причинами. Пресловутый «плюс» был вызван к жизни благими побуждениями владельцев коммерческих ЦОД и арендаторов компенсировать слабости существующей инфраструктуры объекта. Довольно распространенным требованием заказчика является уровень резервирования систем электроснабжения 2(N+1). При этом предполагается, что создаются две цепочки, в каждой из которых N+1 элементов. Любой из элементов может выйти из строя, но при такой схеме обе системы будут работоспособны.

Кстати, в России ситуация, когда категория системы электроснабжения сильно превалирует над остальными, типична. Возникает она, так сказать, «по жизненным показаниям», исходя из существующих реалий.

Вот здесь-то и таится опасность. Исключения из правил, обусловленные определенной ситуацией у конкретных клиентов, некоторые интеграторы начинают декларировать как устойчивое правило. И вот уже Tier III+ сплошь и рядом появляется в ТЗ. По сути дела, получается, что никем не описанный термин возводится чуть ли не в ранг национального стандарта «де-факто».

Иногда он расшифровывается, иногда — нет. Да и расшифровка его имеет множество вариаций. Это ведет к профанации профессионального подхода, к утверждению игры без правил.

На наш взгляд, исправлять ситуацию необходимо сразу по двум направлениям. Во-первых, необходимо отказаться от лишнего

■ **Рисунок. Сопровождение проекта Uptime Institute. Сертификация проектной документации и инженерной инфраструктуры ЦОД.**

смысла термина, который каждый волен толковать на свой вкус или ради своей выгоды. Во-вторых, надо не просто признать, что выход за рамки определенного уровня Tier в ряде случаев необходим, но и четко, скрупулезно анализировать

ситуацию заказчика и фиксировать полученные отклонения в ТЗ в виде дополнительных требований. Подчеркнем: дополнительных требований, отдельных от базовых требований заданного уровня отказоустойчивости Tier.

Носители знаний

В последнее время внимание к дата-центрам возросло, наблюдается устойчивая тенденция к увеличению потребности в независимом аудите проектов и функционирующих ЦОД. Мы прогнозируем, что в России эта тенденция ярко проявится уже в текущем году: переломным моментом станет появление первых сертифицированных коммерческих дата-центров. Арендаторы станут более внимательны к уровню отказоустойчивости ЦОД, что инициирует их сертификацию.

Несмотря на заключение ряда партнерских соглашений, Uptime Institute никому не передает право сертификации ЦОД. Однако очевидно, что обеспечить все сертификационные проекты в мире силами собственного персонала Институт будет не в состоянии. Поэтому в нем разработан и реализуется курс обучения и сертификации специалистов в области проектирования дата-центров на звание Accredited Tier Designer. Курсы организованы сравнительно недавно, поэтому сертифицированных разработчиков уровней инфраструктуры в мире пока насчитывается немного, а в России на сегодняшний день таких специалистов всего одиннадцать, причем все они работают в Москве. Полученный статус ATD подтверждает компетенцию в области разработки уровней инфраструктуры ЦОД в соответствии с принятой во всем мире классификацией Tier I, II, III и IV. Вполне вероятно, что в недалеком будущем Uptime Institute инициирует развитие сети региональных партнеров, и этим специалистам в дальнейшем может быть делегировано право сертификации ЦОД.

Учитывая наметившиеся тенденции и имея в своем штате сертифицированных по международным системам ATD и CDCD (Certified Data Centre Design) специалистов по проектированию и созданию ЦОД, компания «Энвижн Групп» предлагает услуги по аудиту и сертификации центров обработки данных. Мы готовы к созданию ЦОД требуемого уровня отказоустойчивости как на территории России, так и в странах СНГ, привлекая к совместной работе партнеров Uptime Institute Professional Service, а также аналитиков и консультантов из-за рубежа. ◀