В поисках безотказности

Александр КАЛИГИН

Важнейшим показателем надежности дата-центра является отказоустойчивость. Международные организации разработали типовые рекомендации, позволяющие клиентам подобрать ЦОДы, отвечающие требованиям по этому параметру. С целью повышения не только отказо-, но и катастрофоустойчивости некоторые компании создают географически распределенную сеть дата-центров, а другие игроки заключают между собой договоры о взаимном резервировании данных.

Отказоустойчивость определяет уровень надежности дата-центра. В свою очередь, отказоустойчивость ЦОДа во многом зависит от показателей доступности и надежности его инженерной и ИТ-инфраструктуры, а также от степени защищенности данных. По мнению технического директора ЗАО «Караван-Телеком» (телекоммуникационная компания Caravan) Дмитрия Канаева, эти показатели помогают оценить способность дата-центра эффективно решать бизнес-задачи того или иного заказчика.

По словам руководителя отдела инженерных систем ООО «ЛАНИТ-Интеграция» (ГК «ЛАНИТ») Юрия Гурковского, для обеспечения отказоустойчивости необходимо организовать резервирование каждой системы или ее компонентов, чтобы в случае их выхода из строя резервный элемент выполнил функции неисправного, а линии связи и электроснабжения дублируются и разводятся по разным маршрутам. «Соблюдение этих требований необходимо независимо от того, кто является клиентом дата-центра и какие задачи он решает», – считает Юрий Гурковский.

Всегда требуй «да»

Основным критерием отказоустойчивости для заказчиков является минимальное время простоя оборудования, которое напрямую влияет на непрерывность бизнеса. По опыту генерального директора ООО «Дата-Спейс Партнерс» (DataSpace) Сергея Рассказова, требования к отказоустойчивости определяются уровнем зависимости бизнес-процессов предприятия от ИТ-инфраструктуры и ИТ-систем. Например, в компаниях, где информационные технологии являются конкурентным преимуществом, а ключевые операционные процессы – составной частью ИТ-инфраструктуры, любые простои ведут к финансовым потерям, которые могут исчисляться шести- и семизначными цифрами. «Наиболее чувствительны к простоям финансовые компании, банки, биржи, телекоммуникационные операторы. При оценке возможных рисков, которые связаны с надежностью ИТ-инфраструктуры и отказоустойчивостью ЦОДа, такие клиенты предъявляют очень высокие требования и определяют их соглашением об уровне сервиса», – комментирует Сергей Рассказов.

Руководитель направления ЦОД ЗАО «Астерос» Станислав Терешкин уточняет, что обычно клиенты определяют, какой уровень отказоустойчивости дата-центра им необходим. На основании этого разрабатываются технические решения, которые должны быть применены в том или ином проекте. Параметры отказоустойчивости ЦОДа описаны в отраслевых документах, которые периодически корректируются, но в целом идеология остается неизменной. Станислав Терешкин приводит в пример стандарт независимого поставщика консалтинговых услуг, сертификации и обучения в области ЦОДов Uptime

Уровни отказоустойчивости инфраструктуры ЦОДа по рекомендациям Uptime Institute

Стандарт	Уровень отказоустойчивости (%)	Время простоя (часов в год)	Схема резервирования
Tier I	99,671	28,8	**N.** Ни одна из систем не резервируется, и простой каждой единицы оборудования приводит к простою всего ЦОДа
Tier II	99,749	22,0	**N+1.** К N единицам оборудования добавляется одна резервная, что уменьшает риск выхода ЦОДа из строя
Tier III	99,982	1,6	**N+1** с возможностью одновременного проведения профилактических работ
Tier IV	99,995	0,4	**2(N+1).** Каждый элемент системы N+1 дублируется аналогичным

Источник: Uptime Institute

Фото: «Ростелеком»

Начальник отдела управления внедрением и сопровождением решений ПАО «Ростелеком» Валерий Гущин полагает, что стремление клиента к повышенному уровню отказоустойчивости часто возникает в отрыве от вопросов стоимости

Фото: Delta Electronics

Руководитель направления ЦОД подразделения MCIS компании Delta Electronics в регионе EMEA Дмитрий Гуляев сожалеет, что до сих пор не существует единого российского ГОСТа, где были бы определены требования к ЦОДам

Institute, который, по его мнению, является объективным критерием для сравнения функциональности, работоспособности и производительности инфраструктуры ЦОДов.

Некоторые компании предпочитают строить собственные ЦОДы. Директор департамента развития сетей и платформ ОАО «Московская телекоммуникационная корпорация («КОМКОР», торговая марка «АКАДО Телеком») Илья Астахов отмечает, что, как правило, этим занимаются самые крупные игроки рынка. Для остальных компаний более рациональным и экономически выгодным является использование возможностей стороннего дата-центра, качество услуг которого соответствует их требованиям. «Создать надежное отказоустойчивое решение в комплексе с системами информационной безопасности под силу только компании, для которой владение ЦОДом является основным бизнесом», – уверен Илья Астахов.

Генеральный директор ООО «Миран» Игорь Ситников сетует, что требования заказчиков и реальное предложение ЦОДов не всегда равноценны. По его наблюдениям, клиент часто требует 100% отказоустойчивости, но обычно не отдает себе отчета в том, что в реальности нужно сделать, чтобы получить 99% и хотя бы несколько девяток после запятой.

Старший эксперт отдела развития инфраструктуры ЦОДов и тестовых сред ПАО «Мобильные ТелеСистемы» (МТС) Роман Петрухин сообщил корреспонденту «Стандарта», что одним из главных условий заказчиков является уровень доступности инженерных систем и телекоммуникационных сервисов с суммарным временем отказов не более 1,6 часа в год. Это соответствует категории отказоустойчивости ЦОДа Tier III по классификации Uptime Institute. Требование касается как архитектурных особенностей систем ЦОДа, так и организационной составляющей: наличия круглосуточной инженерной дежурной смены, охраны, контрактов с поставщиками топлива для дизель-электростанций и многого другого.

В разных корзинах

Обеспечение отказоустойчивости традиционно подразумевает резервирование всех систем внутри дата-центра. Руководитель ЦОДа Linxdatacenter ООО «Связь ВСД» Тарас Чирков подчеркивает, что в случае угрозы какого-либо внешнего воздействия на ЦОД, например стихийного бедствия, речь должна идти о катастрофоустойчивости и репликации на уровне нескольких дата-центров, однако данный аспект никак не стандартизирован, и необходимость организации такого решения определяется заказчиком в зависимости от его потребностей.

По словам Тараса Чиркова, случаи, когда дата-центр выходит из строя полностью, встречаются крайне редко, поэтому для надежного хранения данных будет достаточно одного ЦОДа с высоким уровнем отказоустойчивости. Однако наличие нескольких дата-центров со взаимной репликацией информации позволяет распределить нагрузку и не требует поддержания высоких стандартов отказоустойчивости отдельного объекта. Нет смысла создавать сложную инфраструктуру резервирования в рамках одного ЦОДа, когда данные надежно реплицируются в другом центре.

По словам директора Санкт-Петербургского филиала ООО «СДН» (Stack Data Network, SDN) Андрея Елисеева, географическая распределенность повышает коэффициент доступности дата-центров до 99,995%, исключая риск фатальной потери инфраструктуры в случае катастроф регионального характера. По его данным, сотрудничество провайдеров – общепринятая практика, так как не все российские операторы дата-центров успели создать географически распределенные сети ЦОДов.

По опыту Сергея Рассказова, кооперация между ЦОДами разных провайдеров, особенно если они географически разнесены, – это стандартная практика. Он уточняет, что, с одной стороны, логично, когда компания является оператором как основного ЦОДа, так и резервного. С другой стороны, некоторые клиенты видят риск в таком сценарии хранения данных и стремятся заключить контракт на резервирование дата-центра у другого провайдера.

Однако генеральный директор DataSpace предостерегает, что географическая разнесенность основного и резервного дата-центров больше чем на 150-200 км влечет сложности с обеспечением репликации данных в режиме реального времени и проблему оперативного перераспределения нагрузки в случае отключения одного из дата-центров. Он добавляет, что существует и так называемый подход active/active, предусматривающий создание инфраструктуры в двух ЦОДах, которые могут иметь более низкие показатели по отказоустойчивости, но при этом быть синхронизированы между собой. В этом случае высокая отказоустойчивость достигается за счет двух активных площадок. «Недостаток этой конфигурации заключается в том, что фактически приходится дублировать всю инфраструктуру, что влечет более высокие капитальные затраты и необходимость наличия двух команд обслуживания», – поясняет Сергей Рассказов.

Начальник отдела корпоративных систем дирекции инфраструктурных и телекоммуникационных решений ЗАО «Астерос» Дмитрий Крупнин отмечает, что в ряде случаев размещение компонентов вычислительной инфраструктуры в дата-центрах, разнесенных по разным регионам, недопустимо в принципе – например, из-за качества каналов связи, требований внутренней безопасности или специфики работы сервисов.

Директор ЦОДа «Траст-Инфо» ООО «Сервионика»

Фото: «Астерос»

Начальник отдела корпоративных систем дирекции инфраструктурных и телекоммуникационных решений ЗАО «Астерос» Дмитрий Крупнин отмечает, что в ряде случаев размещение компонентов вычислительной инфраструктуры в дата-центрах, разнесенных по разным регионам, недопустимо в принципе

Фото: «Инженерные системы и сервис»

Заместитель генерального директора ЗАО «Инженерные системы и сервис» Михаил Поляков утверждает, что заказчики и инвесторы очень взвешенно подходят к формированию требований к отказоустойчивости, поскольку это влияет на стоимость владения корпоративным дата-центром или услуг коммерческого ЦОДа

(ГК «Ай-Теко») Михаил Луковников заявляет, что современные ЦОДы обладают высочайшим уровнем доступности и отказоустойчивости, однако существуют факторы, способные повлиять на предоставление сервисов из ЦОДа, расположенного в конкретном месте. По его мнению, использование второй площадки существенно увеличивает отказоустойчивость сервисов, но приводит к значительному росту стоимости решения для клиента. «Если для бизнеса заказчика критична и недопустима приостановка предоставления сервисов, то наличие нескольких площадок, которые могут обеспечить их работу и обладают актуальным набором данных, – абсолютно правильное решение», – утверждает Михаил Луковников.

Облачные вычисления и распределенность ЦОДов по разным регионам России позволяют не только повысить отказоустойчивость, но и снизить эксплуатационные расходы на электроэнергию. Руководитель направления ЦОД подразделения MCIS компании Delta Electronics в регионе EMEA Дмитрий Гуляев приводит пример, когда вычисления для Московского региона днем могут производиться в дата-центре, размещенном там, где в это время ночь, тем самым позволяя пользоваться более дешевым ночным тарифом на электроэнергию. Такая территориальная схема зачастую применяется в государственных структурах.

Как правило, инициаторами обеспечения георазпределенности выступают клиенты дата-центров. По опыту Игоря Ситникова, в большинстве случаев они арендуют мощности в разных компаниях, не слишком это афишируя. «Если же им интересна работа через одно окно, то большинство дата-центров имеют партнерские отношения друг с другом. У нашей компании такие договоренности и практика есть», – сообщил генеральный директор «Мирана».

SDN также предоставляет заказчикам подобные услуги. Андрей Елисеев уточняет, что это индивидуальные решения, которые разрабатываются с учетом специальных требований заказчика.

ПАО «Ростелеком» обладает развитой сетью распределенных ЦОДов, способной обеспечить полное резервирование клиентских данных. «Тем не менее по требованиям клиентов в отдельных случаях мы сотрудничаем с другими поставщиками для целей резервирования. Также достаточно часто наши мощности используются как резервные для корпоративных ЦОДов», – говорит начальник отдела управления внедрением и сопровождением решений ПАО «Ростелеком» Валерий Гущин.

ООО «Юлмарт РСК» использует модель централизованных вычислений, поэтому требования, предъявляемые компанией к надежности ЦОДов, крайне высоки. «Для обеспечения отказоустойчивости «Юлмарт» использует несколько коммерческих ЦОДов. В соответствии с нашими стандартами их надежность должна быть не ниже 99,99%», – сообщил корреспонденту «Стандарта» директор управления информационных технологий компании «Юлмарт РСК» Павел Чекель.

Онлайн-кинотеатр ООО «ТиВиЗавр» (TVzavr.ru) также пользуется услугами нескольких ЦОДов. По словам генерального директора компании Марины Сурыгиной, это позволяет пользователям сервиса смотреть видео без задержек в любом уголке страны, а также в Белоруссии и на Украине.

Директор по информационной безопасности Qiwi plc Кирилл Ермаков отметил, что сотрудничество с несколькими коммерческими дата-центрами удобно с точки зрения действующих в компании требований к безопасности хранения данных. С учетом принципа географической распределенности два дата-центра Qiwi расположены в разных районах Москвы.

Стандартные схемы

Универсальным инструментом для оценки отказоустойчивости дата-центра является классификация Uptime Institute, которая устанавливает четыре уровня надежности ЦОДов – Tier I, Tier II, Tier III и Tier IV, – отражающие разную зависимость бизнеса от ИТ-процессов. Каждому уровню соответствует набор технологических требований, в частности к отказоустойчивости. По словам Дмитрия Канаева, она определяется несколькими параметрами: длительностью простоя дата-центра за год, его доступностью, планируемыми остановками, возможностью обслуживания без отключения, оптимальным уровнем загрузки оборудования и максимальным количеством аварий за год.

Чем сильнее доходы компании зависят от ИТ, тем выше будут ее требования к отказоустойчивости и надежности ЦОДа. «Например, владельцы небольших интернет-сайтов скорее предпочтут ЦОДы Tier I и II. Для них гарантии безостановочности бизнеса менее значимы, чем для крупных интернет-проектов – известных поисковых систем, порталов операторов сотовой связи, ресурсов информагентств, для которых простой даже в 20-25 минут в течение года может обернуться огромными убытками. Крупные игроки делают выбор в пользу ЦОДов Tier III и IV», – говорит технический директор телекоммуникационной компании Caravan.

Генеральный директор дата-центра BSTelecom ООО «Компания «БС-Телеком» Павел Кулаков отмечает, что большинство клиентов предъявляют требования на соответствие стандарту Tier III. Это предполагает наличие у дата-центра отдельно стоящего здания и периметра безопасности, подключение площадки посредством двух городских энерговводов от разных подстанций. Инженерная инфраструктура должна соответствовать схемам резервирования

N+1 (к N единицам оборудования добавляется одна резервная) и 2N (каждая единица оборудования дублируется) для различных систем с показателями надежности на уровне 99,982%.

Uptime Institute формирует лишь общие требования к проектированию, строительству и эксплуатации площадки. Павел Кулаков обращает внимание, что для заказчика это необходимое, но не достаточное условие для размещения и хранения данных в том или ином коммерческом дата-центре. Он поясняет, что в зависимости от задачи, реализуемой клиентом, акцент делается на дополнительные параметры: например, наличие нескольких магистральных интернет-стыков, помещений для круглосуточного размещения персонала и даже близость к метро. «У каждого клиента свои приоритеты и ожидания, выходящие за рамки рекомендаций Uptime Institute», – уточняет руководитель BSTelecom.

Тарас Чирков из Linxdatacenter также наблюдает, что большинство клиентов предъявляют требование о соответствии коммерческих дата-центров уровню Tier III. По его словам, это подразумевает набор определенных параметров, причем какая-либо дополнительная кастомизация не требуется. «ЦОД – это сложный инженерный проект, и если у клиента возникает необходимость какой-то небольшой модернизации, то подобное решение может быть реализовано. Если же речь идет о более радикальных конструктивных изменениях, то они крайне маловероятны, да и не нужны, ведь если заказчика не устраивает отказоустойчивость ЦОДа, то он вряд ли вообще его выберет», – полагает Тарас Чирков.

По мнению Сергея Рассказова, стандарты Uptime Institute максимально учитывают наиболее распространенные требования клиентов, что существенно снижает необходимость кастомизации. Он подчеркивает, что сертификация Uptime Institute дает независимый взгляд на проектирование, строительство и эксплуатацию дата-центра и гарантирует, что прошедший ее ЦОД соответствует стандартам в конкретных категориях: Design, Constructed Facility и Operational Sustainability.

Требования к отказоустойчивости дата-центров определяются не только рекомендациями Uptime Institute. Параллельно существует стандарт ANSI TIA/EIA-942 (TIA-942), разработанный и утвержденный комитетами American National Standards Institute (ANSI), Telecommunications Industry Association (TIA) и Electronics Industry Association (EIA), который содержит рекомендации по созданию инженерных систем для достижения отказоустойчивости, а также регламентирует условия размещения ЦОДа на местности во избежание чрезвычайных ситуаций природного и техногенного характера.

Однако не все участники рынка считают целесообразным ориентироваться только на стандарты, разработанные зарубежными организациями. Дмитрий Гуляев из Delta Electronics сожалеет, что до сих пор не существует единого отечественного ГОСТа, где были бы определены требования к ЦОДам.

С ним солидарен и Андрей Елисеев из SDN, отметивший, что в стране не разработаны стандарты, которые бы основывались на российских реалиях и требованиях к организациям как частной, так и государственной формы собственности.

«Единых стандартов нет, и говорить можно разве что о лучшей практике», – заявляет менеджер по продукции направления «Качественное электропитание» компании Eaton в России Сергей Амелькин. По его словам, единого показателя надежности, актуального для любого варианта дата-центра, не существует и, чтобы его определить,

Замах на битрубль

Фото: СТАНДАРТ

Новость об изобретении Qiwi plc российской национальной криптовалюты – битрубля – многозначна. Менеджеры Qiwi, утверждающие, что смогут выпустить битрубли уже в 2016 году, раскручивают очень горячую и актуальную сейчас тему. В июле этого года президент Владимир Путин дал понять, что в будущем будет возможно использовать в некоторых расчетах биткоины. Российский Центробанк последовательно выступает против любых суррогатов денег. А пока в России судят и рядят, что делать с этим добром, девять крупнейших инвестбанков – Goldman Sachs, JPMorgan, Credit Suisse, Barclays, Commonwealth Bank of Australia, State Street, RBS, BBVA и UBS – объявили о создании профильного совместного предприятия. Оно займется стандартизацией технологии blockchain (одним из побочных продуктов ее применения может быть и криптовалюта). Технология, позволяющая отслеживать любые изменения в разного рода реестрах и хранить данные об этом на распределенных компьютерах, без единого центра управления, обещает, по мнению экспертов, революцию в банковском деле.

Таким образом, у пока не родившегося битрубля есть еще и идеологическая подоплека. Он не просто идеально ложится в контекст импортозамещения в сфере ИТ, за которое так ратует Минкомсвязи, но и расширяет его. Зачем переходить с импортных программ и оборудования на отечественные, если можно сразу начать торговать деньгами, пусть даже виртуальными и даже почти криминальными, по мнению Центробанка? Однозначно это патриотично: на рынке теневых расчетов российская криптовалюта может потеснить биткоин, придуманный то ли японцами, то ли не японцами, ну, в общем, где-то в странах – потенциальных противниках.

Разница между биткоином и битрублем в том, что первый видится как технология, призванная поднять на новый уровень и без того высокотехнологичную мировую финансовую систему, а о битрублях, похоже, начали говорить тогда, когда кое у кого обычных бумажных рублей стало меньше. Очевидно, что платежным терминалам, бывшим до относительно недавнего времени основным бизнесом Qiwi, в России сейчас неуютно. Как показало исследование J'Son & Partners Consulting, оборот платежей через них в 2014 году вырос всего на 5%: темпы роста год к году снизились втрое. Видно, терминалы не выдерживают конкуренции с традиционными банковскими сервисами, мобильными платежными приложениями, электронными деньгами и т. д. и т. п. А борьба Центробанка с обналичиванием привела к тому, что к началу сентября 2015 года в стране перестали принимать платежи 35-40% терминалов, говорил ранее «Ведомостям» топ-менеджер одной из российских платежных систем. В остальных же, по его словам, комиссия при оплате стала от 3% до 10%.

Выходит, что такое стечение обстоятельств удачно, но не для отечественной криптовалюты и не для бизнеса Qiwi, а для привлечения внимания к компании, то есть, попросту говоря, для пиара. Что ставит битрубль в один ряд с «русскими айфонами», наномойками и другими знаковыми достижениями российских высоких технологий, за которые неудобно перед иностранцами.

Валерий Кодачигов,
корреспондент отдела «Технологии и телекоммуникации» газеты «Ведомости», специально для «Стандарта»

Фото: Eaton

Менеджер по продукции направления «Качественное электропитание» компании Eaton в России Сергей Амелькин убежден, что единого показателя надежности, актуального для любого дата-центра, не существует и, чтобы его определить, нужно учитывать множество факторов

Фото: «ЛАНИТ-Интеграция»

Руководитель отдела инженерных систем ООО «ЛАНИТ-Интеграция» Юрий Гурковский поясняет, что для обеспечения отказоустойчивости необходимо резервирование каждой системы ЦОДа или ее компонентов

нужно учитывать множество факторов.

В конце 2013 года несколько участников российского рынка дата-центров создали Ассоциацию участников отрасли центров обработки данных, одной из основных целей которой должно было стать формирование системы национальных отраслевых стандартов в области строительства и эксплуатации ЦОДов. 14 сентября 2014 года Федеральное агентство по техническому регулированию и метрологии (Росстандарт) издало приказ №1333 «О создании технического комитета по стандартизации «Центры обработки данных». Данный комитет (ТК120) был создан на базе Ассоциации. Но он в первую очередь фокусируется на стандартизации процессов создания ЦОДов, а разработкой отечественных стандартов отказоустойчивости дата-центров в ближайшем будущем заниматься не планирует.

С перламутровыми пуговицами...

Для оценки отказоустойчивости ЦОДа большинству потенциальных клиентов достаточно данных, подтверждающих соответствие стандарту Uptime Institute. Но, по опыту Дмитрия Канаева, некоторые организации с развитой ИТ-инфраструктурой могут предъявлять и более высокие требования к надежности дата-центра. Это выражается, например, в необходимости организовать мониторинг зоны размещения оборудования, видеонаблюдение или многоуровневый контроль доступа к ней, обеспечить несколько недорогих каналов доступа от независимых провайдеров или создать в зале ЦОДа отдельное помещение под стойки с независимым инженерным комплексом. «Решения, отвечающие стандарту Uptime Institute, дорабатываются с учетом индивидуальных потребностей таких заказчиков», – уточняет Дмитрий Канаев.

Зачастую в технических заданиях от клиентов появляются требования к отказоустойчивости по уровню Tier II+ или Tier III++. Это дополнительные требования заказчиков, которые опираются на стандарты Uptime Institute. Юрий Гурковский из ГК «ЛАНИТ» поясняет, что знаки «плюс» в данном случае означают мелкие улучшения, которые, иногда вопреки ожиданиям клиента, никак не влияют на отказоустойчивость.

«Заказчику необходимо убедиться в реальной, а не заявленной и даже подтвержденной сертификатами надежности, а это возможно сделать, только отследив историю эксплуатации ЦОДа», – утверждает Павел Кулаков из BSTelecom. По его наблюдениям, клиенты предъявляют требования не столько к отказоустойчивости как решению, заложенному в проекте для инженерного оборудования, сколько к тем факторам, которые формируют отказоустойчивость в процессе работы. Например, к соблюдению регламента технического обслуживания, времени подвоза поставщиками дизельного топлива, внутренним приказам и процедурам, разработанным в ЦОДе для обеспечения бесперебойности, и многому другому.

Заместитель генерального директора ЗАО «Инженерные системы и сервис» («Инсистемс») Михаил Поляков отмечает, что заказчики и инвесторы очень взвешенно подходят к формированию требований к отказоустойчивости, поскольку это напрямую и в значительной мере влияет на стоимость владения корпоративным дата-центром или услуг коммерческого ЦОДа.

«Некоторые заказчики изначально предъявляют сверхвысокие требования к отказоустойчивости. Почти всегда мы работаем с готовой инфраструктурой клиента и сталкиваемся с разнообразным набором платформ и приложений», – рассказывает Дмитрий Крупнин. Поэтому, по его словам, первичной задачей, которую необходимо решить представителю дата-центра совместно с заказчиком, является расстановка приоритетов: составление списка сервисов по степени критичности, выделение взаимосвязанных сервисов в группы и формирование значений RTO (recovery time objective, допустимое время простоя сервиса в случае сбоя) и RPO (recovery point objective, допустимый объем возможных потерь данных). Представитель «Астероса» сообщил, что часто на этом этапе у заказчика возникает желание зафиксировать параметры RTO и RPO как нулевые, но после объяснения принципа работы средств обеспечения отказоустойчивости и оценки стоимости этих решений, как правило, достигается компромисс между требованиями клиента и возможностями ЦОДа.

По мнению Михаила Луковникова из ГК «Ай-Теко», заказчики понимают, что завышенные требования приводят к существенному увеличению затрат. Каждая девятка после запятой в характеристике отказоустойчивости приводит к увеличению затрат на порядок. «В большинстве случаев мы имеем дело с обоснованными требованиями для каждого конкретного случая. Иногда они очень специфические, но так или иначе имеют под собой основание», – говорит он.

Валерий Гущин из «Ростелекома» полагает, что стремление клиента к повышенному уровню отказоустойчивости часто возникает в отрыве от вопросов стоимости. Как только уровни обслуживания различаются по цене, заказчик понижает первоначальные требования.

Если компания требует технически и организационно невозможного – предоставить высокую надежность по низкой стоимости – и получает это, значит, ЦОД или лукавит, или ведет демпинговую политику, которая рано или поздно заканчивается», – заверяет Игорь Ситников из «Мирана».