

Что обеспечивает надежность ЦОД сегодня и какими они будут в будущем

Мнения экспертов

Редакция журнала "Системы безопасности" подготовила несколько вопросов о наиболее распространенных рисках непрерывной работы ЦОД, выборе инженерного или ИТ-решения, автоматизации ЦОД, дефиците мощностей, законодательной практике и будущем дата-центров. В заочном круглом столе приняли участие независимый эксперт Дмитрий Окишев, представители НВП "Болид", бренда ABSolite, ООО "ЦОДУМ", ООО "ЭнергоТех" и компании Octagram.



Дмитрий Окишев
Независимый эксперт



Александра Симонова
Инженер
АО НВП "Болид"



Павел Нарнов
Технический эксперт
бренда ABSolite

В чем чаще всего кроются риски для непрерывной работы ЦОД: в технике, кадрах, других факторах?

Дмитрий Окишев, независимый эксперт

Наиболее важным является не работоспособность ЦОД как такового, а доступность вычислительных мощностей, программ и сред, а также самих данных, размещенных в ЦОД. В частности, во время блэкаута во Владивостоке ЦОД Tier III остался рабочим и не прерывал предоставление сервисов и услуг, однако часть каналов связи была потеряна и клиенты, которые не резервировали должным образом каналы связи, на время потеряли доступ к своим данным.

Но если рассматривать отдельный ЦОД как часть общей системы и сосредоточиться только на его надежности, то я бы выделил именно процедуры работы (штатные и аварийные), а также команду (кадры).

Обращаю внимание на следующий тезис: при должном уровне проекта и его реализации хорошая команда эксплуатации способна обеспечить надежность площадки и на бюджетном оборудовании с заурядными характеристиками, но даже лучшее оборудование без должного сервиса и эксплуатации рано или поздно "уйдет в аварию".

Последний год внес существенные изменения в оценку рисков: если ранее вероятность повреждения ЦОД в результате террористической деятельности оценивалась как маловероятная и приравнивалась к стихийным бедствиям, то летом из-за атак на НПЗ и логистику об этих рисках заговорили уже серьезно.

Александра Симонова, НВП "Болид"

Чаще всего – в инженерной инфраструктуре (сбои электропитания, охлаждения, пожаротушения): даже при надежном железе отказ этих систем останавливает ЦОД. Кадры тоже критичны: нехватка квалифицированных инженеров и ошибки при эксплуатации усиливают риски. Важны и внешние факторы: аварии на сетях, кибератаки, природные ЧС. Это потому, что ЦОД – единый контур: отказ любого ключевого звена ломает всю цепочку бесперебойности.

Павел Нарнов, бренд ABSolite

Основной источник рисков – люди и организационные процессы, а не техника. Ошибки персонала, недостаток квалификации, переработки и усталость – самые частые причины сбоев. Технические риски, хотя и остаются значимыми, лучше поддаются управлению. Внешние факторы – перебои с энергоснабжением, ограничения поставок, регуляторное давление также влияют на непрерывность. Главный риск не оборудование, а человеческий фактор и качество рабочих процессов.

Константин Струлев, ЦОДУМ

Риски для непрерывной работы ЦОД сегодня чаще кроются не в отдельном оборудовании, а на стыках техники, процессов и действий людей. Современная инженерная инфраструктура изначально строится с резервированием, поэтому отказ одного элемента сам по себе далеко не всегда приводит к аварии. Гораздо опаснее ситуация, когда персонал не видит полной картины: резерв формально существует, но недоступен; оборудование работает близко к пределу; регламентное обслуживание отложено; изменение в одной системе неожиданно влияет на другую.

Поэтому человеческий фактор я бы тоже не сводил к "ошибке оператора". Человек часто ошибается потому, что принимает решение по неполным или устаревшим данным. По мере усложнения ЦОД главным фактором надежности становится качество управления инфраструктурой: насколько точно известны ее текущее состояние, реальные резервы, зависимости между системами и последствия каждого действия. Чем лучше эта информация собирается и анализируется автоматически, тем меньше вероятность, что локальная проблема превратится в остановку сервиса.

Кирилл Шадский, HIGH ENERGY

Я бы не сводил риски непрерывной работы ЦОД к какому-то одному фактору. ЦОД – это сложный живой организм, где надежность формируется не в отдельной системе, а во взаимосвязи решений, людей и процессов на протяжении всего жизненного цикла объекта. Отказ железа или ошибка инженера сами по себе редко становятся первопричиной, чаще всего это следствие более глубокой проблемы. Техника, безусловно, критична: электроснабжение, охлаждение, системы мониторинга образуют единую цепочку. Парадокс в том, что даже топовое оборудование и сильнейшая команда не компенсируют отсутствие процессной культуры. Поэтому главный риск не отдельный отказ, а разрыв между этапами и участниками проекта. Когда проектировщик, генподрядчик, поставщик и эксплуатирующая организация работают без единой логики, локальная проблема может перерасти в остановку. Надежность ЦОД рождается там, где выстроен целостный процесс. Именно он превращает технику, кадры и инженерные системы в единый механизм непрерывной работы.

Александр Орлов, Octagram

Главная угроза непрерывной работе ЦОД кроется не столько в отдельных отказах оборудования, сколько во фрагментации инженерной инфраструктуры. Когда системы контроля доступа, охранно-пожарная сигнализация и сбор телеметрии работают на разнородных аппаратных платформах от разных вендоров, возникают информационные слепые зоны. Усложняется корреляция событий, растет время диагностики, повышается вероятность ошибки персонала, вынужденного работать в нескольких интерфейсах одновременно. Решение – переход к унифицированным программно-определяемым контроллерам. Единый аппаратный уровень, способный выполнять функции разных систем, минимизирует точки отказа, упрощает логистику запчастей и резко снижает квалификационные требования к линейному персоналу. Кадры при таком подходе становятся фактором надежности, а не источником риска.



Константин Струлев
Руководитель
ООО "ЦОДУМ"



Кирилл Шадский
Директор департамента инфраструктуры
ЦОД компании HIGH ENERGY
(ООО "ЭнергоТех")



Александр Орлов
Инженер СКД
компании Octagram

На что ориентируются заказчики при выборе инженерного или ИТ-решения для ЦОД в первую очередь?

Дмитрий Окишев, независимый эксперт

Тяжелая экономическая ситуация и высокие ставки по кредитам заставляют всех частных заказчиков очень внимательно считать финансы и активно искать варианты оптимизации. Но каждый заказчик – это индивидуальный клубок приоритетов, опыта и исторических ограничений, поэтому пазл для каждого свой.

Для объектов с государственным финансированием частым условием выступает реестр Минпромторга, но в текущей конфигурации, на мой взгляд, вреда от него больше, чем пользы.

Александра Симонова, НВП "Болид"

В первую очередь – на уровень отказоустойчивости (Tier III/IV), SLA по доступности и гарантированную мощность на стойку. Далее – на безопасность (физическую и информационную), связность (каналы, пиринг, облака) и прозрачность тарифов. Обусловлено это тем, что простой стоит дорого, а требования к защите данных и низкой задержке растут.

Павел Нарнов, бренд ABSolite

В первую очередь заказчики смотрят на совокупную стоимость владения, надежность и доступность, репутацию поставщика, гибкость и возможность избежать зависимости от одного вендора. Важны также масштабируемость и совместимость с существующей инфраструктурой. Такой подход обусловлен турбулентностью рынка: заказчики ищут баланс между производительностью, затратами на всем жизненном цикле и устойчивостью к внешним шокам.

Константин Струлев, ЦОДУМ

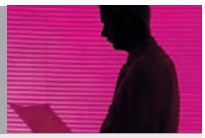
При выборе инженерного или ИТ-решения для ЦОД заказчик в первую очередь ориентируется на надежность, совместимость с существующей инфраструктурой и предсказуемость эксплуатации. Цена важна, но для критической инфраструктуры она редко бывает единственным или главным критерием: ошибка выбора может обойтись значительно дороже самой системы.

Поэтому все большее значение имеют не только технические характеристики, но и то, насколько решение понятно в эксплуатации, интегрируется с другими системами, масштабируется, обеспечивается поддержкой и не создает критической зависимости от одного поставщика или закрытой технологии. Отдельный фактор – наличие реального опыта внедрения в сопоставимых по масштабу и требованиям объектах.

По сути, заказчик старается минимизировать совокупный риск на всем жизненном цикле решения. Чем сложнее становится ЦОД, тем важнее смотреть не на отдельные характеристики оборудования или ПО, а на то, как решение будет работать внутри всей инфраструктуры через пять или десять лет.

Кирилл Шадский, HIGH ENERGY

Уход с рынка части производителей стал для отрасли серьезным вызовом и стимулировал поиск альтернатив. Сегодня можно уверенно сказать, что рынок стабилизировался. Во всех основных системах ЦОД есть выбор поставщиков должного уровня качества. И ориентир при выборе – это, конечно же, накопленный успешный опыт установки оборудования в крупных ЦОД, соответствие заявленных параметров,



НОВОСТЬ В ТЕМУ

За последние шесть лет мощность коммерческих ЦОД почти удвоилась

Электрическая мощность коммерческих центров обработки данных (ЦОД) России по итогам 2026 г. может вырасти на 10–12%. Этот показатель ниже значений предыдущих лет, но в дальнейшем возможен рост до 20%. Об этом рассказал член правления ассоциации участников отрасли центров обработки данных Михаил Саликов в ходе отраслевого вебинара.

"Если мы посмотрим на динамику по электрической мощности коммерческих центров обработки данных России, мы увидим, что за прошедшие шесть лет мощность существующих ЦОД практически удвоилась. Эта тенденция сохраняется, хотя динамика роста сейчас падает. Тем не менее мы рассчитываем, что в 2026–2027 гг. динамика роста будет в районе 10–12%, а в дальнейшем она ускорится и составит 18–20%", – сказал он.

Как следует из материалов Саликова к выступлению, в 2021 г. был зафиксирован пик увеличения электрической мощности коммерческих ЦОД на уровне 24%, до 555,5 МВт. В 2022 г. показатель составил 10% (610,7 МВт), в 2023 и 2024 г. – 13% и 22% соответственно. По итогам прошлого года рост составил 18% и достиг 990,6 МВт. В этом году мощность прогнозируется на уровне 1,1 ГВт.

По данным "Системного оператора", мощность подключенных к российской энергосистеме центров обработки данных и майнинга достигла 4,2 ГВт (по данным на апрель). За минувшие три года доля ЦОД в общей структуре электропотребления увеличилась в два раза: с 1,4% в 2022 г. до 2,2% в 2025 г. В 2026 г. доля ЦОД в структуре потребления электроэнергии возрастет по прогнозу до 2,4%. А в ближайшие пять лет совокупный объем потребляемой мощности центров высокотехнологичных вычислений может достичь 15,3 ГВт.

Ранее в "Системном операторе" поясняли, что мощность подключенных к сетям майнеров и центров обработки данных в РФ в 2025 г. составила 4 ГВт, что на 33,3% больше, чем в 2024 г.

Замминистра энергетики РФ Петр Конюшенко ранее заявил, что мощность "полезных" центров обработки данных в России оценивается в 1,7 ГВт. А согласно данным Правительства РФ, энергопотребление дата-центров в России к 2030 г. увеличится минимум в 2,5 раза и составит 2,5 ГВт. ■

Источник: www.tass.ru

наличие сервисной службы и гарантийная поддержка со стороны производителя. Референсы подтверждают, что решение выдержало реальную эксплуатацию, высокие нагрузки и требования к непрерывности.

При этом действует принцип "Доверяй, но проверяй". Успешный опыт не отменяет обязательных тестирований на всех этапах, в первую очередь непосредственно на производстве. Только так заказчик получает подтверждение, что оборудование приедет на площадку с реальными, а не декларированными характеристиками и готово к реальным условиям эксплуатации.

Александр Орлов, Octagram

В первую очередь заказчики ориентируются на совокупную стоимость владения (TCO) и отказоустойкость. Это обусловлено тем, что минута простоя ЦОД может стоить миллионы, поэтому приоритетом становится не просто набор функций, а возможность централизованного управления разнородными системами через единый интерфейс.

Второй ключевой фактор – масштабируемость без необходимости полной замены аппаратной части. Современные решения позволяют менять логику работы контроллеров путем обновления прошивки, что дает возможность адаптироваться к новым требованиям безопасности или интеграции нового оборудования без капитальных затрат на переработку всей инженерной сети. Критически важна также возможность сбора телеметрии в реальном времени по надежным проводным каналам – это основа для прогнозирования отказов и оптимизации энергопотребления.

Как дополнение в закон "О связи" повлияло на рынок ЦОД? Насколько в целом нормотворчество успевает за практикой эксплуатации современных ЦОД?

Дмитрий Окишев, независимый эксперт

Пока рано говорить о результатах, но я скорее расцениваю данную деятельность как лоббизм. Наше нормотворчество по определению не будет успевать за всеми технологиями, но попытки облегчить жизнь лицам, принимающим решения, для сравнения ЦОД неспециалистами по условному классификатору по сути своей или обречены на провал, или заморозят отрасль в группе описанных и закрепленных документом решений. Система госуправления провалов не допускает. Поэтому итог скорее всего будет где-то между "халатностью по незнанию" и "умышленным вредительством".

Александра Симонова, НВП "Болид"

Поправки в закон "О связи", вступившие в силу 1 марта 2026 г. закрепили требования к инфраструктурной устойчивости ЦОД (резервирование, отчетность по инцидентам, требования к энергоснабжению) и усилили контроль за размещением критической инфраструктуры. Рынок отреагировал ростом спроса на проекты с подтвержденным Tier и прозрачными SLA, удорожанием строительства из-за новых норм, а также консолидацией: мелкие игроки либо уходят, либо объединяются. Нормотворчество частично успевает за практикой, но часто фиксирует уже сложившиеся отраслевые стандарты, а не опережает технологические тренды (например, по высокоплотным стойкам под ИИ).

Константин Струлев, ЦОДУМ

С 1 марта 2026 г. ЦОД впервые получили полноценное определение в российском законодательстве, а для дата-центров появился государственный реестр и формализованные требования к его участникам. Для рынка это важный этап: отрасль фактически признана самостоятельным объектом регулирования, а вместе с этим появляются более понятные правила и критерии того, что государство определяет как ЦОД.

При этом нормотворчество неизбежно движется медленнее самой отрасли. Пока закрепляются базовые понятия и требования, эксплуатация уже сталкивается с высокой плотностью вычислений, дефицитом электроэнергии, новыми схемами охлаждения, автоматизацией и возрастающей взаимозависимостью инженерных и ИТ-систем.

Поэтому регулирование особенно полезно там, где оно задает единые требования к надежности, безопасности и ответственности, но опасно пытаться слишком подробно закрепить конкретные технические решения. Технологии ЦОД меняются быстрее нормативных документов, и правила должны оставлять пространство для их развития.

Александр Орлов, Octagram

Вступление в силу новых норм подчеркивает тренд на суверенитет данных и повышенную отказоустойчивость критической инфраструктуры. Для рынка это означает необходимость гарантированного хранения журналов событий и локализации ключевых узлов управления. Нормотворчество часто отстает от практики, поскольку иногда регламентирует устаревшие подходы, например требования к выделенным контроллерам для каждой подсистемы. Современная практика эксплуатации ЦОД требует гибкости: программно-определяемые платформы позволяют мгновенно адаптировать логику обработки данных под новые нормативные требования путем обновления ПО без физической замены аппаратного обеспечения. Это значительное преимущество в условиях быстро меняющегося регуляторного поля. Рынок выигрывает от перехода к универсальным решениям, которые закрывают задачи нескольких специализированных систем на одном аппаратном уровне.