Надежность инженерных систем ЦОД

Дата-центр *(от англ. data center), или центр (хранения) и обработки данных (ЦОД/ЦХОД) — это специализированное здание для размещения (хостинга) серверного и сетевого оборудования и подключения абонентов к каналам сети Интернет.*

Дата-центр исполняет функции обработки, хранения и распространения информации, как правило, в интересах корпоративных клиентов — он ориентирован на решение бизнес-задач путём предоставления информационных услуг. Консолидация вычислительных ресурсов и средств хранения данных в ЦОД позволяет сократить совокупную стоимость владения IT-инфраструктурой за счёт возможности эффективного использования технических средств, например, перераспределения нагрузок, а также за счёт сокращения расходов на администрирование.

Дата-центры обычно расположены в пределах или в непосредственной близости от узла связи или точки присутствия какого-либо одного или нескольких операторов связи. Качество и пропускная способность каналов влияют на уровень предоставляемых услуг, поскольку основным критерием оценки качества работы любого дата-центра является время доступности сервера (аптайм).

История

История развития дата-центров начинается с огромных компьютерных комнат времен зарождения компьютерной индустрии. Тогда компьютерные системы были сложнее в управлении и требовали обеспечения особых условий для работы. Так как они занимали много места и требовали множества проводов для подключения различных компонентов, в компьютерных комнатах стали применять стандартные серверные стойки, фальшполы и кабельные каналы (проложенные по потолку или под фальшполом). Кроме того, такие системы потребляли много энергии и нуждались в постоянном охлаждении, чтобы оборудование не перегревалось. Не менее важна была безопасность — оборудование весьма дорогостоящее и часто использовалось для военных нужд. Поэтому были разработаны основные конструкционные принципы по контролю доступа в серверные.

В период бурного развития компьютерной индустрии и особенно в 1980-е компьютеры начинают использовать повсеместно, не особенно заботясь об эксплуатационных требованиях. Но с развитием ИТ-отрасли, компании начинают уделять все больше внимания контролю ИТ-ресурсов. С изобретением архитектуры клиент-сервер в 1990-е, микрокомпьютеры, сейчас называемые серверами, стали занимать места в старых серверных. Доступность недорогого сетевого оборудования вместе с новыми стандартами сетевых кабелей сделали возможным использование иерархического проектирования, так серверы переехали в отдельные комнаты. Термин «дата-центр», в те времена применимый к специально спроектированным серверным, начал набирать популярность и становился все более узнаваем.

Бум дата-центров приходится на период 1995—2000 годов. Компаниям было необходимо устойчивое и высокоскоростное соединение с Интернетом и бесперебойная работа оборудования, чтобы разворачивать системы и устанавливать своё присутствие в сети. Разместить оборудование, способное справиться с решением этих задач, было делом непосильным для большинства небольших компаний. Тогда и началось строительство отдельных больших помещений, способных обеспечить бизнес всем необходимым набором решений для размещения компьютерных систем и их эксплуатации. Стали развиваться новые технологии для решения вопросов масштаба и операционных требований столь крупных систем.

В наши дни проектирование и строительство дата-центров — хорошо изученная область. Сформированы стандарты, устанавливающие требования для проектирования дата-центров. К примеру специалисты Telecommunications Industry Association внесли большой вклад в формирование стандартов для дата-центров. Но все же осталось ещё много нерешенных задач в методах работы, а также строительстве дата-центров, не наносящих вреда окружающей среде и т. д.

Дата-центры требуют больших затрат как на этапе строительства, так и в процессе обслуживания, для поддержания работы на должном уровне. К примеру, дата-центр Amazon.com в Орегоне, площадь которого равна 10, 800 кв.м, оценивается в 100 млн.$.

Структура

По соответствию требованиям стандартов

В ряде стран имеются стандарты на оборудование помещений дата-центров, позволяющие объективно оценить способность дата-центра обеспечить тот или иной уровень сервиса. Например, в США принят американский (ANSI) стандарт TIA-942, несущий в себе рекомендации по созданию дата-центров, и делящий дата-центры на типы по степени надёжности. Хотя в России пока нет такого стандарта, дата-центры оснащаются согласно требованиям для сооружений связи, а также ориентируются на требования TIA-942 и используют дополнительную документацию Uptime Institute и ГОСТы серии 34.

Фактически, TIA-942 воспринимается во всем мире как единый стандарт для дата-центров, однако следует отметить что он достаточно давно не обновлялся и его достаточно сложно применить в условиях России. В то же время сейчас активно развивается стандарт BICSI 002 2010 Data Center Design and Implementation Best Practices, появившийся в 2010 и обновленный в 2011. По словам создателей стандарта "стандарт BICSI 002 2010, в создании которого участвовали более 150 экспертов, дополняет существующие стандарты TIA, CENELEC и ISO/IEC для центров обработки данных". Каждый из стандартов, как правило имеет свою внутреннюю классификацию дата-центров по совокупности их параметров.

По размеру

- Крупные дата-центры имеют своё здание, специально сконструированное для обеспечения наилучших условий размещения. Обычно они имеют свои каналы связи, к которым подключают серверы.

- Средние дата-центры обычно арендуют площадку определённого размера и каналы определённой пропускной способности (обычно измеряется в Мбит/с).

- Малые дата-центры размещаются в малоприспособленных помещениях. Часто ими используется оборудование плохого качества, а также предоставляется самый минимум услуг.

- Контейнерные дата-центры. Стойки с оборудованием размещаются в стандартных ISO контейнерах размером 20 и 40 футов. Имеют преимущества т.к. могут перевозиться автомобильным и железнодорожным транспортом.

По надёжности

Основной показатель работы ЦОД — отказоустойчивость; также важна стоимость эксплуатации, показатели энергопотребления и регулирования температурного режима.

Например, стандарт TIA-942 предполагает четыре уровня надёжности дата-центров:

- **Tier 1 (N)** — отказы оборудования или проведение ремонтных работ приводят к остановке работы всего дата-центра; в дата-центре отсутствуют фальшполы, резервные источники электроснабжения и источники бесперебойного питания; инженерная инфраструктура не зарезервирована;

- **Tier 2 (N+1)** — имеется небольшой уровень резервирования; в дата-центре имеются фальшполы и резервные источники электроснабжения, однако проведение ремонтных работ также вызывает остановку работы дата-центра;

- **Tier 3 (N+1)** — имеется возможность проведения ремонтных работ (включая замену компонентов системы, добавление и удаление вышедшего из строя оборудования) без остановки работы дата-центра; инженерные системы однократно зарезервированы, имеется несколько каналов распределения электропитания и охлаждения, однако постоянно активен только один из них;

- **Tier 4 (2(N+1))** — имеется возможность проведения любых работ без остановки работы дата-центра; инженерные системы двукратно зарезервированы, то есть продублированы как основная, так и дополнительная системы (например, бесперебойное питание представлено двумя ИБП, работающими по схеме N+1).

По предназначению

Дата-центры по виду использования подразделяют на корпоративные, предназначенные для обслуживания конкретной компании, и коммерческие (аутсорсинговые), предоставляющие услуги всем желающим. Также разделяют провайдерозависимые и провайдеронезависимые дата-центры. Первые служат для обеспечения деятельности телекоммуникационных операторов, вторые могут использоваться разными компаниями в соответствии с их нуждами.

Услуги дата-центров

- **Виртуальный хостинг.** Крупные дата-центры обычно не предоставляют подобную массовую услугу из-за необходимости обеспечения технико-консультационной поддержки.

- **Виртуальный сервер.** Предоставление гарантированной и лимитированной части сервера (части всех ресурсов). Важная особенность данного вида хостинга — разделение сервера на несколько виртуальных независимых серверов, реализуемых программным способом.

- **Выделенный сервер.** Дата-центр предоставляет клиенту в аренду сервер в различной конфигурации. Крупные дата-центры в основном специализируются именно на подобных типах услуг.

- **Colocation.** Размещение сервера клиента на площадке дата-центра за определённую плату. Стоимость зависит от энергопотребления и тепловыделения размещаемого оборудования, пропускной способности подключаемого к оборудованию канала передачи данных, а также размера и веса стойки.

- **Аренда телекоммуникационных стоек.** Передача клиенту стоек для монтажа собственного или клиентского оборудования. Формально это частный случай colocation, но с основным отличием в том, что арендаторы в основном юридические лица.

- **Выделенная зона (Dedicatedarea).** В некоторых случаях владельцы дата-центра выделяют часть технологических площадей для специальных клиентов, как правило, финансовых компаний, имеющих строгие внутренние нормы безопасности. В этом случае дата-центр предоставляет некую выделенную зону, обеспеченную каналами связи, электроснабжением, холодоснабжением и системами безопасности, а клиент сам создает свой дата-центр внутри этого пространства.

Инженерные системы

Инженерная инфраструктура центров обработки данных представляет собой комплекс технических средств обеспечения доступа к вычислительным ресурсам. Это такие системы, как система бесперебойного электропитания, вентиляции и пожаротушения и т.д.

Инженерные системы дата-центра являются комплексной системой жизнеобеспечения и обеспечивают физическую безопасность вычислительных подразделений от стихийных бедствий, несанкционированного доступа, пожаров и наводнений.

Инженерная инфраструктура вычислительного комплекса еще на уровне проектирования ЦОД создается с учетом его будущего масштабирования и включает ряд резервных подсистем, в том числе обеспечивающих стабильную работу серверов и СХД, установленных в дата-центре. Она составляет большую часть себестоимости ЦОД, нередко доходя до 70%. При этом распределение затрат на подсистемы дата-центров неравномерно. Наибольшая доля, около трети всех потраченных финансовых ресурсов, приходится на стоимость системы гарантированного электропитания (34%). Также значительные траты предусматривают организация кондиционирования (21%) и архитектура самого здания (23%). На коммуникационные сети приходится 7% плюс еще около 9% на оборудование газового пожаротушения, систем управления доступом и видеонаблюдения и шкафную инфраструктуру. Наименьшую долю в крупных затратах составляет организация системы мониторинга (1%). Очевидно, что на три первых системы ложится подавляющая часть расходов (78%). Следовательно, можно добиться значительной экономии за счет их оптимизации.

При этом эксперты советуют не экономить на создании систем кондиционирования и рекуперации тепла, а уж тем более на системах безопасности и мониторинга. Основные направления оптимизации расходов должны быть направлены на создание эффективного обеспечения бесперебойного и гарантированного электропитания, а также на организацию компактной расстановки оборудования. Естественно, что эти работы должны проводиться только специалистами высокого уровня.

Расчет снижения себестоимости создания и эксплуатации ЦОД должен производиться еще на этапе его проектирования, хотя лучше озаботиться этим уже при формировании концепции.

Тщательная проработка на начальных этапах способов обеспечения отказоустойчивости и повышения времени автономной работы центра обработки данных обеспечивает успешное прохождение им необходимых процедур сертификации.

Требования к инженерной инфраструктуре ЦОД

Технологии не стоят на месте, и с течением времени создаются все более сложные информационные комплексы. Соответственно, ужесточаются нормативы, предъявляемые к инфраструктуре.

В современных ЦОД в одном помещении могут работать тысячи серверов с совокупным энергопотреблением до миллиона Вольт-Ампер. Критичность обрабатываемых ими процессов бывает такова, что любая остановка даст колоссальные финансовые потери. Например, всего 20 минут простоя процессинг-центра крупной телекоммуникационной компании приводит к убытку в 1 000 000 долларов США.

Поэтому инженерная инфраструктура ЦОД должна отвечать целому списку жестких требований, счет которых в техзаданиях идет на десятки. Вкратце можно свести их к следующим четырем направлениям:

Надежность

Достигается благодаря учету многих факторов. Это использование только современного оборудования ведущих мировых производителей, привлечение высококвалифицированных специалистов и резервирование основных узлов инженерной инфраструктуры. В общем, в эту группу входит все, что может гарантировать бесперебойное функционирование всех элементов ЦОД.

Управляемость

Управление системами инженерного обеспечения должно позволять своевременно прогнозировать все возможные сбои и поломки оборудования для заблаговременного предотвращения аварий.

Безопасность

Необходима тщательная проработка всех потенциальных угроз, включающих в себя не только технические сбои, но и любые несанкционированные действия (как сотрудников, так и недобросовестных конкурентов, хакеров и так далее). Такая проработка формируется еще на этапе планирования инженерной инфраструктуры дата-центров, позволяя гарантировать должный уровень безопасности.

Масштабируемость

Все системы инженерного обеспечения вычислительных центров должны гибко адаптироваться к растущим потребностям, в первую очередь, путем создания стандартизированных и модульных решений. Естественно, это необходимо планировать на самых ранних этапах создания центра.

Этапы построения инфраструктуры

Построение нового ЦОД – это непростой проект, реализация которого невозможна без практического опыта и видения долгосрочной стратегии развития. При проектировании и строительстве вычислительного центра необходимо учитывать множество факторов, часть из которых может быть неочевидной до начала эксплуатации.

Конкретная реализация может варьироваться, но, как правило, процесс построения ЦОД состоит из четырех этапов:

Формирование концепции (анализ задач и поиск оптимальных решений);

Проектирование ЦОД (разработка проекта и сметной документации, их экспертиза и все необходимые согласования);

Строительство ЦОД (строительно-монтажные работы, установка оборудования, испытания);

Ввод объекта в эксплуатацию (окончательное конфигурирование всех систем и процессов).

Стоимость построения инфраструктуры, а также скорость реализации решений и их эффективность в немалой степени зависят от помещения. При выборе места приходится учитывать воздействия многих внутренних и внешних факторов: техногенных, природных и человеческого. Даже если подходить только с точки зрения построения инженерной инфраструктуры, придется обращать внимание на множество деталей. Например, необходимо учитывать особенности архитектуры, нагрузку на перекрытия, огнестойкость дверей и стен, применяемые для потолочных перекрытий и стен отделочные материалы, а также наличие погрузочно-разгрузочной зоны и грузового лифта. Не меньшее значение имеют системы электроснабжения, кондиционирования, автоматического пожаротушения, охранной сигнализации и видеонаблюдения.

Изучение всех факторов, влияющих на выбор помещения, требует больших трудозатрат. Но в дальнейшем будет намного проще выбрать действительно хорошую площадку и при этом не сталкиваться с непредвиденными расходами на этапе построения ЦОД.

Рассмотрим характеристики самих систем, из которых состоит дата-центр.

Электроснабжение

В первую очередь, требуется обеспечить высокое качество электроэнергии и недопущение перерывов в электроснабжении. В идеале должен быть разработан надежный комплекс, состоящий из систем бесперебойного и гарантированного питания, резервных дизель-генераторов, стабилизаторов напряжения для обеспечения чистого электропитания компьютерной техники, систем освещения и внутреннего электроснабжения.

Система кондиционирования технологических помещений

Здесь уже стало классическим подходом применение следующей схемы охлаждения: совмещение использования промышленных кондиционеров (отличающиеся высокой надежностью, большим ресурсом работы и высокой точностью поддержания параметров микроклимата в помещении) с более «мобильными» сплит-системами полупромышленного класса.

Системы безопасности (СКУД, видеонаблюдение, оповещение, пожарная сигнализация и пожаротушение).

К этой категории относят системы, необходимые для контроля доступа в здания и помещения, отслеживания текущей ситуации, предупреждения об опасности и принятия эффективных мер при авариях. Здесь ключевую роль играют инструменты раннего обнаружения дыма. Они особенно актуальны для площадей с сильным воздухопотоком (серверных и машинных залов), где сложно уловить дым стандартными датчиками. Быстро обнаружив малейшее тление кабелей или оборудования, можно предотвратить аварию и остановку критичных приложений. Физическая безопасность, здесь используются современные технологии, например, 3D-распознавание лица посетителя в пропускной системе. Для крупных объектов формируется несколько рубежей видеонаблюдения и охранной сигнализации. Использование современного оборудования позволяет вести постоянный мониторинг всей ситуации на дата-центре в режиме онлайн.

Системы передачи данных

Вся телекоммуникационная сеть, составляющая единое информационное пространство. Как правило, это структурированная кабельная система, состоящая из отдельных модулей, что позволяет быстро устранять неполадки, восстанавливая связь за счет перехода на резервные линии. С повышением требований к сетевой инфраструктуре и увеличением количества «тяжелых» приложений, повышаются требования к пропускной способности, надежности и защите сети, ее управляемости и снижению стоимости эксплуатации.

Диспетчеризация

В работе ЦОД важен постоянный мониторинг информационных систем. Для этого используются специальные комплексы, позволяющие одновременно контролировать большое количество важных параметров. Причем для каждого дата-центра необходимо создавать собственные решения, с учетом эргономики и биомеханики. Активно применяются графические стены, состоящие из отдельных модулей (видеокубов). Благодаря высокому разрешению проекционных модулей система имеет высокую информационную емкость, что необходимо для эргономики восприятия большого объема данных.

Системы часофикации

Системы часофикации предполагают установку часов — стрелочных и цифровых — и их синхронизацию с единым мировым временем. Также система часофикации позволяет синхронизировать локальные вычислительные сети и другие системы и оборудование, для работы которых важна синхронизация по времени, например, инженерные системы и системы безопасности.

В физической инфраструктуре ЦОД старших уровней инженерные подсистемы рассматривают как единое комплексное решение, интегрированное со службами эксплуатации здания и сетевой инфраструктурой компании-владельца, сюда включаются системы кондиционирования и вентиляции дата-центра, системы бесперебойного электропитания и технической безопасности.

С учетом важности задач, к инженерной инфраструктуре предъявляют ряд обязательных требований:

• надежность эксплуатации

• долгий срок службы

• высокая управляемость

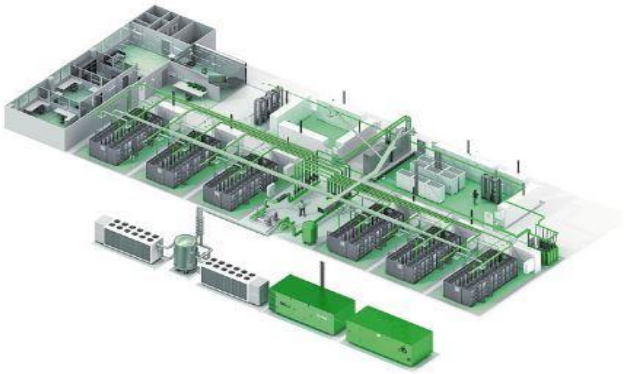
• полная безопасность

• легкий доступ к отдельным компонентам подсистем для ремонта и диагностики

• бесперебойная подача электроэнергии

• низкая совокупная стоимость владения

Общие принципы построения инженерных систем:



• соблюдение отраслевых международных стандартов

• высокая надежность

• эффективность

• физическая безопасность

• модульность с возможностью замены неисправных модулей в режиме «горячей замены»

• технологичность

• управляемость. Высокая управляемость достигается путем подключения активных подсистем к центральной диспетчерской службе через стандартные сетевые интерфейсы.

• централизованное управление инженерным комплексом и удаленная диагностика исключает возможные сбои в сети и позволяет быстро устранять аварийные ситуации.

• информационная и физическая безопасность.

• высокая масштабируемость.

Система технического обслуживания и ремонта инженерной инфраструктуры ЦОД включает в себя следующие виды работ:

- техническое обслуживание;
- плановый текущий ремонт;
- плановый капитальный ремонт;
- внеплановый ремонт;
- наблюдение за работой оборудования;
- периодический осмотр и контроль за техническим состоянием оборудования;
- устранение обнаруженных дефектов;
- регулировка;
- настройка.

Обеспечение надежности дата центра.

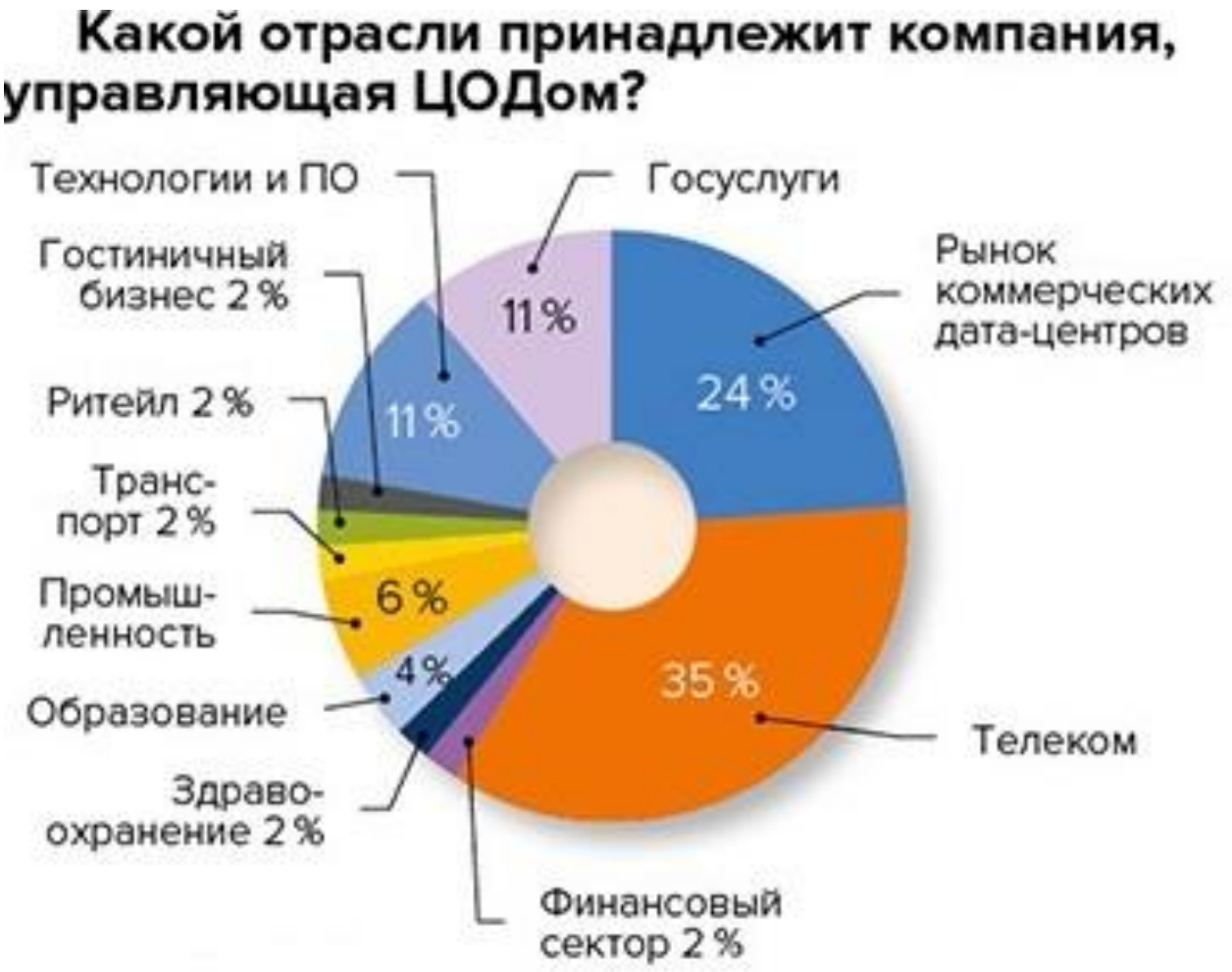
Говоря о надежности дата-центров, в качестве ключевых моментов всегда упоминают время простоя и отсутствие аварий. Как часто они бывают и где случаются — это и будет предметом обзора, который был построен по результатам анкетирования участников российского рынка. Современный бизнес попадает в прямую зависимость от информационных технологий, а им, в свою очередь, требуется для нормальной работы исправное оборудование, в частности функционирующая инженерная инфраструктура дата-центра.

Например, различные регулярные аналитические исследования показывают, что степень зависимости бизнес-процессов компании от ее ИТ составляет от 75 до 95 %. О чем это может говорить? О том, что при нарушении функционирования ИТ-сервисов, которые работают в ЦОДе, функционирование компании или нарушается, или существенно замедляется, что приводит как к прямым издержкам, так и косвенным (недополученной прибыли, репутационным рискам и т. д.).

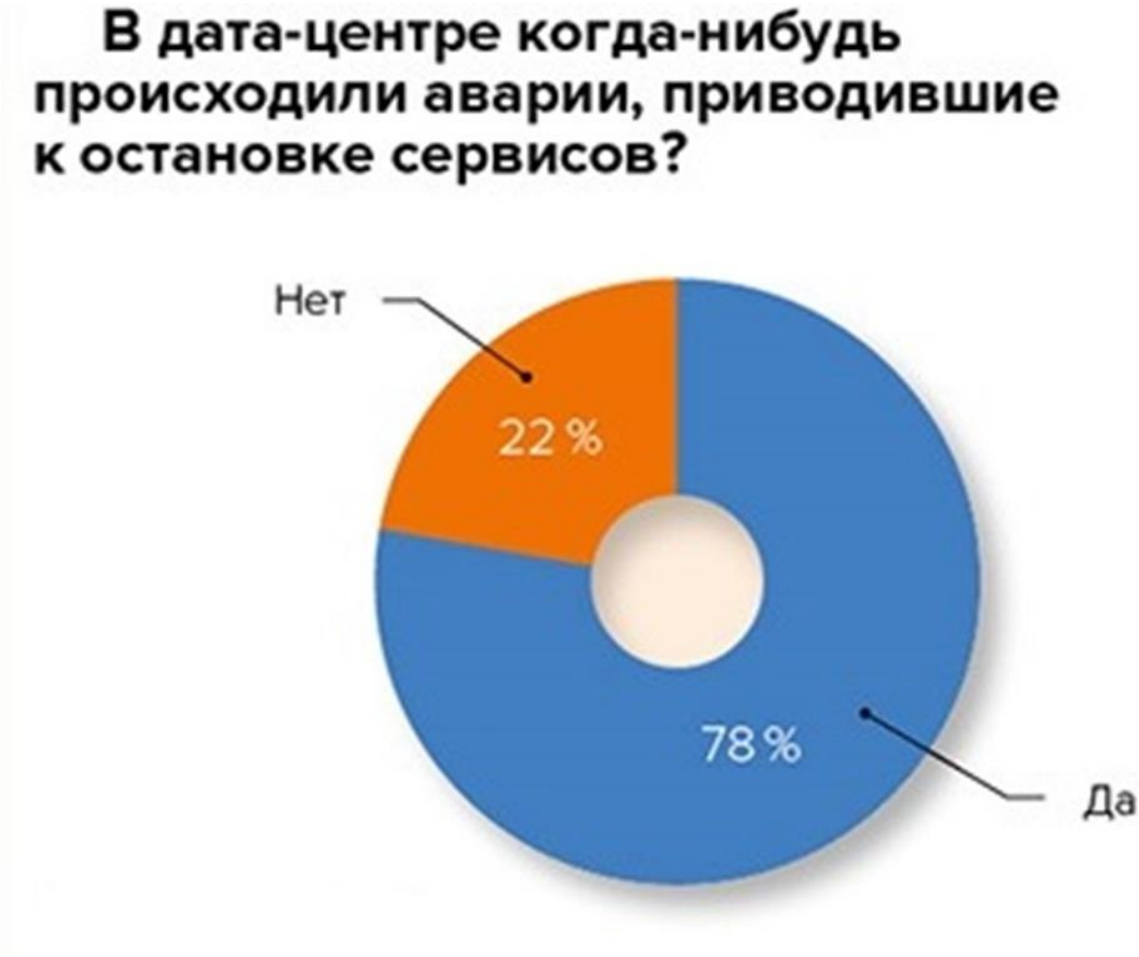
Неполадки в работе ЦОДа приводят к нештатным остановкам бизнес-процессов предприятий. О стоимости и последствиях таких сбоев мы писали в одном из предыдущих обзоров. Теперь же стоит рассмотреть более узкий аспект: что именно выходит из строя, сколько времени занимает решение проблемы и какие действия следует предпринять, для того чтобы избежать инцидентов в будущем. Чтобы ответить на эти вопросы, мы провели анкетирование среди профессионалов, которые занимаются непосредственно эксплуатацией действующих дата-центров. Результаты опроса позволяют обратить внимание профильных специалистов на потенциально проблемные участки инженерной инфраструктуры современных российских ЦОДов. Также надеемся, что нижеприведенные данные помогут в будущем предотвратить различные инциденты, связанные с работой дата-центров, и уже сейчас принять необходимые превентивные меры.

А судьи кто?

В опросе приняли участие 54 респондента, непосредственно задействованных в процессе эксплуатации дата-центров. Выяснилось, что 46 % из них эксплуатируют коммерческие ЦОДы, 39 % — корпоративные и 15 % — государственные (ведомственные). Последние условно можно также отнести к корпоративным, поскольку они предназначены только для собственных нужд. Следовательно, доля коммерческих объектов в исследовании на 4 % меньше корпоративных, а значит, большая часть статистики относится именно к площадкам, которые находятся в собственном или ведомственном управлении. Относительный паритет цифр также говорит о том, что ответы можно рассматривать как некое усредненное мнение службы эксплуатации — без привязки к тому, в чьей зоне ответственности находится эксплуатация.



Опрос также показал, что значительная часть ЦОДов находится под контролем операторов связи — об этом сообщили 35% респондентов. Данный показатель не удивляет, поскольку ЦОДы данного сегмента строятся наиболее активно, к тому же все чаще операторы связи планируют использовать пространство дата-центров не только для своих нужд, но и сдавать площади (или даже ИТ-мощности) в аренду. А вот отсутствие в опросе компаний — эксплуатантов ЦОДов из электронной торговли и медиа, говорит скорее лишь о том, что такие компании предпочитают арендовать ресурсы у коммерческих ЦОДов, не строя собственных или используя облачные технологии (что стало трендом для электронной коммерции).



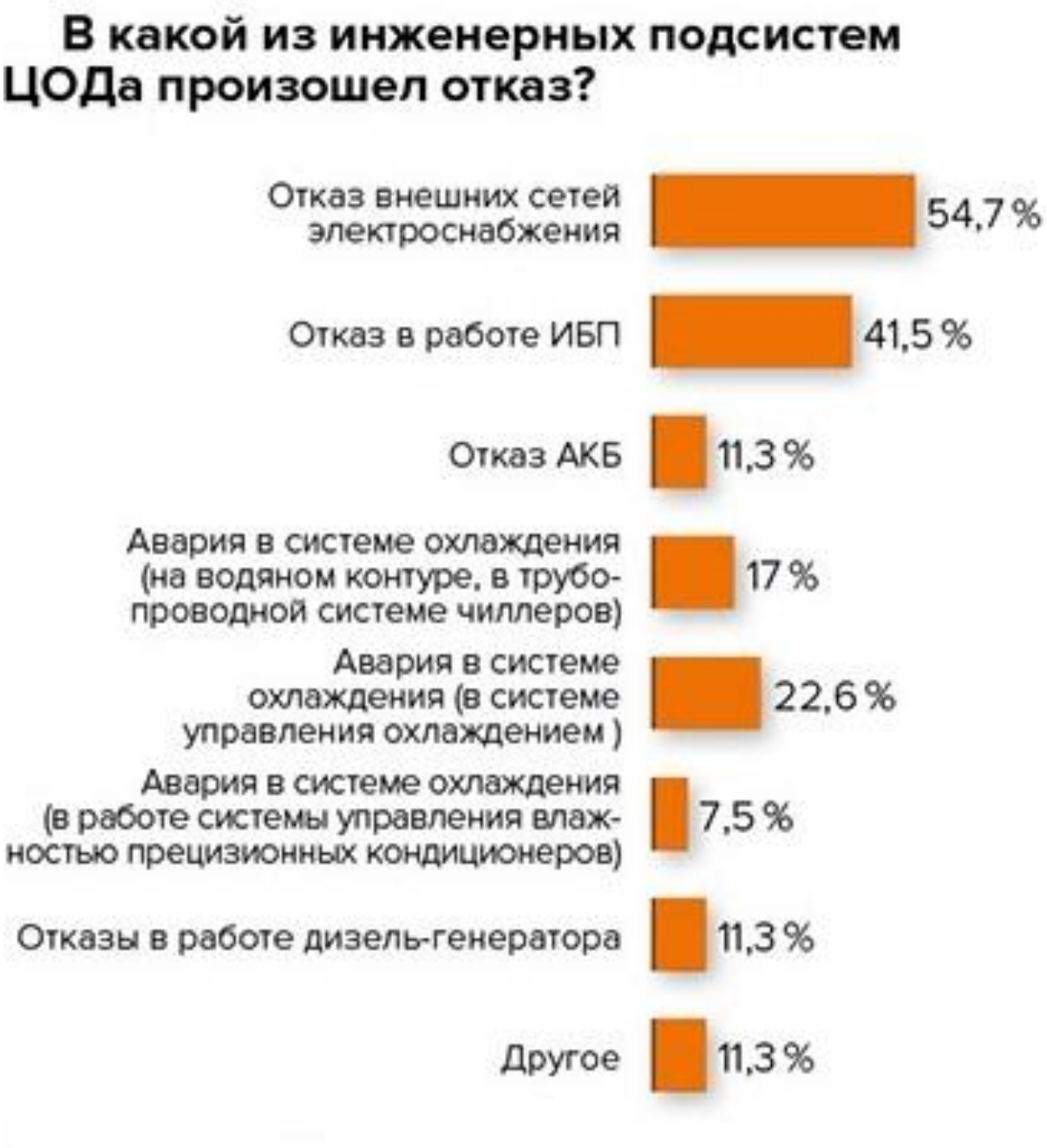
В то же время наличие шести компаний из области программного обеспечения и технологий говорит о том, что, несмотря на развитие рынка услуг коммерческих ЦОДов с их гибким продуктовым портфелем услуг, такие компании все же эксплуатируют свои дата-центры самостоятельно, хотя за рубежом данный сектор как раз активно использует аутсорсинг и аренду мощностей.

Теперь перейдем непосредственно к предмету опроса, а именно к тому, как живется компаниям с дата-центрами и с какими техническими проблемами сталкиваются компании в процессе их эксплуатации.

Источники проблем: рейтинг и анализ проблемных мест

Прежде чем возникла идея проведения анкетирования, были сомнения в том, что участники рынка вообще будут говорить о том, что аварии случаются. Как-то уж исторически сложилось, что ЦОДы у нас воспринимают как этакий форпост нерушимости бизнеса, и говорить об авариях — значит рушить репутацию компании, которой принадлежит ЦОД. В то же время задачей данного обзора является не персонификация аварий в ЦОДах, а как раз систематизация и анализ этих аварий, поэтому мы рассмотрим только саму статистику. И тот факт, что компании уже признают, что форс-мажоры случаются, — это шаг вперед к публичности и обмену опытом, ведь важно находить и устранять слабые звенья, а не замалчивать само их наличие.

В чем была причина незапланированного отказа ЦОДа?
Ошибки проектирования ЦОДа
20,4 %
Отказы инженерного оборудования
Отказы ИТ-оборудования
35,2 %
Нарушение правил эксплуатации оборудования
29,6 %
Случайная/человеческая ошибка
48,1%
Сложные погодные условия
7,4 %
Киберпреступления (DDoS)
13 %
Другое
9,3 %



Как показал опрос, лишь немногим более 22 % компаний никогда не сталкивались с критическими сбоями, приводящими к остановке ЦОДа. Однако есть достаточные основания полагать, что эта цифра занижена, так как толкование термина «авария» может разниться. Следует отличать критические аварии, которые привели к полной остановке ЦОДа, и те, которые повлекли за собой лишь частичное нарушение функционирования систем или отдельных агрегатов. О последних нередко можно услышать в кулуарах, но многие компании считают, что раз подобные нештатные ситуации не привели к глобальным проблемам, то и считать авариями подобные инциденты не следует. Но не нужно забывать, что наиболее частое резервирование на агрегатном уровне допускает

лишь единичный отказ с немедленными сервисными работами, что нередко игнорируется. В итоге «незначительные неполадки» накапливаются, выстраиваются в роковую цепочку событий и приводят к глобальным сбоям. Поэтому не стоит недооценивать любые инциденты — после его устранения необходимо уделить достаточно времени «разборам полетов», ведь авария может не просто повториться, а вызвать более серьезные последствия.

Результаты исследования позволяют сделать вывод о том, что порядка 80 % дата-центров так или иначе переживали серьезные неполадки в работе инженерной инфраструктуры, которые приводили к остановке бизнес-сервисов. Таким образом, проблемы существуют, и, несмотря на все заявления производителей и интеграторов, нет абсолютно надежных решений. Впрочем, их и не может быть, ведь всегда присутствует человеческий фактор и форс-мажоры.

Кстати, производители никогда открыто не рассказывают о проценте сбоев их оборудования в контексте отечественной статистики, однако, судя по опросу, 80 % «пострадавших» свидетельствуют: проблемы с оборудованием возникают чаще, чем хотелось бы. Соответственно, опыт самой службы эксплуатации становится дорогим (как в переносном, так и в прямом смысле) «дополнением» к оценке совокупной стоимости владения ЦОДом. В то же самое время нельзя сказать, что от подобного шага выигрывают и производители, ведь при субъективной оценке очень сложно что-то опровергнуть объективными факторами, поэтому брак в какой-то конкретной партии может наложить негативный отпечаток на всю продукцию производителя в целом, ставя под угрозу его репутацию на рынке. Остается надеяться, что политика открытости все-таки будет набирать обороты в ближайшее время.

Общее число аварийных эпизодов, о которых сообщили нам респонденты, достигло 120. В оценке того, кто является виновником проблемы, наши респонденты разошлись. Наибольшее количество участников опроса (59,3 %) назвали причиной неполадок именно отказ инженерного оборудования, хотя ИТ-оборудование указано в качестве источника проблем значительно реже (35,2 %). С одной стороны, это нелогично: инженерная система имеет больший срок эксплуатации, нежели ИТ-парк, а значит, и количество отказов должно быть меньше. С другой стороны, ИТ-оборудование более унифицировано в производстве и тестировании и часто функционирует «из коробки». Инженерное оборудование даже сегодня на заводах часто собирается с применением большого процента ручного труда, требует правильной пусконаладки на объекте и периодического сервисного обслуживания, которое часто просто игнорируется или проводится недостаточно тщательно. Одновременно с этим унификация производства активно внедряется и здесь: все чаще продукция от одного производителя может покрыть задачи построения инженерной инфраструктуры с нуля, не говоря уже о готовых блоках и решениях (таких как контейнерные решения, модульные ЦОДы и т. д.).

Увидев такой результат, стало интересным разобраться детальнее в этой части: что же именно выходит из строя в самих инженерных системах чаще всего? Статистика показала 94 эпизода, поскольку в некоторых случаях отказывало сразу несколько подсистем. 54,7 % опрошенных сообщили, что отказы связаны с выходом из строя тех

или иных элементов системы электроснабжения, 41,5 % — из-за неисправности ИБП, 11,3 % — из-за отказа батарей. А это весьма немало: в среднем — 61 % по вине систем электроснабжения. Добавляем к этой цифре 11,3 % отказов в работе дизель-генераторных установок (ДГУ) и получаем впечатляющие 67 %. Вот и вывод: две трети проблем — из-за гарантированного электроснабжения потребителей!

Как выяснилось, запуск ДГУ осуществляется довольно редко. Очевидно, характер сбоев не позволяет ДГУ спасти ситуацию или же проблема локализирована внутри сети электроснабжения и не требует запуска ДГУ: только половина опрошенных компаний сообщила, что необходимость запуска дизеля возникает раз в три года или еще реже. Еще около 24 % прибегают к помощи ДГУ только раз в год.

Зачастую службы эксплуатации сталкиваются с проблемами в системе охлаждения. При этом 22,6 % — из-за системы управления охлаждением; 17 % — из-за проблем с контуром теплоносителя и 7,5 % — из-за системы контроля влажности. В сумме — 27 %, а на остальные инженерные системы приходится менее 6 % аварий. Вывод простой: при проектировании, внедрении и эксплуатации уделяйте как можно больше времени системам электроснабжения и кондиционирования, и вы очень повысите надежность функционирования всего комплекса систем ЦОДа, при этом сильно сократив вероятность появления аварий, что, впрочем, и подтверждается методиками известной организации Uptime Institute.

Человеческий фактор по-прежнему высок

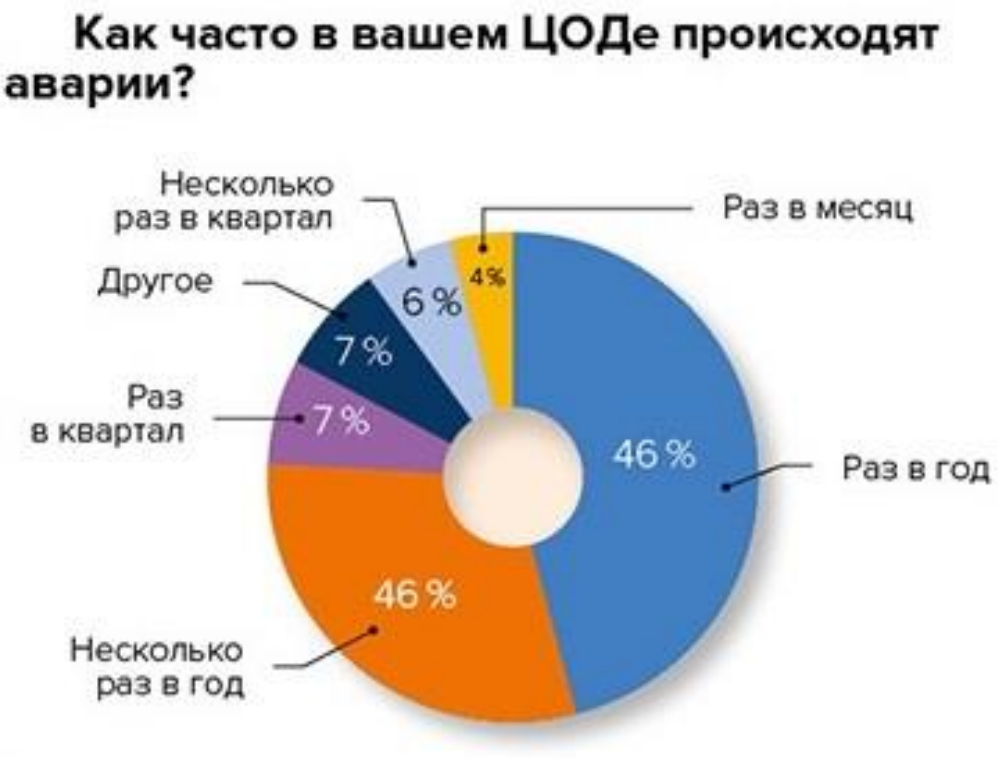
В то же время в перечне источников, которые вызвали отказ, уверенно лидирует человеческий фактор — 44 %, из которых 48,1 % респондентов указали, что причиной аварии была случайная (человеческая) ошибка. О чем это говорит? О том, что обслуживающий персонал должен проходить тщательный отбор и подготовку, прежде чем заступать на «боевое» дежурство. Ведь в случае аварии именно первые действия персонала могут как спасти ситуацию, так и существенно ее усугубить. Для исключения случайностей также необходимо иметь краткие инструкции относительно того, что делать в случае тех или иных нештатных ситуаций; иметь под руками документацию. Также в случае, если ЦОД находится на аутсорсинге, необходимо заключать с обслуживающей организацией SLA с коротким сроком реагирования. Если этого нет, получаем следующий по величине аварийный фактор: 16 % опрошенных указало, что причиной аварии стало нарушение правил эксплуатации оборудования. Такой высокий процент может свидетельствовать о том, что большинство операторов ЦОДов уделяют недостаточно внимания обучению персонала, проверке их квалификации, разработке регламентов работы, контролю за исполнением процедур и т. д.

А вот ошибки проектирования значительно снизились: если ранее во многих обзорах они стояли среди первых по частоте, то в нашем обзоре на них указали только 20,4 % представителей компаний. Что ж, культура и детализация проектирования принесли свои плоды. А ведь именно ошибки на стадии проектирования труднее всего и дороже исправлять. В то же самое время хотелось бы отметить еще одну важную деталь: крайне желательно, чтобы сотрудники, занимающие ключевые посты и отвечающие за эксплуатацию, были подключены к процессу строительства ЦОДа еще на стадии проектирования (особенно это касается коммерческих ЦОДов). Тогда бесценный опыт, накопленный при возведении объекта, не будет утерян, а сама реализация ЦОДа будет максимально отвечать не только бизнес-модели, но и согласовываться с рабочими процессами службы эксплуатации.

Остальные факторы, такие как сложные погодные условия (7,4 %) или атаки хакеров (13 %), значительно отстают. Это говорит о том, что основные причины аварийности ЦОДа все-таки находятся внутри объекта и не настолько подвержены внешним факторам, как может показаться с первого взгляда.

Частота аварий и время восстановления

В начале исследования именно этот момент вызывал наибольший интерес. Ведь фактически интерес представлял не только некий средний период аварий, но и разнообразие ответов участников анкетирования, что прямо бы подтвердило или опровергло глобальную тенденцию на рынке.



Выяснилось, что 50 (почти 93 %) компаний из 54 опрошенных отмечают, что те или иные отказы происходят как минимум раз в год. Из этих компаний 30 % сообщили, что авария случается несколько раз в год, но только 4 % указали, что аварии случаются раз в месяц и не чаще. То есть можно говорить, что в большинстве дата-центров все-таки хотя бы раз в год авария случается, но не чаще, чем несколько раз.

При этом все аварии были устранены достаточно оперативно: ликвидация 93 % аварий уложилась в суточный интервал, из которых почти четверть (26 %) заняла не более пяти часов, а 41 % — и вовсе до часа. При этом речь идет только об авариях, которые стали значительными для участников опроса. Напомним, один из ранее проведенных нами опросов показал: для большинства организаций допустимым временем простоя как раз и является диапазон от получаса до суток. Иными словами, хотя аварии и происходили, но все они были устранены в разумные сроки.

Итоги

Подводя итоги, остановимся на основных ключевых мыслях, к которым привело данное исследование. Во-первых, сбои в отечественных дата-центрах происходят не так уж и редко: как минимум раз в год. При этом неважно, идет ли речь о коммерческих, корпоративных или государственных площадках. Почти в половине случаев причиной аварий является человеческий фактор (причем акцент смещен именно в сторону случайных действий и ошибок эксплуатации), еще треть приходится на инженерные системы, из которых 2/3 составляют аварии с электроснабжением и менее 1/3 — с кондиционированием. В то же время, если технические сбои в ЦОДе и происходят, они, как правило, не оказывают катастрофического влияния — почти всегда их устранение укладывается в суточный интервал, а почти в половине случаев проблемы решаются и вовсе в течение часа.

Подобная статистика аварий однозначно свидетельствует в пользу необходимости резервирования критически важных элементов инженерной инфраструктуры дата-центра, более ответственного отношения к квалификации персонала и его постоянной переподготовке, а также к тщательному документированию и формализации всех процессов. Таким образом, важно понимать, что человеческий фактор может стать причиной ненадежности любого «неубиваемого» оборудования, а исключение этого фактора позволит значительно поднять надежность с минимальными затратами. Ведь с точки зрения экономики клиент (неважно — внутренний или внешний) готов платить лишь за надежность и непрерывность функционирования ИТ-сервисов (именно это и есть ценность ЦОДа для бизнеса), и чем она выше, тем более рентабельным будет функционирование такого бизнес-актива, как ЦОД.

Источник: Журнал «ЦОДы.РФ» № 13