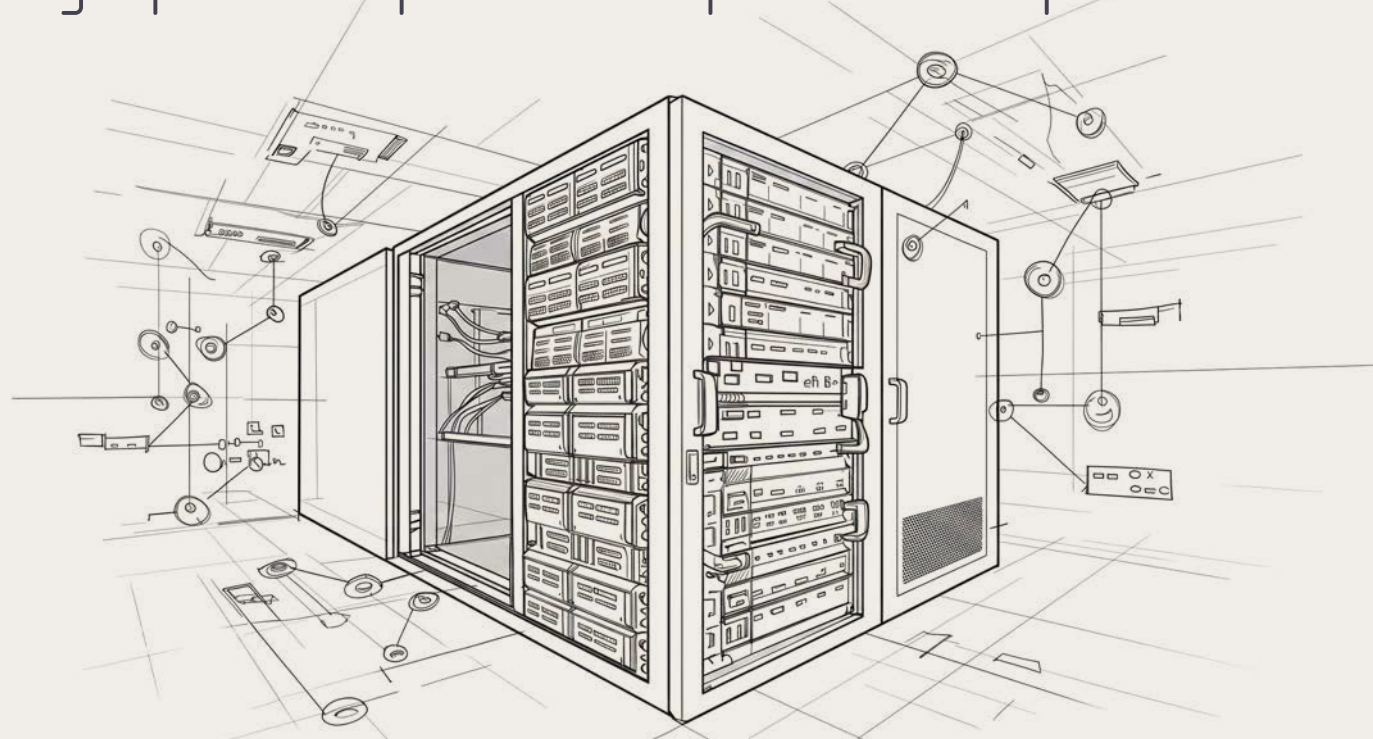


Анализ стандартов для ЦОД: международные практики и российские реалии



Текст:
**Александр
Бахлыков,**
руководитель
инженерного бюро
bimDC

Современные центры обработки данных проектируют и эксплуатируют, опираясь на сложную систему международных и национальных стандартов. Наряду с российскими нормативами в технические задания часто включают отсылки к документам TIA, BICSI, ASHRAE и ISO, а также требования соответствия уровням Tier. Несогласованность терминологии, разные критерии оценки надежности и энергоэффективности, необходимость учитывать обновления создают определенные сложности для проектировщиков и заказчиков.



TIA (Telecommunications Industry Association) — это ассоциация телекоммуникационной промышленности США, объединяющая специалистов по оборудованию связи, телекоммуникационному оборудованию, кабельным системам и компонентам. В 2005 году организация выпустила TIA-942 (Telecommunications Infrastructure Standard for Data Centers) — стандарт телекоммуникационной инфраструктуры для центров обработки данных (ЦОД). Это был первый серьезный и очень популярный документ

в области создания дата-центров. Было несколько переизданий этого стандарта, и на данный момент, с мая 2024 года, действует редакция TIA-942-C, в которой разработчики учли текущее положение дел в отрасли ЦОД и появление искусственного интеллекта. Несмотря на то, что документ разработан для телекоммуникационной инфраструктуры, он описывает требования ко всем основным подсистемам инженерной инфраструктуры ЦОД и проводит классификацию ЦОД по уровням резервирования — от Rated-1 до Rated-4. Существует сертификация по уровням Rating TIA, ее проводят организации EPI и TUV.

EPI — это международный орган по сертификации ЦОД и специалистов отрасли. TUV — группа международных сертифицирующих экспертных организаций, осуществляющих контроль по обеспечению безопасности продукции.

На данный момент TIA ведет работу над еще одним интересным стандартом в области ЦОД в рамках инициативы Data Center Excellence (DCE 9000). Это будет первый стандарт системы управления качеством для современной физической инфраструктуры центров обработки данных. В рабочей группе участвуют компании Google, Oracle, Iron Mountain и Verizon Wireless, а также поставщики оборудования и услуг для центров обработки данных, включая ABB, Eaton, Ever Energy, Johnson Controls, Modine, MTU Solutions (Rolls-Royce), Schneider Electric, Trane, Network Connex, Technavious и TruNorthe. Разработка проекта стандарта запланирована в 2026 году, а публикация и запуск системы сертификации в 2027 году.



Другой популярный стандарт в области ЦОД был создан организацией BICSI (Building Industry Consulting Service International) — международной консалтинговой службой строительной отрасли. Был выпущен BICSI 002 — Data Center Design and Implementation Best Practices. В этом руководстве приведены решения для электрики, охлаждения, архитектуры ЦОД, а приложениях описаны расчеты устойчивости и доступности. На данное время действует редакция 2024 года ANSI/BICSI 002-2024 — The Standard for Data Center Design. В стандарте BICSI также приведена своя классификация ЦОД от Class 0 до Class 4.

Другой стандарт BICSI, касающийся дата-центров, ANSI/BICSI 009-2024 Data Center Operations and Maintenance Best Practices содержит требования по эксплуатации и техническому обслуживанию ЦОД.



В решении вопросов по охлаждению в ЦОД часто используют требования организации ASHRAE — American Society of Heating, Refrigerating and Air-Conditioning Engineers, Американского общества инженеров по отоплению, охлаждению и кондиционированию воздуха. Это одна из старейших

организаций, которая занимается вопросами отопления и охлаждения воздуха, основанная в 1894 году. Общество развивает базу данных по климатическим параметрам, в том числе по температуре и влажности, многие годы собираемую по всему земному шару. База размещена на сайте организации в свободном доступе, ее достаточно часто используют для уточнения и дополнения данных, которые российские проектировщики получают из СП 131.13330 «Строительная климатология».

Один из полезных документов по климату в ЦОД, разрабатываемый и регулярно обновляемый техническим комитетом 9.9 ASHRAE, — Thermal Guidelines for Data Processing Environments, 5th Ed (Рекомендации по тепловому режиму в средах с оборудованием для обработки данных, 5-ая редакция). В издании к существующим классам ИТ-оборудования (от A1 до A4) добавлен класс высокопроизводительного ИТ-оборудования H1, для которого начинают действовать требования по ограничению температурного диапазона. Если для обычного ИТ-оборудования допустим температурный диапазон от 18 до 27 °C, то для оборудования класса H-1 рекомендован диапазон от 18 до 22 °C.



В России и в мире очень популярна классификация ЦОД по уровням Tier, от Tier I до Tier IV, разработанная американской консалтинговой компанией Uptime Institute, которая и проводит сертификацию ЦОД на заявленный уровень. На сайте организации есть описание требований к ЦОД для каждого уровня. Сертификация и выдача сертификата проводится только специалистами компании Uptime Institute и по-прежнему доступна в России для организаций, не находящихся под санкциями.



Европейские национальные стандарты EN серии 50600 были разработаны Европейским комитетом по электротехнической стандартизации с учетом вышеперечисленных национальных американских стандартов.

На базе стандартов EN серии 50600, были разработаны международные стандарты ISO (International Organization for Standardization). Эти стандарты могут применять все члены ISO, в том числе и Российской Федерации.

Для ЦОД была создана серия стандартов ISO/IEC 22237. Их разработкой занимается подкомитет 39 (ISO/IEC JTC 1/SC 39). Стандарты разделены по темам на небольшие документы, которые периодически обновляют.

ISO/IEC 22237-1:2021 Information technology Data centre facilities and infrastructures Part 1: General concepts — «Информационные технологии. Объекты и инфраструктура центров обработки данных. Часть 1. Общие понятия». В стандарте описаны общие принципы работы центров обработки данных, на которых основаны требования серии стандартов ISO/IE C22237. Определена система классификации ЦОД, основанная на ключевых критериях доступности, безопасности и энергоэффективности на протяжении всего планируемого срока службы центра обработки данных. Рассмотрены вопросы анализа бизнес-рисков и определения операционных затрат, даны рекомендации по эксплуатации дата-центра.

ISO/IEC 22237-2:2024 Information technology Data centre facilities and infrastructures Part 2: Building construction — «Информационные технологии. Объекты и инфраструктура центров обработки данных Часть. 2. Строительство зданий». На данный момент к стандарту разрабатывают первую поправку ISO/IEC 22237-2:2024/CD Amd 1. В документе изложены требования и рекомендации по строительству зданий и сооружений, в которых расположены центры обработки данных, на основе критериев и классификации «физической безопасности». Приведены критерии выбора места и участка для размещения ЦОД, рассмотрены экологические риски, планировка участка и здания ЦОД, строительство здания, вопросы физической защиты, в том числе противопожарной защиты.

ISO/IEC 22237-3:2021 Information technology Data centre facilities and infrastructures Part 3: Power distribution — Информационные технологии. Оборудование и инфраструктура центров обработки данных. Часть 3. Распределение электроэнергии. В документы рассмотрены вопросы энергоснабжения центров обработки данных и распределения энергии внутри них на основе критериев и классификаций доступности, физической безопасности и энер-

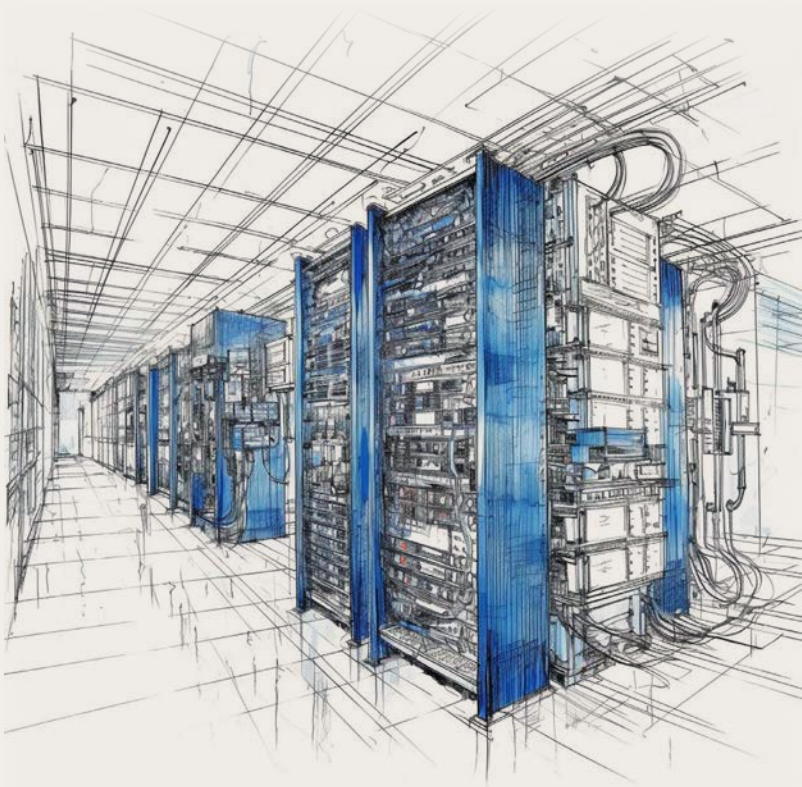
гоэффективности. Рассмотрено применение источников бесперебойного электропитания для ЦОД, описаны системы распределения электропитания, устройства для измерения энергопотребления и определения качества электроэнергии с интеграцией в систему мониторинга, молниезащита ЦОД.

ISO/IEC 22237-4:2021 Information technology Data centre facilities and infrastructures Part 4: Environmental control — «Информационные технологии. Объекты и инфраструктура центров обработки данных. Часть 4. Контроль окружающей среды». В стандарте рассмотрены вопросы контроля окружающей среды в центрах обработки данных на основе критериев и классификаций доступности, безопасности и энергоэффективности. Приведены рекомендации по контролю температуры, влажности, потока жидкости, содержания твердых частиц (запыления), вибрации и физической безопасности систем контроля окружающей среды.

Стандарты ISO, BICSI и TIA нельзя получить в свободном доступе, только за плату и через интернет-магазин, где можно приобрести нормативы в электронном или бумажном виде

ISO/IEC TS 22237-5:2018 Information technology Data centre facilities and infrastructures Part 5: Telecommunications cabling infrastructure — «Информационные технологии. Оборудование и инфраструктура центров обработки данных. Часть 5. Кабельная инфраструктура телекоммуникаций». В ближайшие месяцы ожидается замена стандарта на версию ISO/IEC DIS 22237-5. Стандарт описывает варианты реализации кабельной инфраструктуры в центрах обработки данных на основе критериев и классификаций доступности. Приведены требования к кабельной инфраструктуре для ИТ-оборудования — локальных вычислительных сетей (ЛВС) и сетей хранения данных SAN (Storage Area Network), требования к кабельной системе для системы мониторинга и управления ЦОД. Также приведены требования к кабельным проходкам, телекоммуникационным помещениям и конструктивам (шкафам).

ISO/IEC 22237-6:2024 Information technology Data centre facilities and infrastructures Part 6: Security systems — «Информационные техноло-



гии. Объекты и инфраструктура центров обработки данных. Часть 6. Системы безопасности». В документе изложены требования и рекомендации по обеспечению физической безопасности центров обработки данных на основе критериев и классификаций доступности, безопасности и энергоэффективности. Приведены требования и рекомендации в части защиты от несанкционированного доступа, вторжений, возгораний внутри ЦОД, протечек и прочих внутренних и внешних физических воздействий на оборудование и инженерные системы.

ISO/IEC TS 22237-7:2018 Information technology Data centre facilities and infrastructures. Part 7: Management and operational information — «Информационные технологии. Оборудование и инфраструктура центров обработки данных. Часть 7. Управление и эксплуатация ЦОД». Запланирована замена на версию ISO/IEC CD 22237-7.3. Стандарт описывает процессы управления и эксплуатации центров обработки данных. Основное внимание уделено операционным процессам, необходимым для обеспечения ожидаемого уровня отказоустойчивости, доступности, управления рисками, их минимизации, планирования мощностей, безопасности и энергоэффективности.

Стандарты ISO, BICSI и TIA нельзя получить в свободном доступе, только за плату и через интернет-магазин, где можно приобрести нормативы в электронном или бумажном виде.

РОССИЙСКИЕ СТАНДАРТЫ. ТК 120

На сайте Росстандарта опубликованы актуальные версии документов в открытом доступе. Над нормативной базой для ЦОД работают несколько технических комитетов. Профильный технический комитет №120 «Центры обработки данных» (ТК 120), ТК 022 «Информационные технологии» и ТК 465 «Строительство».

ТК 120 разработаны ряд нацстандартов в области ЦОД, которые действуют в настоящее время.

ГОСТ Р 58811-2020 «ЦОД. Инженерная инфраструктура. Стадии создания». Стандарт устанавливает стадии создания инженерной инфраструктуры центров обработки данных, а также этапы внутри стадий и содержание работ на каждом этапе. Начиная от предпроектного обследования площадки под будущий ЦОД и заканчивая этапом эксплуатации построенного объекта.

ГОСТ Р 58812-2020 «ЦОД. Инженерная инфраструктура. Операционная модель эксплуатации. Спецификация». Стандарт может помочь в формировании подхода к организации эксплуатации инженерной инфраструктуры центра обработки данных. Разработан с учетом методологии ITIL (IT Infrastructure Library) — библиотеку книг, описывающих лучшие практики в области инфраструктуры информационных технологий.

ГОСТ Р 70627-2023 «ЦОД. Инженерная инфраструктура. Документация. Техническая концепция. Требования к составу и содержанию». В стандарте, в соответствии с требованиями ГОСТ Р 58811 для стадии 3 «Техническая концепция», изложена техническая концепция инженерной инфраструктуры ЦОД. Техническая концепция представляет собой комплект документов, предназначенных для описания вариантов реализации инженерной инфраструктуры ЦОД и обоснования выбора варианта, удовлетворяющего требованиям заказчика.

Разработанный ТК 120 ГОСТ Р 70139-2022 «ЦОД. Инженерная инфраструктура. Классификация» в результате бурных дискуссий в отрасли был приостановлен в 2024 году и впоследствии отменен. В стандарте была предпринята попытка сформировать российскую классификацию ЦОД.

Сейчас ТК 120 ведет работу по принятию нового стандарта ГОСТ Р «ЦОД. Инженерная инфраструктура. Термины и определения». Первая редакция стандарта прошла публичное обсуждение, и готовится вторая редакция стандарта с учетом полученных от участников отрасли замечаний и предложений.

СТАНДАРТЫ ТК 022

ТК 022 сфокусировался на разработке российских стандартов на базе соответствующих стандартов ISO/IEC (ИСО/МЭК). Действующие стандарты ЦОД ТК 022 описывают ключевые показатели работы ЦОД.

ГОСТ Р ИСОМЭК 30134-1-2018 (ISO/IEC 30134-1:2016) «Центры обработки данных. Ключевые показатели эффективности. Основные положения и общие требования». Стандарт содержит общие сведения для всех частей серии стандартов ИСО/МЭК 30134 – структуру, определения, термины, сведения о применении ключевых показателей эффективности (КПЭ).

ГОСТ Р ИСОМЭК 30134-2-2018 (ISO/IEC 30134-2:2016) «Центры обработки данных. Ключевые показатели эффективности. Коэффициент энергоэффективности (PUE)». Стандарт описывает коэффициент энергоэффективности (PUE), который используют в качестве КПЭ для оценки рациональности использования энергии в виде электроэнергии.

ГОСТ Р ИСОМЭК 30134-3-2018 (ISO/IEC 30134-3:2016) «Центры обработки данных. Ключевые показатели эффективности. Коэффициент возобновляемой энергии (REF)». В стандарте приведено определение коэффициента возобновляемой энергии (REF), описана методика вычисления и представления REF и доступны сведения, необходимые для правильной интерпретации REF.

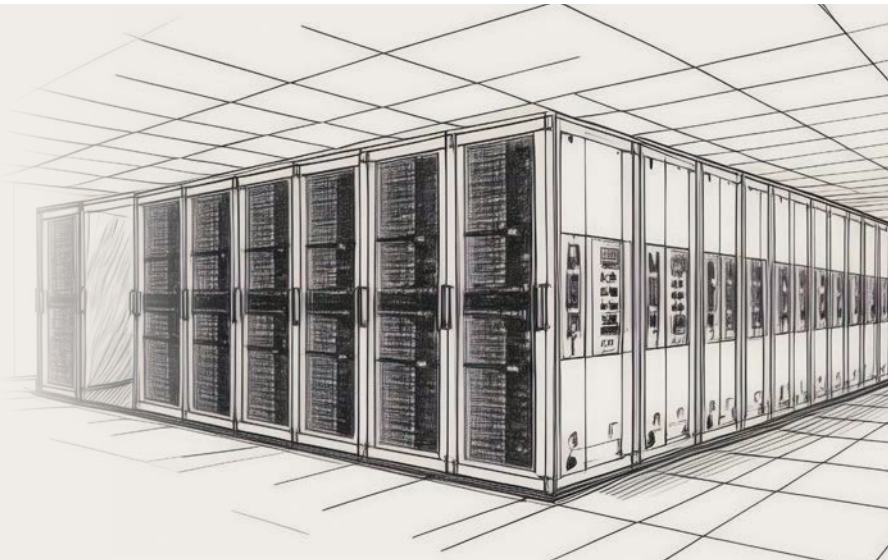
Сейчас ТК 022 ведет работу по выпуску переведенного и адаптированного стандарта ISO/IEC 22237-1:2021. Стандарт ГОСТ Р «Информационные технологии. Объекты и инфраструктуры центров обработки данных. Часть 1. Общие положения». Первая редакция выложена на публичное обсуждение.

СТАНДАРТЫ ТК 465

ТК 465 «Строительство» выпустил свод правил СП 541.1325800.2024 «Здания и сооружения центров обработки данных. Правила проектирования». Документ утвержден Минстроем России 23 декабря 2024 года приказом №898, введен в действие с 24 января 2025 года.

СП 541.1325800.2024 разработан в целях обеспечения соблюдения требований Федерального закона от 30 декабря 2009 года № 384-ФЗ «Технический регламент о безопасности зданий и сооружений».

Положения СП распространяются на проектирование зданий и сооружений центров обработ-



ки данных, а также помещений центров обработки данных в составе зданий.

Ключевое понятие здесь — проектирование помещений, зданий и сооружений ЦОД, то есть архитектура и конструктив. При этом затронуты требования к созданию инженерных систем ЦОД. СП может быть использован как базовый документ при работе над ЦОД, так как включает порядка 70 ссылок на смежные российские нормы и стандарты, применимые к дата-центрам.

В СП приведены требования пожарной безопасности, опираясь на Федеральный закон от 22 июля 2008 года № 123-ФЗ «Технический регламент о требованиях пожарной безопасности». Детализирован ряд требований пожарной безопасности, в частности СП дает ответ на вопрос о том, отключать или нет систему кондиционирования при срабатывании системы автоматического газового пожаротушения: можно не отключать (предусматривать задержку отключения) постоянно работающие по технологическим условиям системы кондиционирования в помещениях, защищаемых установками газового пожаротушения при тушении объемным способом, если работа системы кондиционирования исключает добавление атмосферного воздуха в защищаемое помещение при циркуляции газовой среды.

Рассмотренные актуальные версии национальных, международных и российских стандартов могут служить отправной точкой и ориентиром при работе над проектом создания и дальнейшей эксплуатации ЦОД. Отрасль не стоит на месте, и появление новых технологий приводит к тому, что стандарты регулярно пересматривают и обновляют и при их использовании необходимо проверять наличие актуальных версий.




Александр Бахлыков

Руководитель инженерно-проектного бюро bimDC

Постановление Правительства РФ № 87 от 16.02.2008 г. "О составе разделов проектной документации и требованиях к их содержанию" определяет две стадии проектирования. Разрабатывая стадию "П" (первую часть проекта), проектировщик всегда думает о том, как он будет ее защищать в экспертизе. А эксперты будут проверять проектировщика в первую очередь на соответствие разработанного проекта требованиям технического задания и нормативной базы. При обнаружении несоответствий проектировщик должен их исправить. Другой момент, который проектировщик точно продумывает, – это как ему попасть в ограничения и требования, которые формирует заданный в ТЗ стандарт. Часто говорят, что проект по уровням Uptime institute должен соответствовать Tier-III или Tier-IV.

Как же при таком количестве вводных заставить проектировщика задуматься еще и об эксплуатации? В идеальном случае лучше поставить перед ним два условия:

1. Прописать все пожелания к последующей эксплуатации ЦОД в техническом задании.
2. Привлечь как можно раньше к работе над проектом службу эксплуатации ЦОД. Возникает аналогия с покупкой квартиры и ремонтом. Если вы купили квартиру с готовым ремонтом, то вы, скорее всего, будете много переделывать, потому что существующие решения, которые там реализованы, существующий ремонт вас устроит не полностью. Если же вы делаете ремонт с нуля, вы наймете подрядчиков: архитектора, инженера, дизайнера, строителей. Наняв, вы, вероятно, будете их тщательно контролировать, чтобы все было сделано правильно – так, как вам нужно для комфортной жизни. Если такой надзор не осуществлять, то результат, скорее всего, вас не устроит. С ЦОД то же самое. Какой бы умный проектировщик ни был, если он не узнает ваших требований по эксплуатации, он не учтет их.

Современные тенденции и проблемы управления ЦОД

Работая над проектом, проектировщик центра обработки данных (ЦОД), как правило, думает о технических решениях, которые ему надо разработать и применить согласно полученному от заказчика техническому заданию (ТЗ), об экспертизе проекта. Но достаточно редко он задумывается о периоде дальнейшей эксплуатации. Почему так происходит и какие проблемы это влечет?

Если нет службы эксплуатации

Если строится новый ЦОД и команда абсолютно новая, то служба эксплуатации скорее всего еще не создана. Значит, во время работы над проектом и строительством ЦОД самое время начать ее формирование. К этапу пусконаладочных испытаний вы сможете подойти уже со сформированной командой по эксплуатации ЦОД.

В это время оптимально будет разработать регламенты дальнейшей работы службы эксплуатации, подготовить материально-техническую базу, перечни необходимых инструментов, материалов, разработать и описать процессы эксплуатации, регламенты, случаи штатных-нестатных ситуаций.

Техническое задание и нормативы

Если службы эксплуатации нет или она по какой-то причине не привлечена к работе, для формирования дополнительных требований остается техническое задание. Очень часто в ТЗ упомянута одна только фраза по теме: "Выбранное оборудование и технические решения должны обеспечивать удобство эксплуатации". Следующим шагом проектировщика становится ознакомление с существующей нормативной базой по эксплуатации. В России есть несколько нормативных документов. Существуют также международные и национальные нормы. Среди российских нормативов выделяю ГОСТ Р 58812–2020 "Центры обработки данных. Инженерная инфраструктура. Операционная модель эксплуатации. Спецификация". Многие эксперты считают, что это методология ITIL (Information Technology Infrastructure Library), которую попытались применить к эксплуатации ЦОД. Другой достаточно важный документ, принятый в начале 2024 г., – ГОСТ Р 70627–2023 "Центры обработки данных. Инженерная инфраструктура. Документация. Техническая концепция. Требования к составу и содержанию". Это первый серьезный документ, который должен учитываться при создании ЦОД и с которым должна ознакомиться служба эксплуатации.

В нем описывается не только техническая концепция того, где будет строиться ЦОД, как он будет строиться, но и то, как его эксплуатиро-

вать, какие будут затраты на эксплуатацию, за счет чего они образуются. Проектировщик, обладающий опытом проектирования центров обработки данных, может и сам оценить концепцию затрат, но, если привлечь будущую службу эксплуатации, данные будут более реалистичными.

Недавно в НОПРИЗ состоялось заседание комитета по эксплуатации зданий и сооружений, на котором обсуждались вопросы эксплуатации объектов на стадии проектирования. На нем было предложено:

- разработать дорожную карту создания СП по эксплуатации;
- ввести норму обязательной загрузки эксплуатационной документации в государственные информационные системы;
- внести в ряд нормативных актов поправки, которые закрепляют обязанность застройщика или проектной организации передавать документацию эксплуатирующим организациям до подписи акта о вводе объекта в эксплуатацию;
- ввести необходимость учетов стоимости эксплуатации на стадии проектирования (эта норма из рекомендательной должна стать обязательной).

Обсуждалось еще много пунктов с точки зрения создания новых СП, сфокусированных на эксплуатации, которые надо будет прописывать в ТЗ и учитывать при проектировании.

Международные нормативы

Uptime

У нас широко известны три уровня сертификации от Uptime Institute:

- сертификация дизайна (проекта);
 - сертификация создания ЦОД (объекта после того, как его построили);
 - сертификация операционной устойчивости.
- После сертификации операционной устойчивости ЦОД может быть присвоено три уровня – бронзовый, серебряный и золотой, в зависимости от количества набранных при аудите баллов.

На сайте организации представлена карта сертифицированных ЦОД во многих странах, включая Россию. Если посмотреть на данные по нашей стране, то достаточно много ЦОД имеют сертификат на дизайн, чуть меньше имеют сертификаты на стройку и еще меньше сертификатов на операционную устойчивость.

Сертификат Uptime нужно регулярно обновлять, подтверждать. Для этого организация Uptime Institute регулярно проводит аудит службы эксплуатации ЦОД и закрепляет, подтверждает соответствующий уровень или, в против-

По теме формирования службы эксплуатации я советую изучить две относительно свежие книги:

- Алексей Жумыкин – "Настольная книга эксплуататора";
- Константин Нагорный, Тарас Чирков, Андрей Чеснов – "Эксплуатация ЦОД: практическое руководство".

Авторы материалов – серьезные практики, знающие не понаслышке обо всех проблемах эксплуатации.

ном случае, лишает его. Золотой уровень дается на три года, серебряный – на два, бронзовый – на год. У Uptime также есть программы обучения для специалистов по эксплуатации.

EPI

Другая организация, уделяющая внимание процессу эксплуатации, – это EPI. Она занимается сертификацией ЦОД по стандартам TIA-942. EPI разработали свой стандарт Data Center Operation Standard ("Стандарт эксплуатации центров обработки данных"), проводит по нему аудиты и сертификацию эксплуатируемых ЦОД. В EPI определено 11 дисциплин, в соответствии с которыми ЦОД может быть на одном из пяти уровней зрелости, исходя из того, как подробно каждая дисциплина внедрена в службу эксплуатации. После прохождения сертификации центр обработки данных получает сертификат EPI. Подобный сертификат очень хорошо использовать в маркетинговых целях. Данные о сертификации будут размещены на сайте EPI. Периодически его также нужно подтверждать.

У EPI, как и у Uptime, существуют курсы обучения, например курс "Сертифицированный менеджер по эксплуатации центров обработки данных".

Вызовы, стоящие перед службой эксплуатации

Период эксплуатации, безусловно, сопряжен с рядом вызовов:

- постоянная модернизация оборудования инженерных сетей и систем;
- управление структурой больших данных;
- повышение надежности системы.

Возникновение таких вызовов связано с развитием технологий в ИТ и с искусственным интеллектом (ИИ). По моим наблюдениям, любое уважающее себя мероприятие по ЦОД должно осветить вопрос, как надо изменить технологии в проектировании и в строительстве ЦОД для того, чтобы разместить в нем стойки для развертывания инфраструктуры ИИ, где будут большие мощности, и есть ли специфические требования к охлаждению. Речь о водяном или погружном охлаждении и о том, как это размещение повлияет на всю остальную инфраструктуру: какие площади высвободятся, какие будут, наоборот, заняты и т.д.

Повышение энергоэффективности

Электричество дорожает, в том числе и в связи с развитием информационных технологий и ИИ, возникает дефицит мощностей. Где его взять? Вопрос остается открытым. Но уже понятно, что потребности в электричестве для ИИ превышают возможности его генерации. Работы ведутся, но при этом в существующих ЦОД возникает проблема: как только вы захотите поставить стойку с GPU (стойка (сервер) с графическим процессором), то есть с серверами, которые работают с ИИ, потребуются очень большие мощности, 40 кВт на стойку и выше. Причем вам надо не только где-то взять эти мощности, но и как-то охладить высоконагруженные стойки. Такие решения есть, и они меняют архитектуру инженерной инфраструктуры современных ЦОД.

Безопасность

Новые реалии поставили ребром вопросы безопасности. Причем не только кибербезопасности, но и физической. Практически каждый существующий и новый ЦОД задумывается об антидроновой защите – это радиоэлектронные средства борьбы, физические защиты-сетки, панели и т.д. В новых проектах такие средства защиты стали обычным и чуть ли не обязательным требованием.

Проблемы эксплуатации

Проблем эксплуатации немало, начиная с устаревания техники. Замена старых компонентов – это необходимость. Старые устройства теряют эффективность работы, энергоэффективность, надежность.

Самый большой друг службы эксплуатации – система мониторинга. В зависимости от того, насколько правильно она спроектирована, как она эксплуатируется, что в ней внедряется, используется, зависит, как ЦОД себя ведет, что с ним делать, как его эксплуатировать. Для работы с большой, тяжелой системой мониторинга требуются обучение сотрудников, регулярные тренинги, сертификации. На этом этапе опять встает вопрос нехватки подготовленного, высококвалифицированного технического персонала. Нет соответствующих курсов (их мало, они дорогие), уровень заработной платы для такого персонала недостаточный. Конечно, ЦОД нужны опытные люди, умеющие работать, но при этом важно соблюсти баланс по затратам.

Большие данные

Нельзя не затронуть предиктивную аналитику, она начинает активно использоваться в системах мониторинга ЦОД. Данные сначала собираются, и чем больше датчиков, чем больше оборудования, чем больше сигналов, тем больше становится это озеро или океан данных, с которыми может работать ИИ. Дальше система мониторинга с возможностями ИИ может с этими данными работать и помогать операторам ЦОД предсказывать возможные аварии и инциденты с оборудованием инженерных систем, прогнозировать необходимые замены оборудования.

В большинстве ЦОД замена оборудования происходит по регламенту. При окончании срока службы его надо менять. Неважно, в каком состоянии оборудование, работает или нет, по регламенту его надо менять. И его меняют. Это неэффективно с точки зрения затрат на оборудование, но зато сохраняет спокойствие службе эксплуатации.

Предиктивная аналитика позволяет определять, какое оборудование может в скором времени выйти из строя. В этом случае его замена оправдана. Если таких сигналов нет, оборудование продолжают эксплуатировать.

Это позволяет снизить затраты на эксплуатацию, что является важным конкурентным преимуществом ЦОД как бизнеса.

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

НОВОСТЬ В ТЕМУ

ЦОД и климат

Компания XDI опубликовала доклад о том, насколько мировые дата-центры устойчивы к климатическим изменениям. Проанализировано около 9 тыс. ЦОД по всему миру с точки зрения их уязвимости к восьми видам климатических угроз, включая наводнения, лесные пожары, экстремальную жару, ветер и др.

Анализ охватывает действующие, строящиеся и запланированные ЦОД и делает акцент не только на текущей ситуации, но и на прогнозных ожиданиях вплоть до 2100 г. Отдельно отмечается роль адаптации ЦОД к климатическим изменениям в повышении их устойчивости и в снижении страховых расходов.

Ключевые выводы:

1. К 2050 г. доля ЦОД с высоким риском возрастает по всему миру с 6,25% в 2025 г. до 7,13%. Увеличится и доля центров с умеренным риском – с 15,79% до 19,6%. Таким образом, почти каждый четвертый ЦОД в мире будет находиться под угрозой (высокой или умеренной).
2. Наибольшую угрозу для ЦОД представляют речные и поверхностные наводнения, затопление прибрежных территорий, лесные пожары, тропические штормы, экстремальная жара, сильный ветер. Они вызывают не только физическое разрушение зданий и оборудования, но и длительные перебои в работе, потере данных и отказ систем жизнеобеспечения.
3. В 2024 г. глобальные страховые убытки для ЦОД от катастроф составили более 135 млрд долларов. Повышенный риск делает страхование ЦОД дороже, а в ряде случаев – недоступным.
4. Инвестиции в адаптацию к климатическим изменениям могут снизить убытки на 120 млрд долларов до 2050 г.
5. Риск повреждений ЦОД от климатических угроз в России и Центральной Азии вырастет на 81% к 2100 г.
6. 65–70% мощностей ЦОД в России сосредоточено в Москве и Подмоскovie, на втором месте – Санкт-Петербург. Наблюдается рост строительства в других регионах: Новосибирске, Екатеринбурге, Казани, Владивостоке.
7. Московская область занимает пятое место в глобальном рейтинге по климатическим рискам, уступая только ряду регионов Китая и Индии. Главную угрозу представляют речные наводнения.
8. Модификация конструкций зданий может снизить риск повреждений от климатических угроз почти на 90% к 2050 г.
9. Стоимость страхования ЦОД может вырасти в три–четыре раза к 2050 г.
10. Даже самые защищенные ЦОД уязвимы, если откажет внешняя инфраструктура, включая электросети, транспорт, водоснабжение. Поэтому наряду с укреплением объектов необходимы системные меры по декарбонизации и укреплению инфраструктуры.

Источник: <https://xdi.systems/>

Линейка промышленных уличных IP-камер WUB и AWH UB серии PoE стандарта IEEE 802.3af

Представляет ООО "САРОВИНТЕХ"
www.wizebox.ru



Решаемые задачи

До выпуска новой линейки PoE стандарта IEEE 802.3af приходилось отдельно прокладывать

Потребители

Для промышленных объектов, для объектов ТЭК, для объектов железной дороги и автодорог данная линейка не имеет аналогов и будет, безусловно, полезна и эффективна в применении!

Проект

Стойленский ГОК (Старый Оскол)

Появление на рынке	Январь 2025 г.
Ценовой сегмент	Средний

кабель для питания термокожуха (220 В, 24 В, 12 В, PoE+, UPoE) и отдельно UTP-кабель для передачи данных и питания видеокамеры. Теперь подводить кабель питания для термокожуха отдельно не нужно. Для полноценной работы и термокожуха и видеокамеры достаточно одного UTP-кабеля, который раньше соединял видеокамеру и коммутатор. При этом для работы оборудования подходит любой стандартный, недорогой коммутатор. Это намного упрощает работу оборудования: больше не нужно прокладывать дополнительные кабели на 220 или 240 В, ломать голову над тем, подойдет коммутатор или не подойдет, какие порты в коммутаторе могут быть использованы, а какие останутся незадействованными. С новой линейкой от WIZEBOX все порты вашего коммутатора могут быть задействованы для подключения разработанных видеокамер без исключения. Как говорится, подключил и забыл!

Технические характеристики

- Температурный режим эксплуатации от -65 до +55 °С.
- Температура "холодного старта" -60 °С.

- Питание обычное PoE (стандарт IEEE 802.3af), (≈ 15,4 Вт).
- Все внешние детали сделаны из нержавеющей стали.

Конкурентные преимущества

В настоящий момент на рынке нет решений, подобных этому. Все внешние элементы корпусов и кронштейнов выполнены из коррозионно-стойких материалов – нержавеющей стали 12X18H10T или AISI 321. Видеокамеры работают на самом распространенном PoE (стандарт IEEE 802.3af). Технология стандарта PoE af совместима со всеми существующими стандартами – PoE at и PoE bt. Это делает возможным подключение данного оборудования к коммутаторам, работающим по любым стандартам.

Экономическая эффективность

- Низкая мощность потребления. Экономия стоимости резервного питания.
- Экономия на СКС.
- Уличные камеры из нержавеющей стали по цене аналогов из алюминия благодаря новым технологиям.
- Экономия на коммутаторах. Для работы достаточно коммутатора от класса 3.

см. стр. 128 "Ньюсмейкеры"

МНЕНИЕ ЭКСПЕРТА

Александр Бахлыков

Руководитель инженерно-проектного бюро bimDC



– Какие изменения произошли на рынке в последние два-три года?

– Основное – это уход западных вендоров и последовавшее за этим импортозамещение инженерной инфраструктуры. На данный момент практически нет такого продукта, который не получилось бы в полной мере заместить на продукцию российских или китайских производителей. Не удалось заместить дизель-динамические ИБП, которые просто перестали применять, заменив на классические, статичные, решения.

– Назовите основные тенденции рынка ЦОД.

– Основная тенденция – это появление высоконагруженных стоек с серверами GPU под потребности ИИ. Причем массово такие стойки не устанавливают, это решение очень дорогостоящее и позволить себе его развернуть могут только очень крупные российские компании, такие как Сбер или Яндекс. Но возникший по этому поводу

Услуги ЦОД будут дорожать

хайп, заставляет многих задуматься – готовы ли они к установке таких стоек.

– В каких единицах, по вашему мнению, разумно оценивать мощность ЦОД?

– Основной оценкой должна быть мощность ИТ-нагрузки на ЦОД. Количество стоек и мощность на стойку могут сильно различаться и сильно меняться в пределах одного ЦОД во время его срока эксплуатации. Когда, например, ряд из 10 стоек по 10 кВт могут заменить на одну стойку 100 кВт.

– В последнее время растет спрос на модульные ЦОД. В чем их преимущества?

– Основное преимущество модульных ЦОД – проверенные на практике и оттестированные на заводе-производителе решения, которые не сильно меняются от проекта к проекту. Заставить производителя МЦОД применить что-то новое, неопробованное – это непростая задача. Производителей МЦОД не так много на российском рынке, и они дорожат своей репутацией. Вторым преимуществом является скорость разворачивания ЦОД: обычно это несколько быстрее, чем строить ЦОД с нуля или в существующем здании.

– Как влияет на инфраструктуру ЦОД ИИ?

– Инфраструктура ЦОД под нужды ИИ очень сильно отличается от классической инженер-

ной инфраструктуры ЦОД. Высокие плотности мощности на стойку, водяное охлаждение – это все специфика, которую надо учитывать.

– 24 января 2025 г. начал действовать СП 541. Какие кардинальные изменения повлек этот документ?

– Кардинальных не повлек, у проектировщиков появилась некая замена СН 512, отмененному в 2020 г., но тем не менее требования которого продолжают прописывать в технических заданиях на проектирование ЦОД. Теперь, с выходом СП 541, появилось нормальное нормативное обоснование принимаемых решений, например в экспертизе можно сослаться на требования этого СП и защитить свою позицию.

– К чему нужно готовиться компаниям, которым требуются услуги ЦОД?

– К тому, что услуги будут дорожать. В столичном регионе есть дефицит стойко-мест, в Питере тоже. В регионах нет, но нет и ярко выраженной потребности в услугах ЦОД.

Второй момент – надо подумать про создание собственного корпоративного ЦОД, как минимум в целях обеспечения лучшей безопасности собственной ИТ-инфраструктуры. Гибридная схема резервирования, когда данные хранятся и обрабатываются в собственном и коммерческом ЦОД, является оптимальной.



Александр Бахлыков

Руководитель Инженерного бюро bimDC

Что подготовил для проектировщиков новый нормативный документ СП 541.1325800.2024 "Здания и сооружения центров обработки данных. Правила проектирования"

Проктировщикам инженерной инфраструктуры центров обработки данных (ЦОД) в своей работе надо опираться на действующие стандарты и нормы, в первую голову российские, и конечно же, надо знать международные и американские стандарты и рекомендации. Вы спросите, почему американские? Так исторически сложилось, что основная масса мировых ЦОД строится в Америке и американские институты стандартизации первыми генерируют новые стандарты, а уже опираясь на них, создаются международные.

В российской нормативной базе не так много национальных стандартов, посвященных именно дата-центрам. И радует, что в начале года появился новый российский свод правил – СП 541.1325800.2024 "Здания и сооружения центров обработки данных. Правила проектирования" (далее – СП 541).

СП 541 утвержден приказом № 898 Минстроя России 23 декабря 2024 г. А через один месяц, то есть 24 января 2025 г., документ начал действовать на территории Российской Федерации. Надо сказать, что в течение всего 2024 г. СП 541 проходил многочисленные доработки, подвергался критике и изменениям, пока не приобрел свои окончательные формы.

Связано это с тем, что отрасль ЦОД неоднородна, есть разнообразные группы, которые преследуют свои интересы, в том числе и в таком деле, как стандартизация. Это, конечно, не чисто наша отраслевая особенность. Кому интересно, могут посмотреть, как принимаются стандарты в области информационного моделирования (BIM, или ТИМ на современный лад), когда разработка стандартов передается от одного министерства или организации к другой, уже выпущенные стандарты отменяются и выпускаются новые. Или как принимаются стандарты, например, по пожарной безопасности.

Что такое свод правил?

СП – это документ по стандартизации, содержащий правила и общие принципы в отношении процессов в целях обеспечения соблюдения требований технических регламентов (в ред. Федерального закона от 30.12.2020 г. № 523-ФЗ).

Разработка и утверждение сводов правил осуществляются федеральными органами испол-

24 января этого года начал действовать новый российский свод правил – СП 541.1325800.2024 "Здания и сооружения центров обработки данных. Правила проектирования". В данной статье автор раскрывает основные положения и требования этого нормативного документа, отмечает его роль и потенциальное влияние на процесс проектирования дата-центров.

нительной власти в пределах их полномочий, в нашем случае Минстроем России.

СП 541.1325800.2024 разработан в целях обеспечения соблюдения требований Федерального закона от 30 декабря 2009 г. № 384-ФЗ "Технический регламент о безопасности зданий и сооружений". Исполнитель (разработчик СП) – акционерное общество "Центральный научно-исследовательский и проектно-экспериментальный институт промышленных зданий и сооружений" (АО "ЦНИИПромзданий"). Внесен СП 541 техническим комитетом по стандартизации ТК 465 "Строительство". Коллеги из ЦНИИПромзданий при разработке достаточно плотно консультировались и с профильными организациями, и со специалистами и экспертами в области ЦОД, за что им отдельное спасибо. В частности, Ассоциация участников отрасли ЦОД (<https://dcunion.ru/>) была привлечена для консультаций при работе над СП 541.

Положения СП распространяются на проектирование зданий и сооружений центров обработки данных, а также помещений центров обработки данных в составе зданий.

Ключевое понятие здесь – проектирование помещений, зданий и сооружений ЦОД. То есть в СП 541 описано то, что относится к строительству ЦОД: разделы "архитектура" и "конструктив", а также слегка затронуты требования к созданию инженерных систем ЦОД.

СП не распространяется на проектирование некапитальных, мобильных зданий центров обработки данных.

В СП 541 содержится порядка 70 ссылок на смежные нормы и стандарты.

Термины и определения

Приведены термины и определения следующих понятий:

- горячая зона;
- здания, помещения и сооружения центра обработки данных;
- инженерно-техническая укрепленность;
- машинный зал;
- диспетчерский центр ЦОД;
- серверный шкаф;

- помещение узла взаимной коммутации центра обработки данных;
- холодная зона;
- система бесперебойного электроснабжения;
- система гарантированного электроснабжения;
- оборудование информационных технологий;
- электрогенераторная установка;
- инженерная инфраструктура центра обработки данных;
- информационно-технологическая инфраструктура центра обработки данных;
- техническая концепция инженерной инфраструктуры центра обработки данных;
- техническое обслуживание инженерной инфраструктуры (ИИ) ЦОД.

Всего 16 терминов и определений, из них 11 терминов сформулировано впервые. Например:

1. Помещение узла взаимной коммутации центра обработки данных: помещение, в котором расположено оборудование провайдеров доступа и точки разграничения, а также осуществляется коммутация и, при необходимости, обмен трафиком (met-me room, entrance room). Согласно СП 541 ЦОД могут размещаться в отдельном здании или в здании с помещениями другого назначения.

2. Стадии и этапы проектирования ЦОД должны соответствовать ГОСТ Р 58811–2020 "ЦОД. Инженерная инфраструктура. Стадии создания".

Техническая концепция ИИ ЦОД должна соответствовать ГОСТ Р 70627 "ЦОД. Техническая концепция".

3. Общую, полезную и расчетную площадь, строительный объем, площадь застройки, высоту и этажность здания ЦОД, общую, полезную и расчетную площадь помещения ЦОД следует определять в соответствии с СП 118.13330 "Общественные здания и сооружения".

4. Включать в состав проекта требования по доступности в ЦОД маломобильных групп населения (МГН) и/или организации рабочих мест МГН или не включать – определяется заданием на проектирование, ну а в помещения зоны общего доступа (для персонала и посетителей) доступность надо предусматривать.

Требования к земельным участкам

В СП 541 приведены требования к земельным участкам. Место размещения, расстояние до административного центра, транспортную доступность определяют по заданию на проектирование.

Возможность прохождения транзитных коммуникаций и нахождение сторонних организаций в ЦОД также определяют по заданию на проектирование.

Размещение здания определяют в соответствии с планом застройки территории, площадь участка – по заданию на проектирование с учетом размещения всех необходимых объектов. Размещать здания и сооружения на участке требуется с соблюдением санитарных норм и правил СанПин.

При размещении ЦОД следует также исключить влияние на ИТ-оборудование ЦОД электрических или магнитных полей и вибрацию.

Объекты и технологические зоны

Какие объекты могут быть размещены на площадке ЦОД?

На земельном участке комплекса ЦОД по заданию на проектирование предусматривают:

- здание ЦОД;
- технологическую зону (площадки внешнего энергетического оборудования, оборудования механических систем, холодо- и энергоцентр, топливохранилище, газораспределительную станцию, прочие сооружения, необходимые для функционирования ЦОД);
- административно-бытовой корпус (может быть встроенным в ЦОД);
- внутренние проезды и пешеходные тротуары;
- ограждение земельного участка ЦОД;
- автомобильный контрольно-пропускной пункт;
- контрольно-пропускной пункт;
- погрузочно-разгрузочные зоны;
- место (площадку) для накопления отходов;
- здания вспомогательного назначения;
- стоянку или места для парковки автомобилей сотрудников и посетителей ЦОД и велопарковку;
- места для парковки средств индивидуальной мобильности (СИМ), в том числе оборудованные устройствами для зарядки СИМ с электроприводом;
- место для курения;
- прочие здания и сооружения.

Необходимо предусматривать наличие основных технологических зон:

1. Информационной, в которой находятся помещения машинных залов для размещения ИТ-оборудования, а также вспомогательные по отношению к машинному залу помещения (тамбуры, коридоры, пандусы и др.).

2. Телекоммуникационной. В телекоммуникационной зоне в зданиях и помещениях ЦОД размещают помещения ввода электроэнергии (не менее двух для ЦОД больше 250 кВт), помещения узла взаимной коммутации, телекоммуникационные и аппаратные комнаты, кроссовые помещения.

3. Инженерной, в которой располагают помещения для размещения оборудования ИИ систем общего, бесперебойного и гарантиро-

ванного электроснабжения, для размещения оборудования ИИ механических систем, слабых систем, систем противопожарной защиты и технических средств охраны, а также помещения и зоны вертикальных и горизонтальных коммуникаций.

Для зданий и помещений ЦОД общей суммарной электрической мощностью, требуемой для ИТ-оборудования, менее 250 кВт допускается совмещение зон в одном помещении (или можно действовать по заданию на проектирование).

Могут быть предусмотрены дополнительные зоны (по заданию на проектирование):

- зона общего доступа (для персонала и посетителей);
- помещения диспетчерских центров;
- помещение подготовки ИТ-оборудования;
- мастерская инженерной инфраструктуры;
- вспомогательные и складские помещения запасных частей, инструментов и принадлежностей;
- административные, офисные и бытовые помещения для персонала;
- служебно-технические помещения;
- посты и помещения охраны, пост круглосуточной охраны предусматривают площадью не менее 6 кв. м;
- погрузочно-разгрузочные зоны;
- помещения дополнительных технологических служб;
- мусоросборная камера и др.

В СП 541 (приложение А) приведены также рекомендации по определению площадей зон. Конструктивными решениями в ЦОД следует исключить возможность возникновения:

1. Разрушений и (или) повреждений конструкций, приводящих к необходимости прекращения эксплуатации здания.

2. Недопустимого ухудшения эксплуатационных свойств и (или) снижения надежности конструкций вследствие деформаций или образования трещин.

3. Повреждений конструкций, нарушающих их расчетные параметры.

Конструкции зданий и помещений для размещения ЦОД должны быть рассчитаны на действие нагрузок от собственного веса, веса оборудования и конструкций, снеговых и ветровых нагрузок, нагрузок от коммуникаций согласно СП 20.13330 "Нагрузки и воздействия".

Следует предусматривать меры по устранению передачи вибрации на строительные конструкции от устанавливаемого в здании технологического оборудования (в том числе насосов, вентиляционного оборудования, электрогенераторной установки и т.п.).

В СП 541 приводятся требования к лестницам, фальшполам, стенам, перегородкам, кровлям и прочим строительным конструкциям, к защите от протечек и грунтовых вод – путем ссылок на соответствующие нормативные документы.

Требования СП 541 по пожарной безопасности

В СП 541 приведены требования пожарной безопасности, которые опираются на Федеральный закон от 22 июля 2008 г. № 123-ФЗ "Технический регламент о требованиях пожарной безопасности".

Класс функциональной пожарной опасности принимают для технологических зон – Ф5.1.

Основные требования по пожарной безопасности следующие:

1. Помещения ЦОД, размещаемые в здании иного назначения, следует отделять противопожарными преградами.

2. Технологические помещения для оборудования систем кондиционирования должны быть выделены ограждающими конструкциями с пределом огнестойкости не менее R(EI) 45 и заполнением проемов 2-го типа (предел огнестойкости 30 мин.).

3. Расстояние от наиболее удаленных точек машинного зала до эвакуационного выхода принимают не более 25 м с учетом установленных серверных шкафов, оборудования и ограждений.

4. Помещения с расходными баками топлива должны иметь непосредственный выход наружу, а при наличии второго выхода через другие помещения – быть отделенными от них тамбур-шлюзом с подпором воздуха.

5. В машинных залах ЦОД площадью 24 кв. м и более следует предусматривать автоматическую установку пожаротушения.

6. ЦОД, расположенные в отдельном здании или комплексе зданий, проектируемых специально для ЦОД, подлежат в целом защите автоматической установкой пожаротушения.

7. Для помещений машинного зала и инженерной зоны следует применять системы газового пожаротушения, пожаротушения с использованием тонкораспыленной воды или системы с использованием пригодной для дыхания гипоксической атмосферы.

8. Допускается не отключать (предусматривать задержку отключения) постоянно работающие по технологическим условиям системы кондиционирования в помещениях, защищаемых установками газового пожаротушения, при тушении объемным способом, если работа системы кондиционирования исключает добавление атмосферного воздуха в защищаемое помещение при циркуляции газовой среды.

9. При автоматическом пожаротушении в помещениях ЦОД допускается не отключать (предусматривать задержку отключения) вентиляционные установки, которые обеспечивают безопасность технологического процесса, при этом подача наружного воздуха в защищаемое помещение должна быть исключена путем перевода систем вентиляции на режим полной рециркуляции с охлаждением.

10. В случае если электроснабжение здания или помещения ЦОД или отдельных его частей обеспечивается по особой группе первой категории электроприемников по надежности электроснабжения, системы противопожарной защиты также должны быть запитаны по особой группе первой категории.

В СП 541 приведены требования к проектированию встроенных дизель-генераторных установок (ДГУ) – по отделению встроенных помещений ДГУ, установке газоанализаторов, требования к пожарной безопасности, входам/выходам в помещение ДГУ, требования к покрытию пола, к предотвращению растекания топлива, к мощности и объему встроенного бака ДГУ.

Требования к инженерному оборудованию

В СП 541 приведены требования к инженерному оборудованию:

1. Участок строительства здания ЦОД должен быть подключен к наружным сетям централизованного тепло-, водо- и электроснабжения (допускается устройство автономных источников).

2. Наружное противопожарное водоснабжение следует проводить от кольцевых водопроводных сетей, обеспечивающих расход воды на хозяйственно-питьевые и противопожарные нужды, с установкой не менее трех пожарных гидрантов на расстоянии не более 150 м от продольных сторон здания ЦОД.

3. Здания и помещения ЦОД и вспомогательные здания должны быть оборудованы следующими инженерными системами:

- хозяйственно-питьевое и горячее водоснабжение, канализация (хозяйственно-бытовая и дождевая);
- отопление, вентиляция, кондиционирование, противодымная вентиляция;
- внутренний противопожарный водопровод и системы автоматического пожаротушения;
- электроосвещение и силовое электрооборудование;
- автоматическая пожарная сигнализация;
- оповещение и управление эвакуацией при пожаре;
- лифты для транспортирования пожарных подразделений в зданиях;
- другие инженерные системы в соответствии с заданием на проектирование.

Инженерное оборудование инженерной инфраструктуры ЦОД включает основные и вспомогательные инженерно-технические системы.

Основные инженерно-технические системы включают:

- систему электроснабжения для обеспечения ИТ-оборудования электроэнергией;
- систему холодоснабжения для отвода тепловыделений от ИТ-оборудования.

Остальные инженерно-технические системы являются вспомогательными.

Электроснабжение ЦОД в свете СП 541

Система электроснабжения ЦОД состоит из:

- системы внешнего электроснабжения;
- системы общего электроснабжения;
- системы бесперебойного электроснабжения (СБЭ);
- системы гарантированного электроснабжения (СГЭ).

Нагрузки в ЦОД делятся на критичные и некритичные. К критичным нагрузкам относят нагрузки ИТ-оборудования и инженерного оборудования основных и вспомогательных инженерных систем, отключение которых приведет к нарушению функционирования ИТ-оборудования. Остальные нагрузки некритичные.

Электроснабжение электроприемников критичных нагрузок предусматривают от двух и более независимых источников питания.

Необходимо предусматривать резервирование наиболее важных элементов системы для исключения возможных единичных точек отказа.

В СП 541 приведены также требования по размещению трансформаторных подстанций, трансформаторов и подключению к сетям.

В случае, если определить перспективное потребление электроэнергии ИТ-оборудованием не представляется возможным, для расчетов используют энергонагруженность серверных шкафов по заданию на проектирование.

При расчете параметров электроустановок ЦОД коэффициент использования $K_{\text{и}}$ и коэффициент мощности $\cos \varphi$ определяются заданием на проектирование.

Защиту потребителей критичных нагрузок аппаратами, срабатывающими от дифференциальных токов утечки, не осуществляют.

В случае применения источников бесперебойного питания (ИБП) с аккумуляторными батареями (АКБ) время работы от АКБ при отсутствии электропитания на входе ИБП должно составлять не менее 5 мин. для 100%-ной нагрузки в аварийном режиме.

Для ИБП следует предусматривать внешний байпас для обеспечения возможностей полного отключения ИБП, его замены или перемещения для сервисного обслуживания.

ИБП следует применять с АКБ со сроком службы не менее пяти лет.

Допускается не выполнять СГЭ, если логикой функционирования ИТ-оборудования допускается его отключение или если внешнее электроснабжение обеспечивает электроснабжение особой группы электроприемников первой категории.

Допускается резервирование внешних источников электроснабжения как на уровне низкого напряжения, так и на уровне среднего напряжения.

Требования к системе холодоснабжения ЦОД

Система технологического кондиционирования должна обеспечивать требуемые по заданию на проектирование параметры микроклимата в машинном зале и технологических помещениях.

Систему технологического кондиционирования объединять с другими системами кондиционирования в зданиях и помещениях ЦОД не допускается.

Допустимые диапазоны температур в машинном зале принимают по заданию на проектирование.

Значение температуры в машинном зале ЦОД определяют в зоне забора воздуха ИТ-оборудованием.

Параметры относительной влажности воздуха должны поддерживаться в диапазоне от 20 до 80% для всего заданного диапазона температур в помещении.

Расчетную температуру наружного воздуха принимают по заданию на проектирование с учетом показателей абсолютной минимальной и абсолютной максимальной температуры воздуха для расчетного региона согласно СП 131.13330 "Строительная климатология".

Необходимо предусматривать резервирование ключевых узлов по заданию на проектирование. Системы поддержания влажности в ЦОД не являются критическими.

В машинных залах должно быть обеспечено избыточное давление по отношению к прилегающим помещениям. Допускается не обеспечивать избыточное давление в машинных залах при использовании прямого свободного охлаждения.

Фильтрацию и подготовку наружного воздуха следует осуществлять двухступенчатой очисткой в фильтрах класса не ниже G4 и F7.

Допускается применение систем общеобменной вентиляции для удаления огнетушащих веществ после срабатывания системы газового пожаротушения, а также допускается удаление продуктов горения с помощью передвижных дымососов.

Требования к вспомогательным инженерно-техническим системам

Автоматизированная система диспетчерского управления (АСДУ) должна предусматривать возможность контроля работы оборудования основных инженерных систем, режимов их работы, температурно-влажностных режимов технологических помещений, фактов возникновения аварийных ситуаций.

Для реализации структурированной кабельной системы (СКС) ЦОД следует предусматривать кабели или кабельные сборки, терминированные в промышленных условиях (для ЦОД >250 кВт).

Система кабеленесущих конструкций должна быть единой и учитывать прокладку слаботочных кабелей всех слаботочных систем.

Здания и помещения ЦОД должны быть запроектированы, возведены и оборудованы в соответствии с требованиями безопасности, должны также учитываться требования к безопасной эксплуатации зданий и помещений центров обработки данных, обеспечение санитарно-эпидемиологических требований, энергосбережение.

Приложения

В составе СП 541 выделены два приложения.

Приложение А (рекомендуемое) – "Допустимые диапазоны показателей или соотношений в помещениях центров обработки данных".

Приложение Б (справочное) – "Типовые схемы компоновочных решений серверных шкафов и организации воздухообмена в машинном зале центра обработки данных".

Консенсус заинтересованных сторон

Основной посыл СП – не навредить, не ограничить проектировщика, а направить его в нужную сторону.

Наиболее часто встречающийся в СП термин – "согласно заданию на проектирование (ЗНП)". Если учитывать, что задание на проектирование – это продукт консенсуса всех заинтересованных сторон, то ограничения на проектировщика в основном накладывают разработчики ЗНП, и крайне желательно задание согласовывать с проектировщиком, а лучше разрабатывать совместно с ним. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru



Александр Бахлыков
Руководитель
Инженерного бюро bimDC

В настоящее время данные, получаемые самым различным образом, приобретают всё большую ценность для организаций и ведомств, и конечно же, встает вопрос их хранения и обработки. В мире, и в том числе в России, уже имеется много центров обработки данных (далее – ЦОД) как коммерческих, так и созданных различными компаниями и ведомствами для собственных нужд. Какой путь выбрать организации, решившей обрабатывать свои данные в ЦОД? Обратиться в уже функционирующий центр, с репутацией, или же создавать с нуля корпоративный, то есть свой? Давайте прежде всего разберемся, чем они различаются, а далее поговорим о нюансах создания собственного ЦОД.

Корпоративный и коммерческий ЦОД – в чем различия?

Корпоративный центр обработки данных, конечно же, отличается от коммерческого, хотя и сходства тоже предостаточно.

Три основных отличия корпоративного ЦОД от коммерческого.

1. Коммерческий ЦОД создается для прямого извлечения прибыли, то есть он зарабатывает своим владельцам деньги за счет оказания услуг, будь то сдача мест в аренду для размещения оборудования или оказание услуг облачных сервисов. Цель – прибыль.

Корпоративный ЦОД используется для размещения собственного ИТ-оборудования конкретной организации или предприятия. Цель – безопасность.

2. Коммерческий ЦОД, как правило, имеет огромный масштаб, за счет чего уменьшаются затраты на его создание и содержание в пересчете, например, на одну стойку и увеличивается прибыль.

Корпоративный ЦОД, как правило, небольшой, создается под текущие и перспективные задачи развития бизнеса. Конечно, есть исключения – ЦОД огромных корпораций, например в России это компании “Яндекс” или VK.

3. Коммерческий ЦОД, как правило, обладает профессиональной командой для поддержки и эксплуатации, прямые обязанности которой – поддерживать ЦОД в работоспособном состоянии (договоры с заказчиками с прописанным уровнем обслуживания SLA этому весьма спо-

Планируем и проектируем корпоративный ЦОД

Итак, у компании возникла потребность в ЦОД. Работать с коммерческим или создавать свой? Свой – в уже имеющемся здании или модульный, с нуля? Чем руководствоваться? Ответы на эти вопросы читайте в данной статье.



Фото DC Studio на FreePress – <https://ru.freepress.com/>

собствуют). Риски оператора коммерческого ЦОД – штрафы!

В корпоративном ЦОД или нет выделенной команды, занимающейся только ЦОД (у людей часто масса других задач), или состав такой команды неполный, многие задачи при этом целиком закрываются договорами на обслуживание со сторонними организациями.

Есть и другие различия, можно список продолжить, но сказанного выше достаточно для понимания того, что коммерческий и корпоративный ЦОД – это разные объекты. Обычно надежность корпоративного ЦОД выше, а обслуживание инженерной инфраструктуры (ИИ) коммерческого ЦОД лучше и реализуется быстрее.

Почему организация решает создать собственный ЦОД

У организации возникает потребность в создании корпоративного ЦОД по ряду причин, назовем основные.

1. ИТ-инфраструктура выросла (или в ближайшее время вырастет) настолько, что существующей площадки для ее размещения будет недостаточно.

2. Решаются задачи резервирования, снижения рисков того, что существующий ЦОД по каким-то причинам может остановиться.

3. У организации большая, распределенная сеть отделений и филиалов в разных городах и странах, и нужно приблизить обработку данных к месту их генерации или использования (так называемые edge-ЦОД).

Как можно решать задачу создания корпоративного ЦОД?

Рассмотрим возможные варианты.

Вариант 1

Построить свой собственный ЦОД. Риски, которые возникают в случае такого решения и которые надо попытаться сразу нивелировать:

- результат работы окажется неудовлетворительным, ЦОД не будет выполнять свои функции;
 - будет превышен необходимый бюджет на строительство;
 - будет превышен бюджет на эксплуатацию.
- Основные возможности, которые предоставляет собственный ЦОД:
- лучший уровень безопасности (при соблюдении соответствующих мер);
 - низкие затраты на размещение оборудования в ЦОД (по сравнению с коммерческим ЦОД, например, отсутствует арендная плата);
 - гибкость, возможность просто развернуть любое необходимое бизнес-приложение в любой необходимой среде.

Вариант 2 – этот вариант лучше!

Арендовать себе ЦОД у коммерческого оператора в виде стойко-мест, или даже в виде выделенного машинного зала, или в виде необходимых сервисов в облаке.

Риски, которые могут возникнуть:

- повышенные затраты на поддержку и размещение своего оборудования и/или необходимых сервисов (арендная плата);
- затруднен доступ к своему оборудованию как минимум: если есть необходимость получить физический доступ к нему, нужно ехать на площадку, проходить соответствующие регламентные процедуры у оператора ЦОД;
- более низкий уровень безопасности (это скорее психологическая проблема, так как обычно у операторов пройдены процедуры сертификации по безопасности).

Возможности, возникающие при размещении ЦОД у оператора:

- не нужно единовременно выделять большой бюджет на строительство собственного ЦОД (капитальные затраты/CAPEX отсутствуют);

- возможность за небольшие деньги получить только нужные в текущий момент ресурсы или сэкономить, отказавшись от ненужных;
- скорость разворачивания ИТ-инфраструктуры (разместиться на площадке оператора – это значительно быстрее, строительство своего ЦОД – процедура, затратная по времени).

Нормативная база в помощь

Можно пойти по любому пути или выбрать гибридный вариант.

При принятии решений хорошая практика – опираться на требования и рекомендации нормативных документов в профильной или в смежных областях, причем не только российских, но и международных, американских или других национальных стандартов.

Стандарты – это правила, рекомендованные для применения в случае решения той или иной задачи, подготовленные профессионалами, которые уже сталкивались с такой же или похожей проблемой. Основаны стандарты на лучших практиках, в результате применения которых задача решалась успешно.

Стандарты в РФ – условно бесплатные, вы можете их получить в свободном доступе. Стандарты ISO, TIA и BICSI платные, но обычно предыдущую версию стандарта можно легко найти в свободном доступе, чтобы ознакомиться и понять, есть ли смысл покупать текущую версию.

В основном стандарты отвечают нам на вопросы, как спроектировать и сделать ЦОД, чтобы все было правильно, на какой уровень инженерной инфраструктуры мы бы хотели ориентироваться, чтобы получить соответствующий уровень безопасности.

Российские нормативные документы

Если поднять российскую нормативную базу стандартов ЦОД, то мы увидим следующие документы.

Стандарты, разработанные техническим комитетом ТК 120 "Центры обработки данных":

- ГОСТ Р 58811–2020 "ЦОД ИИ. Стадии создания";
- ГОСТ Р 58812–2020 "ЦОД ИИ. Операционная модель эксплуатации. Спецификация";
- ГОСТ Р 70139–2022 "ЦОД ИИ. Классификация" (действие приостановлено);
- ГОСТ Р 70627–2023 "ЦОД. Техническая концепция".

Стандарты, разработанные техническим комитетом ТК22 "Информационные технологии":

- ГОСТ Р ИСОМЭК 30134-1–2018 "ЦОД КПЭ. Основные положения и общие требования";
- ГОСТ Р ИСОМЭК 30134-2–2018 "ЦОД КПЭ ПУЭ";
- ГОСТ Р ИСОМЭК 30134-3–2018 "Коэффициент возобновляемой энергии (REF)".

В этом году начал действовать свод правил (СП), разработанный АО "ЦНИИПромзданий" и ТК 465, – СП 541.1325800.2024 "Здания и сооружения центров обработки данных. Правила проектирования".

Свод правил распространяется на проектирование зданий и сооружений центров обработки данных, а также помещений центров обработки данных в составе зданий, в том числе описаны требования пожарной безопасности.

В частности, приводятся противопожарные требования к инженерным системам и оборудованию зданий и помещений центров обработки данных.

Например, в этом СП наконец-то решен вопрос с тем, нужно ли отключать систему кондиционирования при срабатывании системы автоматического газового пожаротушения (допускается не отключать, при выполнении ряда условий, см. п.8.3.3 СП).

Международные стандарты

Если мы говорим про международные стандарты, то это стандарты ISO.

Комитет ISO/IEC JTC 1/SC 39 Sustainability, IT and data centres разработал следующие нормативные документы:

- ISO/IEC 22237-1:2021 Information technology Data centre facilities and infrastructures Part 1: General concepts;
- ISO/IEC 22237-2:2024 Information technology Data centre facilities and infrastructures Part 2: Building construction;
- ISO/IEC 22237-3:2021 Information technology Data centre facilities and infrastructures Part 3: Power distribution;
- ISO/IEC 22237-4:2021 Information technology Data centre facilities and infrastructures Part 4: Environmental control;
- ISO/IEC TS 22237-5:2018 Information technology Data centre facilities and infrastructures Part 5: Telecommunications cabling infrastructure;
- ISO/IEC 22237-6:2024 Information technology Data centre facilities and infrastructures Part 6: Security systems;
- ISO/IEC TS 22237-7:2018 Information technology Data centre facilities and infrastructures Part 7: Management and operational information;
- ISO/IEC TS 22237-30:2022 Information technology Data centre facilities and infrastructures Part 30: Earthquake risk and impact analysis;
- ISO/IEC TS 22237-31:2023 Information technology Data centre facilities and infrastructures Part 31: Key performance indicators for resilience.

Обычно данные для разработки международных стандартов берутся из хорошо проработанных и обкатанных национальных стандартов, какими, например, являются американские стандарты.

Основной стандарт относительно инженерной инфраструктуры ЦОД – Telecommunications Infrastructure Standard for Data Centers TIA-942-C, новая версия которого вышла в 2024 г. Он интересен своей классификацией ЦОД от объектов уровня Rated-1 до объектов уровня Rated-4, приведенной в приложении. Требования приведены по каждой инженерной подсистеме из состава ИИ ЦОД в удобной табличной форме. Приложение ANNEX F (INFORMATIVE) DATA CENTER INFRASTRUCTURE RATING – Architecture, Electrical, Mechanical, Telecommunications.

Существует стандарт ANSI/BICSI 002-2024 – The Standard for Data Center Design, в котором, опять же в приложении Appendix B Reliability and Availability (Informative), ЦОД разделяются на классы от Class 0 до Class 4. Стандарт очень полный, основан на реальных практических кейсах, которые могут быть применены для достижения хорошего результата при проектировании и строительстве ЦОД.

Еще одна широко известная группа стандартов – это требования консалтинговой компании Uptime Institute, которая разделяет ЦОД по уровням от Tier I до Tier IV, а также оказывает услуги по сертификации ЦОД по этим уровням. Uptime Institute сертифицирует ЦОД по следующим направлениям:

- сертификация проекта ЦОД Tier Certification of Design Documents;
- сертификация построенного ЦОД Tier Certification of Constructed Facility;
- сертификация операционной устойчивости (по сути, правильности эксплуатации ЦОД) Tier Certification of Operational Sustainability.

Сертификации Uptime Institute платные и проводятся только специалистами Uptime Institute. Очень часто можно увидеть утверждение что, например, ЦОД соответствует уровню Tier III Uptime Institute, без сертификата; скорее всего, если реальная сертификация не проводилась, это утверждение будет ошибочным.

Переходим к выбору варианта корпоративного ЦОД

Для начала следует получить ответ на вопрос, какой ЦОД нужен, и первая задача, которую требуется решить, – определить масштаб будущего корпоративного ЦОД и, при необходимости, количество таких центров.

Основной инициатор создания и потребитель услуг корпоративного ЦОД – это ИТ-отдел или ИТ-департамент предприятия. Обычно именно они иницируют работу над проектом ЦОД.

Масштаб

Для того чтобы определить масштаб будущего ЦОД, проще всего оттолкнуться от текущих потребностей в размещении ИТ-оборудования, которые ИТ-отдел прекрасно знает, и определить будущие потребности в размещении этого оборудования на перспективу срока службы ЦОД.

Для начала, собственно, нужно определить сам срок службы ЦОД, обычно он составляет от 7 до 15 лет. Далее необходимо совместно с коллегами из бизнес-департамента понять перспективы роста вашей организации на этот срок: предполагаемый рост масштабов бизнеса, темпы роста, планы открытия новых филиалов, увеличения сотрудников (показатели бизнеса, которые связаны или могут быть связаны с увеличением ИТ-нагрузок).

Компании развиваются по-разному, у кого-то линия роста может быть экспонентой, у кого-то прямой, а кто-то уже вышел на плато и практически не растет. Так как срок службы ЦОД достаточно велик, а риски того, что за это время экспонента роста бизнеса сменится прямой или прямой сменится плато, существуют, то ориентироваться лучше на максимально реальный сценарий, согласованный с бизнес-потребностями. Допустим, вы заложите 20%-ный рост бизнеса и такой же рост ИТ-нагрузки, тогда ваш ЦОД за 15 лет своего существования должен будет масштабироваться от одной стойки с ИТ-оборудованием до двенадцати.

У ЦОД есть одно прекрасное свойство: они тоже умеют масштабироваться как по количеству стоек, так и по количеству машзалов, и даже по количеству ЦОД, так что и в случае экспоненци-

ального роста есть вероятность справиться, к тому же коммерческие ЦОД с этим с удовольствием помогут.

Количество

С масштабом нашего ЦОД мы определились, а теперь попробуем определиться с количеством ЦОД, или, скажем так, локаций для размещения оборудования.

Коллеги из одного крупного банка привели простой, понятный пример – организацию резервирования базы данных на Oracle (таких баз на практике подавляющее большинство), аналогичная схема будет на PostgreSQL, который оказался в существующей реальности прекрасной альтернативой.

Две базы данных с резервированием не могут гарантировать того, что ваши данные будут в целостности и сохранности. Если нарушится связь между ними (они перестанут видеть друг друга) и при этом обе базы останутся рабочими, то в этих базах возникнут разные записи, что приведет к тому, что при восстановлении связи между узлами база данных перестанет работать, понадобится достаточно много времени, чтобы восстановить ее целостность. Чтобы избежать такой ситуации, вводят третий узел – арбитр, который поддерживает связь с базами данных, и в случае, если база данных теряет связь и с арбитром, и с другой базой данных, она просто отключается и не создает записи.

Важно, чтобы эти узлы находились в разных локациях, например в трех разных шкафах или, что гораздо лучше, в трех разных ЦОД. Причем узел-арбитр не требует большой вычислительной мощности и вполне может быть вынесен просто в отдельный микроЦОД или в коммерческий ЦОД. То есть в идеальной ситуации нам нужно минимум три географически разнесенные локации, или ЦОД.

Вернемся к стандартам и посмотрим на ГОСТ Р 58811–2020 "ЦОД ИИ. Стадии создания", где описаны последовательные этапы создания ЦОД. Тут приведен общий случай, на практике некоторые этапы исключают или объединяют. Например, есть стадии "проектная и рабочая документация", но в случае, если у нас не капитальное строительство, стадия П нам не понадобится, можно обойтись одностадийным проектированием, допустим если мы предполагаем установку модульного ЦОД.

Разработка технической концепции

Крайне не рекомендуется пропускать этап разработки технической концепции. Правильно разработанная техническая концепция позволит в дальнейшем сократить время на проектирование и добавит уверенности и реальных обоснований того, что решение выбрано правильно.

Этап разработки технической концепции описан в ГОСТ Р 70627–2023 "Инженерная инфраструктура. Документация. Техническая концепция. Требования к составу и содержанию".

Чем хороша техническая концепция? Техническая концепция (ТК) – комплект документов, предназначенных для описания вариантов реализации ИИ ЦОД и обоснования выбора варианта, удовлетворяющего требованиям заказчика.

Стоимость разработки этого документа не очень большая, но при этом вы получите подробный план реализации нескольких вариантов ЦОД, например, сможете рассмотреть все плюсы и минусы покупки и установки модульного ЦОД или строительства ЦОД в существующем капитальном здании.

В концепции будет проведена оценка преимуществ и недостатков каждого варианта, сопоставление требований заказчика и характеристик предлагаемой ИИ ЦОД и выбор оптимального варианта, а также будет посчитана стоимость реализации и дальнейшей эксплуатации разных вариантов ЦОД. Имея этот документ, можно предметно общаться с руководством/владельцами предприятия на тему создания корпоративного ЦОД на понятном им языке цифр бюджетов: капитальные затраты/CAPEX будут такими, операционные затраты/OPEX будут вот такие, а совокупная стоимость владения будет вот такая.

Технический аспект реализации корпоративного ЦОД

Отдельно хотелось бы остановиться на выборе варианта технической реализации корпоративного ЦОД в разрезе, что делать – ЦОД модульный или в капитальном строении.

Могут быть ситуации, когда варианты отсутствуют: например, у заказчика нет территории предприятия, чтобы поставить модульный ЦОД (далее – МЦОД) или, наоборот, территории много, но это, допустим, карьер с небольшим АБК, в котором еле-еле помещается персонал, – тут без вариантов придется делать МЦОД.

А если можно сделать и так, и так, то придется рассмотреть, как минимум основные плюсы и минусы разных решений. Попробуем исключить то, что в этих ЦОД будет равноценно, и понять, в чем будут заключаться базовые различия.

Количество и мощность стоек в обоих ЦОД примем одинаковые. Тогда:

- для системы основного, гарантированного и бесперебойного электропитания решения будут примерно одинаковые;
- для системы охлаждения и вентиляции решения также будут примерно одинаковые;
- СКС внутри ЦОД – аналогично, одинаковые решения;
- системы физической безопасности – одинаковые;
- системы пожарной безопасности – примерно одинаковые.

А где же различия?

Основное различие – это конструктив.

В модульном ЦОД производитель путем расчетов и экспериментов подобрал оптимальные параметры для того, чтобы обеспечить оптимальные условия для работы и оборудования и персонала.

В ЦОД внутри капитального здания вы всегда заложите существующего ограничения конфигурации помещения – размеров, высоты, несущей способности перекрытия, защиты от протечек, транзитных коммуникаций и т.д. То есть в уже имеющемся здании вы приспосабливаетесь под существующие ограничения, за счет чего снижается надежность и очень часто – функциональность инженерных систем.

Второй немаловажный момент: МЦОД собирается и тестируется на заводе, надежность решения значительно выше, но есть и минус: гибкость такого решения ниже, производитель не пойдет на установку "любого" оборудования, там будут только проверенные решения.

Как раз установка "любого хорошего" (разрекламированного) оборудования в ЦОД внутри капитального здания несет основные риски того, что система "не полетит" (не будет работать как планировалось), так как обычно интегратора и проектировщика уговорить что-то поменять гораздо проще, чем производителя модульного ЦОД.

ИИ ЦОД консервативна, любит проверенные решения, и новым производителям оборудования доверие надо заслужить как минимум путем заводского тестирования различных конфигураций и режимов работы.

Стоимость реализации МЦОД обычно выше на 20–50% стоимости реализации ЦОД в существующем капитальном здании, но надежность и эффективность МЦОД, как правило, лучше (тут тоже вопрос выбора производителя немаловажен).

И есть еще один момент: выбрав МЦОД, можно получить экономию времени за счет сокращения сроков проектирования и экономию на сроках проведения строительно-монтажных (СМР) и пусконаладочных (ПНР) работ за счет высокой заводской готовности МЦОД.

Заключение

В качестве резюме хотелось бы отметить следующее:

- рассматривать нужно все варианты возможной реализации корпоративного ЦОД, не исключая размещение своего оборудования в коммерческом ЦОД;
- резервирование на уровне нескольких ЦОД позволяет снизить требования по отказоустойчивости инженерной и ИТ-инфраструктуры отдельного ЦОД;
- ЦОД служат годами, при планировании надо учитывать перспективы развития бизнеса;
- ЦОД – это очень дорогостоящее вложение средств, ошибки при выборе решения и проектировании могут быть очень болезненными, нужно найти время на тщательную проработку концепции и проекта;
- стандарты – это ваши помощники, это своды знаний, разработанные экспертами и профессионалами; пользуйтесь ими, чтобы сделать свое решение лучше;

– в ситуации, когда есть выбор, присмотритесь к префаб-решениям (модульным ЦОД).

Многое зависит от масштаба создаваемого ЦОД и времени, которое заказчик готов потратить на реализацию проекта.

Строительство ЦОД – достаточно затратная статья расходов в бюджете организации, и если нет времени, лучше рассмотреть установку ИТ-оборудования в коммерческом ЦОД сейчас с тем, чтобы найти время на тщательную проработку решения и реализацию собственного корпоративного ЦОД. ■

Ваши мнение и вопросы по статье направляйте на ss@groteck.ru



Александр Бахлыков

Руководитель компании bimDC,
ответственный секретарь
ТК 120 "Центры обработки данных"

В каждой развитой стране существуют национальные организации по стандартизации, есть и международные. Стандартизация позволяет сократить время на проектирование и производство, дает возможность применять типовые проверенные решения, облегчает процесс проверки соответствия заявленным характеристикам и т.п.

Однако у стандартизации есть и обратный эффект: стандарты – это шаблон, некие рамки, в случае применения которых ограничивается свобода творчества. Если вы художник, творить по стандарту не получится. Зато выпускать качественную продукцию, повторяя историю успеха, вполне возможно.

Международные организации по стандартизации

Рассмотрим основные международные организации по стандартизации.

ISO

Международная организация по стандартизации ISO (от англ. International Organization for Standardization) создана в 1946 г. 25 национальными организациями по стандартизации. По сути, это было слияние на основе двух международных компаний: ISA (International Federation of National Standardizing Associations), учрежденной в Нью-Йорке в 1926 г. (расформирована в 1942 г.) и UNSCC (United Nations Standards Coordinating Committee), учрежденной в 1944 г.

Фактически работа ISO началась с 1947 г.

СССР являлся одним из основателей ISO, наши соотечественники были постоянными членами руководящих органов, дважды представитель Госстандарта избирался председателем организации. Россия стала членом ISO как правопреемник СССР и 23 сентября 2005 г. вошла в Совет ISO.

Сфера деятельности ISO касается стандартизации во всех областях, кроме электротехники и электроники, относящихся к компетенции Международной электротехнической комиссии (МЭК, IEC). Некоторые виды работ выполняются совместными усилиями этих организаций. Кроме стандартизации, ISO занимается проблемами сертификации.

Нормативные базы для создания ЦОД в России и за рубежом

В этой статье я расскажу про многообразие стандартов, применимых к центрам обработки данных (ЦОД). Одни из них касаются отдельных компонентов, другие строительства, третьи больше затрагивают эксплуатационные особенности ЦОД. Стандартов немало. Хорошо ли это?

ISO выпустила ряд международных стандартов, касающихся ЦОД:

- ISO/IEC 22237-1:2021 Information technology Data centre facilities and infrastructures Part 1: General concepts;
- ISO/IEC 22237-2:2024 Information technology Data centre facilities and infrastructures Part 2: Building construction;
- ISO/IEC 22237-3:2021 Information technology Data centre facilities and infrastructures Part 3: Power distribution;
- ISO/IEC 22237-4:2021 Information technology Data centre facilities and infrastructures Part 4: Environmental control;
- ISO/IEC TS 22237-5:2018 Information technology Data centre facilities and infrastructures Part 5: Telecommunications cabling infrastructure;
- ISO/IEC 22237-6:2024 Information technology Data centre facilities and infrastructures Part 6: Security systems.

Данные стандарты касаются всего, что относится к инженерной инфраструктуре ЦОД: проектирования, строительства, частично затрагиваются вопросы эксплуатации, показателей центров обработки данных.

В соответствии с критериями, описанными в стандартах ISO/IEC 22237-2 и ISO/IEC 22237-5, ЦОД получает оценку класса доступности, а также общий уровень оценки для всего центра обработки данных (1–4). В соответствии с критериями, указанными в стандарте ISO/IEC 22237-6, ЦОД получает класс защиты (1–4).

Помимо указанных стандартов, к основным концепциям, к строительству, которое относится к электрике, к механическим системам, к охлаждению или к кабельной инфраструктуре есть еще масса технических бюллетеней с пометкой TS.

На сайте ISO описываются также не вошедшие в стандарт дополнительные вопросы, которые относятся к построению центров обработки данных. Там можно ознакомиться и с ожидаемыми перевыпусками стандартов, которые происходят примерно раз в пять лет в связи с изменениями в технике и в технологиях.

CENELEC

Европейский комитет по электротехнической стандартизации (European Committee for Electrotechnical Standardization), комитет EN 50600-X Information Technology разработал серию стандартов по проектированию, построению, эксплуатации, ключевым показателям ЦОД – Data Centre Facilities and Infrastructures.

Работа комитета по стандартизации ЦОД стартовала в 2012 г.

Одним из решений стало разделение ЦОД на классы по уровню готовности, физической безопасности и энергоэффективности:

- по уровню готовности ЦОД разделяются на уровни Class 1 – Class 4;
- по уровню физической безопасности ЦОД разделяются на уровни "Зона 1 – Зона 4";
- по уровню энергетической эффективности ЦОД разделяются на "Уровень 1 – Уровень 3".

BICSI

Международная консалтинговая служба строительной отрасли BICSI (Building Industry Consulting Service International) – это профессиональная ассоциация, поддерживающая индустрию информационных и коммуникационных технологий (ИКТ), которая охватывает спектр технологии голоса, данных, безопасности и защиты электронных устройств, аудио и видео, а также технологии автоматизации зданий. Последнее включает в себя проектирование, интеграцию и установку кабельных трасс и мест размещения оборудования, оптоволоконных и медных распределительных систем, беспроводных систем и инфраструктуры, которая поддерживает передачу информации и связанную с ней передачу сигналов между устройствами связи и сбора информации.

Один из самых известных стандартов этой организации – BICSI 002 (Data Center Design and Implementation Best Practices). Последняя его версия вышла в 2024 г. – ANSI/BICSI 002-2024. В этом руководстве много описаний из областей электрики, охлаждения, архитектуры ЦОД, также есть достаточно серьезные приложения с формулами для расчета устойчивости и доступности.

Летом этого года BICSI выпустила новую версию стандарта в части организации обслуживания и технической поддержки ЦОД – ANSI/BICSI 009-2024 Data Center Operations and Maintenance Best Practices.

EIA

Альянс электронной индустрии EIA (Electronic Industries Alliance) – это объединение производителей США в сфере ИТ.

EIA была создана специально для разработки единых стандартов для всех производителей, для того чтобы выпускаемая ими продукция была совместима между собой. История EIA начинается с 1924 г., когда была создана Ассоциация производителей радиооборудования (Associated Radio Manufacturers – ARM). Все выпускаемые EIA стандарты обозначаются буквами RS и номером стандарта. Одним из наиболее известных стандартов является RS-232.

Национальные организации по стандартизации

Касательно ЦОД, из национальных нас в первую очередь интересуют американские организации по стандартизации.

TIA

Ассоциация телекоммуникационной промышленности США TIA (Telecommunication Industry Association) известна всем профессионалам своим стандартом TIA-942.

TIA – это ассоциация телекоммуникационной индустрии, объединение ведущих производителей в области связи в США, занимающаяся разработкой стандартов в области связи.

Историю TIA можно проследить с 1924 г., когда небольшая группа поставщиков телефонного оборудования собралась, чтобы разработать план развития этой отрасли.

Ассоциация телекоммуникационной индустрии входила когда-то в Альянс электронной индустрии, потом он был реорганизован в 2011 г. За то время, пока ассоциация TIA входила в Альянс, она успела выпустить в 2005 г. стандарт, очень известный в мире, – TIA-942, который развивался довольно интенсивно.

Первая версия этого стандарта была без номера, в свое время она была переведена на русский язык, и многие им пользовались. В 2014 г. вышло обновление с буквой А. В 2017 г. вышла действующая на данный момент редакция стандарта с буквой В: TIA-942В.

В мае 2024 г. была выпущена третья редакция стандарта телекоммуникационной инфраструктуры для центров обработки данных ANSI/TIA-942. Эта редакция, известная как ANSI/TIA-942-С, основана на предыдущих версиях и продолжает описывать новые технологии для повышения производительности центров обработки данных в условиях появления новых данных и новых технологий, таких как искусственный интеллект (AI) и виртуальная реальность (VR).

В первую очередь стандарт затрагивает кабельную инфраструктуру в ЦОД, но также и организацию помещений в ЦОД, требования к электрике и охлаждению и прочие вопросы создания инженерной инфраструктуры.

Основное приложение, которое используется в стандарте, – приложение F, касающееся рейтинга инфраструктуры и центров обработки данных. В приложении есть четыре таблички, относящиеся к архитектуре, к электрике, к механике, к охлаждению и к телекоммуникационной инфраструктуре. В зависимости от того, какого уровня ЦОД строится или сертифицируется, у них будет разный рейтинг по этим четырем направлениям. Причем рейтинг может варьироваться по разным направлениям, например два по архитектуре и три-четыре по электрике.

Uptime Institute

Uptime Institute (UI) – независимый поставщик консалтинговых услуг, сертификации и обучения в области центров обработки данных. Это консалтинговое агентство, которое предоставляет очень хорошую экспертизу именно по рынку центров обработки данных. Агентство оказывает услуги по сертификации дата-центров во всем мире, и в том числе в России.

Список сертификатов Uptime Institute:

1. Tier Certification of Design Documents (TCDD) – сертификация проектной документации.

Консультанты Uptime Institute просматривают полностью всю документацию, включая электрические, механические, мониторинговые и автоматические подсистемы. Они знакомятся

с фундаментальными положениями и проверяют, нет ли слабых звеньев в цепи.

2. Tier Certification of Constructed Facility (TCCF) – сертификация построенного ЦОД и проверка на соответствие требованиям, заявленным в проектной документации. Консультанты Uptime Institute посещают объект и выполняют необходимые проверки.

3. Tier Certification of Operational Sustainability – сертификация текущей работы дата-центров.

Процесс сертификации включает сравнительный анализ возможностей управленческой команды по специальному чек-листу с обязательным выездом консультантов на место.

Есть четыре уровня надежности дата-центров по стандарту Tier:

- Tier I – базовый уровень. Такой центр располагает выделенным помещением под оборудование, снабжен источниками бесперебойного питания и кулерами. Максимальное время простоя составляет 28,8 часа.

- Tier II – резервирование мощностей. Дата-центр оборудуется запасными источниками бесперебойного питания (ИБП) и охлаждением, фальшполами для прокладки кабелей и труб. Нормативная пауза составляет менее 22 часов за год.

- Tier III – техническое обслуживание (ТО) и ремонт без остановок. ЦОД третьего уровня распространены больше всего и являются оптимальным решением для ИТ-сервисов, для которых неприемлемы продолжительные паузы и возможные перебои. Предельное время простоя снижается до 1,6 часа благодаря дублированию всей инфраструктуры.

- Tier IV – максимальная отказоустойчивость. Это самый надежный класс ЦОД. Его отличительная особенность состоит в 100%-ном дублировании всех компонентов инфраструктуры по схеме 2(N+1).

Сертификаты UI достаточно кратковременные: какие-то выдаются на год, какие-то на три.

В 115 странах на данный момент выполнено порядка 2 650 сертификаций Uptime. Эта американская организация сейчас представлена и в России.

ASHRAE

Стандарты Американского сообщества инженеров по отоплению, охлаждению и кондиционированию ASHRAE (The American Society of Heating, Refrigerating and Air-Conditioning Engineers) в основном интересны тем специалистам, которые отвечают за охлаждение ЦОД.

В пятом издании Рекомендаций по тепловому режиму в средах с оборудованием для обработки данных (Thermal Guidelines for Data Processing Environments, 5th Ed) к существующим классам ИТ-оборудования (от А1 до А4) добавлен класс оборудования Н1.

К этому классу относятся системы с тесно интегрированными высокопроизводительными компонентами (серверными процессорами, ускорителями вычислений, микросхемами памяти и сетевыми контроллерами). Так, если у вас в ЦОД предполагается размещение высокопроизводительных серверов, то у вас начинают действовать требования по ограничению температурного диапазона. Если для обычного оборудования температурный диапазон колеблется от 18 до 27 °С, то для оборудования класса Н-1 это от 18 до 22 °С.

В руководстве ASHRAE представлены I-d диаграммы, на которых изображен неправильный прямоугольник с возможными разрешенными значениями температуры и влажности.

На сайте ASHRAE вы также найдете карту, на которой можно выбрать любую местность, где планируется строительство ЦОД, и посмотреть значение минимальной и максимальной температуры воздуха за много лет, эта информация поможет рассчитать параметры установки для охлаждения.

Российская нормативная база

За время своего существования технический комитет ТК 120 "Центр обработки данных" выпустил определенное количество стандартов, которые также можно использовать в своей работе.

Среди них:

- ГОСТ Р 58811–2020 "ЦОД. Инженерная инфраструктура. Стадии создания";

- ГОСТ Р 58812–2020 "ЦОД. Инженерная инфраструктура. Операционная модель эксплуатации. Спецификация";

- ГОСТ Р 70139–2022 "ЦОД. Инженерная инфраструктура. Классификация";

- ГОСТ Р 70627–2023 "ЦОД. Инженерная инфраструктура. Документация. Техническая концепция. Требования к составу и содержанию".

Технический комитет ТК 22 "Информационные технологии" также выпустил ряд стандартов по показателям ЦОД:

- ГОСТ Р ИСОМЭК 30134-1–2018 "ЦОД. КПЭ. Основные положения и общие требования";

- ГОСТ Р ИСОМЭК 30134-2–2018 "ЦОД. КПЭ. Пуэ";

- ГОСТ Р ИСОМЭК 30134-3–2018 "Коэффициент возобновляемой энергии (REF)".

ГОСТ на классификацию – это один из самых проблемных стандартов, в котором много открытых вопросов. Классификация получилась достаточно сложная, по ней выделяется пять уровней, пять классов для ЦОД, и для коммерческих, и для государственных. При этом у профессионалов отрасли ЦОД постоянно возникают вопросы по параметрам классификации.

Некоммерческая организация АНО КС ЦОД параллельно выпустила свою альтернативную классификацию. Есть два противоположных мнения: одно, что эти классификации сильно противоречат друг другу и сосуществовать не могут, другое – что нужно придерживаться общемировой практики, где принято использовать одновременно множество классификаций. Сейчас ведется работа АО "ЦНИИ Промзданий", которое разрабатывает СП "Здания и сооружения центров обработки данных. Правила проектирования".

Видно, что и в мире, и в России отрасль ЦОД активно развивается, работа по стандартизации активно ведется, стандарты постоянно обновляются или появляются новые, и, чтобы оставаться в курсе последних событий в проектировании, строительстве и эксплуатации ЦОД, надо регулярно отслеживать появление новых версий, вникать, какие произошли изменения в требованиях. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru

