Как построить ЦОД для транспорта

Рост рынка цифровых сервисов для транспорта, автоматизация бизнес-процессов в отрасли, а также стремительная интеллектуализация городских транспортных систем способствуют постоянному увеличению объема хранимых и обрабатываемых данных. Транспортные компании и объекты инфраструктуры явственно нуждаются в надежных и энергоэффективных дата-центрах. Вот только стоит помнить, что соответствующие качества закладываются на стадии проектирования и строительства ЦОДов.

Текст: Петр Вашкевич, главный инженер ЗАО «КРОК инкорпорейтед»

ПРЕДПОСЫЛКИ

В настоящее время в сумме несколько десятков вычислительных центров имеют РЖД и Росавтодор, введены в строй дата-центры «Аэрофлота», ЦОДы отдельных аэропортов — например «Шереметьево», «Домодедово», «Внуково», в Сочи… Перечислять можно еще очень долго.

Крупные транспортные хабы ежегодно обслуживают несколько миллионов человек. Здесь параллельно протекает множество процессов: планирование и управление расписанием, установление статусов рейсов, диспетчеризация прибытия и отправления, регистрация пассажиров, покупка и продажа билетов и т. д.

Городские транспортные системы собирают и анализируют характеристики трафика, метеоданные, сообщения об инцидентах на дороге, плановых перекрытиях и изменениях в организации дорожного движения.

Помимо этого, на всех объектах транспортной инфраструктуры и транспортных средствах реализуются мероприятия по обеспечению безопасности пассажиров. И они также требуют значительного количества вычислительных ресурсов и мощностей.

При этом остановка процессов или потеря данных могут повлечь за собой не только убытки, но и критическое снижение уровня безопасности объектов транспортного комплекса.

Перечисленные факторы служат драйверами строительства все новых и новых дата-центров.

НЕРИТОРИЧЕСКИЕ ВОПРОСЫ: ГДЕ И КАК

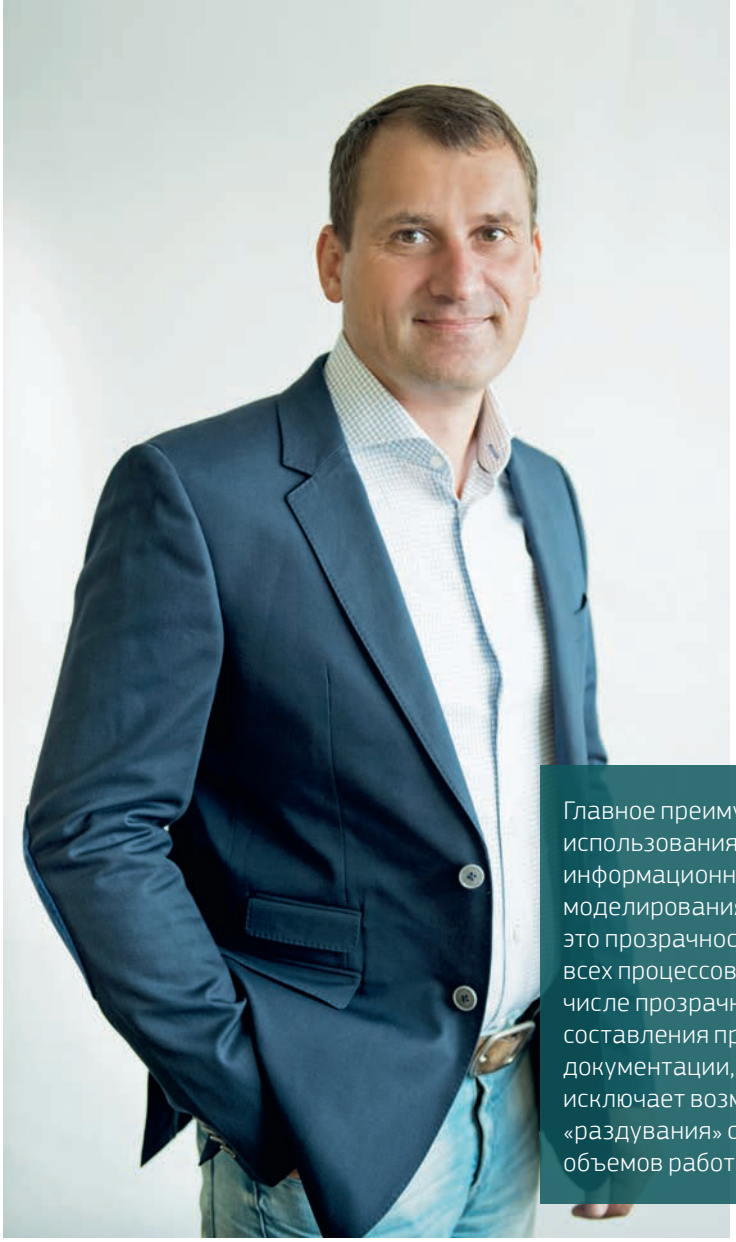
Правильный выбор места — отдельная серьезная задача, к решению которой нужно подходить очень тщательно. Дата-центр — это уникальный в своем роде продукт, поэтому для его строительства подойдет далеко не любая территория.

Чтобы избежать проблем с электроснабжением, безусловно, нужно размещать ЦОД в тех местах, где исключена ситуация энергодефицита. Причем важно учитывать и массу других параметров, таких как обеспеченность сетями связи и персоналом, доступность площадки.

Говоря о самой структуре ЦОД, нужно помнить, что если серверные системы легко и оперативно масштабиру-

How to build DPC for transport / By Petr Vashkevich, Chief Engineer, CROC Incorporated JSC

The growth of the digital services market for transport, the automation of business processes in the industry, as well as the rapid intellectualization of urban transport systems contribute to the constant increase in the amount of stored and processed data. Transport companies and infrastructure facilities clearly need reliable and energy efficient data centers. Although it should be remembered, that the corresponding qualities are laid at the stage of design and construction of data processing centers.



Главное преимущество использования информационного моделирования — это прозрачность всех процессов, в том числе прозрачность составления проектной документации, что исключает возможность «раздувания» смет или объемов работ

ются без влияния на уже запущенную инфраструктуру, то для инженерных необходим целый комплекс пусконаладочных работ, порой даже с отключением части систем, что для функционирующего объекта, конечно, недопустимо. Поэтому о правильном соотнесении скорости заполнения ЦОД и возможности его масштабирования необходимо задуматься именно на этапе проектирования.

По опыту выполненных проектов можно сказать, что масштабировать крупные ЦОД лучше всего с шагом около 1 МВт. Если же говорить об объектах малой мощности, то лучше всего использовать готовые модульные решения, где шаг будет порядка нескольких десятков киловатт.

ИСКЛЮЧАЯ КОЛЛИЗИИ

Безусловно, ЦОД можно считать сложным объектом строительства, в том числе и из-за его инженерной инфраструктуры.

Мало того что большое количество инженерных систем интегрированы друг с другом, зачастую также возникает необходимость вписывать их в уже существующие архитектурные решения. В этом случае цена ошибок при проектировании возрастает.

Если учесть, что стоимость корректировки решений увеличивается на протяжении всего жизненного цикла объекта, при проектировании ЦОД важно создать как можно более точный комплект рабочей документации — с возможностью строить дата-центр и размещать там оборудование по плану, а не искать обходные пути уже на месте. Решать указанные задачи помогают технологии информационного моделирования (BIM).

В целом сейчас производители оборудования, в том числе для инженерных систем и систем безопасности, идут по пути формирования библиотек информационных моделей, однако пока не все библиотечные элементы (семейства) можно корректно применять.

На одном из проектов мы столкнулись с тем, что готовые библиотеки от производителей были только у поставщиков динамических дизельных источников бесперебойного питания (ДДИБП) и шинопроводов. Поэтому также использовали собственные наработки и элементы из общедоступных источников.

Однако, стоит признать, постепенно использование BIM-технологий становится негласным стандартом, причем на всех этапах жизненного цикла — от проектирования до эксплуатации.

Главное преимущество использования информационного моделирования — это прозрачность всех процессов, в том числе прозрачность составления проектной документации, что исключает возможность «раздувания» смет или объемов работ.

BIM-модель позволяет выбрать из различных компоновок всех систем здания наиболее оптимальный вариант и за счет наглядности элементов выявить все коллизии и нестыковки.

На этапе строительства она обеспечивает обратную связь со стройплощадки и контроль за фактическим продвижением работ. Исходя из нашего проектного опыта можно сказать, что использование BIM-модели при проектировании и строительстве помогает сэкономить порядка 10-20% на капитальных затратах. Помимо этого, на этапе эксплуатации информационная модель становится единой площадкой, объединяющей средства контроля и планирования работ по обслуживанию ЦОД.

ОПТИМИЗАЦИЯ ПРЕЖДЕ ВСЕГО

На фоне нестабильной экономической обстановки в стране, сокращающихся бюджетов и увеличения стоимости электроэнергии на первый план выходит энергоэффективность ЦОД. При этом главный критерий высокого результата — хорошие показатели PUE (коэффициент эффективности использования энергии) без увеличения капитальных затрат.

Эта задача должна решаться за счет глубокой оптимизации всех инженерных систем. В первую очередь это, конечно, касается системы охлаждения: если грамотно выбрать основные составляющие (чиллеры, фанкойлы, насосы, градирни и т. д.) и улучшить параметры каждого, то в результате можно получить заметную экономию.

Любое уже существующее на рынке решение можно сделать еще эффективнее с учетом поставленных бизнес-задач. Например, в одном из проектов путем оптимизации классической системы охлаждения «чиллер–фанкойл» мы добились среднегодового значения PUE — 1,25, пикового — 1,4, что на 20% лучше средних показателей дата-центров по миру.

Также при строительстве ЦОД стоит взять на вооружение принцип «делай как можно проще». Например, простая топология системы электроснабжения поможет заметно снизить энергопотери и обеспечить безопасное обслуживание.

К дата-центрам, обеспечивающим непрерывность процессов на транспорте, предъявляются высокие требования к бесперебойности питания. Поэтому для ЦОД, мощностью от 1 МВт, лучшим решением будет применение дизельных динамических ИБП — при прекращении подачи электроэнергии из основных источников ротор ДДИБП продолжает вращаться, сохраняя прежние параметры сети до ввода питания от дизеля. Они просты и надежны в использовании, имеют длительный срок эксплуатации.

Конечно, внедрение оптимизированных решений и обеспечение бесперебойной работы сложно себе представить без автоматизации и диспетчеризации — для современных ЦОДов этот пункт уже можно считать обязательным. Во-первых, это позволяет регистрировать работу всех систем в соответствии с заданными параметрами, во-вторых, обеспечить быстрое реагирование на возможные инциденты.

> Для подтверждения реального уровня отказоустойчивости стоит провести на объекте тесты, предусмотренные в демонстрационном списке Uptime Institute, на соответствие определенному уровню

МАКСИМУМ ЗАЩИТЫ

Дата-центр — ключевая часть ИТ-инфраструктуры. Зачастую потеря или утечка хранящихся и обрабатывающихся там данных может стоить десятки миллионов долларов.

Большую роль играет обеспечение информационной безопасности, однако даже она не поможет, если злоумышленник сможет беспрепятственно попасть, например, в машинный зал и организовать там диверсию. Именно поэтому физической безопасности также уделяется пристальное внимание.

Всего должно быть выделено несколько периметров безопасности (как минимум Территория, Здание, Машзал), причем чем важнее зона, тем бóльшие требования предъявляются к системам безопасности.

Для постоянного контроля за ситуацией нужно реализовать систему интеллектуального видеонаблюдения, работающую в режиме 24/7/365 — как на прилегающей территории, так и внутри зданий. Чтобы исключить возможность пронести на объект запрещенные предметы, необходимо оборудовать точки входа досмотровым оборудованием. Исключить использование чужого пропуска лучше всего поможет двухфакторная идентификация — личная карта доступа плюс биометрические параметры человека. Особенно это актуально для самой важной части дата-центра — машинного зала.

ПРИДЕРЖИВАЯСЬ СТАНДАРТОВ

Для владельцев коммерческих ЦОДов сертификация играет достаточно важную роль. Только оценка независимой консалтинговой компании рассматривается клиентом в качестве достоверного подтверждения уровня резервирования систем. Именно он является главным показателем надежности ЦОД. Самой популярной системой считается сертификация по стандарту Tier (от I до IV), разработанная американской компанией Uptime Institute.

В случае с ЦОДом для транспортной инфраструктуры получение сертификата, конечно, не первоочередная задача. В таком случае критерии системы сертификации стоит рассматривать в качестве некоего чек-листа с необходимыми техническими требованиями для проектирования и построения объекта.

Для подтверждения реального уровня отказоустойчивости стоит провести на объекте тесты, предусмотренные в демонстрационном списке Uptime Institute, на соответствие определенному уровню. На мой взгляд, оптимальным выбором является ЦОД уровня Tier III — с резервированием не менее чем N+1 и возможностью проведения технического обслуживания любого из компонентов (в том числе добавление и удаление вышедшего из строя оборудования) без остановки работы дата-центра.

Контроль доступа в ЦОД

Александр Чижов
генеральный
директор
ООО «Агрегатор»

Как сказано выше, самое ценное в ЦОДе — это серверное оборудование, установленное непосредственно в шкафах. С точки зрения экономики не очень логично финансировать вопросы, связанные с доступом к этому оборудованию, по остаточному принципу. Особенно учитывая, что бюджет на все системы безопасности ЦОДа (видеонаблюдение, СКУД, периметр и пр.) зачастую не превышает 5% от общего бюджета объекта.

При этом в реальных проектах с завидным постоянством ограничение доступа и разграничение прав заканчивается на этапе двери, ведущей в помещение машинного зала. При необходимости применить какое-либо решение для контроля шкафов с ценнейшим оборудованием начинают возникать сложности. Компании, строящие ЦОДы и эксплуатационные службы, выходят из этой ситуации по-разному.

Кто-то на уровне административных решений — бумажный журнал, куда сотрудники должны записывать время вскрытия шкафа, а потом вешать на него пластиковую пломбу. Здесь достаточно простая и понятная проблематика (еще из прошлого века): а кто вообще открыл шкаф на самом деле, записал/не записал, сколько времени реально шкаф оставался открытым, закрыл/не закрыл, как положено, и так далее.

Кто-то применяет решения, предлагаемые самими производителями шкафов. Но, как правило, в данном случае появляется ряд функциональных ограничений. Данные решения создавались в основном людьми из ИТ и для людей из ИТ, без учета ряда требований, которые с точки зрения службы безопасности просто «must have». И по большей части вписываются в идеологию мониторинговых систем, где приоритет не в том, чтобы должным образом и с соответствующим функционалом вписать ограничение доступа к шкафам в существующую на объекте систему контроля уровня доступа (СКУД), а в том, чтобы промониторить различные показатели с подключенных датчиков (влажность, температуру и пр.). Каждый подобный контроллер — это некая «вещь в себе», которая не объединяется в единую систему. А все, что объединяется, — тем не менее по-прежнему «живет своей жизнью», отдельно от системы СКУД всего ЦОДа.

Обратный случай — когда решение предлагают люди, всю жизнь проектирующие и создающие исключительно системы безопасности, в частности СКУД. Их опыт, конечно, является ценным и проверенным в том, что касается решения для точек прохода на объект и дверей, ведущих в какие-либо помещения. Но как это совместить с необходимостью контроля шкафов и необходимостью передачи данных в SCADA или другие системы — мало кто представляет. В основе существующей проблемы — слабое взаимодействие между ИТ и СБ, которое уже стало притчей во языцех.

Поэтому наша компания предложила заказчикам и интеграторам решение, которое отвечает всем вышеупомянутым требованиям, — программно-аппаратный комплекс AGRG Castle ЦОД. Это — контроллер, в одноюнитовом исполнении, который устанавливается непосредственно в шкаф и подключается к его ручке (от 1 до 4 на контроллер), в которую встроен считыватель карт различных форматов. Частью комплекса также является программное обеспечение, функционал которого позволяет вести логирование доступа к оборудованию, отслеживать и автоматически реагировать на какие-либо события и ситуации (к примеру, дверь в шкафу открыта дольше, чем положено, попытки несанкционированного доступа и пр.).

Данное решение может являться как локальной системой, защищающей шкафы в рамках машинного зала, так и быть частью общей системы СКУД ЦОД или даже работать в составе системы, объединяющей территориально распределенные ЦОДы.

В реальных проектах с завидным постоянством ограничение доступа и разграничение прав заканчивается на этапе двери, ведущей в помещение машинного зала

Комплексная безопасность и интеграция систем

Вячеслав Гудков
независимый эксперт рынка систем безопасности

В последние годы заказчики все чаще прибегают к использованию видеоаналитики, и не только для решения задач безопасности, но и в интересах оптимизации бизнес-процессов транспортного комплекса: подсчет находящихся в здании вокзала пассажиров, измерение длины очереди в кассы продажи билетов и т. п.

Кроме того, системы безопасности транспортных объектов все чаще интегрируют с системами АПК «Безопасный город», где нейросетевые технологии применяются для поиска лиц из базы розыска, выявления общественно опасного поведения и т. д. Видеоаналитика в транспортной отрасли также широко применяется в интересах фотовидеофиксации нарушений ПДД, для регулирования потоков автомобилей.

Обозначенные потребности заказчиков приводят к постоянному росту объема собираемых видеоданных и метаданных с камер видеонаблюдения. Что, в свою очередь, служит драйвером роста рынка ЦОД для транспорта. Сами дата-центры усложняются, для хранения данных требуются все большие площади и сложные инженерные системы для электропитания и охлаждения.

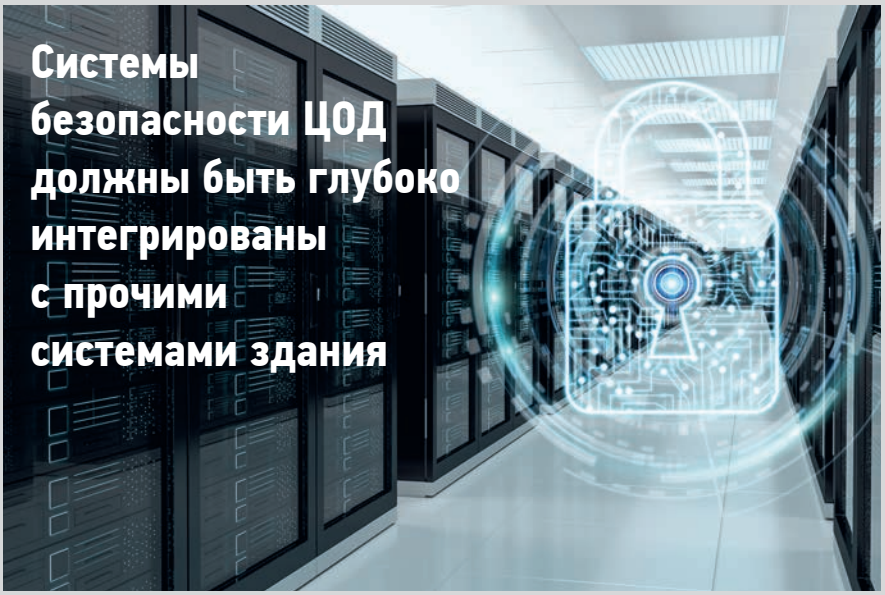
К центрам обработки данных изначально выдвигаются повышенные требования безопасности, т. к. оборудование и информация, размещаемая в них, имеет высокую ценность. На этих объектах работает много различных подразделений с отведенными под их задачи зонами. Поэтому система контроля доступа должна удовлетворять запросам и задачам как службы ИТ, так и службы КСБ, должна контролировать пребывание персонала в зонах, где определены их полномочия по доступу.

Несмотря на то что владельцы ЦОД стараются максимально тщательно контролировать перемещение посетителей и сотрудников по всей территории объекта, наиболее ограниченная в доступе зона ЦОД — «чистая зона», ее называют еще зоной «машинных залов». Доступ туда производится через идентификацию каждого сотрудника, как правило, по двум идентификаторам: карте и биометрии.

Основная задача системы безопасности — не дать возможному нарушителю проникнуть в «чистую зону» без идентификации. Поэтому на объекте должны отсутствовать непросматриваемые для видеонаблюдения зоны. А система охраны должна контролировать все точки проникновения, включая контроль возможного пролома стен в машинный зал, а также контроль открытия дверей в шкафы с ИТ-оборудованием и инженерными системами.

В последнее время заказчики все чаще требуют реализовать контроль доступа непосредственно к серверным шкафам из-за разделения полномочий ИТ-специалистов. Рынку в данном случае требуется единое решение, позволяющее и службе ИТ и службе СБ контролировать доступ в зоны. А в случае инцидентов проводить совместные расследования.

В целом системы безопасности ЦОД должны быть глубоко интегрированы с прочими системами здания.



Стоит добавить, что со вступлением в силу постановления правительства № 969 на средства, обеспечивающие транспортную безопасность, возложены дополнительные требования, что напрямую влияет на безопасность центров обработки данных, создаваемых под размещение вычислительных мощностей систем безопасности на транспорте. Фактически возникла необходимость дополнительных проверок оборудования в специализированных учреждениях, а также тренд на импортозамещение.