доверить крупной ИТ-компании с опытом в этой сфере деятельности. Желательно, чтобы в команде, отвечающей за разработку и функционирование ЦОД, присутствовал хотя бы один сертифицированный специалист — например, со статусом Accredited Tier Designer (ATD) или Accredited Tier Specialist (ATS) от вышеупомянутого Uptime Institute. Международная сертификация повышает вероятность того, что ЦОД будет построен в соответствии с требованиями международных отраслевых стандартов, а значит, будет иметь высокий уровень надежности и эффективности.

Список литературы

1. *Жилкина Н.* Дата-центр на аутсорсинг: рынок на подъеме // Компьютерра. 2013. март. http://www.computerra.ru/cio/2722.
2. *Ицкович Э.Л.* Современные SCADA-программы разных производителей: их свойства и отличия, важные для потенциальных заказчиков // Автоматизация в промышленности. 2007. №4.

Цыганков Вячеслав Анатольевич *– эксперт компании "Энвижн Груп".*
Контактный телефон (495) 641-12-12.
Http:// www.nvg.ru

ИТ-инфраструктура предприятия: особенности, тренды, опасности в кризис и не только

И.И. Батов, А.В. Переведенцев (Компания Техносерв)

Построение и оптимизация ИТ-инфраструктуры, удовлетворяющей бизнес-процессам организации – сложная и многогранная задача. Рассмотрены современные инновационные подходы, применяемые при создании ЦОД: виртуализация задач, систем хранения данных и инфраструктуры сетей передачи данных, а также организационные вопросы – кибербезопасность, аудит инженерной инфраструктуры предприятия, создание модульных ЦОД, использование аутсорсинговых ЦОД.

Ключевые слова: центр обработки данных, кибербезопасность, виртуализация, инженерная инфраструктура, аутсорсинг.

Свой или чужой ЦОД: кому и что выбрать?

Информационные системы играют важную роль в деятельности предприятий, повышая эффективность и поддержку бизнес–процессов. Перед предприятиями, потребности которых в обработке информации неуклонно растут, лежат два пути. Первый — установка своего оборудования или информационной системы в коммерческом центре обработки данных (ЦОД). Этот вариант дает возможность воспользоваться «всеми благами» готовой инфраструктуры ЦОД, предлагающих свои ресурсы в аренду. Второй вариант — создание собственного корпоративного ЦОД.

Компании, которые выбирают вариант ЦОД на аутсорсинг — это предприятия, бизнес которых не находится в прямой зависимости от непрерывного функционирования ИТ-систем. Возможна ситуация, когда компания — аутсорсер является родственной или дочерней компанией заказчика услуг (это позволит контролировать работу ЦОД, сделать ее более прозрачной). Многие компании отдают на аутсорсинг часть задач, которые не являются критичными или конфиденциальными.

Почему же ряд предприятий не доверяют аутсорсинговым ЦОД критичные задачи?

Прежде всего, это различный уровень зрелости. Компании, предлагающие ЦОД на аутсорсинг, достаточно молоды. Как правило, они не обеспечивают соглашение об уровне предоставления услуги (Service Level Agreement SLA) высокого уровня, удовлетворяющего заказчика.

Остается еще ряд проблем: возможные утечка информации, потеря контроля над собственными ресурсами, проблемы у компании-аутсорсера (например, банкротство), а также непредсказуемые последствия при аварийной остановке ЦОД (нет контроля над инфраструктурой ЦОД).

Построить ЦОД в кризис

Понимая минусы аутсорсинговой модели, рассмотрим вариант создания собственного ЦОД. Сформулируем задачу предельно конкретно: как построить «бюджетную» инфраструктуру, но при этом обеспечить базу для стабильного функционирования ЦОД на протяжении многих лет?

В текущих экономических условиях в создании ЦОД заинтересованы крупные организации энергетического сектора для получения технологического фундамента и расширения бизнеса, операторы связи, компании, ориентирующиеся при создании ЦОД на эксплуатацию его в коммерческих целях, и, конечно, промышленный сектор, наращивающий затраты на ИТ-услуги ввиду усиления долевого участия государства и роста экспортных продаж вооружения. Впрочем, компании, которые будут строить ЦОД в ближайшие годы можно разделить на два сектора: компании с государственным участием и компании со стабильно развивающимся спросом (например, Internet и телеком-компании).

На первых этапах при строительстве ЦОД необходимо выяснить, насколько глубоко бизнес-процессы компании зависят от ИТ-решений (зависимость бизнеса от информационных систем). Эта информация

поможет определить сроки окупаемости комплекса, его технологическую конфигурацию, срок службы, а также период модернизации и развития ЦОД. Если проанализировать реализованные ЦОД таких потребителей, как промышленные предприятия, операторы связи, финансовые организации, госструктуры (Технопарк), транспортные компании, то очевиден будет различный подход к строительству их инфраструктуры. Применение одного и того же технологического решения для различной целевой аудитории практически невозможно.

В начальной стадии разработки решения (при написании концепции, технико-экономического обоснования) необходимо обеспечить баланс капитальных и эксплуатационных затрат.

Желательно учесть, что реализация инженерной инфраструктуры ЦОД с высокой степенью энергоэффективности не оправдывает себя в текущих экономических условиях по следующим причинам: рост цен на импортное оборудование и материалы приводит к существенному росту капитальных затрат, увеличение процентных ставок ведет к росту ценности денег в настоящий момент и снижению ценности в будущем, рост тарифов на электроэнергию не компенсирует дополнительные капитальные затраты, возникающие с внедрением энергоэффективных решений. В современных условиях решающее значение приобретает оптимизация капитальных затрат.

Специалисты Техносерв последние полгода активно занимаются поиском компаний-производителей отечественного оборудования, в частности, по инженерным системам, а также участвуют в разработке и продвижении такого оборудования на российский рынок. На данный момент степень локализации инженерных систем при реализации ЦОД специалистами Техносерв достигла 30%, а при реализации решений высокой готовности — не менее 40%. Одним из таких решений является последняя версия модульного ЦОД «ИТ ЭКИПАЖ». Это решения себя очень хорошо зарекомендовало в качестве резервной площадки для компании «Аэрофлот». Модульная конструкция с разделением серверной и инженерной зон была возведена и запущена в эксплуатацию в течение 6 мес. Такие сроки не реальны для строительства или модернизации стационарного объекта. Дополнительными плюсами решения являются возможность масштабирования и переноса ЦОД на другую площадку, если того потребует бизнес. Применение модульной конструкции ЦОД позволяет существенно снизить капитальные затраты при реализации его инженерной инфраструктуры, что особенно актуально сегодня в условиях, когда многие компании сформировали свои бюджеты до повышения курса валют [1].

Аудит инженерной инфраструктуры предприятия — в чем суть?

Отдельно необходимо обратить внимание на важность аудита ИТ и инженерной инфраструктуры, а также аудита экономической эффективности ЦОД. Специалисты компании — независимого эксперта проверяют и анализируют организацию производства работ в ЦОД, применяемых технических и технологических решений, состояния оборудования и инженерных систем. Также методология аудита включает проверку проектной документации и отчетов проведения технического и сервисного обслуживания, работы персонала.

В зависимости от целей и объемов аудита формируется рабочая группа. Она может включать как специалистов по инженерной и ИТ-инфраструктуры ЦОД, так и экономистов. Среди задач, которые ставит заказчик при проведении аудита, могут быть анализ и документирование актуального состояния ИТ-инфраструктуры; анализ ключевых систем, размещенных на разных площадках, и предложения по их перепрофилированию с последующей миграцией в единый ЦОД; выявление проблем, узких мест, оценка их влияния на качество работы, производительность, надежность и эффективность функционирования; определение необходимости, объемов и направлений оптимизации и модернизации ИТ-инфраструктуры ЦОД.

Наша компания предлагает различные варианты оценки ЦОД: это может быть технический аудит, аудит энергоэффективности или аудит в целом экономического эффекта ИТ-инфраструктуры для предприятия. Аудит может включать расчет сроков окупаемости (ROI) как всего комплекса ЦОД, так и анализ эффективности внедрения какого-либо продукта, системы или решения в частности. Масштаб предстоящей оценки зависит только от целей и задач заказчика.

Примером результативности комплексного подхода в аудите может стать проект Техносерв, в котором первоначально срок окупаемости ЦОД при проектировании оценивался примерно в три года. Однако после проведения аудита и выполнения сформулированных рекомендаций ROI составил всего 17 мес. Это стало возможным благодаря правильной организации инфраструктуры. Многие из выгод появились с разъяснением имеющегося инструментария.

Однако, как бы грамотно ни была поставлена работа по обслуживанию ЦОД, человеческий фактор — ошибочное действие персонала — всегда будет влиять на работу инфраструктуры, а это дополнительные риски и соответственное снижение уровня отказоустойчивости.

Наиболее радикальный способ снизить риски, связанные с человеческим фактором в работе ЦОД, как и в работе любых производственных предприятий, — это автоматизация максимально возможного числа систем и интеграция их в единую среду для увеличения производительности и удобства управления.

Де-факто виртуализация везде

Говоря об основных направлениях развития ИТ-инфраструктуры сегодня, ее трендах следует упомянуть о виртуализации. Тема виртуализация суще-

ствует очень давно, но действительно массовой она стала после выхода и закрепления на рынке решений стандартной архитектуры. Полезно окунуться в историю и вспомнить, как решения по виртуализации вычислительной инфраструктуры проникали на рынок. Еще в первой половине 2000 гг. это были достаточно слабые решения на уровне настольных ПК, и широкого распространения в корпоративном сегменте они не имели. Потом появились первые решения под управлением основных серверных операционных систем, и виртуализация начала проникать на корпоративный рынок. Основной областью применения во второй половине 2000 гг. являлись всевозможные тестовые среды, виртуальные лаборатории и т. п. И лишь с появлением гипервизоров, не требующих для своего функционирования установленной операционной системы, началось активное завоевание решениями по виртуализации корпоративного рынка. Так или иначе, но преимущества от применения виртуализации вычислительной инфраструктуры стали настолько очевидны, что уже продолжительное время их применение при построении ИТ-инфраструктуры организации стали стандартом де-факто. Возможность создания отказоустойчивых кластеров, обеспечивающих динамическую балансировку виртуальных серверов между узлами и перезапуск виртуального сервера в случае отказа узла, вывело доступность сервисов на новый уровень.

Системы хранения данных — в отрыве от «железа»

Следующим этапом развития темы виртуализации можно назвать виртуализацию систем хранения данных. Первые решения, появившиеся в середине 2000 гг., такие как Hitachi Data Systems Universal Storage Platform (HDS USP), позволяли скрыть существующий парк используемых систем хранения за контроллерами новой системы, что значительно упрощало администрирование сети хранения данных и облегчало переход с устаревших систем. Изначально поддерживались все дисковые массивы HDS и относительно небольшое число устройств других производителей. Примерно в это же время на рынок вышли программно-аппаратные комплексы IBM SVC и EMC Invista. Эти решения позволяли обеспечивать актуальную на тот момент стратегию управления жизненным циклом информации (Information Life Cycle, ILM). Прорыв произошел в 2011 г., когда компания EMC представила виртуализатор нового поколения VPLEX, позволявший создавать географически распределенные виртуальные кластеры, узлы которых могли работать в режиме active-active. С точки зрения взаимодействия клиентов с системой хранения такой виртуализатор представляет несколько географически разнесенных систем хранения данных как одну, обеспечивает управление репликацией данных между этими системами хранения и предоставляет отказоустойчивый доступ к виртуализованной системе хранения данных.

Сейчас практически у всех основных производителей систем хранения данных есть продукты, позволяющие виртуализировать системы хранения. В связи с этим сегодня параллельно существуют два описанных подхода: виртуализатор как отдельно стоящее устройство и обеспечение виртуализации средствами самой системы хранения.

Опыт компании Техносерв позволяет утверждать, что во всех последних проектах, связанных с разработкой или модернизацией ИТ-инфраструктуры, система виртуализация является одной из самых значимых систем. Например, в 2014 г. такие решения были разработаны в составе проектов по созданию единых территориально-распределенных корпоративных (ЕТРК) ЦОД СО ЕЭС в пяти регионах России, единой информационной системы третьей очереди Росфинмониторинга, центра обработки вызовов Новосибирской области (Система 112), комплексной информационно-аналитической системы контроля и надзора за перевозкой пассажиров и опасных грузов Министерства транспорта и т. д.

Безусловно, есть специфика при использовании серверной виртуализации на промышленных предприятиях, выполняющих заказы для силовых и ряда иных государственных структур, связанная с выполнением требований по обеспечению режимов секретности. Если еще несколько лет назад о применении систем виртуализации на подобных предприятиях речи идти не могло, то сейчас разработаны и допущены к использованию такие решения, как vGate-S от компании «Код безопасности», позволяющие обеспечить выполнение действующих требований. Специалисты компании Техносерв также имеют опыт в этой сфере, например, ими разработана инфраструктура ЦОД РФЯЦ в г. Саров.

Повышаем отказоустойчивость

Дальнейшим развитием систем виртуализации является весьма перспективная тема — виртуализация инфраструктуры сетей передачи данных (SDN — программно-определяемая сеть) и ЦОДов (SDDC — программно-определяемый ЦОД). Пока эта тема еще не имеет такого широкого распространения, как описанные выше, но вектор развития сетевых решений у основных производителей не оставляет сомнений, что все впереди. По сути своей программно определяемый ЦОД включает решения по виртуализации на всех уровнях — вычислительная инфраструктура, системы хранения данных и сеть. Одновременное применение этих решений и технологий позволяет существенно повысить гибкость и эффективность управления ресурсами, обеспечивает возможность создания виртуальных ЦОДов и предоставления их как сервис.

Развитие решений по виртуализации позволило существенно повысить отказоустойчивость ИТ-инфраструктуры. Конечно, решения для обеспечения отказоустойчивости сервисов существовали и рань-

ше. Это в первую очередь различные отказоуточивые кластеры. Но применялись они точечно лишь для критичных сервисов. Использование виртуализации позволило обеспечить «массовую» отказоустойчивость и эффективность использования вычислительных ресурсов.

На катастрофоустойчивые и территориально распределенные решения развитие систем виртуализации повлияло кардинально — стоимость создания таких решений снизилась в разы. Существующие решения позволяют обеспечивать безостановочный перенос сервисов с одной серверной площадки на другую, что может быть востребовано территориально распределенными организациями. Эффект от создания территориально распределенных ЦОД может быть особо ярко выражен в странах масштаба России, с большим числом часовых поясов. На выбор площадки для функционирования сервиса в конкретный момент времени могут влиять разные факторы, например время суток, так как ночью стоимость электроэнергии ниже.

Следует отметить существенно возросший интерес заказчиков к подобным решениям, что в немалой степени обусловлено их возросшей доступностью. Если раньше к катастрофоусточивой ИТ-инфраструктуре многим предприятиям было не подступиться, то сейчас обладая информацией об относительной дешевизне решения, заказчики все чаще выбирают распределенные ЦОД. Говоря о промышленных предприятиях, необходимо помнить, что для многих характерен непрерывный производственный/технологический процесс, и каждая минута простоя либо выливается в ощутимые финансовые потери, либо может привести к аварии или катастрофе. И именно на таких предприятиях требуется предоставление сервисов с самым высоким уровнем обслуживания.

При реализации проектов ЕТРК ЦОД СО ЕЭС в пяти регионах России компанией Техносерв были созданы катастрофоустойчивые территориально распределенные ЦОДы с использованием технологий виртуалиазации вычислительной инфраструктуры и систем хранения данных».

О главном — о безопасности

Отдельно остановимся на вопросах информационной безопасности в контексте промышленных предприятий и относительно нового понятия «кибербезопаность» [2]. Если в прошлом информационная безопасность рассматривалась на уровне отдельной организации или узкой отрасли, то сейчас имеет место перенос действий злоумышленников в информационное поле (кибервойны). А под злоумышленниками теперь понимаются не отдельные личности и конкуренты, а развитые хакерские сообщества, преступные группы, занимающиеся шантажом, и крупные структуры иностранных государств (кибервойска). Очевидно, что против злоумышленников такого уровня не устоит ни одна организация, насколько крупной, технически развитой и финансово обеспеченной она бы ни была. Именно поэтому следует делегировать основные задачи по защите критических информационных сервисов и критической информации организациям, обладающим соответствующими техническими средствами защиты, аналитиками и экспертами в области информационной безопасности.

В обеспечении информационной безопасности ЦОД ключевую роль играет защита от DDoS-атак и APT-атак. В случае успешной атаки критические вычислительные мощности и каналы связи всех критически важных сервисов и систем компании становятся частично или полностью недоступными на продолжительное время, что может привести к угрозам чрезвычайных ситуаций на производстве (в том числе выводу из строя критически важных промышленных объектов, сбоя логистических поставок оборудования и сырья для производства, сбоев в сбыте продукции, приводящих к нарушению контрактных обязательств).

По результатам опроса одной из ведущих мировых компаний в области информационной безопасности, развивающиеся страны, включая страны БРИКС, внедрили только половину ключевых мер по защите энергосетей от киберугроз по сравнению с такими странами как Китай, Япония и Италия.

Согласно этому же исследованию, наиболее развитой страной в вопросах кибербезопасности является Китай, где руководство страны уделяет пристальное внимание вопросам защиты критической инфраструктуры, включая аудиты государственных регуляторов.

Часть энергетических компаний отметили в вышеуказанном опросе, что являются постоянным объектом проверок и атак со стороны внешних злоумышленников, не исключая рекогносцировку и планирование последующих кибератак военными структурами зарубежных стран, при этом основной целью является вывод из строя энергосистемы страны.

Более того, если ранее эксперты считали, что потенциально наиболее опасной категорией кибератак являются DoS и DDoS атаки на объекты ИТ-инфраструктуры, то после обнаружения вируса Stuxnet на первый план вышла реальная угроза вывода из строя критических объектов на продолжительное время. Напомним, что данный вирус как представитель нового класса угроз выводит из строя определенный класс центрифуг, изменяя программную логику только определенных моделей микропроцессоров. При этом степень его распространения по всему миру, включая критические объекты инфраструктуры, поражает своим охватом. Так, в среде электроэнергетики Stuxnet был обнаружен 46% компаний, вне зависимости от используемого оборудования. Вирус находился необнаруженным и никак не проявлял себя достаточно продолжительное время.

Обнаружение доселе неизвестного источника угрозы привело энергокомпании по всему миру к осознанию необходимости проведения трениро-

вочных проверок кибербезопасности критических объектов электроэнергетики, которые и ранее показывали неутешительные результаты. Так, согласно отчету по учебным тестовым кибератакам, проведенным в Idaho National Labs в 2007 г., команде подготовленных специалистов удалось получить удаленный доступ к системе управления генератором и удаленно изменить его рабочее состояние, выведя его физически из строя. Если бы эта атака проводилась на действующем объекте электроэнергетики, это могло привести к локальному отключению электроэнергии на несколько дней.

Согласно современным исследованиям, с развитием электроэнергетики и информационной составляющей в ней, угрозы безопасности электросетям необходимо рассматривать в комплексе по всей стране в рамках единого киберпространства, а не только отдельных сегментов сети одной организации, так как атака на один или несколько критических объектов может иметь лавинообразный эффект каскадного отключения систем по всей стране.

Подход к обеспечению безопасности критических объектов с приоритетом обеспечения доступности и целостности не только информации, но и других материальных и нематериальных активов является нестандартным с точки зрения информационной безопасности, где во главу угла из триады конфиденциальность-целостность-доступность ставится конфиденциальность, а основным защищаемым активом является информация.

Именно поэтому так важно рассматривать угрозы и меры безопасности в промышленности и ТЭК не только с точки зрения информационной безопасности, но и кибербезопасности, а также непрерывности деятельности информационно-коммуникационных систем компаний.

Список литературы

1. *Корсунский А.* Мобильные? Контейнерные? Модульные!//ЦОДы.РФ Проектирование. Строительство, Эксплуатация. 2013. № 5 (ноябрь).
2. *Евдокимов Д.С.* Разработка эксплойтов для АСУТП: двойная игра // Автоматизация в промышленности. 2015. №2.

Батов Иван Игоревич *– директор департамента «Инжиниринговый центр»,*
Переведенцев Александр Владимирович *– главный специалист департамента поддержки продаж компании Техносерв.*
Контактный телефон (495) 648-08-08.
Http://www.technoserv.com

Модульные ЦОД: особенности российского рынка

В.С. Фосс (Компания Утилекс)

Модульные центры обработки данных (МЦОД) – один из самых заметных трендов российского ИТ-рынка. В условиях экономической нестабильности идея такого ЦОД кажется особенно привлекательной, поскольку утверждается, что создание МЦОД дешевле и быстрее строительства капитальных. Однако у этого рынка есть свои особенности и свои «подводные камни». Своим взглядом на этот сегмент рынка делится российский производитель МЦОД – компания «Утилекс».

Ключевые слова: модульный центр обработки данных, масштабируемость, инженерная инфраструктура.

Российский рынок модульных ЦОД глазами разработчика

Рынок МЦОД сегодня на подъеме во всем мире. Однако рост этого сегмента отечественного ИТ-рынка в последние годы был особенно интенсивным (в 2011–2013 гг. он составил 190% по данным аналитического агентства DCD Intelligence). Появляются все новые и новые российские производители МЦОД, все больше компаний предлагают именно модульные решения. Однако такой впечатляющий скачок развития не отражает реальной картины. На деле доля собственных разработок на российском рынке мала. Кроме того, как только принцип модульного построения вычислительных центров на базе готовых стандартизованных решений стал модной тенденцией мирового ИТ-рынка, производителям и ритейлерам стало выгодно прибавлять приставку «модульный» ко всем сколько-нибудь родственным этой идее ЦОДам. В результате возникла терминологическая путаница, которая порой идет во вред репутации «настоящих» модульных дата-центров [1].

Вопрос определения

Какие решения следует считать модульными ЦОДами? Дать однозначный ответ на этот вопрос зачастую мешает тот факт, что сегодня в России, да и во всем мире МЦОДы ошибочно отождествляют с мобильными конструкциями, а также контейнерными решениями, которые положили начало развитию концепции модульного дизайна. Характерен пример компании Compass Datacenters (США), продвигавшей идею «по-настоящему модульного ЦОД» и столкнувшейся с недопониманием клиентов, увидевших у них крупные стационарные здания вместо ожидавшихся небольших мобильных решений.

Если разобраться в сути, то становится ясно, что определение «модульный ЦОД» относится скорее к типу дизайна подсистем ЦОД, в первую очередь, к ограждающей конструкции, а не к готовым продуктам. В этом термине заложена возможность поэтапного создания ИТ-инфраструктуры с помощью стандартизованных модулей в соответствии с развитием бизнеса и его возрастающими потребностями. Таким образом, модульный ЦОД вовсе не равно «портативный» или