Деловой журнал | ИТ • Телеком • Медиа | www.iksmedia.ru

ИнформКурьер-Связь

ИКС

издается с 1992 года

№ 2 2018

ТЕМА НОМЕРА

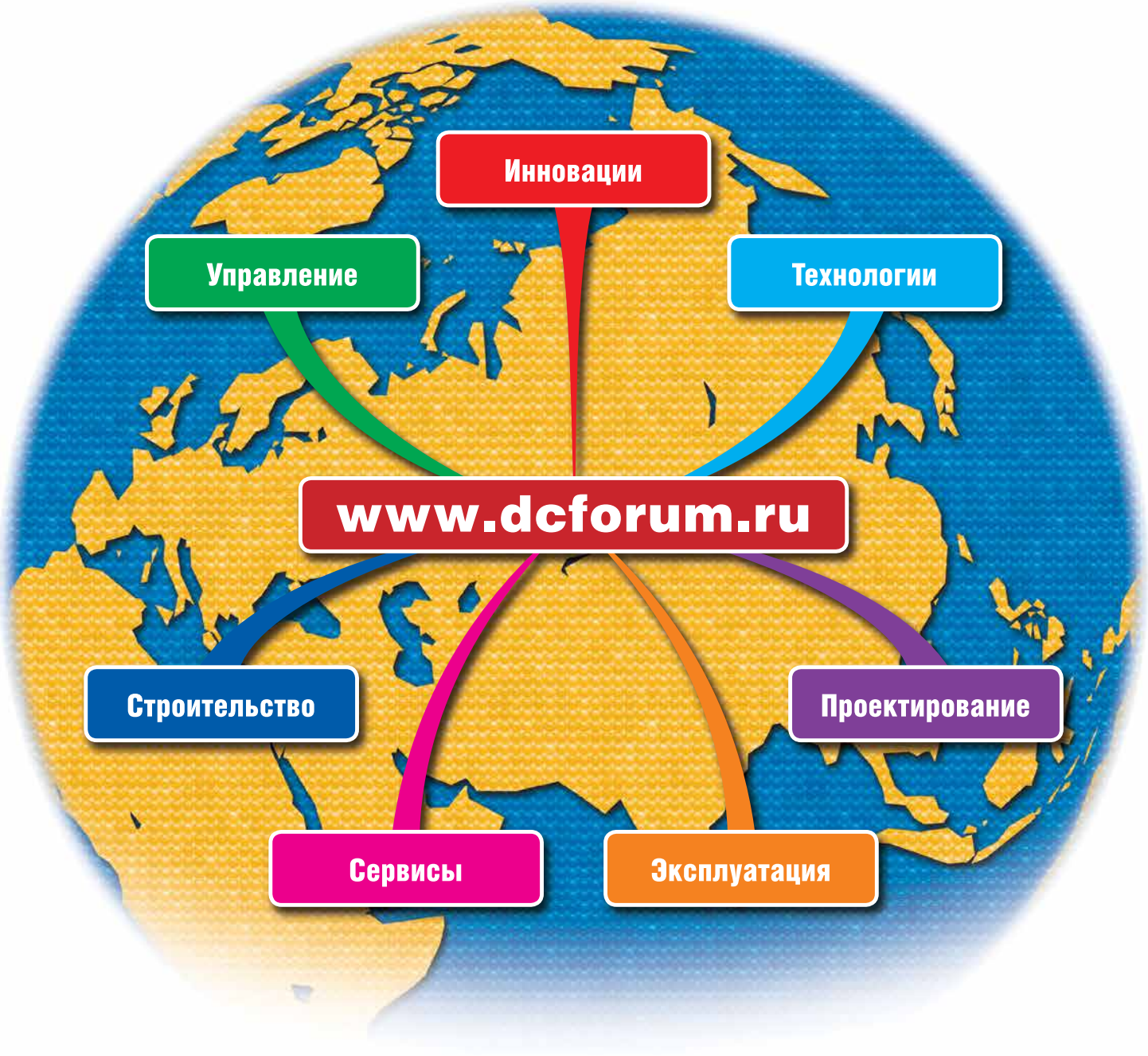
Безопасный ЦОД

13-я международная конференция

ЦОД

13 сентября 2018
Москва, Центр Digital October

XIII DATA CENTER FORUM



Издается с мая 1992 г.

Издатель
ООО «ИКС-Медиа»

Генеральный директор
Д.Р. Бедердинов
dmitry@iks-media.ru

Учредители:
ООО «ИКС-Медиа»,
МНТОРЭС им. А.С. Попова

Главный редактор
А.Г. Барсков
a.barskov@iks-media.ru

РЕДАКЦИЯ
iks@iks-media.ru

Ответственный редактор
Н.Н. Шталтовная
ns@iks-media.ru

Обозреватели
А.Е. Крылова, Н.В. Носов

Корректор
Е.А. Краснушкина

Дизайн и верстка
Д.А. Поддъяков, Е.В. Денисова

КОММЕРЧЕСКАЯ СЛУЖБА
Г. Н. Новикова, коммерческий директор – galina@iks-media.ru
Ю. В. Сухова, зам. коммерческого директора – sukhova@iks-media.ru
Е.О. Самохина, ст. менеджер – es@iks-media.ru
Д.А. Устинова, менеджер по работе с ключевыми клиентами – ustinova@iks-media.ru
Д.Ю. Жаров, координатор – dim@iks-media.ru

СЛУЖБА РАСПРОСТРАНЕНИЯ
Выставки, конференции
expo@iks-media.ru
Подписка
podpiska@iks-media.ru

Журнал «ИнформКурьер-Связь» зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций 02 февраля 2016 г.;
ПИ №ФС77-64804.

Адрес редакции и издателя:
105066, Москва, ул. Новорязанская, д. 31/7, корп. 14
Тел./факс: (495) 150-6424
E-mail: iks@iks-media.ru
Адрес в Интернете: www.iksmedia.ru

№2/2018 подписан в печать 24.08.18.
Тираж 8 000 экз. Свободная цена.
Формат 64x84/8

ISSN 0869-7973

12+

Цифровая экономика начинается с безопасности ЦОДа

В ходе цифровизации экономики ИТ становятся неотъемлемой составляющей все большего числа производственных и бизнес-процессов. Соответственно, растут риски, связанные с нарушением безопасности ИТ-комплексов.

Всего пара примеров. При кибератаке на одно из нефтяных предприятий была отключена система мониторинга скорости закачки нефти в резервуар. Превышение предельной скорости закачки привело к электризации топлива и взрыву. Во время тушения пожара погиб сотрудник технической службы... Атака элементами Stuxnet на системы одного крупного предприятия вызвала простой конвейера в течение четырех-шести суток. Проблема повторялась. Финансовые потери – $1,2 млн в месяц...

Безопасность ИТ – это безопасность ЦОДов. Центров обработки данных в широком понимании: от гигантских мегаЦОДов и крупных корпоративных дата-центров до совсем небольших edge-ЦОДов, развернутых, например, на производстве. Когда лет пятнадцать назад мы ломали копья в дискуссиях, что же такое ЦОД, то пришли к выводу, что дело не в размере, а в важности для бизнеса. Даже самые большие, на сотни стоек, серверные остаются просто серверными, если они вторичны для компании. А маленький «эдж», например с контроллерами системы прокачки нефти, – это настоящий ЦОД!

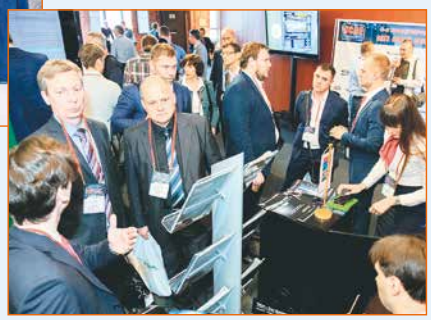
Безопасность – это, конечно, современные технические решения – от СКУД со средствами биометрии до виртуализированных МСЭ. Но главное – не технологии, а процедуры и люди. Вместо того чтобы разрабатывать хитроумную систему взлома, проще и дешевле подкупить кого-нибудь из сотрудников. И он принесет вам желанную информацию на флешке «с голубой каемочкой» или откроет лазейку для атаки на информационную систему.

Важно разработать и реализовать процедуры, сводящие к минимуму пресловутый человеческий фактор. Одно из направлений – автоматизация. Впрочем, здесь важно не переусердствовать. Пусть автоматика берет на себя весь мониторинг и оповещение о негативных трендах, однако ключевые решения, к примеру об отключении или смене режима работы кондиционеров, лучше доверить людям. Другое направление – разделение зон доступа. Скажем, инженеров по обслуживанию климатического оборудования лучше не пускать в зал с ИТ-оборудованием, ну а айтишникам нечего делать в помещениях с «инженеркой».

Сегодня проблемы, связанные с безопасностью ИТ, приводят к огромным финансовым и репутационным потерям, зачастую невосполнимым, и даже к человеческим жертвам...

Будьте бдительны.
Александр Барсков

с. 4



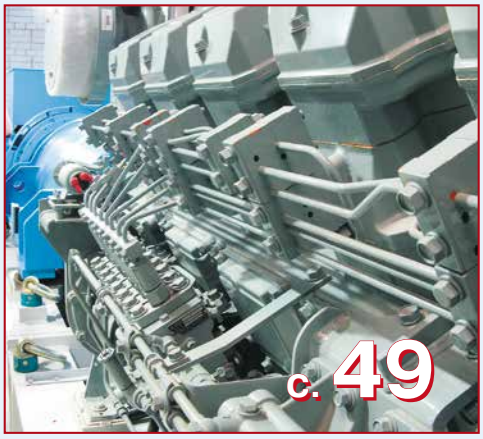
На пороге серьезных изменений

с. 12

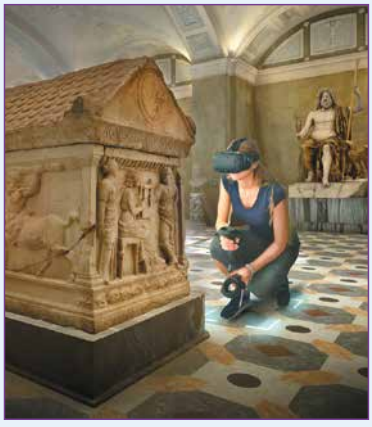
Дейв Джонсон: «Смещаем акценты в сторону ПО и сервисов»

с. 22

Н. Носов. Трансформируем всё!



А. Барсков. Пока крутится маховик



И. Симонов. Реальность дополненной стоимости

Н. Носов. Безопасный ЦОД

На пороге серьезных изменений

Новые технологии меняют подходы к проектированию ЦОДов.

Тенденции развития рынка ЦОДов, распределение нагрузок по нескольким площадкам, «теплолюбивые» серверы, новые подходы к охлаждению и электропитанию – эти темы были в центре внимания экспертов по инженерной инфраструктуре дата-центров на шестой международной конференции Data Center Design & Engineering, проведенной «ИКС-Медиа».

Куда движется рынок? Последние годы рынок коммерческих ЦОДов развивался волнообразно. В 2013–2014 гг. наблюдался двузначный рост, который в последующие два года замедлился. Для рынка это было не так плохо. «Установился баланс спроса и предложения, падающие цены стабилизировались», – пояснил ведущий консультант iKS-Consulting Станислав Мирин. Ввод в строй площадок, планировавшихся к запуску в кризисные годы, был перенесен на 2017 г., что привело к росту рынка на 21%.

Компания «Авантаж» заявила о вводе более 2 тыс. стойко-мест. Свыше 1 тыс. стоек ввели в эксплуатацию компании «Ростелеком» и DataLine каждая.

На рынке появился новый игрок – компания «ГДЦ Энерджи Групп». Первая очередь ее ЦОДа GreenBush DC (около 700 стоек) запущена в эксплуатацию в нынешнем году. Общая мощность дата-центра составит 21 МВА. Статус резидента особой экономической зоны дает компании преимущества: нулевые таможенные пошлины, нулевой НДС на ввозимое на территорию дата-центра импортное оборудование и пониженную ставку налога на прибыль. Это должно положительно сказаться на цене облачных сервисов и услуг, предоставляемых по модели colocation.

По-прежнему уменьшается доля корпоративных ЦОДов, растет доля коммерческих дата-центров и облачных провайдеров. Движение в облака стало устойчивой тенденцией на российском рынке. Предлагающие услуги по модели colocation коммерческие ЦОДы лидируют и на рынке облачных услуг.

Продолжаются работы, направленные на снижение PUE. Увеличить эффективность дата-центра можно путем изменения архитектуры кондиционирования, построения гермозон, использования более эффективного оборудования для электропитания и охлаждения. Повышению отдачи от вложений в вычислительную инфраструктуру служат виртуализация серверов, системы управления инфраструктурой (DCIM) и переход к открытым стандартам оборудования OCP (Open Compute Project).

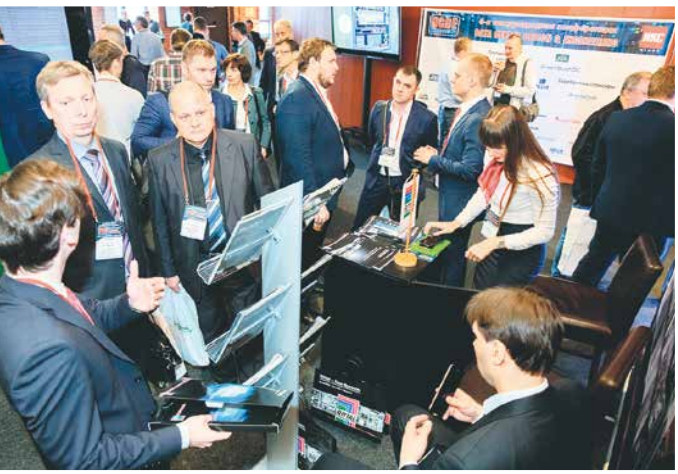
Все чаще при строительстве крупных дата-центров применяется модульный подход. В небольших компаниях растет популярность мини- и микроЦОДов, активно используются контейнерные ЦОДы.

Идет внедрение технологий BIM-моделирования, позволяющих объединить в единой трехмерной модели здание и инфраструктуру. Подход помогает избежать нестыковок и конфликтов инженерных систем на стадии моделирования, уменьшает стоимость строительства и время запуска ЦОДа в эксплуатацию.

Новым трендом стало использование дата-центров для майнинга. Для ЦОДов это вторичный бизнес, доля которого, по оценкам iKS-Consulting, не превышает 10%. Майнеры могут использовать свободные площади в дата-центрах и резервные каналы электропитания. Удобно, что при необходимости аппаратуру для майнинга можно в любой момент выключить. Майнинг помогает ЦОДам повышать утилизируемость площадей в ожидании более выгодных клиентов и позволяет тестировать работу вычислительных комплексов на полной мощности.

Новая парадигма. Облачные технологии прочно вошли в нашу жизнь. Но крупные заказчики не готовы отказаться от своей вычислительной инфраструктуры и полностью уйти в облака. Причем дело не только в сохранении сделанных инвестиций, но и в особенностях бизнес-процессов, требующих проведения вычислений вблизи объекта.

Отвечая на запросы рынка, поставщики облачных услуг предлагают переход на гибридные среды. Развиваются периферийные вы-



числения (Edge Computing). Современный пользователь работает с многоуровневой системой.

«Наша парадигма организации дата-центров нуждается в серьезном развитии», – считает технический директор подразделения IT Division компании Schneider Electric Алексей Соловьев. Современные представления о доступности ЦОДа фокусируются на отдельных аспектах, например, предельно допустимом времени простоя. Но конечного пользователя интересует работоспособность приложения. Проблемы же могут возникать в центральном, локальном или региональном ЦОДе. Поэтому требуется организация надежной работы всей гибридной среды.

Следует повысить время доступности периферии, переосмыслить подход к надежности архитектуры локальных ЦОДов, сосредоточиться на их безопасности, резервировании систем охлаждения, электропитания и каналов связи. Развернуть в локальных дата-центрах системы DCIM, дистанционного управления и автоматизации.

Надежные ЦОДы для размещения оборудования конечных пользователей на рынке уже есть. Так, Schneider Electric предлагает выполненный в дизайне обычного офисного шкафа микроЦОД, который можно поставить в любом кабинете. Компания Rittal показала на выставке в рамках конференции DCDE свой вариант компактного дата-центра в одной стойке.

Интересно наблюдать развитие вендоров инфраструктурных решений. «Rittal изначально была инженерной компанией, но теперь мы предлагаем решения под ключ», – заявил старший менеджер по продукции для ИТ-инфраструктуры Rittal Александр Нилов. В этом году Rittal построила в России модульный ЦОД и провела его сертификацию по Tier III.

Повышая надежность ИБП. Пока ЦОД трудно представить без систем бесперебойного электропитания. ИБП состоит из силовой установки, системы распределения питания и батарей, причем батареи – самое слабое звено, причина 50% случаев неработоспособности ИБП.

До 5% батарей теряют емкость в течение срока гарантии, сообщил директор по развитию бизнеса трехфазных ИБП компании CyberPower Systems Алексей Лобов. Он подчеркнул, что это приводит к выходу из строя всего батарейного массива. Повысить надежность систем ИБП и снизить расходы на эксплуатацию можно при помощи систем управления аккумуляторами (BMS, Battery Management System). Система отслеживает работу каждой батареи и выявляет неисправности. А благодаря выравниванию напряжения на батарейных блоках увеличивается срок их службы. Особенно актуально использование BMS при работе с литий-ионными батареями.

Прекрасное далеко. Переход от свинцовых батарей к литий-ионным – один из трендов в развитии систем бесперебойного питания. Но появляются и другие варианты решений, связанные с отказом от ставших уже классическими больших ИБП для ЦОДов, например, размещение легких ИБП на литий-ионных батареях в стойках или даже размещение батарей прямо в компьютерах.

Еще более революционными могут быть изменения в системах охлаждения. Во многих местах становится возможным охлаждение путем прямого фрикулинга. Такой подход использован в новом ЦОДе компании «Яндекс». Появились «теплолюбивые» серверы, работающие при температуре окружающей среды выше 40°C. Правда, как указывают эксперты, при повышении температуры воздуха срок эксплуатации жестких дисков сокращается, а при динамично меняющейся вычислительной нагрузке необходимо будет устранять локальные перегревы в стойках.

Важную роль может сыграть использование открытой архитектуры (соответствующей стандартам OCP), позволяющей оптимизировать сервер с точки зрения термодинамики, распределения воздушных потоков внутри сервера, в том числе на уровне расстановки процессоров, памяти и дисков. Переход к стандартам OCP дает возможность построить на обычных аппаратных средствах конфигурацию, стабильно работающую при повышенных температурах, считает технический директор «АМД-технологии» Виктор Гаврилов.

Окружающий мир стремительно меняется. Изменения затрагивают и традиционно консервативные инженерные системы ЦОДов, которые стоят на пороге больших перемен.

Николай Носов

ЦОДы Казахстана: время роста

Реализуемая в Казахстане государственная программа цифровизации может стать катализатором развития индустрии ЦОДов.

Текущее состояние и перспективы этой индустрии обсуждались в Алматы на организованной «ИКС-Медиа» конференции «ЦОД-2018: модели, сервисы, инфраструктура».

По данным iKS-Consulting, в 2017 г. объем рынка услуг коммерческих ЦОДов в Казахстане вырос на 16% до 5,9 млрд тенге (около 1,1 млрд руб.). Всего в коммерческих ЦОДах страны установлено чуть больше 1 тыс. стоек, из них задействовано лишь 67%. По количеству установленных стоек российский рынок больше примерно в 35 раз, тогда как по уровню ВВП Россия превосходит Казахстан в 9,6 раз. Как видно, у казахстанского рынка большой потенциал для роста.

Об этом потенциале говорят и используемые крупными предприятиями модели получения ИТ-сервисов: примерно 80% размещают ИТ-инфраструктуру на собственной площадке, причем из них только 16% применяют частные облака. Из 20% компаний, пользующихся услугами коммерческих ЦОДов, больше половины предпочитают необлачную инфраструктуру.

Курс на облака. Тем не менее движение в сторону облаков очевидно и в Казахстане: доля традиционных услуг аренды площадей, стоек и серверов снижается, а доля облачных услуг растет (33% в 2017 г. против 29% годом ранее).

В частности, компания Kaztranscom, которая начинала как оператор связи, ориентированный на обслуживание корпоративных заказчиков, сегодня предоставляет широкий набор облачных сервисов на платформе kCloud. Владея двумя ЦОДами (в Астане и Атырау) уровня Tier 3, она имеет развитую сетевую инфраструктуру (7 тыс. км собственной волоконно-оптической сети), что позволяет дотянуться до клиентов по всей стране. По словам Максима Попова (Kaztranscom), основными заказчиками услуги IaaS являются компании среднего и крупного бизнеса, эксплуатирующие собственные ЦОДы. Помимо классических инфраструктурных облачных сервисов, Kaztranscom успешно развивает облачные услуги Wi-Fi, видеонаблюдения, защиты от атак DDoS, «глубокого» анализа трафика DPI.

Основной драйвер роста. Аналитики полны оптимизма относительно будущего рынка коммерческих ЦОДов республики. По мнению Светланы Черненко (iKS-Consulting), этап недоверия пройден, число сторонников использования услуг коммерческих ЦОДов и облачных сервисов растет. Среди сдерживающих факторов она выделяет стремление ИТ-руководителей сохранить контроль над ИТ-бюджетами, отсутствие «моды» на облака и аутсорсинг ИТ, а также низкую конкуренцию в большинстве отраслей – компании не рассматривают цифровизацию бизнес-процессов как конкурентное преимущество.

Драйвером развития рынка коммерческих ЦОДов может стать выполнение государственной программы «Цифровой Казахстан». Одно из основных ее направлений – создание «цифрового Шелкового пути», т.е. высокоскоростной и защищенной инфраструктуры передачи, хранения и обработки данных как для внутренних потребностей, так и для транзита. Ключевой аспект решения этой задачи – формирование современной и высокоэффективной сети ЦОДов.

Аналитики отмечают и то, что предусмотренная программой трансформация подходов к взаимодействию государства с гражданами и бизнесом предполагает переход к принципам открытой архитектуры, согласно которым будет выстраиваться «качественно новый уровень кооперации с коммерческим сектором».

От облака к мультиклауду. Понятно, что ведущие мировые поставщики ИТ-решений готовы помочь в реализации программы «Цифровой Казахстан» своими наработками. Например, Huawei, за плечами которой опыт реализации более 330 облаков для правительственных заказчиков, в том числе для полицейских структур, предъявляющих высокие требования к надежности и безопасности, представила решение FusionCloud, предполагающее использование распределенной сети ЦОДов и выделение из общего пула виртуализированных ИТ-средств ресурсов для предоставления необходимых сервисов.

Чтобы модернизировать и трансформировать ИТ, необходимо иметь четкое и полное представление о те-

кущем состоянии ИТ-среды, понять, какое влияние оказывают друг на друга рабочие нагрузки в общей среде с течением времени. Для этого может служить бесплатное онлайн-ПО Live Optics от Dell EMC. Эта система, работающая с решениями от любых вендоров, собирает и анализирует данные из операционных систем, а также аппаратных и виртуальных сред. Полученные данные позволяют оптимизировать и спланировать проведение модернизации ИТ-инфраструктуры. Саму модернизацию, по мнению Михаила Орленко (Dell EMC), проще всего осуществить, используя интегрированные, конвергентные или гиперконвергентные системы, в которых объединены все необходимые компоненты.

Все больше экспертов рассматривают гиперконвергентные системы как оптимальные решения не только для «отдельно стоящих» облаков, но и для гибридных и мультиоблачных сред. Максим Шапошников (Nutanix) называет их ИТ-платформой «под ключ», объединяющей хранение и обработку данных, сеть и виртуализацию. Использование таких систем для частных облаков позволяет «прозрачно» расширять их и задействовать внешние облачные сервисы, многие из которых построены на решениях, основанных на принципах гиперконвергенции.

Системы на основе открытого кода – еще одна категория продуктов, интерес к которым стремительно растет. Как отметил Владимир Главчев (SUSE), если еще несколько лет назад развертывание облачной платформы на базе OpenStack было «большой болью», то сегодня все в корне поменялось: решения «дозрели», на их базе успешно выполняется все больше проектов. Он предлагает пересмотреть роль «железа» и строить «программно реализуемые» (именно так в SUSE предпочитают переводить термин software-defined) ЦОДы – открытые и гибкие, с поддержкой методологии DevOps. Среди множества преимуществ такого подхода – эффективная поддержка как традиционных, монолитных приложений, так и новых приложений, реализуемых на основе контейнеров и микросервисов.

Новая парадигма безопасности. При все более глубоком проникновении ИТ во все сферы деятельности резко возрастают негативные последствия халатности в отношении кибербезопасности. Например, как рассказал Евгений Питолин («Лаборатория Касперского»), успешная кибератака на одну из нефтяных компаний позволила злоумышленникам отключить систему мониторинга скорости закачки нефти. Это привело к превышению предельной скорости закачки нефти в резервуар, электризации топлива и последующему взрыву.

В условиях, когда более 95% всех киберинцидентов вызваны человеческими ошибками (данные IBM), на первое место выходят киберучения – такой термин используют в «Лаборатории Касперского». Эксперты компании указывают на необходимость формирования культуры ИБ на всех уровнях: от рядовых пользователей до топ-менеджеров. «Наша практика показывает, что реализация проектов повышения ИБ-грамотности персонала позволяет на 80% снизить число инцидентов», – утверждает Е. Питолин.

Современные ИТ устраняют «привязку» сотрудников к офису, столь же эффективно теперь можно трудиться из дома, аэропорта, отеля и т.д. Но при этом, как отмечает Сергей Халяпин (Citrix), размывается периметр безопасности, и традиционные подходы защиты фиксированного периметра перестают работать. Эксперт Citrix предлагает реализовать программно определяемый периметр безопасности, перенеся усилия специалистов ИБ с уровня конечных устройств на уровень, не зависящий от специфики устройств и платформ.

Важны и вопросы физической безопасности ЦОДов, особенно противопожарная защита. По словам Валерия Кустова (Minimax), зачастую ЧП происходят в связи с тем, что обслуживающий персонал не представляет принципов работы систем пожаротушения. Он указывает, что для создания действительно эффективной системы противопожарной защиты ЦОДа необходимо рациональное сочетание трех компонентов: возможности раннего обнаружения возгорания; системы автоматического газового пожаротушения; реализации комплекса мер, направленных на предотвращение возгорания.

■ ■ ■

Прошедший в Алматы форум позволил специалистам Казахстана познакомиться со всем комплексом решений для построения ЦОДов и предоставления на их базе различных сервисов, в первую очередь облачных. Знание мировых трендов, наилучших практик и учет региональной специфики – залог успешной работы на любом рынке.

Александр Барсков,
Алматы – Москва

Будущее ЦОДов и DCIM Взгляд из Монако

Нас ждет развитие водяного охлаждения и решений Open Compute, уход DCIM в облака и, возможно, постепенное вытеснение ДГУ аккумуляторными батареями.

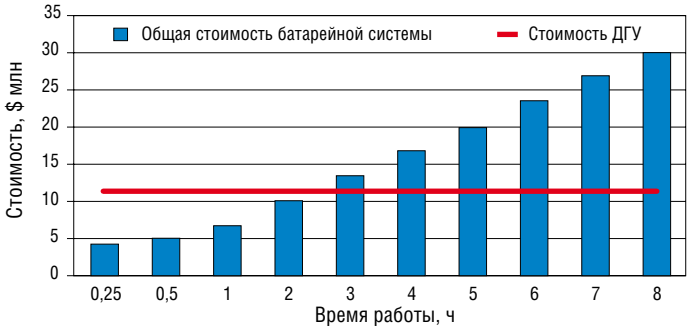
Такие выводы сделали ведущие эксперты в области ЦОДостроения, обсуждая тенденции индустрии на конференции DataCloud Europe 2018 в Монако. Особенностью этого форума является акцент на профессиональное сообщество. Здесь трудно встретить представителей крупных корпоративных потребителей, но легко пообщаться с топ-менеджерами мировых производителей программно-аппаратных средств, поставщиков услуг colocation и cloud. Дополнительный пафос событию придает место его проведения, которое, безусловно, помогает привлекать представительную аудиторию со всех уголков мира, где развивается ЦОДостроение. Княжество Монако – это яркая точка богатства и роскоши на двух квадратных километрах суши. Здесь приятно вести разговоры о перспективных технологиях и идеях, о дальнейшем развитии бизнеса и дискутировать о моделях сотрудничества.

Триггером обсуждения технологических трендов в области создания ЦОДов стало выступление старшего вице-президента по инновациям и СТО подразделения IT Division компании Schneider Electric Кевина Брауна. Он обратил внимание на статистику последнего десятилетия, связанную с повышением энергоэффективности дата-центров. По его данным, с 2007-го по 2017 гг. коэффициент PUE снизился на 80% (с 1,84 до 1,17).

Действительно, индустрия сделала огромный шаг в энергоэффективности ЦОДов. Но какие тренды станут причиной дальнейших улучшений? Их несколько:

- На уровне ПО будет расширяться интерактивное взаимодействие между инженерной инфраструктурой, электрическими сетями и ИТ-оборудованием.
- За счет распределения вычислений на уровне сети максимальные нагрузки на ИБП и энергосеть уменьшатся.
- Развитие решений Open Compute потребует оптимизации архитектуры электроснабжения.

Сравнение стоимости ДГУ и полностью батарейных решений (для системы 10 МВт). Прогноз на 2020 г.



- Продолжится совершенствование водяного охлаждения, которое будет стимулироваться дальнейшим увеличением мощности и плотности чипов.

К. Браун представил несколько перспективных технологий и решений, развитие которых будет оказывать влияние на то, какими ЦОДы станут в ближайшие годы. Это префабы, микроЦОДы, рамные решения для ИТ-стоек, топливные элементы и др.

Также было высказано важное, хотя могущее показаться спорным утверждение, что уже к 2020 г. при определенных параметрах ЦОДа аккумуляторные батареи полностью вытеснят дизель-генераторы (см. рисунок).

Конечно, говоря о трендах, нельзя было обойти стороной вопрос управления инфраструктурой ЦОДов. Коллеги из Schneider Electric верят в дальнейшее логическое развитие систем DCIM. На новом витке произойдет значительное расширение спектра подключенных в ЦОДах устройств и переход к автоматизированной облачной платформе сбора и обработки всей поступающей информации. Это позволит предсказывать возможные сценарии развития событий, используя при желании статистику сторонних дата-центров. В подтверждение своих усилий в этом направлении компания анонсировала выход новой облачной платформы EcoStruxure IT.

■ ■ ■

Как показала конференция и, в частности, общение с зарубежными коллегами, по уровню технологических компетенций и экспертизы в области строительства и проектирования дата-центров Россия уже не отстает от развитых стран. Наши специалисты готовы создавать и создают дата-центры, сравнимые по надежности и не уступающие по инновационности мировым аналогам. Жаль, что масштаб подобных объектов пока несравним с североамериканскими и североевропейскими ЦОДами.

Дмитрий Бедердинов,
Монако – Москва

Discover the Edge.

Smart Solutions. Real Business.

ENCLOSURES | POWER DISTRIBUTION | CLIMATE CONTROL | IT INFRASTRUCTURE | SOFTWARE & SERVICES

RITTAL

FRIEDHELM LOH GROUP

www.rittal.ru

Энди МакДональд: «Работать на развивающемся рынке – приключение»

За три года поднять бизнес-показатели на новый уровень – так видит свою задачу Энди МакДональд, региональный вице-президент компании Citrix в регионе Emerging Markets.

В январе 2018 г. Citrix объявила о назначении Энди МакДональда на должность регионального вице-президента в регионе «Развивающиеся рынки» (Emerging Markets), куда входит и Россия. До прихода в Citrix г-н МакДональд около 20 лет проработал в Cisco, причем последние 10 лет отвечал за создание и развитие стратегии продаж для поставщиков услуг в странах Ближнего Востока, Африки и России. В интервью на форуме Citrix Synergy 2018 он рассказал о планах работы в России, новых подходах и решениях компании.

– Какие страны находятся в зоне вашей ответственности и какова специфика работы в регионе, который в Citrix называют Emerging Markets?

– Это большой регион, помимо России и стран СНГ, в него входят страны Восточной и Юго-Восточной Европы, Ближнего Востока и Африки, а также Турция и Израиль. Хочу сразу пояснить, как термин Emerging Markets понимают в Citrix. Сам по себе рынок той или иной страны, например России, может быть вполне развитым, но продукты и сервисы Citrix на нем представлены недостаточно, есть большой потенциал для роста. Таким образом, это развивающиеся рынки именно для Citrix. Я бы назвал их рынками больших возможностей для компании. Моя задача – поднять бизнес-показатели в довольно короткий срок – за три года.

Российский рынок в сегменте Emerging Markets – ключевой для нас. В России мы располагаем внушительной базой заказчиков, включающей, в том числе, крупнейшие компании, со многими из которых я работал ранее. С ними у нас уже выстроены крепкие партнерские взаимоотношения, но стоит задача вывести их на новый уровень.

– Есть ощущение, что сейчас не лучшее время для развития бизнеса американского производителя в России...

– Последние 10 лет я регулярно посещаю Россию, и мне нравится ваша страна. Выскажу свое личное мнение: последние несколько лет были очень хорошими для России. В стране начали развивать внутренний рынок, активизировали собственные разработки, стали более эффективно внедрять новые технологии. И нам, компании Citrix, важно вписаться в новую конфигурацию, которая формируется в России. Работать на развивающемся рынке – это в какой-то степени приключение.

Понятно, в мире происходит много такого, что мы не в состоянии контролировать: санкции в отношении России, война в Сирии, падение курса национальной валюты в Анголе... Но есть вещи, которые я контролировать могу: в первую очередь это качество работы Citrix, привлекательность компании для новых сотрудников в России, адекватность наших ценовых предложений, своевременная реакция на изменения в законодательстве, которые позволят нашим клиентам чувствовать себя максимально комфортно.

Если бы я был правительственным чиновником, то в нынешней ситуации меня не слишком радовало бы подписание контракта между госкомпанией и крупным иностранным производителем. Но правильно ли будет, если правительство запретит компаниям работать с лучшими производителями на рынке, ограничив их выбор продуктами локальной разработки посредственного качества?

Мы намерены продолжить инвестировать в российский рынок, работая в той конфигурации, которую предлагает российское государство, доказывая безопасность наших решений. Допускаю, какие-то категории заказчиков не смогут использовать наши решения. Но даже с учетом этих ограничений у нас огромные возможности.

– Главным анонсом на форуме Citrix Synergy 2018 стал сервис Citrix Workspace App для создания «объединенной цифровой рабочей среды». Что дает такое решение?

– Сегодня на работу приходит много молодых людей, которые привыкли к постоянному подключению к Сети, удобным сервисам, высокой производительности работы приложений – и они хотят получить тот же пользовательский опыт и на рабочих местах. Новые рабочие места должны обеспечить все это, гарантируя контроль со стороны ИТ-службы и высокий уровень безопасности. Причем необходимо обеспечить эффективную и безопасную работу и из дома, и в дороге с мобильного устройства.

Выпустив Citrix Workspace, мы предложили наиболее полную и интегрированную рабочую среду, которая позволит пользователям получить защищенный доступ ко всем приложениям, включая мобильные и облачные, а также к данным из любого места и с любого устройства. При этом обеспечиваются возможность однократной идентификации и согласованный пользовательский интерфейс для всех типов устройств. Это дает вам возможность начать работу дома, скажем, со своего планшета, затем продолжить ее на смартфоне во время поездки в офис и завершить в офисе, используя настольный ПК.

– Citrix Workspace App – это облачный сервис, однако многие российские заказчики с настороженностью относятся к перспективам работы с облаками, особенно размещенными за границей. Что вы можете им возразить?

– Никто не говорит о том, что надо все вынести в облако. Часть наиболее важных данных находится и будет находиться в самих компаниях – и это логично. Как правило, людей отпугивают пресловутые проблемы безопасности облаков. Но по факту многие из этих проблем давно уже не существуют.

Я знаю немало российских компаний, которые успешно предоставляют облачные сервисы из ЦОДов, расположенных на территории России. И чтобы соответствовать ряду нормативных требований, Citrix должна вписаться в эту схему. Это необходимо, чтобы убедить определенные категории заказчиков в безопасности наших решений. И мы планируем сделать это, предложив наши сервисы из локальных ЦОДов. Более того, мы рассчитываем, что через Citrix Workspace App российским пользователям будут доступны и национальные сервисы – например, «Яндекса» и Mail.Ru.

Важным преимуществом наших решений является то, что заказчики могут легко переносить рабочие нагрузки из собственных ЦОДов в облачные среды по своему выбору и по мере необходимости, реализуя функцию мобильности облачных технологий. Более того, заказчики могут запускать свои рабочие нагрузки в любом облаке – AWS, Azure, Google, Oracle или в частных средах. Таким образом реализуются преимущества так называемого мультиклауда.

– Большое внимание делегатов Citrix Synergy привлекает технология SD-WAN. Какие преимущества дают соответствующие технические решения?

– Технология SD-WAN позволяет существенно упростить построение и обслуживание территориально распределенных сетей, повысив при этом их отказоустойчивость и снизив TCO. Решения SD-WAN дают возможность задействовать для подключения удаленного филиала или офиса все имеющиеся каналы связи – интернет, выделенные линии, спутниковую, сотовую связь, – автоматически распределяя трафик с учетом приоритета конкретного приложения. Механизмы SD-WAN автоматически определят неисправность в канале связи (или ухудшение его характеристик) и переведут трафик на другие каналы.

Решение SD-WAN от Citrix способно определять трафик более 4 тыс. приложений, что открывает широкие возможности для регулирования их использования. Например, можно запретить просмотр Facebook, оставив при этом функции мессенджера. Или наоборот: блокировать мессенджер, разрешив просмотр новостей Facebook. Кроме того, наше решение развертывается по принципу zero touch: достаточно подключить доставленное в филиал устройство, и конфигурационные параметры будут автоматически загружены и активированы.

Полагаю, что в России, помимо конечных заказчиков, решения SD-WAN заинтересуют «Ростелеком», «Мегафон» и других крупных операторов, которые могут стать провайдерами соответствующих сервисов Citrix. Мы уже ведем такие переговоры.

– Значит ли это, что Citrix ориентирована на работу с крупными телеком-операторами?

– Нет, конечно. Мы ориентированы на работу со всеми категориями заказчиков. Я уже упоминал интерес к сотрудничеству с коммерческими ЦОДами, которые могут стать площадками для продвижения наших облачных сервисов. Мы обсуждаем такое сотрудничество, в частности, с компанией «Сервионика».

В рамках модели прямых продаж мы активно работаем с крупными корпоративными заказчиками, такими как АФК «Система», «Газпром», Сбербанк, Газпромбанк и др. Для компаний малого и среднего бизнеса наши предложения доступны через сеть наших партнеров. Еще раз повторю: мы работаем со всеми категориями заказчиков.

Беседовал Дмитрий Бедердинов
Анахайм – Москва

Дейв Джонсон: «Смещаем акценты в сторону ПО и сервисов»

Движение ИТ-рынка в сторону периферийных вычислений, Edge Computing и облачной модели увеличивает роль, которую играют программные решения и сервисы в индустрии ЦОДов.

Прошедший в июне в Монако конгресс Datacloud Europe стал авторитетной площадкой для обсуждения ключевых направлений развития индустрии ЦОДов, в том числе их инженерной инфраструктуры. Компания Schneider Electric сделала акцент на презентации своей платформы EcoStruxure IT, которая позиционируется как система DCIM нового поколения. Об особенностях этого решения и общих тенденциях индустрии – в интервью, которое «ИКС-Медиа» дал Дейв Джонсон, исполнительный вице-президент подразделения IT Division компании Schneider Electric.

– В понимании большинства российских специалистов IT Division – это подразделение компании Schneider Electric, поставщик инженерных hi-end-решений и систем для обеспечения жизнедеятельности ИТ-инфраструктуры. Как меняется и будет меняться бизнес IT Division с выходом на рынок решений, подобных EcoStruxure IT?

– Если сегодня наши основные продажи связаны с оборудованием, то в будущем все большая доля доходов, как мы планируем, будет поступать от ПО и сервисов. Как показывает конференция Datacloud Europe, в целом ИТ-рынок смещается в сторону периферийных вычислений, Edge Computing, а также облачной модели. Мы тоже идем в этом направлении, и программные решения и сервисы будут играть важную роль в этом движении.

Когда мы выводили на рынок платформу EcoStruxure IT, то рассчитывали, что ее программные компоненты будут использоваться в первую очередь крупными ЦОДами для мониторинга инфраструктуры и анализа собираемых данных. Но оказалось, что они не менее востребованы в небольших дата-центрах, создаваемых для периферийных вычислений (Edge Computing). И это понятно: для сети распределенных по большой территории объектов необходимы самые современные инструменты удаленного контроля. В большом же ЦОДе все ресурсы размещены локально, многие вещи можно контролировать непосредственно.

Мы прогнозируем, что количество Edge-ЦОДов будет стремительно увеличиваться. В том числе и ЦОДов размером с одну стойку. Такие решения будут устанавливаться на производственных площадках, в торговых центрах, отелях, медицинских учреждениях и т.д. И для контроля работы таких ИТ-объектов потребуются «продвинутые» инструменты.

– Какое влияние на взаимодействие с вашими корпоративными клиентами оказывает рост популярности модели аутсорсинга ИТ? Для вас это сокращение количества потребителей?

– Очевидный тренд: рост популярности модели аутсорсинга и услуг аренды площадей и размещения оборудования в коммерческих ЦОДах. Корпоративные заказчики передают все больше задач таким площадкам, используют облачные сервисы. Но при этом они активно модернизируют свои ЦОДы. Наши сервисные предложения ориентированы, в том числе, на то, чтобы помочь им решать эти задачи.

Все чаще возникают ситуации, когда одна часть ресурсов компании находится в собственном ЦОДе, другая – отдана на colocation. Применение в такой ситуации решений EcoStruxure IT привлекательно тем, что они позволяют управлять распределенной инфраструктурой централизованно. Облачные сервисы EcoStruxure IT дают возможность эффективно осуществлять мониторинг ИТ-оборудования, систем электропитания, охлаждения и пр. Для таких сервисов не важно, где размещается оборудование. Заказчик видит полную картину состояния его ресурсов вне зависимости от того, насколько сложно они распределены.

Повторю, рынок корпоративных ЦОДов сокращается, но рынок коммерческих ЦОДов и облачных провайдеров находится на подъеме. И это нас радует.

– В России для многих потенциальных покупателей систем DCIM экономическое обоснование их внедрения представляет проблему. Полагаю, что подобные сложности есть и в других странах. Как EcoStruxure IT сможет помочь решить такие проблемы?

– Классические системы DCIM часто с большим трудом внедрялись и обслуживались. Для некоторых заказчиков решение оказывалось дорогостоящим. Во многом поэтому DCIM не востребованы на рынке абсолютно всеми операторами ЦОДов. При переходе на EcoStruxure IT большая часть системы приходится на облачный сервис, и проблемы внедрения устраняются. Запуск ПО становится более автоматизированным, и исчезают основные сложности, связанные с его развертыванием и обновлением. Кроме того, решение прекрасно масштабируется, и первоначальные вложения могут быть минимальными.

Отзывы первых заказчиков, использующих EcoStruxure IT, очень положительны. Они отмечают, что могут контролировать свою инфраструктуру, получая необходимые уведомления на мобильные устройства – даже катаясь на горных лыжах или находясь на футбольном матче. Таким образом, облачное решение – это проще, дешевле и гораздо удобнее.

– Какие категории заказчиков, по вашим расчетам, будут в первую очередь применять это решение?

Большинство заказчиков – поставщиков услуг colocation точно заинтересованы в такой системе. Кроме того, она дает очевидные преимущества компаниям с большим числом Edge-ЦОДов. Эти категории компаний – в числе первых заказчиков нового решения. Сюда же относятся финансовый сектор и промышленность – и те, кто уже использует наши решения DCIM, и те, кто по ряду причин не успел их развернуть. Теперь решение станет доступнее, а необходимый результат будет достигнут в кратчайшие сроки.

– Как традиционные решения DCIM соотносятся с EcoStruxure IT?

– Традиционные продукты DCIM являются частью нашей архитектуры EcoStruxure. Это продукты, которые по-прежнему востребованы, и мы будем их поддерживать. Но надо понимать, что EcoStruxure IT – принципиально новое ПО, функционирующее как облачный сервис и дающее множество преимуществ пользователям. То, что традиционно входило в наше портфолио DCIM, образует базовый уровень, обеспечивающий наиболее полный охват инженерной инфраструктуры. EcoStruxure IT может дополнять классическое решение, а может внедряться независимо.

В новой облачной системе реализованы более мощные средства анализа собираемых данных, включая средства искусственного интеллекта. Недавно представители Google заявили, что, используя технологии искусственного интеллекта, им удалось повысить эффективность систем охлаждения на 30%. Далеко не у всех заказчиков достаточно данных и экспертизы, чтобы самим внедрять подобные наработки. У Schneider Electric огромное число заказчиков по всему миру. Собирая данные с их ЦОДов (естественно, по договоренности с владельцами) и обрабатывая их в облаке с применением технологий анализа Big Data и искусственного интеллекта, мы получаем ценные сведения, которые могут существенно повысить эффективность работы ЦОДа конкретной компании.

– Наряду с использованием облачных сервисов для управления ЦОДами, среди наиболее обсуждаемых тенденций – развитие альтернативной энергетики: солнечных батарей, ветрогенераторов и пр. Что вы думаете о перспективе применения таких решений в ЦОДах?

– В энергосистемах класса micro-grid солнечные батареи и ветровые генераторы используются уже достаточно давно. Появляются примеры применения таких решений и в ЦОДах. В ближайшее время у нас появится хорошее решение для накопления энергии, что позволит шире задействовать альтернативную энергетику для ЦОДов. Многие не любят дизель-генераторы: они занимают много места, требуют особых условий установки, сложной обвязки и обслуживания. Поэтому накопители энергии будут постепенно их заменять. Это важный тренд.

Развитию такой тенденции способствует и то, что новые элементы, используемые в ИТ-оборудовании, потребляют существенно меньше электроэнергии в неактивном состоянии. Если раньше уровень пассивного потребления составлял примерно 60% полной нагрузки, то теперь он опустился почти до 10%. Соответственно, на порядок выросло соотношение мощности, потребляемой серверами в активном и пассивном состояниях. Значит, уже нет необходимости проектировать ЦОД с расчетом на длительную работу при полной мощности. Можно использовать накопители, способные в пиковые моменты дать необходимую энергию. Поставщиками этой энергии могут быть солнечные батареи и ветрогенераторы.

Пока такие решения мало применяются, поскольку в большинстве проектов это экономически не оправдано. Они слишком дорого стоят. Но если удастся эффективно интегрировать их с системой накопления энергии, одновременно снизив мощность, получаемую от энергосистемы, то решение вполне может получиться экономически выгодным. Понятно, что эффективность использования таких технических решений зависит от места нахождения объекта.

Беседовал Дмитрий Бедердинов
Монако – Москва

На CeBIT со своим литий-ионом

На прошедшей в Ганновере выставке компания Delta Electronics представила ряд новинок. В первую очередь внимание привлекли компактные ИБП средней и большой мощности с литий-ионными батареями.

Литий-ионные батареи пользуются все большей популярностью у заказчиков. Их хорошо известные преимущества (компактность, малый вес, долгий срок службы, быстрый заряд) долгое время не могли перевесить такие недостатки, как пожароопасность и высокая стоимость. Но в последние годы проблемы с безопасностью были решены, а стоимость снижена настолько, что при расчете TCO решения с литий-ионными батареями стали все чаще выигрывать у традиционных со свинцово-кислотными АКБ.

Практически все поставщики ИБП используют литий-ионные батареи сторонних производителей. Delta Electronics пошла по другому пути: приобретя соответствующее подразделение одного из известных производителей, она теперь имеет такие батареи в своем портфеле продуктов. На CeBIT 2018 компания представила сразу несколько вариантов ИБП с литий-ионными батареями. При этом сами ИБП (силовые блоки) отличаются компактностью под стать батареям.

Например, новый модульный ИБП DPH мощностью до 500 кВА занимает всего одну стойку. Система необходимой мощности набирается из силовых модулей по 50 кВА. А устанавливаемые в стандартные стойки ИБП серии RT при высоте всего 2U обеспечивают мощность до 20 кВА. Они могут комплектоваться блоками литий-ионных батарей, выполненных в таком же корпусе.

В рамках CeBIT компания провела награждение наиболее значимых из числа выполненных на основе ее оборудования проектов. Два победителя оказались из России. Один проект – установка систем ИБП (общей мощностью более 15 МВт) на пяти стадионах, на которых прошли игры Чемпионата мира по футболу. Другой – оснащение четырех ЦОДов для одной из крупных промышленных групп. Особенность проекта в том, что все объекты расположены за Полярным кругом, где температура опускается до –55°C. В этих ЦОДах установлены более 50 стоек, 15 блоков кондиционеров, 100 устройств распределения электропитания (PDU). Бесперебойное электропитание обеспечивают ИБП PHP мощностью 80–120 кВт. В данном проекте компания выступила как поставщик комплексного решения для инженерной инфраструктуры, предложив все основные ее элементы.

Собственно говоря, Delta Electronics уже несколько лет назад вошла в узкий круг компаний, способных помочь заказчикам построить моновендорный ЦОД. Как и другие «члены клуба», Delta может предложить все основные системы как по отдельности, так и в виде предсобранного на заводе решения. Таковым является, например, показанный на CeBIT модульный ЦОД. В его состав входят все необходимые конструктивы, датчики (для работы в составе системы управления DCIM), блоки бесперебойного электропитания и охлаждения.

«Delta Electronics уже завоевала у российских заказчиков репутацию поставщика качественных и надежных систем бесперебойного электропитания. Теперь наша задача сделать так, чтобы нас воспринимали не только как поставщика отдельных продуктов, но и как партнера, способного предложить полное решение в области инженерной инфраструктуры на всех этапах – от проектирования и реализации до последующего обслуживания и развития», – отметил Михаил Гребенников, директор направления ИБП и ЦОД Delta Electronics в России.

Александр Барсков,
Ганновер – Москва

Panasonic
BUSINESS

ДАЙТЕ МНЕ UC-ПЛАТФОРМУ, И Я ПЕРЕВЕРНУ МИР

UC-платформа KX-NSX2000/1000
SIP-видеотелефон KX-HDV430

Унифицированные коммуникации. Передовые технологии. Оптимизация расходов.

UC-платформа KX-NSX – это переворот в представлении о традиционных офисных коммуникациях от Panasonic. Современные IP-технологии и все необходимые сервисы позволят сотруднику работать из любой точки мира.

- Высокая надежность системы за счет «горячего» резервирования
- Возможность подключения до 2000 IP-абонентов
- Поддержка всех существующих коммуникационных сервисов

Мы создаем платформу для вашего бизнеса, чтобы вы перевернули этот мир!

www.panasonic.com b2b.panasonic.ru

ПЯТЬ ЛЕТ ГАРАНТИИ
5
ПРИ УСЛОВИИ ИСПОЛЬЗОВАНИЯ ОБОРУДОВАНИЯ АВТОРИЗОВАННЫМИ СПЕЦИАЛИСТАМИ
ПОДРОБНЕЕ НА САЙТЕ WWW.PANASONIC.COM

Международная конференция и выставка

«ЦОД-2018: модели, сервисы, инфраструктура»

28 ноября 2018, Екатеринбург, Hyatt Regency Ekaterinburg

Основные вопросы конференции:

- Аналитика iKS-Consulting. Анализ потребности в дата-центрах и их востребованности в УФО
- Развитие рынка облачных услуг в РФ и регионах
- Мировые тренды в области развития сервисных моделей и инфраструктуры ЦОДов
- Географические, климатические, экономическиепреимущества развития ЦОДов в УФО
- Современные технологии и решения для инженерной и ИТ-инфраструктуры ЦОДов
- Переход в облако. Конвергентные и гиперконвергентные решения
- Edge и Fog Computing – помощники или конкуренты Облаку?

При поддержке

Uptime Institute™

Организатор:

ИКС МЕДИА

www.ekb.dcforum.ru

За дополнительной информацией обращайтесь по тел.: +7 (495) 150-64-24 и e-mail: dim@iksmedia.ru

Платиновый спонсор

DATALINE

Золотой спонсор

RITTAL

Спонсоры

CABERO HEAT EXCHANGER

ПОЖТЕХНИКА

Партнер выставки

POWERCONCEPT
ПРОМЫШЛЕННЫЕ АККУМУЛЯТОРЫ

IXcellerate
MOSCOW ONE DATACENTRE | MOSCOW ONE ДАТА-ЦЕНТР

Большой и элегантный

Компания IXcellerate ввела в эксплуатацию третью фазу своего московского ЦОДа. Ленточку торжественно перерезали руководители IXcellerate, ARUP (генеральный проектировщик) и Vertiv (основной поставщик инженерных систем). Главный на церемонии открытия – технический директор IXcellerate Сергей Вышемирский (второй справа), возглавлявший штаб строительства нового зала.

Гибридный вариант выбран при реализации комплекса охлаждения нового зала. Во-первых, задействованы неиспользуемые ресурсы чиллерной системы охлаждения второй фазы (фото вверху). Во-вторых, установлена система фреонового охлаждения с фрикулингом (на фото справа вверху – конденсаторные блоки с модулем Vertiv EconoPhase™, обеспечивающим работу в режиме

Работа коммерческого ЦОДа IXcellerate Moscow One началась в 2013 году с ввода в эксплуатацию зала на 220 стоек. Затем была реализована вторая фаза – на 515 стоек.Третья фаза – самый большой машинный зал в России вместимостью 1100 стоек с ИТ-оборудованием.

В проекте воплощены самые современные технологии. Так, система бесперебойного электропитания построена с использованием литий-ионных батарей. При расчете TCO на 10 лет такое решение оказывается примерно в два раза дешевле, чем решение на базе свинцово-кислотных батарей.

Принцип монообъемности, заложенный при проектировании, позволил существенно увеличить полезную площадь нового машинного зала и сократить капитальные затраты на его строительство и оснащение.

фрикулинга). Наконец, в-третьих, разворачивается новая чиллерная система с адиабатическим охлаждением. Такую комбинацию трех систем специалисты IXcellerate и ARUP посчитали оптимальной.

Уникальна развернутая в ЦОДе IXcellerate автоматическая система пожаротушения HI-FOG™. В ней использован принцип тушения тонкораспыленной дистиллированной водой, подаваемой по сухотрубной системе. Система обеспечивает возможность размещать инфраструктуру клиентов без создания гермозон, как в случае газового пожаротушения, что стало одним из условий построения большого зала.

Безопасность – в числе приоритетов современных ЦОД. На входе в ЦОД IXcellerate – полноростовой турникет и система сканирования ладони. Такая же система – на входе в машзал. А для доступа в зону, выгороженную для конкретного заказчика, – сканер отпечатков пальцев.

Надежность предоставления сервисов во многом определяется работой службы эксплуатации. Тщательный подбор персонала, отработанные процедуры действий в типовых и нестандартных ситуациях, эффективная система управления с высокой степенью автоматизации – залог обеспечения высокой готовности ИТ-комплексов.

iKS CONSULTING

Ситуация, сложившаяся на рынке коммерческих дата-центров по итогам 2017 г., во многом определялась поисками нового клиентского предложения для усиления конкурентных позиций и существенным пересмотром приоритетов под воздействием ряда факторов.

По оценкам iKS-Consulting, рынок коммерческих ЦОД в 2018 году:

Новые механизмы развития регионального рынка и возможные модели партнерства

44,5 тыс. стойко-мест

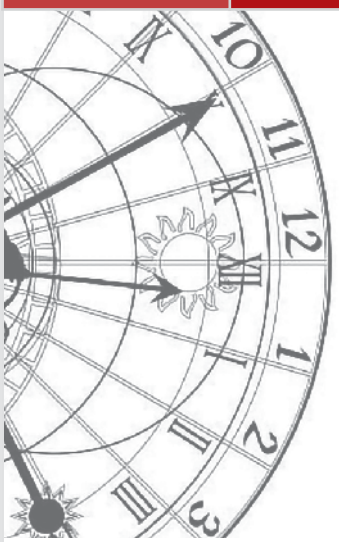
5,9 тыс. новых стойко-мест введено на рынок игроками (+21%YY)

Наращивание экспертизы в области управления клиентской инфраструктурой и реализации проектов системной интеграции

Явно выраженная сегментация предложения на рынке кЦОД

Рост предложения облачных услуг, в том числе мульти- и гибридных решений

Современная инфраструктура для цифровой экономики и реализации экспортного потенциала российских кЦОД



Отчет дает углубленное представление о состоянии всего рынка коммерческих ЦОД: от исторических показателей и наращиваемых и вводимых емкостей до анализа площадок по таким показателям, как возраст, число стоек, доходы, географическое расположение и региональные сегменты, другие характеристики. iKS-Consulting представляет всю структуру игроков и рассматривает развитие рынка под влиянием различных факторов в целях реализации оптимального сценария его развития. Кроме того, отчет дополнен информацией об облачных провайдерах, партнерских альянсах и другими интересными данными и выводами, дающими широкое и углубленное представление обо всем рынке.

Структура отчета Российский рынок коммерческих дата-центров 2017-2022

Параметры отчета

Стоимость: 159 000 руб. (без НДС)
Объем отчета: более 100 страниц
Количество иллюстраций: более 50

Подробная информация и заказ отчета

Феоктистова Дарья
E-mail: fd@iks-consulting.ru
Тел.: +7 (495) 150-64-24

Дата выхода: 13 сентября 2018

IoT в России обзаводится инфраструктурой

Строительство беспроводных сетей по технологии LoRaWAN в разных регионах страны сегодня ведут сразу несколько операторов.

А. Чуб: «В первую очередь мы предлагаем нашим партнерам опоры двойного назначения – наиболее эффективный инфраструктурный объект для городской агломерации».

Компания МТТ и ГК «Русские Башни» объявили о сотрудничестве в сфере создания инфраструктуры для IoT и IIoT в Москве и Московской области. Они подписали долгосрочный договор, по условиям которого МТТ на территории Москвы и Московской области будет размещать базовые станции стандарта LoRaWAN на антенно-мачтовых сооружениях и других объектах, находящихся в управлении ГК «Русские Башни».

Преимущества технологии LoRaWAN хорошо известны. Она относится к классу радиотехнологий с низким энергопотреблением, полностью стандартизована, работает в нелицензируемом диапазоне частот, отличается высокой энергоэффективностью и изначально создавалась для передачи телеметрических данных на большие расстояния.

По словам Александра Чуба, президента ГК «Русские Башни», до конца 2018 г. компания МТТ планирует арендовать до 100 объектов в разных районах столицы и Подмосковья, далее масштаб сотрудничества будет расти. (Сегодня «Русские Башни» готовы предложить партнерам 2500 объектов в Москве и в Московской области.)

Как пояснили в пресс-службе МТТ, на первом этапе проекта, инвестиции в который оцениваются в несколько десятков миллионов рублей, оператор планирует развернуть сеть LoRaWAN из 50–70 базовых станций в Центральном административном округе столицы. В качестве потенциальных клиентов услуг передачи данных с различных IoT-устройств компания рассматривает логистических операторов, ритейлеров, сельхозпроизводителей, негосударственные компании в сфере ЖКХ, а также бизнес- и торговые центры, выставочные пространства. С рядом таких компаний МТТ уже ведет переговоры и тестирует сервисы.

Строительство сети LoRaWAN в Москве и в Московской области – это шаг к достижению новой цели МТТ: занять значительную долю на рынке IoT-решений, о которой Евгений Васильев, генеральный директор компании, объявлял при подведении итогов прошлого года. До конца 2018 г. МТТ планирует развернуть беспроводные сети этого стандарта в Петербурге, Екатеринбурге, Казани и Нижнем Новгороде.

Надо сказать, что беспроводные сети LoRaWAN сегодня в России строят несколько операторов связи. В их числе «ЭР-Телеком Холдинг», в начале этого года подписавший соглашение с компанией Activity о развертывании сети LoRaWAN федерального масштаба и об управлении этой сетью с помощью платформы ThingPark Wireless. Оператор уже объявлял о запуске такой сети в Ярославле, а с августа она заработала в Уфе.

Другим игроком, также претендующим на долю нового рынка, является «Ростелеком», этим летом заключивший договор с компанией «Лартех», оператором на рынке услуг передачи данных в сфере интернета вещей, на поставку оборудования и ПО для строительства сети LoRaWAN на территории Центрального федерального округа России.

«Операторов, которые заявляют, что строят или будут строить LoRaWAN-сети, не так много. Это "Лартех", "Сеть868", "ЭР-Телеком", МТТ, – комментирует Татьяна Толмачева, основатель iKS-Consulting. – Как правило, размеры покрытия их сетей пока определяются проектами, реализуемыми в интересах тех или иных заказчиков». Эксперт считает, что риски операторов, связанные с утверждением отличного от LoRaWAN стандарта в качестве единого для интернета вещей, будут минимизированы после гостирования этой технологии в России, первые шаги к которому уже предприняты.

Александра Крылова

Медицинские карты на блокчейне

Московская область планирует использовать технологии распределенного реестра для хранения медицинских карт граждан.

Это позволит пациенту просматривать и предоставлять свою единую медицинскую карту государственным и коммерческим медицинским организациям для записи результатов анализов и лечения без привязки к конкретному медицинскому учреждению. Об этом сообщил заместитель председателя правительства Московской области – министр государственного управления, информационных технологий и связи Московской области Максут Шадаев.

Пациенты посещают районные поликлиники, находятся в больницах, получают консультации и проходят процедуры в государственных и коммерческих медицинских организациях. Каждое медицинское учреждение заводит карты пациентов, информация о болезнях и курсах лечения разбросана по разным базам, граждане сдают лишние анализы, тратя время и деньги. «Наша задача номер один – перевести медицинские карты в формат, когда каждый житель может давать доступ к содержимому своей карты любому врачу в любом учреждении, в том числе негосударственном, и контролировать внесение изменений в историю болезни. Дальше на базе технологии блокчейн надо автоматизировать выставление счетов по каждой услуге страховым компаниям, чтобы избежать приписок в медицинских организациях», – пояснил М. Шадаев.

Технология блокчейн обеспечивает доверие, что очень важно в медицине. Например, разрабатываемая в Оксфордском университете платформа Medichain позиционируется как система, позволяющая пациентам безопасно хранить свои данные и предоставлять к ним доступ специалистам в любой точке мира, независимо от медицинской сети или используемой электронной медицинской карты (ЭМК).

Созданный в лаборатории Массачусетского технологического института на платформе Etherium сервис MedRec дает возможность просматривать и редактировать информацию о лекарствах, которые принимает пациент, и объединять данные с медицинских карт в разных медицинских учреждениях. Организацию взаимодействия пациентов, страховых компаний и лечебных учреждений на технологии блокчейн предлагает американский стартап Gem.

В России медицинских блокчейн-стартапов не много, но они есть. Так, проект Robomed разрабатывает систему применения смарт-контрактов для регулирования отношений между потребителями и поставщиками медицинских услуг. Разработкой блокчейн-решения для Robomed занимается команда проекта Blockchain.ru. В блокчейне с помощью смарт-контракта фиксируется

Филипп Миронович (Robomed): «Узел блокчейн-сети входит в установочный пакет системы моделирования бизнес-процессов медучреждения».

факт заказа и оценка качества услуги. Такой подход позволяет получать независимые оценки и иметь систему хранения записей, защищенную от подделок.

Результаты оказания медицинской услуги по смарт-контракту записываются в блокчейн вместе с зашифрованным адресом расположения протокола, созданного медицинским персоналом. Благодаря индивидуальному ключу шифрования в мобильном телефоне информация о нахождении связанных с ним протоколов доступна только клиенту.

Подход вполне здравый – не стоит хранить в публичном, медленном и дорогостоящем блокчейне персональную информацию пациентов, достаточно записать хеш услуги, подтверждающий ее подлинность, а сами данные держать в обычных базах медицинских учреждений. Стоматологу не обязательно знать результаты обследования, проведенного окулистом. Пациент на приеме сам должен определять, открывать ли доступ врачу к результатам своих анализов. А обезличенные данные могут использоваться для анализа, например, динамики заболеваемости или эффективности лекарственных препаратов.

В настоящее время реализована часть мобильного приложения Robomed и идет отладка работы на базе одного медицинского учреждения.

Николай Носов

Надежный ЦОД – безопасные полеты

Безопасное и регулярное движение воздушного транспорта сегодня невозможно без информационных технологий, а значит, и без центров обработки данных. Новый ЦОД ФГУП «Государственная корпорация по организации воздушного движения в Российской Федерации» построен с использованием передовых технических решений Schneider Electric.

«Госкорпорация по ОрВД», ведущая свою историю от Единой системы управления воздушным движением СССР, обслуживает в год более 1,5 млн полетов, которые проходят над территорией более 26 млн кв. км. Одновременно под управлением предприятия находятся свыше 1000 воздушных судов.

Новый ЦОД по плану станет первым элементом катастрофоустойчивого комплекса из нескольких объектов, развернутых в разных регионах страны. Этот комплекс обеспечит централизацию ИТ-сервисов, используемых административно-управленческими подразделениями Госкорпорации. По сути, он станет основой частного облака для предоставления современных ИТ-сервисов. Кроме того, комплекс может стать технологическим центром для управления инфраструктурой имеющихся в корпорации серверных и небольших ЦОДов.

ЦОД построен в специально подготовленном помещении нового офисного здания «Госкорпорация по ОрВД». Генеральным подрядчиком проекта выступил «Концерн ВКО «Алмаз-Антей», а основным поставщиком инженерного оборудования – компания Schneider Electric.

Как рассказывает Антон Шувалов, заместитель генерального директора по ИТ «Госкорпорации по ОрВД», основные требования к новому ЦОДу – это высокий уровень безопасности, надежности и управляемости.

Для достижения современных характеристик на объекте были внедрены технологии управления жизненным циклом физической инфраструктуры, включившие инструменты мониторинга, проактивного управления и планирования развития. Основой системы стали продукты StruxureWare Data Center Expert и Data Center Operation.

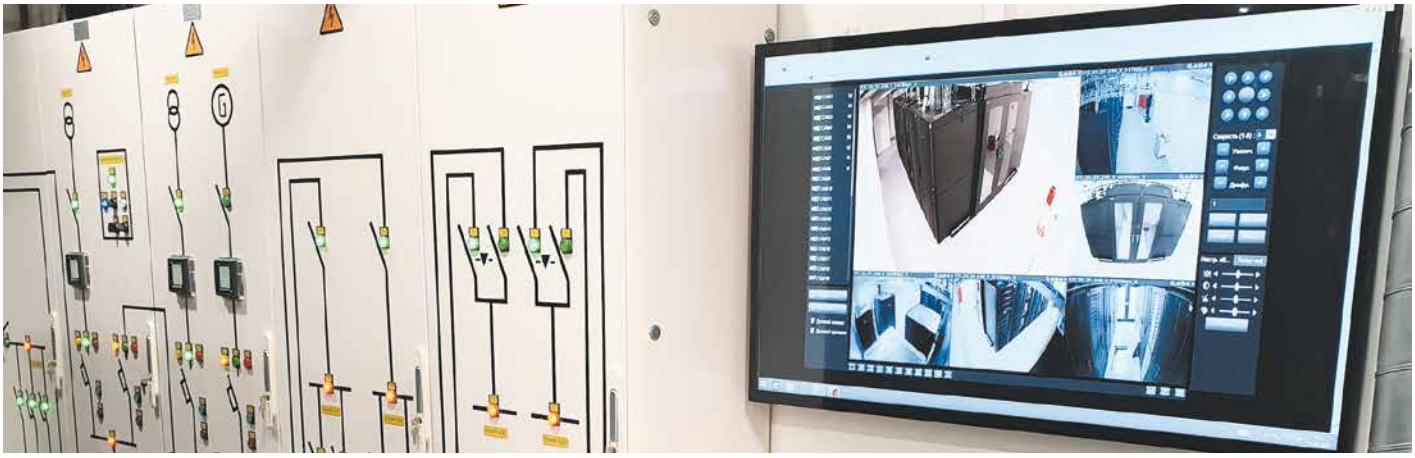
«И заказчик, и поставщик понимали, что ЦОД нового поколения, соответствующий современным требованиям по надежности, отказоустойчивости и управляемости, невозможен без средств проактивного управления. Поэтому системам мониторинга и планирования уделялось большое внимание с самого начала проекта», – рассказывает Вячеслав Потапов, руководитель направления по работе с заказчиками в Центральном и Южном регионах, подразделение IT Division компании Schneider Electric.

В последнее время все больше заказчиков стараются ориентироваться на моновендорные решения. Их привлекают такие преимущества, как отличная совместимость всех компонентов, максимальная функциональность, сокращение срока поставки, «одно окно» для сервисного обслуживания и пр. Однако на практике далеко не всегда есть возможность реализовать моновендорную инженерную инфраструктуру.

Так получилось и в случае с ЦОДом «Госкорпорации по ОрВД». У предприятия уже была развернута чиллерная система, закуплены внутрирядные кондиционеры. Новый ЦОД требовалось построить с использованием имеющегося оборудования. И надо сказать, что специалисты Schneider Electric с пониманием отнеслись к задаче сохранения уже сделанных заказчиком инвестиций, а решения компании были полноценно интегрированы с элементами других производителей.

Имеющиеся у заказчика кондиционеры отлично вписались в ряд с серверными шкафами Schneider Electric – в проекте использованы шкафы увеличенной глубины AR3300 и AR3340 (всего 12 шкафов). Более того, полученный в результате расстановки шкафов в два ряда «горячий» коридор был закрыт системой контейнеризации (изоляции) коридора EcoAisle.

В данном проекте EcoAisle интегрирована с системой пожаротушения, построенной на основе технических ре-



шений отечественного производителя. При срабатывании средств пожаротушения соответствующая информация отражается в системе мониторинга, а потолки EcoAisle автоматически сбрасываются – чтобы пожаротушащее вещество поступило к стойкам с оборудованием.

Система бесперебойного электропитания реализована на базе модульных ИБП Symmetra PX. Резервирование N + 1 выполнено на уровне модулей, которые можно заменять в «горячем» режиме. ИБП установлены внутри рядов шкафов, а вот аккумуляторные батареи (АКБ) вынесены за их пределы. Это связано с большим количеством АКБ. Требование заказчика – обеспечить автономность 45 мин при полной нагрузке. Как поясняет Антон Шувалов, это время необходимо для корректного завершения работы и/или миграции ИТ-приложений.

Для создания максимально достоверной картины о состоянии ЦОДа на всех критических элементах установлены необходимые датчики, а активное оборудование объединено в сеть и подключено к системе мониторинга Data Center Expert. Система поддерживает оборудование как Schneider Electric, так и других производителей, что позволяет предоставить инженерной службе единую картину о состоянии инфраструктуры, текущих нагрузках, состоянии систем электроснабжения и охлаждения. В случае возникновения аварийных ситуаций своевременное оповещение (e-mail и голосовое) позволит устранить неполадку в кратчайшие сроки, а затем провести анализ ситуации и причин ее возникновения.

Система Data Center Expert значительно более универсальна, чем большинство иных систем мониторинга и автоматизации, поскольку обеспечивает ряд функций безопасности (включает возможности видеонаблюдения и контроля доступа). Так, на данном объекте была использована система управления доступом в серверные шкафы, которая контролируется централизованно. Многие руководители служб эксплуатации отмечают, что это не только ограничивает возможный несанкционированный доступ, но и предотвращает элементарные человеческие ошибки, а также позволяет проводить более полный анализ инцидентов, возникающих на границах зон ответственности ИТ- и инженерных служб.

И конечно, ЦОД не управлялся бы настолько эффективно без внедрения инструментов анализа и планирования Data Center Operation. Набор возможностей Operation позволяет внедрить целый набор регламентов для проведения изменений в ЦОДе – от подбора оптимального места для установки оборудования, инвентаризации, контроля подключений до моделирования отказов и оценки долгосрочной эффективности инфраструктуры.

В ИТ-шкафах установлены интеллектуальные блоки розеток (PDU) с функциями мониторинга – есть возможность посмотреть нагрузку на каждой розетке. Реализована двухлучевая система (2N) – в каждом шкафу по два PDU. В некоторых шкафах, где размещается критичная нагрузка с одним вводом питания, установлены стоечные автоматы ввода резерва (АВР).

Как уже говорилось, в проекте акцент был сделан на мониторинг, проактивное управление и планирование инфраструктуры ЦОДа. «Наше ПО позволяет прописывать, что в ЦОДе уже установлено, где остался резерв, например, по энергетике. Вся информация представляется в удобном для планирования работ виде, – поясняет Вячеслав Потапов. – Если надо разместить новый сервер, ПО «покажет», куда (в какой шкаф) его можно поставить, и «предупредит», куда ставить нельзя».

В новый ЦОД заложены модули StruxureWare, позволяющие в дальнейшем задействовать центральную систему для мониторинга удаленных объектов. Это позволит вывести всю ИТ-инфраструктуру в единое информационное поле.

Характеризуя решения Schneider Electric, помимо их удобства, функциональности и качества Антон Шувалов отмечает работу компании по локализации производства, что «важно как для “Госкорпорации по ОрВД”, так и для страны в целом». Schneider Electric уже вложила более $1 млрд в российские производственные мощности и продолжает инвестировать. Более 60% продукции, поставляемой российским клиентам, производится в России на шести собственных заводах компании.

17--19 октября в Сочи (Главный медиацентр Олимпийского парка) пройдет **Форум инновационных финансовых технологий Finopolis**.

В эпоху цифровизации, внедрения технологий во все отрасли жизни, уже недостаточно просто следить за тенденциями. Важно уметь заглядывать вперед и задавать направление развития. Это особенно важно в финансовом секторе, который обеспечивает потребности всех отраслей экономики. Форум Finopolis, собирающий на одной площадке ведущих представителей финансового и ИТ-сектора, позволяет взглянуть на ситуацию с разных сторон и выработать план действий на ближайшую перспективу.

Finopolis – крупнейшая в стране площадка для обсуждения и анализа тенденций и возможностей применения современных цифровых технологий в финансовом секторе. Ежегодно форум собирает около полутора тысяч участников из российских и зарубежных компаний, экспертов и представителей органов власти. В рамках форума 17 октября также состоится молодежный день FinTech, в котором примут участие студенты российских вузов.

Организатор: Банк России.

www.finopolis.ru

выставки, семинары, конференции

Дата и место проведения, организатор, сайт	Наименование мероприятия
12.09. Москва **ITWeek** itweek.ru/ecm/recs	Russian Enterprise Content Summit 2018
13.09. Москва **ИКС-МЕДИА** dcforum.ru	**13-я ежегодная международная конференция и выставка «ЦОД-2018»**
20.09. Москва **Fujitsu** fujitsu.com/ru/microsite/world-tour-2018	Конференция «Fujitsu World Tour 2018. Сотрудничество для достижения успеха»
19–21.09. Москва **«Лаборатория Касперского»** ics.kaspersky.ru/conference	6-я международная конференция «Промышленная кибербезопасность: цифровая трансформация – вызовы и возможности»
20.09. Санкт-Петербург **Министерство цифрового развития, связи и массовых коммуникаций РФ** itdialog.info	5-й всероссийский форум в области информационных технологий «IT Диалог 2018»
25.09. Москва **Smile-Expo** iotconf.ru/ru	5-я международная конференция «Интернет вещей»
01–02.10. Казань **Redenex** iotworldsummit.ru	2-й всемирный цифровой саммит IoT World Russia Summit 2018
03.10. Москва **«ТелеСпутник»** 4k.telesputnik.ru	3-я международная конференция Digital TV & Video in Russia. 4K&HDR
10–11.10. Москва **Ассоциация российских банков** vbaforum.ru	5-й международный форум «Вся банковская автоматизация 2018»
15.10. Санкт-Петербург **JUG.ru Group** smartdataconf.ru	Конференция SmartData 2018

Присылайте анонсы ваших мероприятий на IKSMEDIA.RU

Еще больше на

С 1 по 2 октября в Казани (Korston Club Hotel) пройдет 2-й мировой цифровой саммит **IoT World Russia Summit**, посвященный цифровой трансформации промышленных и бизнес-процессов, применению технологий интернета вещей, монетизации данных и перспективам развития искусственного интеллекта.

IoT World Summit Russia расскажет о множестве мировых и отечественных кейсов по IoT, последних трендах и путях развития индустрии в сегментах интернета вещей и «умных» технологий. В программе этого года будут выделены 10 специализированных конференц-потоков: «Промышленность 4.0», «Цифровые корпорации», «Умный город и цифровое правительство», «IoT: энергетика и ЖКХ», «Big Data & аналитика данных», «Искусственный интеллект», «Блокчейн», «IoT: кибербезопасность, «IoT: коммуникации и связь», «Технологическое предпринимательство».

Участники саммита смогут познакомиться с опытом лучших международных экспертов, внедривших у себя технологии IoT. Спикеры поделятся секретами успеха и расскажут об использовании «умных» технологий в различных производственных и социальных сферах.

Организатор: Redenex.

iotworldsummit.ru

15 ноября в Москве (отель Holiday Inn Lesnaya) состоится Второй всероссийский бизнес-форум **«Развитие сетей беспроводной связи в России – 5G Future Russia 2018»**.

Сети 5-го поколения станут платформой для вывода экономики страны на новый уровень и обеспечения ее стабильного роста. В числе обсуждаемых на конференции тем будут следующие:

- Госполитика развития национальной цифровой инфраструктуры и дальнейшее развитие программы ликвидации цифрового неравенства.
- Стандартизация новых технологий и сетей 5G.
- Новые полосы радиочастот для сетей 5G в России, принципы их распределения и условия использования.
- Стратегии операторов в деле построения и развития инфраструктуры сетей 5G, эволюция сетей LTE к сетям 5G.
- Виртуализация ядра и сетевых функций (NFV), программно определяемые сети (SDN).
- Новые услуги в сетях 5G на платформе Mobile Edge Computing.

Организатор: TelecomDaily.

tmtconferences.ru/5g2018.html

выставки, семинары, конференции

Дата и место проведения, организатор, сайт	Наименование мероприятия
17.10. Сочи **Росконгресс** finopolis.ru	Форум инновационных финансовых технологий Finopolis 2018
18.10. Санкт-Петербург **ИКС-МЕДИА** spb.dcforum.ru	**Международная конференция и выставка «ЦОД-2018: модели, сервисы, инфраструктура»**
24–25.10. Казань **OCS Distribution** difpartners.ru	Digital Infrastructure Forum (DIF 2018)
30–31.10. Москва **Icons** icons.events/forumone	Forum One: цифровая революция
31.10. Москва **TargetSummit** targetsummit.ru/	Конференция Target Summit 2018
06–09.11. Москва **«Мессе Франкфурт РУС»** interlight-moscow.ru.messefrankfurt.com/moscow/ru.html	Международная выставка Interlight Moscow 2018
09.11. Москва **ИКС-МЕДИА** itmedforum.ru	**5-я ежегодная конференция IT & Med'2018**
15.11. Москва **TelecomDaily** tmtconferences.ru/5g2018.html	Международный бизнес-форум «Развитие сетей беспроводной связи в России – 5G Future Russia 2018»
21–23.11. Москва **«Гротек»** all-over-ip.ru/strategy-2018-f	Форум All-over-IP 2018
28.11. Екатеринбург **ИКС-МЕДИА** ekb.dcforum.ru	**Международная конференция и выставка «ЦОД-2018: модели, сервисы, инфраструктура»**

20--21 сентября в Санкт-Петербурге (Дворец А.А. Безбородко) состоится Пятый всероссийский форум в области информационных и коммуникационных технологий **«IT Диалог»**.

В 2018 г. основным мероприятием форума станет конференция-выставка «Цифровое равенство регионов» (сессия презентаций инновационных решений и проектов для создания цифровой городской / региональной среды).

На территории Музея связи им. А.С. Попова будут развернуты тематические стенды, на которых регионы-участники и партнеры форума представят свои решения – внедренные проекты, новые технологические решения и инновационные концепции для цифровой трансформации различных элементов городской и региональной среды. Российские и международные ИКТ-компании презентуют участникам форума лучший мировой и отечественный опыт в этих сферах. Главная задача форума в 2018 г. – эффективный обмен лучшими практиками между всеми регионами России и их активное распространение по всей стране.

Организатор: Минкомсвязь России.

itdialog.info

25 сентября в Москве (КВЦ «Сокольники») пройдет 5-я международная конференция «Интернет вещей».

Интернет вещей – самая громкая новинка года. В кругах специалистов постоянно разворачиваются дискуссии о том, как заставить его работать максимально эффективно. Уже в ближайшем будущем, по прогнозам экспертов, всеобъемлющий интернет будет производить огромное количество данных, открывая безграничные возможности для различных сфер деятельности.

Конференция «Интернет вещей» – главное событие в России, посвященное новейшим IoT-достижениям. Его участники обсудят реальные возможности IoT-технологий для бизнеса, промышленности и разработки инновационных продуктов и обозначат направления развития рынка на ближайшие годы. Гости IoT-форума протестируют новые продукты интернета вещей, наладят полезные бизнес-связи и узнают, как внедрить современные разработки в производство. Ежегодно конференция становится площадкой для нетворкинга топовых разработчиков, интеграторов, основателей стартапов, предпринимателей, операторов сетей, инвесторов и представителей власти.

На конференции «Интернет вещей» эксперты расскажут о разработке программного и аппаратного обеспечения IoT-технологий, о концепции «умного» города, а также об изменении деловых процессов благодаря smart-устройствам.

Помимо выступлений спикеров, на форуме пройдут две дискуссионные панели. Одна из них – «Эффективные городские технологии будущего» – посвящена внедрению разработок IoT в городскую инфраструктуру: транспорт, рынок жилья, ЖКХ, обеспечение безопасности. В процессе второй дискуссии – «Промышленный интернет вещей: Индустрия 4.0» – эксперты обсудят перспективы развития промышленности при внедрении и использовании smart-решений.

В рамках мероприятия будет работать выставочная зона, где отечественные и зарубежные игроки отрасли представят инновационные IoT-разработки. Посетители увидят в действии и протестируют инновационные модули, контроллеры, чипы, датчики, приложения и другие smart-продукты. В программе события предусмотрена 3-я международная «Битва стартапов» – презентация самых перспективных IoT-проектов. Их разработчики получат квалифицированные рекомендации от экспертов отрасли и возможность найти финансирование. В свою очередь, инвесторы ознакомятся с лучшими решениями рынка.

Организатор: Smile-Expo.

iotconf.ru/ru

Трансформируем всё!

Николай Носов

Цифровизация бизнеса, использование новых компьютерных технологий, перестройка бизнес-процессов необходимы для выживания компаний в стремительно меняющемся мире.

Принятие летом 2017 г. программы «Цифровая экономика Российской Федерации» показало, что необходимость изменений понимают и на самом высоком уровне. Программа обозначила направления развития и выделила «сквозные» технологии, в частности, анализ больших данных, блокчейн и искусственный интеллект.

Конкретные шаги по реализации программы только обсуждаются. Дискуссии идут в том числе на профессиональных мероприятиях, таких как 7-я международная конференция Cloud & Digital Transformation 2018, организованная «ИКС-Медиа».

Трансформация энергетики

Электроэнергетика – базовая отрасль страны. Авария на Саяно-Шушенской ГЭС выявила проблемы безопасности при эксплуатации энергетических установок и контроле их состояния. С экономикой тоже не все хорошо – себестоимость 1 кВтч в России без учета топливной составляющей и возврата инвестиций более чем в 5 раз превышает аналогичный показатель в европейских странах и США.

Министерство энергетики планирует провести трансформацию отрасли в пять этапов. На первом этапе, как сообщила Елена Медведева, заместитель директора департамента оперативного контроля и управления в электроэнергетике Минэнерго России, предполагается создать и внедрить единую отраслевую доверенную цифровую среду компаний с передачей технологических данных объектов электроэнергетики в режиме реального времени. Скорее всего, это будет решение на базе облачной платформы.

Второй этап – переход к использованию риск-ориентированного управления, внедряемого российскими регуляторами. Риск-ориентированная модель управления концентрирует ограниченные ресурсы на приоритетных рисках. Новые модели взаимодействия и управления будут способствовать уменьшению совокупной стоимости владения активами и снижению стоимости электроэнергии.

Третий этап – создание системы мониторинга и управления надежностью энергоснабжения. Оцифровка параметров надежности для каждого из уровней управления позволит определить уровень надежности в целом.

Следующие этапы цифровой трансформации – формирование отраслевых заказов для стимулирования российского машиностроения и микроэлектронной промышленности, снижение затрат на логистику, а также развитие клиентских сервисов для потребителей.

Первые шаги в цифровой трансформации электроэнергетики уже делаются. Пока на роль поставщика инфраструктуры для единой отраслевой доверенной цифровой среды претендует «Ростелеком», но, как пояснила Е. Медведева, окончательный выбор будет сделан на конкурсной основе, так что и у конкурентов шансы есть.

Цифровая трансформация в металлургии

Новолипецкий металлургический комбинат (НЛМК) – один из лидеров цифровой трансформации российской промышленности. Крупнейший металлургический комбинат страны уже несколько лет для повышения эффективности производства активно внедряет современные компьютерные технологии, в том числе Big Data, машинное обучение и искусственный интеллект (Artificial Intellect, AI). Для решения производственных задач приходится собирать данные и моделировать процессы в режиме реального времени.

Жизненный цикл данных о производстве стали состоит из шести стадий, начиная со сбора и первичной обработки и заканчивая обеспечением работы промышленных приложений (рис. 1).

Рис. 1. Жизненный цикл данных металлургического производства

Источник: НЛМК

Использование более точной модели, обученной на данных истории плавок и способной быстро анализировать множество вариантов решения, по словам директора по анализу данных и математическому моделированию НЛМК Анджея Аршавского, позволяет на 5% снизить расход дорогих ферросплавов, уменьшить количество потребляемой электроэнергии и экономить 150 млн руб. в год.

Трансформация нефтегазовой отрасли

Возможность значительной экономии, наличие большого количества данных и сложность моделей – основные предпосылки для успешного использования систем AI в промышленности, выделенные генеральным директором компании Mechanica AI Александром Хайтиным. Такие предпосылки существуют и в нефтегазовой отрасли, где количество собираемых данных огромно. Например, большие геоданные (Big Geo

Data) о добыче, логистике, транспорте, переработке и разведке новых месторождений. Много данных собирается во время эксплуатации скважин и в процессе бурения.

Первая «умная» скважина была запущена в России в 2006 г. В 2009 г. в Уренгое уже вступило в строй «умное» месторождение, в 2015-м в Ханты-Мансийске – первое безлюдное месторождение (рис. 2).

Применение буровых роботов трансформирует буровую установку в роботизированный буровой комплекс, а для диагностики газопроводов, в том числе бесконтактной диагностики методом магнитной томографии, могут служить мультикоптеры. Именно так, по словам заместителя директора по инновационной работе Института проблем нефти и газа РАН Николая Ерёмина, диагностировался водный переход газопровода компании «АЛРОСА – Газ» через реку Большая Батуобия в Якутии.

Блокчейн для логистики

Дроны можно использовать не только для контроля трубопроводов. Уже обсуждается возможность доставки с их помощью товаров и продуктов жителям Заполярья. Предпринимались попытки применения беспилотных летательных аппаратов для перевозки грузов в других районах страны.

Для решения задач логистики дроны могут работать в сочетании с технологиями распределенного реестра. Компания QIWI создала на основе технологии смарт-контрактов операционную платформу для беспилотной грузовой логистики SKYFchain. Как сообщил директор по развитию криптотехнологий QIWI Алексей Архипов, платформа объединяет информацию о событиях, происходящих с грузовыми роботами на протяжении жизненного цикла, – от момента выпуска, периодического технического обслуживания до деталей и маршрутов полетных заданий. В платформе используется гибридный блокчейн, включающий приватные распределенные реестры SKYFchain и публичный блокчейн на базе сети Ethereum. В публичной части не будут храниться данные, составляющие коммерческую тайну, а только подтверждения их достоверности в виде хешей. Узел сети SKYFchain будет содержать программное обеспечение узла приватного блокчейна и интеграционный слой для связи с каналом и сетью Ethereum.

Гибридная схема объединяет преимущества публичного блокчейна, повышающего уровень доверия к данным, и приватного, обеспечивающего конфиденциальность информации и контроль участников системы.

«Нефть» новой экономики

Данные – «нефть» новой экономики. Программные интерфейсы приложений (API) – точки доступа к этой «нефти» других организаций. «Способы взаимодействия с клиентами сдвигаются в сторону API», – считает специалист по техническим продажам компании IBM в Европе Иван Пряничников.

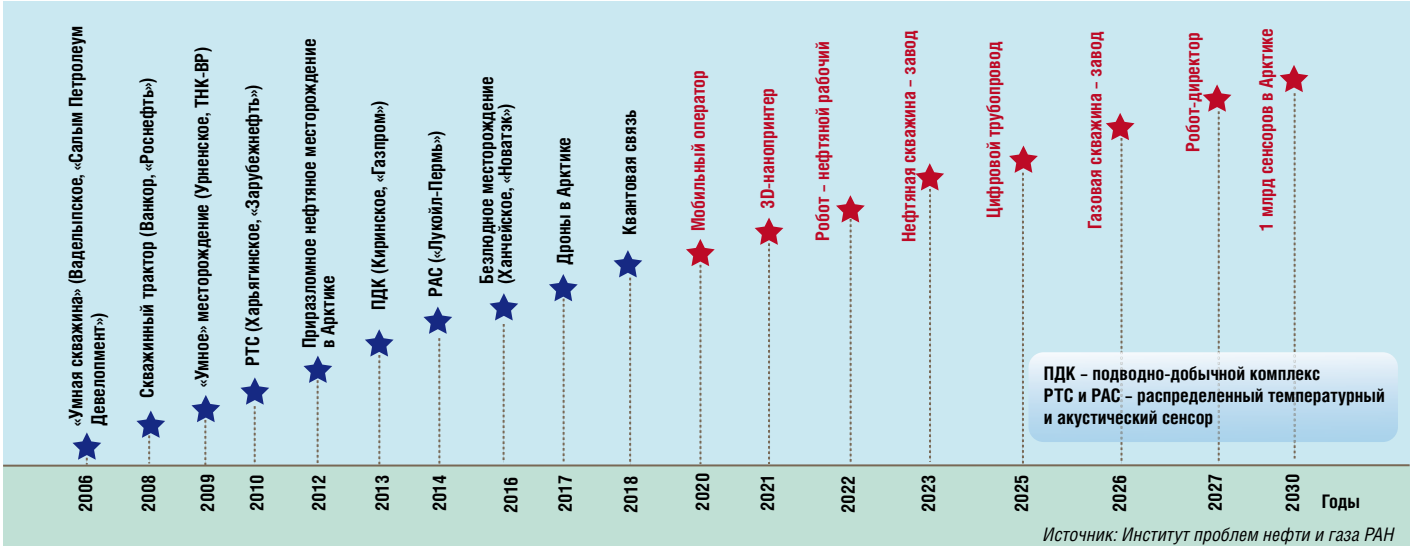
Внутренние API повышают гибкость процессов в компании. Партнерские API доступны не только сотрудникам, но и ограниченному кругу партнеров компании, что помогает унифицировать взаимодействие. Публичные API, открытые широкому кругу разработчиков, обеспечивают создание экосистемы, расширяют рынок и способствуют дополнительной монетизации.

Работа с API включает не только разработку и внедрение программных интерфейсов приложений, но и обеспечение безопасности, создание моделей монетизации, сервисов и приложений.

Организация каналов связи

Трансформация бизнеса предъявляет новые требования к гибкости архитектуры сети пред-

Рис. 2. Цифровая модернизация нефтегазовой отрасли



Источник: Институт проблем нефти и газа РАН

приятия и возможностям ее оперативного изменения при появлении новых территориально распределенных узлов.

Старый подход, при котором сетевые администраторы вручную перенастраивали топологию сети и управляли каналами, становится неэффективным, особенно в условиях использования гибридных облаков, когда часть инфраструктуры переносится в облака и надо оперативно перенастраивать каналы для связи с расположенными в них приложениями.

Миграция приложений в облако без правильной организации каналов в глобальной сети (WAN) опасна. Это может не только привести к неэффективному использованию пропускной способности сети и снижению скорости работы приложения, но и сделать приложение неработоспособным, считает Дэнни Тан, старший менеджер департамента Cloud & Security services компании CITIC Telecom CPC Limited.

Гибкость может обеспечить технология программно определяемых каналов связи SD-WAN. Китайская компания предлагает свой вариант реализации – размещение в подразделениях организации программно определяемых граничных устройств подключения к глобальной сети (рис. 3).

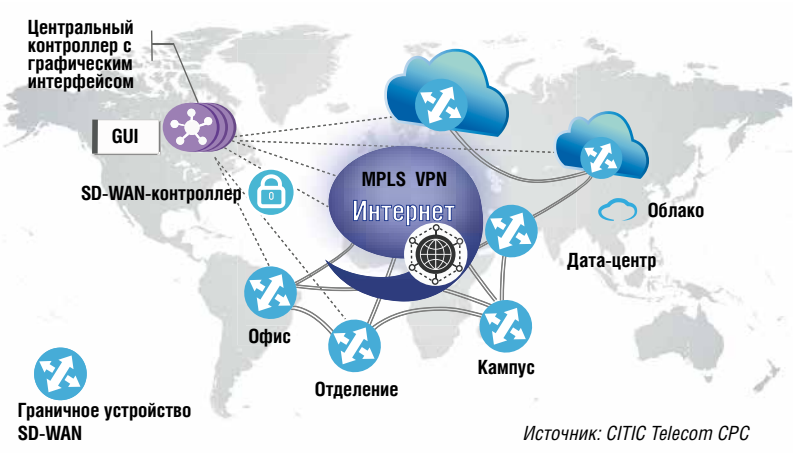
Такое Edge-устройство может быть направлено в подключаемый офис даже по почте. Запуск не требует квалифицированного персонала – достаточно подсоединить устройство к интернету. Конфигурация и сетевая политика будут автоматически загружаться с контроллера SD-WAN, что значительно ускорит развертывание сети. В результате организация оперативно получит зашифрованные VPN-соединения для передачи данных, не зависящие от используемых каналов связи.

Основываясь на важности процессов, типе приложения или определенных правилах трафика, Edge-устройство SD-WAN выбирает наилучший вариант доступа к облачным системам. Например, бизнес-трафик, такой как VoIP, будет, вероятно, маршрутизироваться через сеть MPLS, а связь с критически важными приложениями – через IPSec VPN.

Edge-устройство SD-WAN будет непрерывно контролировать состояние и производительность каналов глобальной сети. Если одно из соединений WAN недоступно, контроллер SD-WAN автоматически перенаправит трафик на другой канал.

Платформы трансформации

Процессы цифровой трансформации ставят проблемы контроля работы систем при использовании облачных приложений, масштабирования сервисов в условиях роста числа пользователей, поддержки производительности и гибкости систем в гибридных инфраструктурах.



Источник: CITIC Telecom CPC

▲ **Рис. 3. Схема работы сети SD-WAN**

Для цифровой трансформации требуются быстрая сеть, облачная платформа и облачные ресурсы, считает менеджер по продукту Virtual Data Center компании Interoute Александр Грендель. Он привел пример успешной цифровой трансформации крупного международного предприятия, управляющего 6 тыс. парковок в 12 странах: новая архитектура сети была построена на базе корпоративной цифровой платформы Interoute, включающей виртуальные ЦОДы, облачную фабрику (Cloud Fabric) и Edge-устройства SD-WAN и NVF. Заказчик отдал на аутсорсинг компании управление своей критически важной инфраструктурой. Interoute обеспечивает работу операционных систем (Windows server, Linux), СУБД (Microsoft SQL Server, MySQL, PostgreSQL, MongoDB, Oracle Database), виртуальных устройств (межсетевых экранов, балансировщиков нагрузки, автоматизированных облачных хранилищ) и приложений (Apache Tomcat, Apache HTTP, Microsoft IIS, Microsoft Active Directory, Microsoft Exchange), организует взаимодействие различных облачных платформ в рамках единой экосистемы и защищает трафик.

В итоге управляющая парковками компания перешла от использования своего централизованного ЦОДа, к которому были подключены все страны, на решение с несколькими виртуальными ЦОДами Interoute. При этом для связи с критическими для бизнеса приложениями задействуется глобальная сеть MPLS и сеть SD-WAN (Interoute Edge Access), а менее важные приложения в целях экономии подключаются через обычный интернет.

■ ■ ■

Облачные платформы дают возможность специалистам применять самые современные средства анализа данных и разработки приложений. Компании могут тестировать новые технологии и выбирать оптимальные пути цифровой трансформации предприятий без капитальных затрат на развертывание у себя дорогостоящих систем. ИКС

Цифровизация медицины споткнулась об регулирование

Александра Крылова

Федеральный закон № 242-ФЗ был принят год назад, однако участники формирующегося рынка цифрового здравоохранения до сих пор сталкиваются с регуляторными барьерами, перекрывающими пути к развитию.

Напомним, что вступивший в силу с 1 января 2018 г. закон ФЗ-242, содержащий поправки к Федеральному закону от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан», регулирует несколько направлений. Это телемедицина, электронный документооборот в медицинской организации и электронные рецепты, а также Единая государственная информационная система в сфере здравоохранения (ЕГИСЗ). Каждое из этих направлений значится сегодня в повестке цифровой трансформации медицинской помощи населению. И по большому счету цифровизация сферы охраны здоровья без достижения прогресса во всех четырех областях невозможна.

Принятие ФЗ-242 и отдельных подзаконных актов к нему (см. «Нормативные правовые документы в области цифрового здравоохранения») – несомненный прогресс в области формирования «цифровой» нормативной базы отрасли.

Однако и эксперты в области информатизации здравоохранения, и специалисты в сфере медицинского права считают, что для регулирования процессов цифровой трансформации медицины нормативных документов все еще недостаточно, и отмечают наличие в них большого количества «серых зон».

Кого консультировать дистанционно?

Ключевой вопрос, с которым столкнулись и медицинские организации, и компании – агрегаторы услуг дистанционных консультаций в сегменте «врач – пациент»: откуда и как врач может применять телемедицинские технологии. Предметом дискуссии участников рынка с регулятором являются лицензионные требования, которые предъявляются к медицинской организации, планирующей оказывать медпомощь пациентам с применением телемедицинских технологий. Согласно новым нормативным документам, для дистанционных консультаций нужно выделить отдельный кабинет, разместить в нем автоматизированное рабочее место врача, чтобы потом в его стенах он мог проводить телемедицинские сеансы с пациентами. И, как пояснил регулятор в своем письме № 18-2/0579, по-другому – из офис-

Нормативные правовые документы в области цифрового здравоохранения

- Федеральный закон от 29.07.2017 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья»
- Приказ Минздрава России от 30.11.2017 №965н «Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий»
- Постановление Правительства РФ от 12.04.2018 № 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями»
- Приказ Минздрава России от 09.01.2018 № 2н «О внесении изменений в приказ Министерства здравоохранения России от 15.12.2014 № 834н “Об утверждении унифицированных форм медицинской документации, используемых в медицинских организациях, оказывающих медицинскую помощь в амбулаторных условиях, и порядков по их заполнению”»
- Письмо Минздрава России от 09.04.2018 № 18-2/0579 «О порядке организации и оказания медицинской помощи с применением телемедицинских технологий»
- Постановление Правительства РФ от 05.05.2018 № 555 «О единой государственной информационной системе в сфере здравоохранения».

ного центра, из колл-центра, из дома врача – консультировать пациентов с применением телемедицинских технологий нельзя. А использовать в ходе дистанционного оказания медицинской помощи мобильные устройства разрешается только выездным бригадам скорой помощи.

Не менее серьезным барьером для формирующегося рынка таких услуг является требование идентификации врача и пациента, участвующих в телемедицинском сеансе, через Единую систему идентификации и аутентификации (ЕСИА). «На сегодняшний день не созданы технические условия для того, чтобы компании – организаторы таких консультаций могли использовать эту систему», – констатирует Борис Зингерман, руководитель направления цифровой медицины «Инвитро» и эксперт АРМИТ по правовым вопросам.

Так, учетную запись на портале госуслуг предусмотренной ФЗ-242 и приказом Минздрава № 965н степени подтвержденности в настоящее время имеют только 25% россиян. К тому же надо понимать, что некоторые граждане принципиально не регистрируются на портале госуслуг, скажем, по религиозным соображениям. Также нет в новых нормативных документах отрасли указаний на способ идентификации потенциальных пациентов, которые в принципе не могут иметь учетной записи в ЕСИА, – детей до 14 лет, иностранных граждан и лиц без гражданства.

«Таким образом от телемедицинских технологий отсекается значительная прослойка пациентов, не зарегистрированных в ЕСИА», – подчеркивает Полина Габай, генеральный директор компании «Факультет медицинского права», юрисконсульт по медицинскому праву. По ее мнению, трудности с использованием Единой системы идентификации и аутентификации неизбежно будут возникать и у врачей, ведь, согласно постановлению Правительства РФ от 28.11.2011 № 977, доступ к ЕСИА могут получать только должностные лица организаций, коими врачи в лечебных учреждениях не являются. В медицинских организациях уровень должностных лиц начинается с заведующих отделениями. Для преодоления этого барьера, препятствующего развитию телемедицины в нашей стране, эксперт предлагает включить в нормативные акты альтернативные способы идентификации участников дистанционной консультации в формате «врач – пациент», такие как, к примеру, отсканированный паспорт.

Отдельным нормативным документом – Постановлением Правительства РФ от 12.04.2018 № 447 – утверждены правила взаимодействия «иных информационных систем» с информационными системами в сфере здравоохранения и с медицинскими организациями. Под операторами «иных ИС» подразумеваются коммерческие организации, в частности, провайдеры разнообразных облачных сервисов. Правила разрабатывались для того, чтобы регламентировать их подключение к ЕСИА. Однако, и это признают все эксперты, руководствоваться этими правилами сегодня невозможно, поскольку в качестве первого условия такого подключения требуется зарегистрировать сервис в качестве «иной информационной системы» в ЕГИСЗ, а для этого нужно подать документы по форме, которую Минздрав еще не разработал. Так же, по словам Б. Зингермана, не отработано пока и взаимодействие регулятора с Минкомсвязью России, в обязанности которой как оператора ЕСИА входит предоставление доступа к этой системе коммерческим организациям.

Кто заплатит за УКЭП для врача?

Важная роль в обеспечении оказания медицинской помощи с помощью телемедицинских технологий в новых нормативных документах отводится информационным системам, позволяющим хранить и обрабатывать медицинскую информацию в форме электронных документов. О том, что регулятор это понимает, свидетельствует факт появления приказа Минздрава России № 2н, вносящего изменения в приказ этого же ведомства № 834н «Об утверждении унифицированных форм медицинской документации...».

Однако уже из названия этого приказа, отмечает Б. Зингерман, видно, что он не охватывает все виды медицинской документации. А в тексте говорится, что, к примеру, карта или справка «формируется в виде электронного документа, подписанного усиленной квалифицированной электронной подписью в соответствии с поряд-

ком организации системы документооборота в сфере охраны здоровья в части ведения медицинской документации в форме электронных документов». Разработка такого порядка даже не значится в планах ведомства, и его отсутствие можно считать барьером на пути систем электронного документооборота в медицинские организации.

В свою очередь, специалист в области медицинского права П. Габай видит проблему в том, что регулятор связывает телемедицинские консультации исключительно с электронной документацией и не предполагает пользование традиционной бумажной медицинской документацией. «Данной нормой отсеивается множество медицинских организаций, работающих с бумажными, а не электронными медицинскими картами», – аргументирует она свою позицию.

Как барьер можно рассматривать и требование использовать для документирования результатов телемедицинских консультаций и вообще для подписания любых электронных медицинских документов усиленную квалифицированную электронную подпись. Во-первых, УКЭП сегодня есть далеко не у каждого врача, во-вторых, ее стоимость, будучи умножена на количество врачей в организации, выливается в круглую сумму. В-третьих, пока не до конца понятно, кто – сам врач или медицинская организация, в которой он работает, – должен эти подписи приобретать. В-четвертых, если медорганизация берет закупку УКЭП на себя, то ей трудно точно оценить необходимое количество усиленных квалифицированных цифровых подписей.

Может статься, считает Б. Зингерман, что врачу понадобится целых три УКЭП: одна для документирования результатов телемедицинских консультаций, вторая – для подписания электронных медицинских документов, а третья – для выписки электронных рецептов. При этом, напоминает П. Габай, чтобы не пришлось доказывать действительность ЭЦП в судебном порядке, надо учитывать, что квалифицированный сертификат проверки ключа электронной подписи имеет определенный срок действия.

Что касается регулирования выписки электронных рецептов, то и тут, по мнению экспертного сообщества, необходим основополагающий документ – порядок обращения электронных рецептов. И хотя о его разработке в Минздраве пока ничего неизвестно, уже понятно, что получить рецепт в электронной форме даже по итогам телемедицинской консультации пациенту будет непросто.

Пазл из 13 подсистем

Изменение концепции ЕГИСЗ, с которой с 1 января 2018 г. должны взаимодействовать все государственные медицинские организации, а с 1 января 2019 г. и все частные клиники, зафиксировано в Постановлении Правительства РФ от 05.05.2018 № 555.

Из единой государственной информационной системы, охватывающей все уровни информатизации медицины – от федерального до уровня медицинской организации, она превратилась исключительно в федеральную ГИС, состоящую из 13 различных подсистем. В их числе, к примеру, Федеральный регистр медицинских работников и Федеральный реестр медицинских организаций.

В первую подсистему собирается информация обо всех лицах, участвующих в осуществлении медицинской деятельности, она же обеспечивает размещение связанных с профессией данных в интернете. В задачи второй подсистемы входит учет сведений обо всех медорганизациях – государственных, муниципальных и частных. Согласно постановлению, им придется передавать в Федеральный реестр информацию об оборудовании, помещениях, сотрудниках, их зарплатах и т.д., которая тоже будет размещена в интернете и доступна всем желающим. (Исключение сделано для сведений, составляющих коммерческую тайну, и показателей финансово-хозяйственной деятельности).

Однако механизмы реализации этих норм – кем, где и как будет размещаться информация из Федерального регистра и Федерального реестра – в постановлении не прописаны. И подобных «белых пятен» в регулировании взаимодействия медицинских организаций с ЕГИСЗ остается немало. В качестве еще одного примера можно привести требование получать согласие на размещение персональных данных в ЕГИСЗ у того, кому эти данные принадлежат, что тоже вызывает у экспертов вопросы.

Ответ на них частично содержится в п. 31 постановления № 555, который гласит: «Формирование подсистем единой системы... осуществляется в соответствии с требованиями, установленными Министерством здравоохранения Российской Федерации». По словам Б. Зингермана, для этого регулятору еще предстоит разработать и утвердить положения о каждой из этих 13 подсистем.

■ ■ ■

Для того чтобы преодолеть недостаточность регулирования в сфере цифрового здравоохранения, хотя бы телемедицины, электронного документооборота или ЕГИСЗ, и выработать всеобъемлющие правила игры на этом поле для всех участников рынка, Минздраву России совместно с экспертным сообществом предстоит еще скорректировать часть готовых нормативных правовых документов и принять множество новых. ИКС

5-я ежегодная конференция IT&Med`2018

ИТ-помощь медицине

Для профессионалов в области ИТ и здравоохранения

9 ноября 2018 г., Москва

К участию приглашаются:
информатизаторы здравоохранения, представители регулятора, врачи, руководители ИТ-направлений медучреждений, ИТ-компании.

В фокусе мероприятия:

- ЕГИСЗ, ГИСы субъектов РФ и МИС МО: изменение архитектурного контура
- ИТ-сервисы для электронного здравоохранения
- Грани телемедицины: организационная, экономическая, правовая. Безопасность персональных медицинских данных
- Оснащение телемедицинских кабинетов: ВКС, веб-трансляции, средства документирования дистанционных консультаций, хранилища данных
- Электронный документооборот в медорганизации. Какие задачи решает, кому и чем может быть полезен? Препоны и успешные кейсы
- Персональная медицина и m-Health. Технологии интернета вещей для профилактики заболеваний и реабилитации
- Системы поддержки врачебных решений: кому и чем поможет искусственный интеллект?
- Вакантная позиция для вашей инициативы!

Предложения по экспертным докладам ждем по адресу:
ak@iksmedia.ru

Для представителей медучреждений и госструктур участие бесплатное

ИКС МЕДИА

www.itmedforum.ru

По вопросам участия обращайтесь по тел.: +7 (495) 150-64-24
и e-mail: expo@iksmedia.ru

Спонсор: CABERO HEAT EXCHANGER

Партнер выставки: Медицинская Информационная Система ЭЛЕМЕНТ

Миграция ЦОДа Правовые аспекты

Сергей Смолин, заместитель руководителя юридического департамента, DataSpace

Перенос ЦОДа на новую площадку – сложный процесс, чреватый разнообразными рисками для владельца ИТ-оборудования. В чем эти риски заключаются и как их избежать?

Необходимость переместить функционирующее ИТ-оборудование в новую локацию может возникнуть по многим причинам – из-за нехватки места на прежней площадке, некачественной системы охлаждения или энергообеспечения, недостаточной отказоустойчивости, частых отклонений уровня услуг от заявленного и т.п. Во всех случаях приходится организовывать миграцию ЦОДа. Любые просчеты и ошибки в этом процессе могут значительно увеличить расходы, а просрочка запуска дата-центра на новом месте – нанести владельцу ИТ-оборудования репутационный ущерб.

Помимо технических и логистических аспектов переезда, большое значение имеет его юридическая сторона, поскольку с миграцией ЦОДа неразрывно связаны риски причинения ущерба владельцу ИТ-оборудования: некорректное подключение систем, срыв сроков запуска ЦОДа на новой площадке, потеря или повреждение критически важного оборудования или конфиденциальной информации и т.д. Минимизация этих рисков напрямую зависит от четкого разграничения зон ответственности всех сторон, вовлеченных в процесс переезда ЦОДа.

Выбор новой площадки

Новая площадка для ЦОДа должна соответствовать определенным правовым критериям: не являться предметом спора о праве собственности и обеспечивать возможность беспрепятственного доступа к ИТ-оборудованию его владельцу. Поскольку новое помещение предоставляется в пользование владельцу ИТ-оборудования на длительный срок, оно должно находиться у арендодателя в собственности или долгосрочной аренде. Грамотная юридическая и техническая экспертиза новой площадки отсеивает недобросовестных арендодателей офисных помещений и некачественные ЦОДы, поэтому к этой работе целесообразно привлекать экспертов, специализирующихся на due diligence недвижимости, в том числе недвижимости, используемой для размещения ЦОДов.

Нужно обратить внимание на оформление договорных отношений с владельцем нового офиса или оператором дата-центра – в договоре должна быть зафиксирована возможность беспрепятственной и оперативной разгрузки ИТ-оборудования на новой площадке. Еще на этапе согласования необходимо исключить или минимизировать любые препятствия, затягивающие миграцию ЦОДа, – это могут быть чрезмерная формализация процесса въезда и выезда или ограниченное время на погрузку и разгрузку.

Крайне нежелательно откладывать процедуру согласования договоров с провайдерами услуг, сопутствующих функционированию ИТ-систем, например, с оператором связи. К моменту запуска ИТ-оборудования на новой площадке его владелец должен иметь полностью согласованные и подписанные договоры с провайдерами всех требуемых услуг. В противном случае может оказаться невозможным запустить ИТ-системы в запланированный срок. Более того, в договоре с владельцем площадки должна быть зафиксирована его обязанность допустить подключение именно того провайдера, который необходим владельцу ИТ-оборудования.

Аудит ИТ-оборудования

Перед началом миграции ЦОДа необходимо осуществить аудит и инвентаризацию всего ИТ-оборудования на предмет выявления устаревших систем, некорректных соединений и т.д. Игнорирование этого процесса может привести к значительному увеличению длительности миграции из-за некорректного подключения ИТ-систем на новой площадке, а также к дополнительным расходам, вызванным срочной заменой устаревшего ИТ-оборудования. Определенный риск несет в себе проведение такого аудита силами владельца ИТ-оборудования – не всегда компетенции сотрудников

компании достаточно для организации перемещения ЦОДа в новую локацию.

В данной ситуации целесообразно обратиться за помощью к организациям, специализирующимся на миграции ЦОДов. Помимо профессионального подхода к анализу всех систем, такие компании способны дать рекомендации по планированию поэтапного переноса ИТ-систем на новую площадку и проконсультировать по вопросу замены устаревшего оборудования, что значительно упростит переезд. Немаловажно и то, что ответственность за успешность процесса миграции ЦОДа в таком случае перейдет от владельца ИТ-оборудования к аудитору.

Транспортировка ИТ-оборудования

Физическое перемещение оборудования связано со многими рисками: некачественная погрузка, разгрузка и хранение ИТ-оборудования, потеря или повреждение информации, просрочка доставки и т.д. Как правило, владелец ИТ-оборудования обращается за помощью к логистическим компаниям, специализирующимся на перевозке ценных и хрупких вещей. Основной риск при этом заключается в том, что владение оборудованием на определенное время переходит к третьему лицу – перевозчику, который может повредить его при погрузке или разгрузке, что, в свою очередь, может привести к повреждению или уничтожению информации, хранящей на данном оборудовании. Кроме того, есть ИТ-оборудование, к эксплуатации (включая перевозку), которого предъявляются жесткие требования, и их нарушение может стать основанием для отказа производителя от его гарантийного обслуживания.

Помимо очевидных технических мер (резервное копирование данных и т.д.), для предотвращения подобных инцидентов необходимо предусмотреть юридическую защиту владельца ИТ-оборудования. В первую очередь – это грамотная фиксация зоны ответственности перевозчика. Каждый этап перевозки должен сопровождаться соответствующим актом приема-передачи, в котором стороны фиксируют состояние оборудования путем визуального осмотра. Данный документ предоставляет владельцу ИТ-оборудования возможность в дальнейшем требовать от перевозчика компенсацию за ущерб, причиненный его имуществу. Договор с перевозчиком должен содержать также жесткие условия в отношении сроков перевозки, что станет для него дополнительным стимулом осуществить доставку вовремя.

При перевозке дорогостоящего оборудования целесообразно требовать от перевозчика страхования перевозимого имущества и своей ответственности – такой подход гарантирует владельцу ИТ-оборудования возможность получения компенсации за поврежденное оборудование и более оперативное урегулирование споров.

Иногда прерывание функционирования ИТ-оборудования недопустимо. В таких случаях прибегают к услугам дублирования ЦОДа с передачей данных по каналам связи. Данный сервис позволяет осуществить миграцию ЦОДа без остановки работы ИТ-оборудования, однако с ним сопряжены риски потери или хищения данных. Для того чтобы избежать таких неблагоприятных сценариев, рекомендуется пользоваться услугами компаний, предоставляющих защищенные каналы связи и услуги гарантированного качества.

> Минимизация рисков при миграции ЦОДа напрямую зависит от четкого разграничения зон ответственности всех сторон, вовлеченных в процесс переезда

Еще один риск в процессе перемещения ЦОДа – некорректный план миграции. Неправильная синхронизация процессов может привести к остановке работ по подключению нового ЦОДа, когда перевозка ИТ-оборудования задерживается, или вызвать дополнительные расходы на хранение оборудования, если его перевезли слишком рано. Эффективный план миграции, как правило, подразумевает согласование ее этапов с техническими, юридическими и финансовыми специалистами.

■ ■ ■

Переносить ЦОД на новую площадку большинству компаний приходится нечасто, поэтому трудно рассчитывать, что владелец ИТ-оборудования сможет осуществить этот процесс силами своих сотрудников. Критические риски здесь заключаются в повреждении или потере ИТ-оборудования, в срыве сроков его запуска на новой площадке или в его некорректной работе. В этой ситуации целесообразно обратиться за помощью к компаниям, компетентным в вопросах миграции ЦОДов, включая правовые аспекты. Взаимодействие с такими компаниями обеспечит владельцу ИТ-оборудования правильное разграничение зон ответственности участников перемещения ЦОДа и правовую гарантию защиты его интересов. Сопровождение миграции ЦОДа может быть разного уровня – от консультирования по ключевым вопросам до переезда «под ключ». ИКС

Гиперконвергентная инфраструктура как сервис

Николай Носов

Интегрированные решения выходят на уровень платформ и начинают предлагаться по сервисной модели.

Гиперконвергенция – объединение ИТ-ресурсов в целостное решение с помощью типовых аппаратных блоков и программно определяемых устройств – стала одним из самых модных трендов в ИТ. Попробуем разобраться в преимуществах гиперконвергентных систем, направлениях дальнейшего развития решений и сценариях их использования в бизнесе.

Этапы развития вычислительных инфраструктур

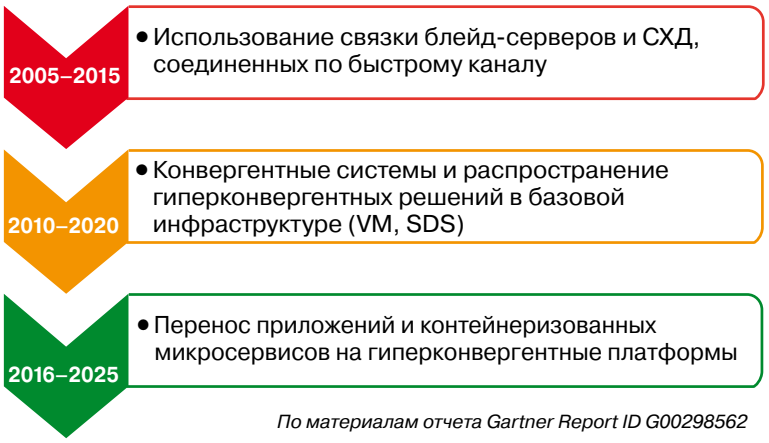
Виртуализация машин, которая применялась еще в советское время, позволила оптимизировать использование вычислительных ресурсов компьютера, отделить выполнение кода от конкретного аппаратного обеспечения. Она создала предпосылки возникновения масштабируемых виртуальных вычислительных мощностей на блейд-серверах, которые содержат добавляемые по необходимости «лезвия» – материнские платы с процессорами, устанавливаемые в блейд-корзины.

В начале 90-х появилась возможность наращивать объем дискового пространства путем добавления дисков в выделенное хранилище данных – СХД. Для работы с ними использовалась разработанная в 1987 г. технология виртуализации данных RAID, объединяющая диски в логические элементы, с которыми и работали операционные системы.

Архитектура, включающая кластер компьютеров или блейд-серверов и связанных с ними скоростным каналом (fibre channel) СХД, де-факто стала стандартом в 2005 г. и по сей день используется многими компаниями.

Цифровая трансформация ставит перед разработчиками компьютерных систем все новые задачи. Сложность решений постоянно растет, вычислительные системы нужно запускать быстро, обеспечивая необходимую гибкость при дальнейших изменениях конфигурации. В ответ на запросы рынка появились облачные технологии, предоставляющие вычислительные мощности как сервис по требованию, и конвергентные решения – заранее интегрированные вычислительные модули, включающие вычислительные мощности, системы хранения, сетевое оборудование, средства виртуализации и оркестрации.

Раньше компания покупала компьютеры и СХД, соединяла их и разворачивала платформу виртуализации. Это требовало много времени и участия квалифицированных специалистов. С появлением конвергентных систем (в терминологии Gartner – интегрированных инфраструктур) стало достаточно купить заранее интегрированный модуль (стойку), готовый для установки прикладных программ.



По материалам отчета Gartner Report ID G00298562

Эволюция архитектуры ИТ-инфраструктур

Следующий шаг – развертывание платформы виртуализации на интегрированных блоках или серверах с объединением в единое целое их внутренних дисков/дисковых полок на программном уровне. Таким образом формируется виртуальное отказоустойчивое хранилище. С точки зрения наращивания вычислительных мощностей получающиеся гиперконвергентные инфраструктуры (Hyper-Converged Infrastructure, HCI) уже не ограничены возможностями одного интегрированного модуля устройства или сервера – платформа объединяет их ресурсы в единое целое, из которого можно нарезать нужные для конкретной задачи вычислительные мощности.

Весь «интеллект» HCI для обеспечения отказоустойчивости и производительности опирается на программно определяемые технологии (виртуальные машины, программно определяемые хранилища).

Такой подход сильно упрощает управление сложной системой, которое теперь осуществляется через общую консоль администрирования, обеспечивает большую гибкость и масштабируемость, а также выполнение заранее заданных требований к отказоустойчивости и производительности. При этом можно обойтись без дорогостоящих СХД, отказаться от сетей fibre channel и

Преимущества гиперконвергентных решений по сравнению с традиционными

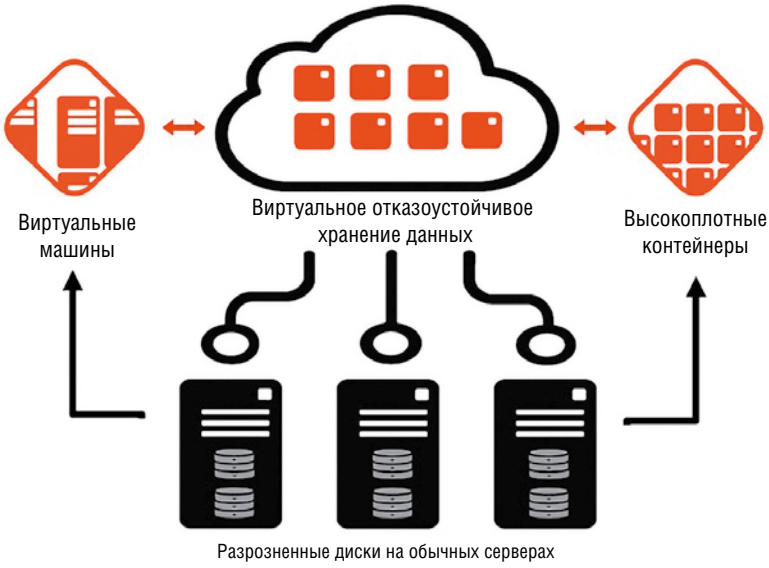
внешних сетей хранения данных – гиперконвергентные системы, как правило, состоят из коммодити-решений, построенных на стандартной для отрасли архитектуре x86, что значительно повышает экономическую эффективность их использования.

Что предлагает российским компаниям рынок?

Аналитики предсказывают гиперконвергентным системам большое будущее. Согласно прогнозу MarketsandMarkets, к 2022 г. рынок гиперконвергентных инфраструктур достигнет $12 607,4 млн при среднегодовом темпе роста 43,59%.

За новый рынок идет борьба между крупнейшими вендорами. Если в 2016 г. в магическом квадранте Gartner в разделе лидеров было семь компаний, то в 2017-м их число сократилось до четырех. Стали сильнее после объединения компании Dell и EMC, упрочила свои позиции

Пример реализации гиперконвергентной системы



Источник: «Росплатформа»

Nutanix, сохранила лидирующее положение компания HPE, купившая SimpliVity, и впервые к лидерам примкнула VMware.

В российском медийном поле компания Nutanix выглядит скромно, лишь изредка участвуя в конференциях, хотя доля на нашем рынке у нее есть. Самый известный российский проект компании – федеральная система «Платон». Очень активна VMware, недавно предложившая весь спектр услуг, включая гибридные решения, в российском облаке Selectel VMware Cloud. Динамично продвигает решения в области гиперконвергенции компания Dell EMC.

Все больше российских пользователей задумываются о санкционных рисках. Из компаний, попавших в магический квадрант Gartner, минимальные риски имеет Huawei. Китайцы хорошо понимают ситуацию, энергично выходят на наш рынок, предлагая локализованные на российской облачной платформе решения.

Другой вариант защиты от санкций – использование продуктов open source. В области гиперконвергенции стоит выделить связку OpenStack и Ceph. Система хранения Ceph бесшовно интегрируется с компонентами OpenStack: Cinder (блочное хранилище), Glance (образы), Nova (управление пулами вычислительных ресурсов) и Keystone (управление идентификацией). Связку предлагает в качестве промышленного решения для гиперконвергентных систем компания Red Hat, формулируя при этом жесткие требования к используемой аппаратной части.

Среди российских поставщиков решений для гиперконвергентной инфраструктуры наиболее деятельна компания «Росплатформа», решения которой включены в реестр российского программного обеспечения. В их число входят система серверной виртуализации «Р-Виртуализация» и программно определяемое хранилище «Р-Хранилище» (на основе исходных кодов и технологий Virtuozzo от Parallels Group). Первым российским программно-аппаратным гиперконвергентным решением на базе продуктов «Росплатформы» стала платформа «Скала-Р» компании IBS. Другие российские системные интеграторы и производители серверов тоже разрабатывают свои программно-аппаратные комплексы на базе ПО «Росплатформы», делая возможным разворачивание собственного гиперконвергентного частного облака или отдельного серверного сегмента «из коробки».

«В плане совместимости с “железом” у нас правило такое: если на сервер устанавливается Linux, а в серверном сегменте таких моделей подавляющее большинство, то на этом сервере заработает и наше ПО. Секрет прост – мы опираемся на экосистему Linux-драйверов для взаимодействия с “железом”», – поясняет управляющий директор компании «Росплатформа» Владимир Рубанов. При этом система поддерживает любые гостевые операционные системы, выполняемые внутри системы виртуализации.

Сценарии применения

HCI не является решением на все случаи жизни. Масштабирование может получиться несбалансированным: например, клиенту нужно только нарастить вычислительную мощность, а приходится докупать весь блок. Кроме того, есть проблемы с развертыванием некоторых приложений в виртуальных средах.

«Два основных сценария использования гиперконвергентных систем – удаленные офисы и

виртуализированные рабочие места», – считает Илья Воронин, директор центра проектирования вычислительных комплексов компании «Инфосистемы Джет». При гомогенной нагрузке, как в случае VDI, проявляется основное преимущество гиперконвергентной системы – легкая масштабируемость. Допустим, сегодня требуется 1 тыс. рабочих мест – покупаем десять узлов HCI. Завтра нужно 1,5 тыс. – покупаем еще пять. Таким образом сильно упрощается развертывание вычислительной инфраструктуры удаленного офиса или филиала. При этом не надо искать местных специалистов для запуска и поддержки системы, тем более что их может и не быть.

Впрочем, возможны и другие сценарии применения. Например, объединение разнородных вычислительных систем при слиянии компаний легче осуществить при интеграции на HCI-системах. Да и не только при объединении – миграция с дорогих высоконадежных вычислительных систем, на которых работают бизнес-критичные приложения, на коммодити-решения, используемые в HCI, может сэкономить много денег, не снижая при этом показатели надежности.

И, конечно, гибкие гиперконвергентные системы удобны для разработки и тестирования новых бизнес-приложений.

Клиенты в России

Российский рынок гиперконвергентных систем находится в стадии становления. По данным iKS-Consulting, уровень их проникновения в средних и крупных компаниях на начало 2018 г. составил 22%. Аналитики ожидают рост рынка на 25–30% в год. Сдерживается этот рост во многом тем, что значительная часть ИТ-специалистов не знакома с подобными решениями. Так, по опросам, проведенным в начале 2018 г., 18% тех, кто не использует системы гиперконвергенции, не знают, что это такое, а 39% не знакомы с их преимуществами.

Тем не менее спрос на HCI в России есть. Интерес к гиперконвергентным решениям проявляют российские банки: в крупных финансовых организациях развита разработка, а чем больше проектов, тем сложнее ИТ-инфраструктура и выше потребность в ресурсах. Из свежих примеров – развертывание VDI на базе Dell EMC VxRail в СКБ-банке.

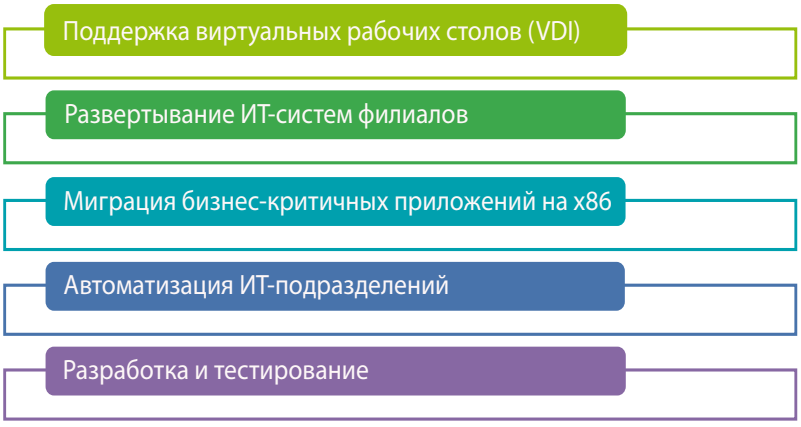
В числе российских заказчиков гиперконвергентных систем есть предприятия из промышленности, розничной торговли и госсектора. В частности, в администрации Екатеринбурга осуществляется проект миграции ЦОДа классической архитектуры на гиперконвергентную.

ПО «Росплатформы» используется в Федеральной налоговой службе, Министерстве транспорта РФ, на судостроительном заводе «Янтарь» и ряде российских университетов. За рубежом гиперконвергентные системы также активно задействованы в сфере медицины, но в России пока такого спроса нет.

Переход на HCI

Самый простой способ перейти на гиперконвергентную систему – купить заранее интегрированный программно-аппаратный комплекс. Сделать это можно, например, у HPE (платформа SimpliVity), IBS («Скала-Р») или Scale Computing. Такой подход эффективен при развертывании новых филиалов предприятий и банков, создании новых компаний.

Но уже работающие на рынке организации имеют свою ИТ-инфраструктуру и не хотят терять сделанные в нее инвестиции. У компаний существуют программы закупок, ориентированные на конкретных вендоров, есть экспертиза по работе с оборудованием и ПО конкретных производителей.



▲ **Сценарии использования гиперконвергентных решений**

Поставщики в ответ на запрос рынка начали предлагать разные варианты гиперконвергентных систем. Поставщики аппаратных решений обеспечивают возможность работы с разными системами виртуализации. Так, Dell EMC предлагает гиперконвергентные системы на базе VMware, Nutanix и Azure Stack, но может поставить серверы и со всем интегрированным стеком Red Hat.

Поставщики программных решений также провели диверсификацию аппаратных платформ. «Изначально мы поставляли программно-аппаратный комплекс Nutanix. Но теперь позиционируем себя как software company. У нас есть множество сертифицированных партнеров: IBM, Dell, Lenovo, Fujitsu, а также Cisco и HPE. Де-факто идем к тому, чтобы продавать в основном ПО. Клиент может купить, например, серверы

Dell, а потом у нас – лицензии на ПО», – поясняет технический директор компании Nutanix в России и странах Восточной Европы Максим Шапошников.

Написать программу, работающую с конкретным аппаратным комплексом, значительно проще, чем обеспечить ее работу со всем спектром «железа», представленным на рынке. Это задачи разного масштаба. Решения повзрослели и теперь с определенными ограничениями могут быть запущены практически на любом стандартном оборудовании. Но, как отмечает эксперт по облачным платформам компании Dell EMC Андрей Николаев, тут есть подводные камни. Работа ПО зависит от особенностей аппаратной части и версий ее прошивки. Например, продукт Dell EMC ScaleIO работает через гипервизор и мало связан с «железом». Но с определенного времени его перестали продавать как отдельное ПО, поскольку клиенты иногда устанавливали его на экзотическое самосборное «железо», а потом предъявляли претензии компании Dell EMC. Поэтому было принято решение продавать ScaleIO только на сертифицированном оборудовании, по сути по модели гиперконвергентной инфраструктуры VxRail. Проводят сертификацию конкретных серверов для своих гиперконвергентных решений компании VMware и Red Hat.

Что дальше?

В единое целое можно объединить не только вычислительные мощности и системы хранения данных, но и виртуализированные сети, что уже становится стандартом для HCI. Предлагаются решения, интегрированные с системами резервирования и аварийного восстановления данных.

Так, у Dell EMC помимо классической гиперконвергентной инфраструктуры VxRail появилось более сложное гиперконвергентное решение Dell EMC VxRack SDDC на базе VMware Cloud Foundation, куда входят виртуальное хранилище vSAN и программно определяемые сети VMware NSX. Решение расширяется практически любыми продуктами VMware, включая систему автоматизации управления ИТ-процессами VMware vRealize Operations, систему создания персонализированной инфраструктуры, приложений и специализированных ИТ-услуг VMware vRealize Automation. Причем все это может поставляться как предварительно интегрированный комплекс «из коробки».

Таким образом, гиперконвергентные решения выходят на новый уровень. Если раньше предоставлялась только инфраструктура, на которой специалисты заказчика «поднимали» свои системы, то теперь гиперконвергентные решения предлагаются как платформа, подобно облачной PaaS. Это сильно облегчает труд разработчиков, позволяя автоматизировать создание сред исполнения программ, развертывание виртуальных машин, контейнеров и микросервисов.

Еще одно направление развития гиперконвергентных систем – предоставление их облачным провайдером в аренду по модели dedicated. Компания может не покупать HCI-систему, а пользоваться ею из ЦОДа провайдера по сервисной модели. Или развернуть у себя и масштабировать в ЦОД провайдера, создавая растянутый кластер. Аналогичный кластер можно создать, объединив со своей локальной гиперконвергентной системой HCI-систему, размещенную в ЦОДе провайдера по модели colocation.

На Западе уже появились предложения HCI-as-a-Service, например на базе NetApp HCI. В России компания Selectel анонсировала создание гибридных систем с облаками VMware в своих ЦОДах, расположенных вблизи клиентов, что должно гарантировать время отклика менее 5 мс. Это позволит клиентам строить гиперконвергентные решения с облаком VMware, объединив локальные и облачные виртуализованные системы хранения с помощью vSAN в растянутый кластер. До конца года компания планирует развернуть дата-центр в Москве для того, чтобы обеспечить клиентам минимальные задержки.

В этом году компания Linxdatacenter получила премию DC AWARDS 2017 в номинации «Лучший проект облачного решения для ЦОДа» за первое в России гиперконвергентное облачное решение. Развернутая в ЦОДе компании в Москве на базе платформы Cisco HyperFlex виртуальная инфраструктура HyperCloud дает возможность предприятиям среднего и крупного бизнеса создавать публичные, частные, гибридные облака и эффективно связывать их друг с другом и существующей ИТ-инфраструктурой по выделенным каналам и через интернет. Предусмотрена поддержка bare-metal и контейнерных сред. По мнению компании, облачное гиперконвергентное решение имеет ряд преимуществ для заказчика, прежде всего на этапах проектирования, развертывания и масштабирования систем.

Сегодня вычислительная инфраструктура предприятий включает в себя все больше разнообразных систем и ее развитие направлено на переход от обеспечения работоспособности вычислительных систем к обеспечению доступности и работоспособности предлагаемых клиенту сервисов. В этих условиях одно из главных преимуществ гиперконвергентных систем – упрощение управления вычислительной инфраструктурой, причем как на площадке заказчика, так и у провайдера. ИКС

Зеленый – значит экологичный

ТМ ITK вывела на рынок кабель из витых пар, отвечающий жестким стандартам по экологичности и пожарной безопасности.

Ольга Дроздова, продакт-менеджер, ТМ ITK

Пожар в торгово-развлекательном комплексе «Зимняя вишня» в Кемерово, который привел к многочисленным жертвам в результате отравления людей продуктами горения, заставил общество по-новому взглянуть на токсичность используемых в строительстве материалов. Резко ужесточились меры противопожарной безопасности, сократилось число центров сертификации, многие из которых раньше давали заключения формально, без проведения испытаний, стало значительно труднее получать сертификаты.

Для выполнения жестких требований регуляторов ТМ ITK вывела на рынок кабели категорий 5E, 6, 6A и 7 для внутренней прокладки в новой оболочке LSZH HFLTx. Зеленый цвет оболочки подчеркивает экологичность — используемый материал недымный, негорючий, не выделяет токсичных галогенов, таких как фтор, хлор, бром и йод.

Экологичный кабель — ответ на запрос рынка, на котором уменьшается доля проектов с применением дешевого, но горючего кабеля в оболочке из поливинилхлорида (ПВХ). Причем такая тенденция наблюдается не только при строительстве объектов с массовым пребыванием людей, но и при оборудовании офисных помещений и даже квартир. Использование экологичного кабеля тем более оправдано, что разница в цене незначительна – кабель в оболочке LSZH дороже всего на 5–10%.

Аббревиатура LSZH (Low Smoke Zero Halogen) расшифровывается как «малодымный безгалогенный». Кабели только с такой оболочкой по требованиям законодательства должны прокладываться в дошкольных учреждениях и больницах. ТМ ITK тесно сотрудничает с лечебными учреждениями и поставляет для таких проектов экологичную безопасную продукцию. Кроме того, «зеленый» кабель от ТМ ITK использовался при строительстве стадиона «Зенит-Арена» и музея «Россия — Моя история» в Санкт-Петербурге.

Оболочки LSZH характеризуются разными классами пожарной опасности. Независимые пожарные сертификационные органы с государственной лицензией (теперь их осталось очень мало) во время испытаний оценивают продукцию по четырем основным показателям: горючесть, дымовыделение, коррозийность и выделение токсичных веществ, после чего кабелю присваивается класс пожарной опасности в соответствии с ГОСТ.

«Зеленый» кабель ITK прошел испытания с наивысшим баллом по всем показателям, причем это произошло уже после событий в Кемерово, когда требования были ужесточены. Протокол испытаний находится в открытом доступе, и клиент может убедиться, что сертификационный орган имеет действующую государственную лицензию. Это важно, поскольку некоторые вендоры предъявляют сертификаты органов, не прошедших государственную проверку либо уже несуществующих или лишившихся государственной аккредитации.

Кабель ITK изготавливается на производственной площадке, выпускающей продукцию для наиболее дорогих мировых брендов. Производство полностью автоматизировано, что исключает ошибки персонала. Качество каждой партии непосредственно на заводе контролирует постоянно прикрепленный инженер ТМ ITK.

На кабель дается системная гарантия 25 лет. Бухты выпускаются стандартной длины 305 м. Они помещаются в жесткую удобную коробку из экологичного материала, на которую при необходимости может встать монтажник. Внутри коробки намотка кабеля осуществляется на пластиковый барабан, что обеспечивает равномерную, без перекручивания подачу провода.

Позиционирование «зеленого» кабеля ориентировано на средний ценовой сегмент, при этом по качеству он не уступает изделиям премиум-сегмента. Сравнимого по качеству кабеля за ту же цену на российском рынке сегодня нет.

СКС монтируется не на один год. Требования к используемым при ее создании комплектующим постоянно ужесточаются, и нельзя дать гарантии, что применение ПВХ-кабелей, провоцирующих горение и разлагающихся при высоких температурах, не будет запрещено полностью. Таким образом, сэкономив сейчас, можно столкнуться с необходимостью перемонтажа системы в будущем. Может быть, лучше сразу выбрать «зеленое» решение?

www.itk-group.ru

«Умные» решения современных бизнес-задач

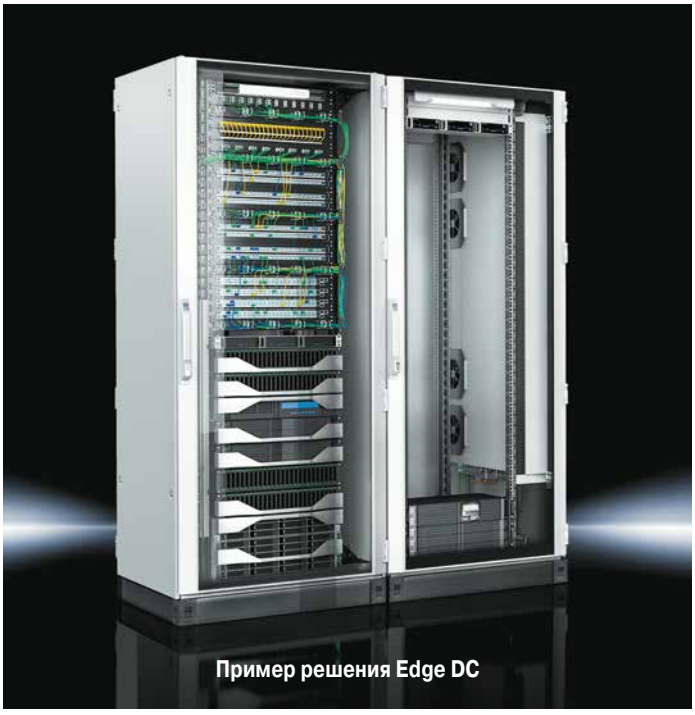
Гибридные холодильные агрегаты, второе поколение межрядных водяных кондиционеров, расширенная линейка фреоновых машин – эти и другие «умные» решения Rittal предлагает в рамках года ИТ-инфраструктуры.

Кирилл Дмитриев, менеджер по продукции (ИТ-охлаждение), Rittal

История Rittal насчитывает уже более 50 лет. За эти годы бренд стал известен благодаря качеству и надежности своей продукции. Основываясь на этом опыте и компетенции сотрудников, мы объявили 2018-й годом ИТ-инфраструктуры и готовы представить ряд новинок для решения задач заказчиков.

На недавно прошедшей выставке CeBIT компания Rittal анонсировала новую концепцию «SmartSolutions: от компонентов к решениям», в рамках которой были продемонстрированы возможности применения новых холодильных агрегатов. В частности, были представлены решения для Edge-ЦОДов, микроЦОДов и блокчейн-платформ.

С учетом растущих требований к мощности, надежности и эффективности инженерных систем, в том числе систем охлаждения, мы решили расширить и обновить линейку оборудования для ИТ-охлаждения. В этом году в рамках различных готовых кейсов были представлены новые фреоновые холодильные агрегаты мощностью 20 и 35 кВт, обновленная линейка водяных межрядных кондиционеров LCP CW и первая в своем роде гибридная система охлаждения со встроенным непрямым охлаждением наружным воздухом, мощностью 35 кВт. Таким образом, портфолио продуктов для ИТ-охлаждения охватывает диапазон мощностей от 3 до 55 кВт на один агрегат с возможностью выбора решений под конкретные задачи проекта.



Пример решения Edge DC

Гибридное охлаждение – новый шаг к энергоэффективности

Rittal впервые представляет гибридный холодильный агрегат Liquid Cooling Package (LCP) DX/CW, оборудованный раздельными контурами хладагента (DX) и водно-гликолевого раствора (CW). Благодаря такой конструкции холодильный агрегат способен работать не только в «компрессорном» режиме, но и в режиме частичного или полного непрямого охлаждения наружным воздухом (фрикулинга).

Все элементы гидравлического контура – инверторный насос, регулировочные клапаны и расширительный бачок – встроены во внутренний блок. Такое решение, а также применение электронно-коммутируемых вентиляторов и инверторных технологий управления приводами дает возможность получать в каждый момент времени ровно столько холода, сколько необходимо, при минимальном электропотреблении, что позволяет существенно снизить эксплуатационные затраты на электроэнергию и коэффициент PUE.

SmartMobility: компактные и эффективные решения для Edge Computing и микроЦОДов

Все шире используются малые локальные ИТ-ячейки, выполняющие функцию местного вычислительного ядра или хранилища оперативной информации, которая доступна с минимальной задержкой. Эти ячейки могут создаваться как в формате группы стандартных ИТ-стоек, так и в формате защищенного микроЦОДа. Особенность таких инсталляций в том, что вся инфраструктура, в том числе охлаждение, интегрирована в стойки.

Для охлаждения отдельно стоящей стойки с нагрузкой до 3 кВт в нашем портфолио есть потолочный холодильный агрегат. Это моноблочное решение, устанавливаемое на крышу шкафа, с типичным для ИТ-применения движением воздуха спереди назад. Размещение всех элементов в едином корпусе и низкий уровень шума делают его пригодным для установки в офисных помещениях.

Альтернативным решением может служить встраиваемый в стойку ИТ-кондиционер LCU DX. Данное семейство агрегатов представлено в классах мощности до 3 кВт и до 6,5 кВт, каждый из которых имеет исполнение с резервированием холодильных контуров. Внутренний блок монтируется непосредственно внутрь стойки по принципу «0U» и не

занимает дополнительного места, что позволяет достичь высокой эффективности агрегата за счет охлаждения внутреннего объема стойки, а не всего помещения. Наружный блок компактен и устанавливается на наружной стене или кровле. Благодаря максимальной длине трубопроводов 50 м данная система предоставляет широкие возможности размещения оборудования друг относительно друга.

Исполнение LCU с резервированием отвечает высочайшим требованиям надежности и отказоустойчивости, что является неотъемлемым требованием к современной ИТ-инфраструктуре. Благодаря резервированию магистралей, холодильных контуров и вводов питания пользователь может быть на сто процентов уверен в безотказности системы охлаждения. А встроенная система ротации и переключения в случае аварии гарантирует равномерную выработку ресурса и доступность системы при любых условиях.

SmartFinance: дальновидные инвестиции без риска

Сегодня потребители желают получать банковские услуги в любое время и в любом месте. Это требует максимально оптимизированных систем, в которых информация не перенаправляется в облако, а обрабатывается периферийным ЦОДом. В условиях рыночной экономики, где время решает все, периферийные ЦОДы должны обеспечивать максимально быстрые и безопасные транзакции. Для таких систем обычно используются контейнерные платформы, которые характеризуются высокой масштабируемостью и безопасностью.

Именно для такого применения мы дополнили семейство холодильных агрегатов DX двумя новыми моделями: 20 и 35 кВт, предназначенными для охлаждения ИТ-инсталляций малого и среднего масштаба. Наличие шести датчиков температуры воздуха и инверторное управление всеми приводами позволяет поддерживать температуру с максимально высокой точностью, исключая появление зон локального перегрева. При необходимости восемь агрегатов можно объединить в единую логическую группу для отработки специфического сценария или для равномерной выработки ресурса агрегатов.

SmartGovernment: эффективное управление социальными сервисами

В наши дни общество уже не может функционировать без «умных» устройств и сервисов. Особенно высокие требования предъявляются к обработке данных от экстренных служб, систем наблюдения, социальных и бытовых сервисов. Все эти данные требуют надежной и отказоустойчивой инфраструктуры с максимально высокой доступностью.

Поэтому в текущем году мы обновили наши водяные межрядные кондиционеры LCP CW. Основные изменения коснулись обслуживания: теперь вентиляторные модули заменяются за секунды без использования инструментов, а электрический модуль и плата управления не требуют доступа сверху для обслуживания. Семейство водяных агрегатов может похвастаться крайне широким диапазоном применений, они могут охлаждать как отдельные стойки, так и целые ряды. Кондиционеры LCP CW – самые мощные агрегаты в своем классе, поскольку развивают мощность до 55 кВт при занимаемой площади всего 0,36 кв. м. Задействование этих кондиционеров вместе с тепловыми насосами или высокотемпературной водой открывает новые горизонты в достижении максимальной энергоэффективности, в частности, за счет применения непрямого естественного охлаждения при высоких температурах наружного воздуха.


Новая гибридная система охлаждения

Отличительная особенность некоторых моделей линейки LCP Inline CW – каплеуловитель нового типа, благодаря которому улучшается контроль конденсата. Инженеры Rittal решили отойти от стандартной концепции лабиринтных каплеуловителей и разработали новый «карманный» тип. При такой конструкции исключается возможность уноса капель влаги при высокой скорости благодаря наличию обратно загнутых лопаток. При этом конструкция рассчитана так, чтобы создавать минимальное аэродинамическое сопротивление. Такое нововведение делает решение идеальным для использования в средах с высокой влажностью воздуха или при низкой температуре подаваемой воды.

SmartFuture: экспресс-линия в будущее

Сегодня поток данных постепенно превращается из тонкого ручейка в полноводную бурлящую реку. Он постоянно меняет свое основное русло, трансформируется и диктует новые правила и требования к основным игрокам рынка. Rittal пытается идти в ногу с современными тенденциями и радовать своих старых партнеров неизменным качеством и новинками, а новых привлекать продуманными и эффективными решениями. Следите за нашими новостями! Discover the Edge вместе!

Майнинг и ЦОДы

Николай Носов

Услуги ЦОДов для майнеров – новый тренд развития рынка. Этот вторичный для дата-центров бизнес может помочь им утилизировать площади в ожидании более выгодных клиентов.

Огромный рост курсов криптовалют в прошлом году привел к настоящей цифровой «золотой лихорадке». Майнингом стали заниматься даже далекие от ИТ люди.

Криптовалютная лихорадка

Вытащить счастливый билет, первым решить криптографическую задачу, подписать блок и получить за это криптовалюту не так уж легко. Скоро пришло понимание, что использовать стандартный компьютер нецелесообразно – не окупятся затраты на электричество. Эффективнее майнить на видеокартах, а еще лучше – на «асиках» (ASIC, application-specific integrated circuit), т.е. специализированных чипах, предназначенных для решения конкретной задачи (рис. 1). Выполнение микропроцессором строго ограниченного количества функций увеличивает скорость расчетов и, как следствие, эффективность работы. Широкое распространение получили специализированные устройства, предназначенные непосредственно для майнинга, – майнеры.

Рис. 1. «Асик», погруженный в охлаждающую жидкость ▶

Заниматься майнингом дома некомфортно – майнеры шумят и нагревают помещение. Лучше установить вычислительные устройства в гараже, особенно если есть возможность бесплатно подключиться к сети электропитания. Делаются попытки получать криптовалюту на рабочем месте (в феврале нынешнего года ФСБ арестовала двух инженеров закрытого ядерного центра в Сарове за попытку майнить биткоины на рабочем суперкомпьютере) или на чужих компьютерах: появились вирусы, осуществляющие майнинг на зараженных вычислительных системах. Причем самые продвинутые из них (CPU Miner и Vnlgp Miner) маскируют себя, выполняя расчеты в то время, когда не работает хозяин компьютера.

Из гаража – в ЦОД

В целом майнинг повторяет в своем развитии классические вычислительные системы. В наших банках тоже начинали с отдельных компьютеров, стоящих на рабочих местах сотрудников. Потом появились серверные, затем ЦОДы. Крупные игроки рынка майнинга уже доросли до понимания, что поддержание работоспособности большой вычислительной инфраструктуры – это отдельный и сложный бизнес, который лучше отдать на аутсорсинг.

Пионером российского рынка ЦОДов для майнинга стала компания Inoventica, которая в прошлом году официально предложила услугу colocation серверных ферм для пользователей, майнящих криптовалюты. Аналогичные услуги предлагают ЦОДы компаний «Авантаж» и Selectel.

Для ЦОДов это вторичный бизнес, доля которого, по оценкам iKS-Consulting, не превышает 10%. Предоставление услуг майнерам помогает дата-центрам повышать утилизируемость площадей в ожидании более выгодных клиентов. Кроме того, оборудование для майнинга используется ЦОДами как тестовая нагрузка для проверки функционирования инженерных комплексов при работе на полной мощности.

Оборудование для майнинга не предъявляет высоких требований к инфраструктуре ЦОДа. Но расчеты энергоемкие: объем электроэнергии, потраченной на майнинг биткоина в 2017 г., по данным ресурса powercompare.co.uk, превышает потребление многих стран мира, в том числе Ирландии и большинства стран Африки.

Интернет-омбудсмен Дмитрий Мариничев считает, что ЦОДы могут сами заняться майнингом, задействуя для этого резервный канал электропитания. В случае проблем с основным каналом майнеры отключаются от резервного,

и он начинает питать основную вычислительную нагрузку ЦОДа. «При таком подходе мы имеем стопроцентную утилизацию мощностей, подведенных к дата-центру», – отмечает Д. Мариничев.

В майнинговом центре своей компании Radius Group Д. Мариничев использует майнеры собственного производства и уверен в их качестве. Но для других владельцев ЦОДов безопасность майнеров неочевидна. Во всяком случае, в ЦОДе Selectel майнеры клиентов проходят входной контроль – компания не разрешает размещать в своем дата-центре самосборные устройства сомнительного качества. И дело не только в пожарной безопасности – перегорание блока питания может привести к короткому замыканию и отключению соседних устройств.

Майнинг не требует от ЦОДов высокой надежности – недоступность устройств ведет к финансовым потерям, но они не столь критичны, как в случае неработоспособности вычислительных систем в промышленности или финансовом секторе. Майнеров не интересуют сертификаты Uptime Institute и вопросы резервирования мощностей. Главное – дешевое электричество и отвод тепла. А для этого достаточно ЦОДов с невысокими показателями доступности или майнинговых ферм – недорогих дата-центров, специально построенных для майнинга.

Еще одна особенность майнинга – разнообразие формфакторов устройств. Нет никаких общепринятых стандартов на размеры корпусов, предусматривающих установку в стойки. Как следствие, устройства для майнинга размещают в ЦОДах на полках, в простейших случаях отводя тепло из помещения с помощью вентилятора или кондиционера (рис. 2).

▲ **Рис. 2. Размещение оборудования на майнинговой ферме**

Проблемы охлаждения

При работе ASIC-компьютеров выделяется много тепла – 1,5–6,5 кВт•ч. Установка промышленного кондиционера приводит к дополнительным расходам на электроэнергию. Кроме того, кондиционеры требуют обслуживания, очистки, фильтрации воздуха. Но без охлаждения все же не обойтись – перегрев может привести к пожару.

В майнинговом центре Radius Group, расположенном на территории бывшего автозавода «Москвич», применяется водяное охлаждение, при котором обычная вода отводит тепло от расположенных в майнерах радиаторов. Такие разработанные специалистами компании «асики» используются для майнинга биткоина и других

МНЕНИЕ ЭКСПЕРТА

Как бороться с нелегальным майнингом в ЦОДах?

Роман Жуков, руководитель экспертного направления по информационной безопасности, «Гарда технологии»

В авангарде нелегального майнинга сегодня – ЦОДы крупных предприятий. Безопасники все чаще сталкиваются с тем, что сотрудники компаний злоупотребляют корпоративными ресурсами, используя их для добычи криптовалюты.

Специалистам по информационной безопасности обычно трудно предъявить какие-либо обвинения нелегальным майнерам, поскольку, применяя штатные средства контроля, крайне сложно собрать доказательную базу по поводу ущерба, нанесенного организации. Однако если в базах службы безопасности нет сигнатур по обнаружению «добычи» определенной криптовалюты, то майнеров можно выявлять по паттернам их поведения.

Весьма популярный технологический тренд последних лет – UEBA (user and entity behavior analytics). С помощью современных программных средств анализируется поведение пользователей и отдельных компьютеров. Полученные результаты сравниваются с их нормальным ежедневным поведением либо с поведением коллег по отделу или бизнес-единице.

Оценить вредоносность можно также по профилю трафика. Рассмотрим простейший случай: менеджер нагружает свою машину в рабочее время с 9 ч до 18 ч и, как правило, делает это неравномерно. Если же с определенного момента нагрузка на канал связи стала равномерной и круглосуточной, то такое поведение подозрительно и требует тщательной проверки службой информационной безопасности.

Злоумышленники используют самые современные разработки, не скованы законодательством и имеют в своем распоряжении базу для тестирования в виде разных ЦОДов, поэтому они фактически всегда на шаг впереди защиты. Поведенческий анализ как раз и дает возможность сократить технологическое отставание от нарушителей, в том числе в области информационной безопасности дата-центров.

криптовалют, опирающихся на алгоритм хеширования SHA-256. Остальные криптовалюты майнятся традиционным путем на графических картах.

Другой путь решения проблемы – использование двухфазного жидкостного охлаждения. Вычислительное оборудование проходит специальную подготовку (очистку от остатков флюса на платах, настройку температурных режимов в BIOS, отключение вентиляторов) и помещается в резервуар со специальной жидкостью. Конструкция герметически закрывается. При нагревании устройств жидкость испаряется и охлаждает микросхемы. Пар охлаждается в сухой градирне, которая отводит тепло, конденсируется, и получившаяся жидкость опять поступает в резервуар. Такая технология была впервые применена в ЦОДе компании Allied Control (входит в ГК BitFury) в 2012 г. в Гонконге.

Исполнительный директор ГК «Пожтехника» Антон Анненков считает двухфазное охлаждение экономически выгодным. Моделирование размещения майнинговой фермы в нежилой одноэтажной постройке площадью 10 кв. м показывает, что такой способ охлаждения хотя и увеличивает CAPEX на 7%, но снижает OPEX на 36%, повышает производительность ASIC-компьютеров на 30% и ускоряет окупаемость на 28%.

ЦОД как майнер

Оптимальный путь для ЦОДа – не предоставление услуг майнерам, а самостоятельный майнинг, уверен Д. Мариничев. Место под майнеры можно выделить в любой технической зоне, желательно ближе к источнику электричества. Срок окупаемости оборудования – от 10 до 14 месяцев, и еще в течение двух лет дата-центр будет получать доход. Благодаря такому подходу значительно повышается экономическая эффективность, а высокоуровневые сервисы, оказываемые ЦОДом клиентам, будут иметь нулевую себестоимость с точки зрения электроэнергии и обслуживания, так как ЦОД будет самоокупаемым.

Рис. 3. Макет контейнерного ЦОДа для майнинга

Дата-центр можно строить сразу ориентированным на майнинг. Такие предложения на рынке есть, например, контейнерное решение, которое представила компания Bitferma.ru на Blockchain Conference Moscow 2018. В нем все, как в классических контейнерных ЦОДах, – при необходимости дата-центр масштабируется 20- или 40-футовыми контейнерами с подготовленной для установки майнеров инженерной инфраструктурой (рис. 3).

Д. Мариничев считает, что с осени текущего года криптовалюту в России можно будет официально перевести в рубли. Пока этого нет, и предпринимателям приходится искать обходные пути – различные «серые» схемы, например, обналичивать полученную криптовалюту в Европе, переводить валюту по фиктивным контрактам в Россию с дальнейшей конвертацией в рубли. Это не выгодно ни бизнесменам, ни государству, которое недополучает налоги. По поручению президента с сентября прошлого года Минфин и ЦБ занимаются разработкой законопроекта о финансовых активах. Поэтому рынок смотрит на процесс легализации криптовалют с оптимизмом. Московская биржа сообщила, что приступила к созданию платформы для торгов криптовалютой, в том числе платформы посттрейдингового обслуживания криптоактивов.

Майнинг и закон

Законопроект – это хорошо, но пока криптовалюты по-прежнему находятся в «серой» зоне. Это накладывает отпечаток и на майнинг. Как отметил эксперт iKS-Consulting Станислав Мирин, многие ЦОДы «стесняются» отвечать на вопросы о майнинге. На блокчейн-конференциях докладчики зачастую уклоняются от ответа на вопрос, где территориально находится майнинговая ферма, предлагающая услуги размещения оборудования.

Непосредственно к майнингу у правоохранительных органов, как правило, претензий нет. Проблемы возникают в случае кражи электричества или незаконного использования чужого вычислительного оборудования. Появляются претензии и при контрабандном ввозе устройств для майнинга. Импортное оборудование зачастую не имеет документов о легальном ввозе и таможенном оформлении. И это надо учитывать предпринимателям.

Юридически майнинг не запрещен, а что не запрещено законом, то разрешено – утверждали еще «прорабы перестройки». В обществе отношение к майнингу настороженное, но процесс легализации криптовалют идет, так что ЦОДам стоит обратить внимание на возможности нового рынка. ИКС

С заботой об АКБ

Системы бесперебойного электропитания – ключевые элементы, определяющие надежную работу ИТ-комплексов. О тенденциях в области ИБП и о том, как снизить стоимость владения энергосистемой, – Алексей Лобов, директор по развитию трехфазных ИБП компании CyberPower.

Алексей Лобов

– Системы бесперебойного питания – одна из самых консервативных областей, но влияние технологических и рыночных факторов заметно и здесь. Сегодня стало возможным создавать устройства высокой плотности мощности, при этом сохраняя на максимальном уровне показатели надежности и КПД. Скажем, ИБП CyberPower HSTP3T15KE при весе 31 кг и компактных габаритах способен выдавать в нагрузку до 15 кВА. Современная элементная база, в частности силовые IGBT-транзисторы, позволяют формировать выходную синусоиду с минимальными искажениями. Это дает возможность отказаться от громоздких фильтрующих контуров, одновременно повышая надежность, уменьшая габариты и, что немаловажно, снижая издержки на регламентную замену ряда элементов (например, конденсаторов). Так, благодаря тому, что КПД устройств серии HSTP достигает 96% в нормальном режиме и 98% в ECO-режиме, уменьшается тепловая нагрузка на сам ИБП и соответственно затраты на утилизацию выделяемого тепла, увеличивается надежность системы в целом.

Оказывает влияние на ИБП и цифровизация различных отраслей бизнеса. Фактически к ИБП и оригинальному ПО предъявляются требования как к программно-аппаратному комплексу, способному интегрироваться в устанавливаемую среду. Так, на базе модульных ИБП CyberPower серии SMX и ПО CyberPower Data Center Infrastructure Management можно создавать энергетические кластеры, вести энергоучет, статистику потребления, управления и администрирования. Данный аппаратно-программный комплекс оптимизирован для встраивания в существующую систему предприятия.

– В последнее время растет интерес к литий-ионным АКБ. Насколько они готовы к массовому использованию на таких критически важных объектах, как ЦОДы?

– Безусловно, технология прогрессивная и за ней будущее. Главным сдерживающим фактором массового применения литий-ионных батарей пока еще является стоимость. При всех своих плюсах решения остаются дорогими на этапе покупки, а выгода в сравнении с традиционными ИБП появляется лишь в расчете десяти и более лет эксплуатации. Осторожность заказчиков понятна.

Тем не менее мы «держим руку на пульсе». В портфеле CyberPower есть серия HSTP, промышленные трехфазные ИБП и модульные серии SM/SMX, которые полностью готовы к оснащению литий-ионными батареями. При появлении специфических задач у заказчика и его готовности рассмотреть более прогрессивные технологии мы такое предложение делаем.

– Как меняется отношение заказчиков к системам мониторинга состояния АКБ?

– Эта тема всегда вызывала интерес у эксплуатационных служб. Фактически АКБ является ресурсной частью, параметры которой зависят от ряда факторов: режим работы, температура, скрытый брак и др. Любой из перечисленных факторов способен кардинально влиять как на одну батарею, так и на весь батарейный массив и, как следствие, на всю энергосистему. Современная система BMS (Battery Monitoring System) позволяет поэлементно отслеживать АКБ, тестировать их, прогнозировать выход из строя и даже компенсировать заряд соседних АКБ, если одна из батарей начала терять заявленную емкость. Тем самым продлевается жизнь всего массива и существенно сокращаются затраты на замену батарей. Поскольку такие системы имеют подключение к Ethernet, получать сведения можно удаленно в режиме реального времени или из журнала событий. Все это снижает стоимость владения батареями.

CyberPower разработала и представила на российском рынке такую систему в начале 2018 г. BMS состоит из контроллера BM100 и датчика BP100-12, который крепится на батарею. Система достаточно гибкая, может работать с кислотными батареями емкостью 5—200 А•ч и обслуживать от одной до нескольких сотен АКБ. Наибольший интерес к новинке проявляют на объектах, где установлено ответственное оборудование и от работы АКБ зависит надежность всей системы (например, питание запуска ДГУ, системы постоянного тока, дежурного освещения, пожарной сигнализации, систем контроля доступа).

Экономические показатели делают систему BMS интересной для широкого круга заказчиков. Согласно статистике, до 27% отказов системы гарантированного электропитания происходят из-за АКБ; до 5% АКБ в батарейном массиве выходят из строя в течение гарантийного срока. При применении BMS ежегодная экономия, в том числе снижение издержек на эксплуатацию, может достигать 20%, при этом срок службы батарейного массива можно увеличить на год относительно расчетного.

Надежные, безотказные, инновационные

Александра Крылова

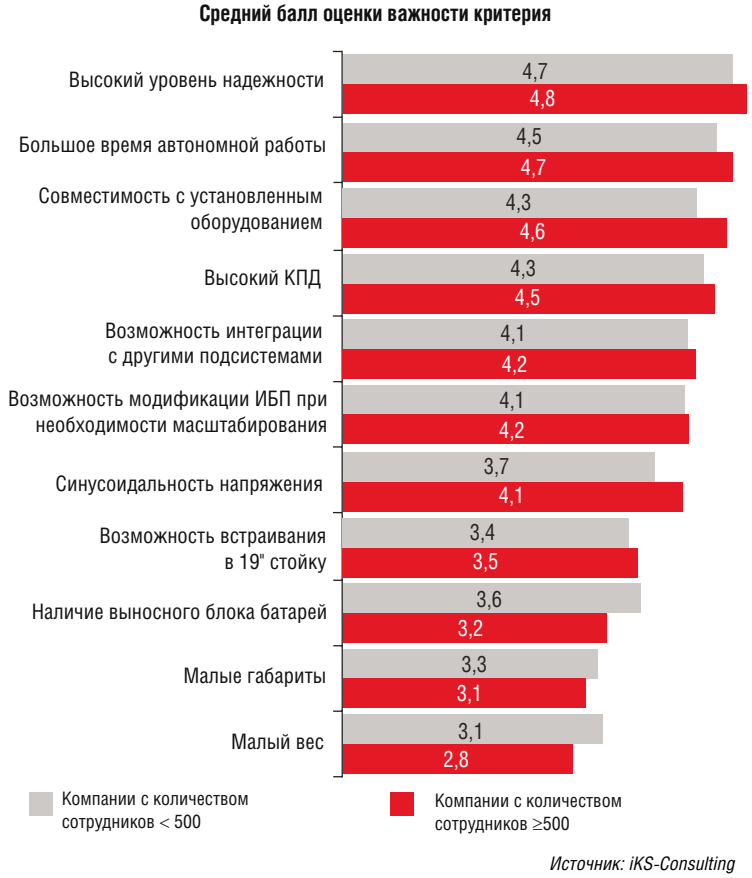
Несмотря на приверженность создателей ИБП проверенным схемотехническим решениям, в 2017 г. у ведущих вендоров появилось немало новаторских разработок.

Рынок ИБП, глобальный и российский

Объем глобального рынка источников бесперебойного питания составил по итогам 2016 г. $7,2 млрд, подсчитали аналитики компании IMS. Из этой суммы $4,2 млрд пришлось на сегмент систем средней ($1,7 млрд) и высокой мощности ($2,5 млрд). В том, что к 2020 г. рынок, по прогнозам, вырастет до $8 млрд, немалая «заслуга» цифровизации, которая сегодня охватывает большинство отраслей экономики.

В России, по оценкам аналитиков iKS-Consulting, объем рынка источников бесперебойного питания мощностью 10 кВА и выше за 2016 г. достиг $279 млн, или 18,6 млрд руб., что свидетельствует о его восстановлении после спада, начавшегося в 2013 г. и продолжившегося в 2014-м и в 2015-м.

Рис. 1. Критерий выбора ИБП



Источник: iKS-Consulting

Оживлению на рынке в 2016 г. способствовали меры государственной поддержки российских товаров, тендеры и конкурсы в рамках подготовки к Кубку Конфедераций и Чемпионату мира по футболу 2018. Еще одним драйвером стало принятие «закона Яровой», реализация которого требует от операторов связи многократного увеличения объемов хранимых данных, а значит, и систем, обеспечивающих работу хранилищ, в том числе ИБП.

Все эти факторы позволили аналитикам спрогнозировать дальнейший рост сегмента систем бесперебойного электропитания мощностью 10 кВА и выше и увеличение его доли в структуре российского рынка ИБП в денежном выражении с 25% в начале 2017 г. до 34% к 2020-му.

Тон задают заказчики

Годы экономического спада научили российские компании серьезному отношению к показателю ТСО – совокупной стоимости владения активами, в том числе ЦОДами, где чаще всего и применяются ИБП высокой мощности.

Поскольку современные системы бесперебойного питания мощностью 10 кВА и выше – сложное оборудование с высокой интеллектуальной составляющей, и в их разработку вкладываются большие средства, для защиты инвестиций вендоры вынуждены постоянно изучать потребности потенциальных заказчиков.

Стремление к оптимизации ТСО систем бесперебойного питания, как отмечают в компании Delta Electronics, останется основным вектором развития линеек ИБП всех производителей на ближайшие годы. Собственно, с этим вектором связаны все запросы заказчиков: интерес к модульным системам, к ИБП с повышенной плотностью мощности, к комплексным решениям, помимо оборудования включающим в себя систему мониторинга и управления, а также к услугам аудита инженерной инфраструктуры.

А компания Schneider Electric при создании Galaxy VX – мощных ИБП, предназначенных для крупных ЦОДов и промышленных предприя-

тий, – выявила заинтересованность заказчиков в снижении CAPEX и OPEX нового оборудования и одновременно в повышении его надежности.

Иными словами, заказчики мощных ИБП сегодня хотят вместе с оборудованием получить энергоэффективность, надежность, простоту и безопасность его эксплуатации. Также им нужны системы с КПД выше 96% и с максимальным значением активной выходной мощности. Для применения в промышленности важно исполнение ИБП в корпусах с дополнительной защитой модулей и компонентов от неблагоприятных внешних воздействий.

Еще одна группа требований связана с упрощением обслуживания ИБП (его обеспечивает модульная архитектура), расширенными функциями контроля состояния устройства и качества электропитания.

По данным опроса iKS-Consulting, проведенного в 2017 г. и охватившего более 100 крупных компаний, в топ-3 критериев выбора ИБП входят уровень надежности, время автономной работы и совместимость с уже установленным оборудованием (рис. 1).

На аппаратном уровне

Несмотря на консерватизм сферы разработки ИБП, поиски новых технических решений, которые позволят повысить их КПД, удешевить производство, уменьшить массогабаритные характеристики и улучшить параметры входного напряжения, продолжаются.

Компания Schneider Electric представила в 2017 г. блочный масштабируемый ИБП Galaxy VX мощностью 500–1500 кВт с возможностью параллельной работы для построения более мощных схем или схем с резервированием и с поддержкой литий-ионных батарей (рис. 2).

Главная конструктивная особенность этого ИБП – четырехуровневый инвертор. Это схемотехнически непростое решение, оправданное на высоких мощностях, позволяет снизить нагрузку на силовые компоненты инвертора, что особенно ценно в жаркую погоду. Благодаря ему ИБП работает при температуре +40°C без ухудшения характеристик – выходной мощности и перегрузочной способности (150% в течение 1 мин).

Летом 2018 г. производитель начал обновлять линейку небольших ИБП: на замену Galaxy 300 вышла система Easy UPS 3S с диапазоном мощностей 10–40 кВт. При ее разработке основной упор был сделан на максимальную компактность: в результате ширина Easy UPS 3S без батарей составляет всего 25 см, а вес – менее 100 кг. Такие габариты никак не повлияли на надежность ИБП. Наоборот, по КПД, выходному коэффициенту мощности, перегрузочной способности, мощности зарядного устройства Easy UPS 3S превосходит Galaxy 300.

▲ **Рис. 2. ИБП Galaxy VX**

Для новых семейств ИБП характерны выходной коэффициент мощности, равный 1, КПД до 96% в режиме двойного преобразования и наличие режима нагрузочного самотестирования без подключения реальной нагрузки. Дизайн систем стал однотипным: ярко-белые корпуса с зелеными ручками придают оборудованию более позитивный вид.

Мощность систем Galaxy VX наращивается как на уровне шкафов (это не требует дополнительных кабельных работ), так и путем параллельного подключения нескольких ИБП. Поскольку Easy UPS 3S входит в линейку устройств среднего ценового сегмента, он масштабируется только путем параллельного подключения устройств (до четырех ИБП).

Компания Eaton недавно анонсировала ИБП, которые комплектует вместо батарей суперконденсаторами собственной разработки. Такие источники бесперебойного питания имеют значительно меньший вес и не нуждаются в дополнительном охлаждении, обеспечивая резервирование в диапазоне от нескольких секунд до нескольких минут, т.е. представляют собой экономичную альтернативу дизельно-роторным ИБП. В такой компоновке они могут работать в температурном диапазоне от –40°C до + 65°C, что делает их незаменимыми для эксплуатации в сложных условиях. В настоящее время суперконденсаторами могут быть оснащены все новые модели трехфазных ИБП Eaton мощностью от 8 до 7700 кВт.

Рис. 3. ИБП серии LevelUPS ▼

Новинки в портфеле компании Makelsan – серия ИБП LevelUPS мощностью до 1000 кВА и высокоэффективная серия ИБП LevelUPS T3 (рис. 3) со встроенным трансформатором гальванической изоляции (мощностной диапазон 10–200 кВА).

Основная техническая особенность серии LevelUPS – применение технологии трехуровневого преобразования энергии с использованием современных IGBT-модулей. Это обеспечивает КПД до 97% с сохранением всех преимуществ устройств предыдущих поколений. Выходной коэффициент мощности новых ИБП равен 1. При этом они способны питать как емкостную, так и индуктивную нагрузку без снижения выходного уровня мощности.

В сегменте однофазных ИБП компании Powercom появились новые источники бесперебойного питания серии MAC и MRT с коэффициентом мощности 1, позволяющим подключать к ним больше нагрузки, и с функцией «горячей» замены батарей, которая ускоряет обслуживание ИБП в аварийной ситуации.

Серьезной переработке подверглись трехфазные системы вендора. Благодаря полному обновлению силовой части с применением новых электронных элементов, а также изменению компоновки плат и расположения АКБ удалось уменьшить массогабаритные характеристики оборудования, улучшить вентиляцию силовой части, снизить запыленность внутреннего пространства ИБП, значительно увеличить его срок работы и, что важно, сократить расходы на обслуживание.

В результате новая серия систем VGD-II, пришедшая на смену линейке VGD, отличается от своей предшественницы более высокой надежностью, улучшенным дизайном и повышенным удобством подбора ИБП для различных видов нагрузки. Также изменилась архитектура трехфазных промышленных ИБП высокой степени надежности серии ONL: так как все новые устройства построены по модульному принципу, серия получила название ONL-M.

Компания «Импульс» представила модульные решения с мощностью одного фрейма до 600 кВА и возможностью создания систем общей мощностью до 2400 кВА. Такие ИБП отличаются компактностью (могут встраиваться в ряды стоек с ИТ-оборудованием), высокой плотностью мощности и обладают всеми необходимыми коммуникационными интерфейсами. КПД таких модульных систем, по данным компании, достигает 97% при нагрузке в диапазоне 25–100%. На случай аварии есть функции «горячей» замены силовых модулей, модуля электронного байпаса, а также блока синхронизации и управления.

Компания Huawei сделала ставку на модульность. По крайней мере все новинки, которые она вывела на российский рынок в 2017–2018 гг.: ИБП серий UPS5000-S, UPS5000-E, UPS5000-S-IPB и FusionPower5000, – имеют такую архитектуру.

У каждой из серий источников бесперебойного питания свои особенности. Так, модели серии UPS5000-S позиционируются как высокоэффективные: их энергоэффективность достигает 97,1%. Интегрированный источник бесперебойного питания серии UPS5000-E мощностью до 75 кВт имеет модульные АКБ. Высокоэффективный ИБП серии UPS5000-S-IPB мощностью до 200 кВт со степенью защиты IP42 предназначен для применения в промышленности. Источник бесперебойного питания FusionPower5000 – лидер среди новинок по мощности (до 1,2 МВт).

В целом все новые серии ИБП отличают компактность, высокая плотность мощности каждого модуля, высокая эффективность и резервирование всех компонентов.

Эксклюзивный дистрибьютор Socomec в России, компания «Преора», представила в этом году две линейки моноблочных ИБП средней мощности четвертого поколения. Линейка Masterys GP мощностью 60–160 кВА позиционируется производителем как система для управления электропитанием ИТ-оборудования, поддерживающего работу критически важных приложений «умного» производства и интеллектуальных зданий. ИБП линейки Masterys BC+ мощностью 100–160 кВА универсальны и могут использоваться для защиты электропитания самых разных систем.

Новые ИБП поддерживают стандартный режим двойного преобразования электроэнергии и экорежим. В первом режиме КПД систем линейки Masterys GP достигает 96,5%, а Masterys BC+ – 95%, в экорежиме этот показатель возрастает у Masterys GP до 99,2%, а у источников линейки BC+ – до 99%. Благодаря тому, что переключение между режимами занимает всего 2 мс, ИБП обеих линеек применимы в ЦОДах.

Задачи масштабирования и резервирования производитель предлагает решать с помощью параллельного подключения систем: таким образом можно подключать до шести ИБП.

Курс на локализацию производства

В ответ на меры государственной поддержки российских товаров некоторые зарубежные поставщики приняли решение о локализации своего производства в России.

Одной из первых стала компания Legrand. В 2016 г. на ее заводе в Ульяновске были запущены новые сборочные линии для выпуска моноблочных ИБП серии Keor T мощностью 10–120 кВА. В 2017 г. Legrand совместно с компанией «Инсистемс» представила проект производства ИБП моноблочной серии Keor T 10–120 кВА

во Владивостоке. Сегодня там проводятся сборка и выходной контроль качества систем ИБП мощностью до 120 кВА. Проверка продукции осуществляется более чем по 20 параметрам, включая соблюдение правильности сборки устройств, установки и проверки батарей, силового каркаса. При необходимости на заводе могут осуществляться калибровка отдельных узлов и общая настройка ИБП.

В 2017 г. Legrand представила в России однофазные онлайн-ИБП серии Daker DK Plus мощностью 1–10 кВА (в вертикальном исполнении и для установки в стойку), предназначенные для обеспечения бесперебойной работы серверных комнат в медицинских учреждениях и на промышленных объектах.

На сентябрь 2018 г. намечен запуск новой линейки ИБП серии Keor T EVO – трехфазных моноблочных онлайн-ИБП с двойным преобразованием и мощностью 10–20 кВА. Новые системы способны сами «выбирать» наиболее эффективный режим работы в зависимости от характеристик сети и гарантируют высокое качество электроэнергии на выходе с КПД до 96%.

По пути локализации пошла и GE Industrial Solutions, подписавшая в 2017 г. лицензионное соглашение с компанией «Абитех» о предоставлении последней права на сборку, тестирование и продажу источников бесперебойного питания GE на территории России.

Сегодня в портфеле российской компании несколько линеек ИБП, как производимых в рамках соглашения с GE, так и собственной разработки. Коньком «Абитеха» являются новые трехфазные системы серии KP33 мощностью 10–600 кВА. Все эти монолитные ИБП построены на IGBT-выпрямителях, имеют «широкое окно» входного напряжения (–65%...+20%), версии, предназначенные для работы с внутренними и с внешними АКБ, и поддерживают параллельную работу до восьми устройств. Есть в портфеле «Абитеха» и модульные ИБП серии MP 33 мощностью 25–600 кВА, которые в зависимости от потребностей заказчика могут строиться из силовых блоков 25 и 40 кВА.

Батарейная поддержка

Тренд 2017–2018 гг. – готовность литий-ионных батарей к использованию в мощных ИБП. По сравнению со свинцово-кислотными и никель-кадмиевыми аккумуляторами такие АКБ служат дольше, так что позволяют сэкономить на их замене. Вместе с тем капитальные вложения в литий-ионные батареи пока в несколько раз выше, чем в другие.

Первой батареи этого типа применила в мощных ИБП компания Schneider Electric, вскоре за ней потянулись Socomec, Delta Electronics, Eaton, Huawei и некоторые другие вендоры.

Не отстают от них в стремлении закрепиться в новом сегменте и производители АКБ. Так, компания Saft, известный поставщик батарейных систем для промышленного сектора, в ноябре 2017 г. представила новую линейку литий-ионных батарей Flex'ion (рис. 4), спроектированную специально для применения в ИБП высокой мощности, защищающих критически важную нагрузку. Безопасность и надежность эксплуатации батарейной системы обеспечивает проприетарная технология SLFP (Super Lithium Iron Phosphate – супер-литий-железо-фосфат).

Рис. 4. Система литий-ионных батарей Flex'ion

По сравнению с VRLA-батареями Flex'ion дают возможность уменьшить размеры батарейной системы в три раза по объему и в шесть раз по весу, что интересно для ЦОДов. Кроме того, у этих аккумуляторов более высокая удельная мощность и более широкий диапазон рабочих температур. Батареи Saft Flex'ion не требуют никакого периодического технического обслуживания, срок их службы превышает 20 лет. Эффективность цикла заряда-разряда приближается к 100%, что позволяет избежать дополнительных потерь энергии.

Каждая батарея Flex'ion может через PLC-интерфейс обмениваться информацией по наиболее распространенным протоколам с другими инженерными системами ЦОДа, а система мониторинга батарей Intelli-Connect работает даже при отключении зарядного устройства.

Контролируйте это

Все инновационные аппаратные решения новых источников бесперебойного питания поддержаны на программном уровне. Так, компания ABB предлагает в составе своих модульных ИБП интеллектуальные решения ABB Ability для их мониторинга с использованием облачных технологий передачи и хранения данных.

Источники бесперебойного питания Makelsan поддерживают коммуникационные интерфейсы и ПО, которые легко интегрируются в систе-

мы диспетчеризации и мониторинга объектов. В устройства могут быть встроены интерфейсные карты, поддерживающие все распространенные современные протоколы обмена данными.

Новые модели ИБП компании Powercom работают под управлением более мощных и «умных» процессоров, чем системы прошлых поколений. В ходе работы над ними изменилось ПО интерфейса, что упростило настройку, текущее обслуживание и мониторинг оборудования.

Системы мониторинга работы ИБП очень важны, поскольку повышают эффективность обслуживания, уменьшают показатель PUE и в конечном счете помогают клиентам оптимизировать операционные затраты, считают в компании Huawei. В портфеле вендора за решение всех этих задач «отвечает» система интеллектуального управления iPower.

В каждом силовом модуле ИБП Socomec есть плата управления, контроллер, а также стандартные (MODBUS RTU) и дополнительные («сухие контакты», MODBUS TCP, PROFIBUS) средства коммуникаций. Для мониторинга состояния оборудования и управления свертыванием нескольких операционных систем служит веб- и SNMP-интерфейс Net Vision, который подходит для «общения» и с высокопроизводительными компьютерными системами, и с электронным оборудованием.

В портфеле Eaton для усиления линейки устройств распределения электропитания появились блоки третьего поколения Eaton ePDU G3. Их специализированные версии способны измерять различные параметры, удаленно управлять питанием и перезагрузкой оборудования, а также работать вместе с программным обеспечением Intelligent Power Manager (IPM), которое служит для управления питанием физических и виртуальных серверов облачной инфраструктуры, а также для контроля состояния устройств и режимов их работы.

Это ПО просто масштабируется от уровня локальной сети с несколькими ИБП и ePDU до уровня корпоративных критических энергосистем и при необходимости интегрируется с VMware vCenter и SCVMM от Microsoft, позволяя повысить продуктивность работы и упростить техобслуживание.

Возможность не только контролировать состояние систем электропитания в ЦОДах, но и оказывать на них управляющее воздействие обеспечивает Smart PDU RPCM. С помощью этого «умного» модуля удаленного управления электропитанием, разработанного российской компанией RCNTEC, можно одновременно управлять розетками по сети передачи данных из любой точки планеты, защищать от короткого замыкания потребителей электропитания на каждом выводе, учитывать потребление электроэнергии на каждой розетке, диагностировать корректность подключения заземления, а также автоматизировать процесс включения «зависшего» оборудования.

Компания CyberPower в 2018 г. представила систему контроля и управления зарядом батарей (BMS), позволяющую обнаружить батарею, которая, судя по характеристикам, скоро выйдет из строя, и заблаговременно оповестить об этом сервисную службу. Кроме этого, BMS выравнивает заряд, не давая «слабым» батареям влиять на заряд соседних АКБ, тем самым значительно продлевая срок службы батарейного массива, повышая надежность ИБП и снижая издержки от внеплановой замены АКБ.

А для контроля самого разного оборудования электропитания, оснащенного SNMP-адаптером, в ЦОДах компания CyberPower предлагает комплексное решение – PowerPanel Enterprise. Это ПО может применяться самостоятельно или интегрироваться в SCADA-систему предприятия. С его помощью можно контролировать состояние устройств как в централизованной, так и в распределенной системе, и управлять ими.

Поскольку ПО глобальное, оно работает с оборудованием разных производителей, а количество подключенных устройств ограничивается только возможностями сервера. В режиме реального времени оно отображает состояние системы в целом и поэлементно. Группировка устройств позволяет получать информацию в удобном формате, а поэлементное информирование о внештатной работе любого из них дает возможность оперативно принимать меры. Кроме того, это ПО выполняет архивацию данных, на основе которых можно проводить анализ и разрабатывать эффективные алгоритмы управления.

Задел на будущее

Идя навстречу пожеланиям клиентов, производители мобилизовали интеллектуальные ресурсы своих инженеров для решения нетривиальной задачи: разработать надежные и эффективные ИБП, которые не требуют высоких капитальных вложений и операционных затрат или позволяют со временем компенсировать высокие CAPEX за счет низких OPEX. И, судя по характеристикам новых систем, им это удалось. Тем самым создан задел на будущее. При реализации концепции Fog Computing, предполагающей приближение вычислительных систем к управляемым ими инфраструктурам или процессам и использование многоуровневых облачных архитектур, потребуется множество новых периферийных дата-центров. А это значит, что спрос на надежные и недорогие ИБП будет только расти. ИКС

Пока крутится маховик…

Динамические ИБП сегодня претендуют на роль основного элемента систем бесперебойного гарантированного электропитания мега-ЦОДов. А некоторые их производители уже задумались о «захвате» объектов меньшей мощности.

Александр Барсков

Мы собрали и проанализировали аргументы поставщиков в пользу динамических систем. Сразу заметим, что сравнение «лоб в лоб» динамических ИБП и их статических «коллег» далеко не всегда корректно. Дело в том, что классический динамический ИБП – это, по сути, система бесперебойного гарантированного электропитания «все в одном». Защиту от кратковременных перебоев в подаче электричества в ней берет на себя маховик, а во время длительных перерывов подключается входящий в состав ДИБП дизель-генератор. Статический же ИБП (СИБП), укомплектованный аккумуляторными батареями (АКБ), отвечает только за бесперебойное снабжение нагрузки электричеством при кратковременных перебоях – как правило, АКБ способны «держать нагрузку» до 10 мин. Для гарантированного электроснабжения при длительных отключениях обычно устанавливают внешний дизель-генератор. И его надо всегда учитывать при сравнении ДИБП с СИБП.

Один из главных вопросов, возникающих при строительстве ЦОДа, связан с капитальными затратами. Согласно оценке Владислава Ротаня, директора по развитию бизнеса и продажам компании Piller, CAPEX решений на базе ДИБП становится равным капзатратам на СИБП, начиная с мощности нагрузки бесперебойного электропитания 1,5 МВт – если сопоставлять равнозначные комплексы энергоцентра «под ключ». При больших мощностях ДИБП позволяет получить выигрыш в капитальных затратах.

«Ахиллесова пята» СИБП

Слабым местом традиционных статических ИБП являются используемые ими свинцово-кислотные АКБ. Эти элементы очень чувствительны к температурному режиму: оптимальной для них считается температура +20–25°C, а превышение рекомендованной температуры на 10°C сокращает срок службы АКБ примерно в два раза. Значит, батарейные помещения необходимо оснащать системами кондиционирования воздуха, что увеличивает расходы и PUE. А ДИБП не требуют кондиционирования, поскольку способны работать в температурном диапазоне 0–50°C.

Впрочем, сейчас в комплекте со статическими ИБП все активнее применяют литий-ионные АКБ, которые менее критичны к температурным условиям. Кроме того, они легче, компактнее, имеют более долгий срок службы, поддерживают большее число циклов разряда и более быстрый заряд. Пока они остаются дороже свинцово-кислотных батарей, но при расчете TCO все чаще выигрывают у традиционных решений. Более широкое использование литий-ионных АКБ может лишить сторонников ДИБП многих аргументов «против СИБП». Более того, по прогнозу экспертов Schneider Electric, уже к 2020 г. при определенных параметрах ЦОДа батареи могут полностью вытеснить дизель-генераторы.

Но сегодня на рынке все же доминируют свинцово-кислотные АКБ. Помимо температурной «чувствительности» у них немало дру-

В большинстве ДИБП все главные элементы – синхронный генератор, накопитель и дизельный двигатель – собраны на одном валу

ДИБП в одном из крупнейших российских коммерческих ЦОДов

гих минусов. Например, медленный заряд, что может негативно сказаться на непрерывности электропитания в случае повторных отключений электроэнергии. «Аккумуляторные батареи восстанавливают заряд до 90% емкости в течение 6–12 ч. Это относится к случаям полного разряда батарей, что может произойти даже при кратковременных пропаданиях сети, когда выбираются бюджетные решения с временем резервирования нагрузки 5–10 мин. Время полного восстановления энергии на маховиках в ДИБП составляет всего 1–10 мин в зависимости от модели и конфигурации системы», – подчеркивает В. Ротань.

Надежность батарейных решений тоже далека от идеальной – по крайней мере об этом говорят поставщики ДИБП. Как отмечают эксперты компании Hitec, схема с батареями сложнее и содержит больше составных элементов, что снижает общую надежность схемы в целом. В. Ротань добавляет, что по сравнению с кинетическими накопителями АКБ обладают значительно более низким показателем MTBF (средним временем наработки на отказ). На практике это выражается в том, что уже через два-три года эксплуатации в батареях ИБП с АКБ выявляются неисправные элементы, требующие замены.

Поставщики ДИБП также критикуют системы на базе СИБП за большую занимаемую площадь. По данным Hitec, таким системам требуется на 40–60% больше места, чем решениям на базе ДИБП. Подобные цифры приводят и другие поставщики ДИБП. «Применение динамических дизель-роторных ИБП позволяет существенно (до 60%) уменьшить площадь, необходимую для энергоцентра. Этот эффект проявляется начиная с мощности 500 кВт, и выигрыш тем больше, чем выше мощность объекта», – делится своими данными В. Ротань.

А если мегаватт не нужен?

Как уже говорилось, даже по оценке самих поставщиков ДИБП, выбор в пользу их решений дает выигрыш по CAPEX при мощности 1,5 МВт и выше. А что для объектов меньшей мощности?

У динамических решений есть ряд важных свойств, которые делают их применение оправданным и на небольших объектах. Это высокая перегрузочная способность и возможность работы с нагрузками разного электрического характера. «ДИБП – универсальное устройство, оно используется не только в индустрии ЦОДов, но и в машиностроении, химическом производстве, фармацевтике, добыче и переработке энергоносителей, – объясняет Александр Зайцев, генеральный директор российского офиса компании Euro-Diesel. – В ряде проектов ДИБП невысокой мощности востребованы для защиты технологических линий, которые нельзя останавливать, пока идет рабочий процесс. В подобных проектах задействовать СИБП можно только с двух- или трехкратным увеличением мощности. Есть проекты, где СИБП со всей инфраструктурой и ДГУ просто невозможно разместить, здесь также выигрывают ДИБП невысокой мощности – за счет своей компактности».

Высокая перегрузочная способность обеспечивает лучшее поведение систем ДИБП при сценариях коротких замыканий (КЗ). В качестве примера В. Ротань приводит характеристики изделий Piller: они имеют возможность поставлять ток при КЗ до $16\times I_{nom}$ на стороне нагрузки, сохраняя при этом выходное напряжение в заданных пределах, скажем, не хуже –30%. В то же время, по его данным, установки СИБП, оснащенные IGBT-транзисторами, способны обеспечивать поставку тока КЗ в нагрузку лишь до $5\times I_{nom}$.

За рубежом ДИБП небольшой мощности часто применяются не только на промышленных объектах, но и для защиты ответственной нагрузки в госпиталях и больницах (в частности, для поддержки системы электроснабжения реанимации и операционных блоков). Пример многолетнего успешного использования ДИБП на нецодовском объекте приводит Сергей Соколов, коммерческий директор компании АКСИ: ДИБП Hitzinger мощностью 150 кВА (именно с такой мощности начинается модельный ряд этого производителя) установлен в Тендерном комитете Правительства Москвы для поддержания системы электроснабжения, включая систему торгов. «Как показывают расчеты с учетом срока службы ДИБП по сравнению с классической схемой построения СБГЭ, экономический эф-

фект от внедрения достигается даже на машинах небольшой мощности», – утверждает специалист АКСИ.

Но вернемся к ЦОДам, где, к счастью, высокой перегрузочной способности, как правило, не требуется. Есть ли варианты ДИБП, которые способны конкурировать по стоимости со статическими ИБП при мощностях менее 1 МВт?

Оказывается, такие варианты есть: это гибридные решения, в которых используются не все элементы классического ДИБП. Скажем, в линейке продукции Piller подобное оборудование представлено ИБП серии CleanSource Active Power мощностью 225 и 625 кВт, в которых устройством накопления энергии является маховик (как в классических ДИБП), а выпрямитель и инвертор выполнены на базе IGBT-транзисторов (как в статических ИБП). Как утверждает В. Ротань, такие гибриды сравнимы по стоимости с СИБП для систем до 1 МВт. В России ИБП CleanSource ActivePower установлены, например, в ЦОДах «Яндекса» – всего 32 устройства CleanSource HD625.

ДИБП поэлементно

Практически все поставщики ДИБП предлагают варианты использования этих систем без отдельных элементов или, наоборот, отдельных элементов ДИБП с другими системами. Правда, мы не получили каких-либо данных об экономических преимуществах их применения на субмегаваттных объектах.

Так, у компании Hitec есть решение без дизельного двигателя – PowerKEM. Такие установки имеют мощность 400–2000 кВА и, как утверждают в Hitec, подходят для использования на небольших объектах, позволяя получить все преимущества больших машин. В компании также отмечают, что кинетический накопитель PowerKEM можно интегрировать в существующую систему электроснабжения. Решения без дизельного двигателя пока не очень распространены в России, но на мировом рынке данное оборудование пользуется популярностью.

Euro-Diesel тоже предлагает решение без дизельного двигателя: данная установка за счет накопления кинетической энергии может питать критическую нагрузку в течение нескольких секунд, которые требуются для переключения электрических вводов или запуска сторонней ДГУ. Однако, комментируя возможность использования такого решения, А. Зайцев делает ряд важных замечаний. В частности, он предупреждает, что при набросе нагрузки на ДГУ при переходе с ДИБП (маховика) дизель-генератор может «завалиться» по частоте и/или «просесть» по напряжению, что повлечет обратный переход на ДИБП, в котором уже не останется запаса кинетической энергии, и может последовать полное отключение нагрузки. Важно также понимать, что бездизельный ДИБП «не несет ответственности» за пуск ДГУ, а если тот не запустится, то произойдет аварийное отключение нагрузки.

Некоторые особенности конструкции оборудования Hitzinger позволяют задействовать дизель-генератор и альтернатор в качестве аварийного источника электроснабжения при проведении технического обслуживания КИН-модуля (кинетического накопителя). Также в линейке продуктов Hitzinger имеются так называемый кондиционер питания, используемый совместно с газопоршневыми ДГУ, и система, разработанная для насосных станций, которая присоединяется к валу насосов.

Пожалуй, наибольшее число вариантов применения отдельных элементов ДИБП предлагает Piller. Выше уже упоминалась возможность использования маховика совместно с

Проекты ДИБП в России и СНГ

- Euro-Diesel: в России запущено в работу 15 установок ДИБП общей мощностью 22 МВА, шесть установок суммарной мощностью 12 МВА находятся в стадии монтажа (запуск – осенью 2018 г.).
- Hitec: в России 109 установок общей мощностью 212 МВА. Одна установка в Казахстане.
- Hitzinger: ДИБП установлены в четырех ЦОДах в России.
- Piller: по состоянию на июнь 2018 г. в России и Казахстане работают 45 установок Piller (включая ДИБП ActivePower) общей мощностью 41,8 МВт.

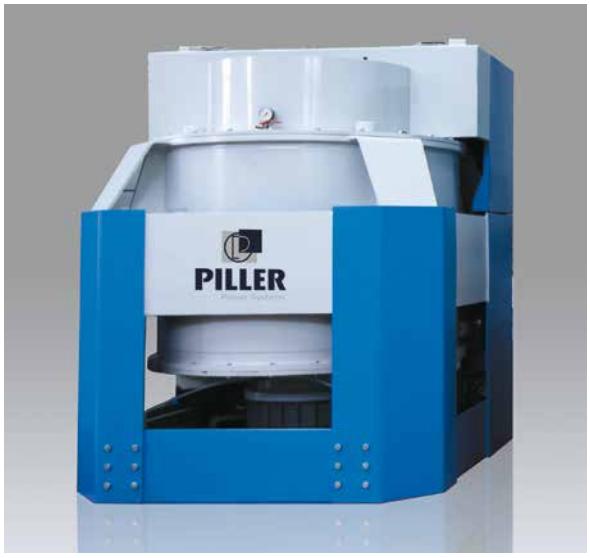
Замена подшипника на ДИБП 1 МВт через 12 лет эксплуатации на ММВБ

транзисторными выпрямителем и инвертором. Есть и обратный вариант: установки UBT+ позволяют в качестве устройств накопления энергии задействовать АКБ (можно и маховик). Они также предусматривают подключение дизельных двигателей в качестве внешних устройств. ДГУ может подключаться как со стороны сети («сверху», классический подход), так и «снизу» – на стороне нагрузки – в случае установки маховика. Для данного решения теоретически пригодна любая ДГУ, в том числе уже работающая на объекте заказчика.

В числе наиболее интересных объектов, на которых используются устройства UBT+, – ЦОДы NEXT DC (Австралия) и Telehouse (Германия). На них вариант включения ДГУ «снизу» реализован с применением конфигурации IP Bus (изолированно-параллельная шина). ЦОД NEXT DC с IP Bus был сертифицирован в сентябре 2017 г. по уровню Tier IV. При этом топология решения IP Bus предусматривает резервирование N + 1 (или N + 2), что обеспечивает более высокую энергоэффективность по сравнению со схемой 2N. Еще один интересный пример: реализация систем UBT+ и UBTD+ с АКБ, в том числе литий-ионными. В ноябре 2016 г. южнокорейский Hana Bank построил ЦОД с мощностью ИТ-нагрузки 8,5 МВт, установив в нем 10 устройств UBTD (1500 кВА) с литий-ионными АКБ в конфигурации IP Bus. Как утверждает представитель Piller, это первая в мире реализация ДИБП с литий-ионными батареями.

Когда приходит время менять подшипник

Приводя аргументы в пользу ДИБП, их поставщики подчеркивают, что срок капитального ремонта этого оборудования (в первую очередь замены подшипников) наступает только через 10 и более лет эксплуатации. За это время владельцам объектов со статическими ИБП приходится по несколько раз менять АКБ, что во многом объясняет преимущества ДИБП при расчете OPEX с горизонтом планирования более 10 лет.



Кинетический накопитель (маховик) Piller PB60+, способный обеспечить автономное питание нагрузки 1 МВт более 60 с

Однако, по имеющимся у «ИКС-Медиа» данным, на практике замена подшипника может потребоваться и раньше. Как это обстоятельство комментируют поставщики?

Как нам сообщили в Hitec, в зависимости от условий эксплуатации и обслуживания замена подшипника может потребоваться как раньше, так и позже, чем через 10 лет. Системы мониторинга вибрации и температуры подшипников, которые входят в состав ДИБП Hitec, позволяют проводить ремонт, исходя из реального состояния подшипников, а не по наработке. По данным Hitec, стоимость капитального ремонта ДИБП сопоставима со стоимостью замены батарей при использовании статического ИБП.

В случае с ДИБП Euro-Diesel, как утверждают в компании, при своевременном выполнении регламентных работ срок в 10 лет выдерживается полностью. «Например, в лондонском дата-центре Global Switch поэтапно были установлены 26 ДИБП Euro-Diesel, часть из которых уже проработала более 10 лет. Заказчик ведет планирование по выводу ДИБП для капитального обслуживания, соответственно установки продолжают работать», – рассказывает А. Зайцев. При этом он отмечает, что затраты на такое обслуживание значительно ниже, чем расходы на замену парка аккумуляторных батарей СИБП эквивалентной мощности.

«Действительно, подшипники генератора меняются после 10 лет эксплуатации, но часто умалчивают о подшипниках КИН-модуля, замена которых производится после пяти-семи лет. У многих производителей замена этих подшипников совмещается с техобслуживанием КИН-модуля, поэтому они не раскрывают детали», – поясняет С. Соколов (АКСИ). По его утверждению, замена подшипников в устройствах серии NBDD компании Hitzinger (модели с маховиками мощностью от 150 до 1250 кВА) производится только после 10 и более лет эксплуатации.

«Стоимость замены подшипников некритична по сравнению со стоимостью самого оборудования и складывается из двух основных частей: стоимости подшипников и стоимости нормо-часа, – продолжает специалист АКСИ. – У нашей компании есть опыт замены подшипников генератора ДИБП мощностью 1 МВА после почти 12-летней эксплуатации в России. Это непростая процедура, требующая участия квалифицированных обученных специалистов».

Говоря о замене подшипников в ДИБП, В. Ро-

тань (Piller) обращает внимание на конструктивные особенности таких устройств. Большинство представленных на рынке ДИБП (производства Hitec, Euro-Diesel, Hitzinger) имеют горизонтальное расположение всех рабочих узлов системы (мотор-генератор, кинетический накопитель, дизельный двигатель на одном общем валу). В подобных системах подшипники испытывают двойную нагрузку: от вращения валов и от силы гравитационного воздействия массы роторов, которая направлена вниз. Кроме того, отвод тепла от внутренних подшипников в таких ИБП затруднен. Все это, считает В. Ротань, приводит к тому, что капитальный ремонт требуется уже через пять-шесть лет эксплуатации.

ДИБП Piller имеют принципиально иную конструкцию: кинетический накопитель связан с мотор-генератором электрической, а не механической связью – через тиристорный конвертор, – и имеет вертикальную конструкцию. Ротор маховика вращается на двух подшипниках, верхнем и нижнем. При этом подшипники работают в разгруженном режиме за счет управляемого электромагнитного компенсатора, установленного сверху. Например, в накопителе PB21 при массе ротора порядка 2,5 т на подшипники по вертикальной оси воздействует масса не более 50 кг. Все это обеспечивает ресурс работы подшипников 11–12 лет. На выполнение ремонта ДИБП такой конструкции требуется не более 6 ч, производится он непосредственно на объекте, а в качестве подъемного устройства используется только домкрат.

Развитие рынка и технологий

Развитие систем ДИБП, по мнению А. Зайцева, будет направлено на повышение эффективности, сокращение количества операций и времени обслуживания и исключение влияния человеческого фактора на работоспособность систем. Он приводит несколько примеров технических решений, уменьшающих влияние человеческого фактора. Так, у Euro-Diesel существуют решения с автоматической смазкой подшипников, при эксплуатации которых обслуживающий персонал контролирует уровень необходимой смазки в резервуаре и работу данной системы, но не осуществляет собственно смазку подшипников – это делает автоматика. Другой пример – использование бесщеточного возбуждения электрических машин системы ДИБП (щетки – дополнительный расходный материал). Нагрузку на службу эксплуатации снижает и применение необслуживаемого электромагнитного сцепления, простого и надежного элемента, который не требует столь пристального контроля и обслуживания, как механические аналоги.

Панель управления ДИБП, установленного в одном из коммерческих ЦОД в Москве

Технологии и рынок ДИБП следуют за трендами рынка ЦОДов. А в области ЦОДостроения отчетливо проявляются такие тенденции, как повышение рабочей температуры воздуха в серверных залах и рост числа проектов создания мегаЦОДов (Hyper Scale DC) с одновременным повышением требований к сокращению капитальных затрат, повышению энергоэффективности и снижению вредного воздействия на окружающую среду. Как указывает В. Ротань, техника ДИБП в эти тенденции вписывается отлично: ДИБП без аккумуляторов способны работать при температурах до 50°C без кондиционирования, они дешевле, чем СИБП с АКБ (при мощностях от 1,5–2 МВт), имеют более высокий КПД даже при низких уровнях нагрузки (30–40%) и не требуют утилизации АКБ.

Еще одна важная тенденция индустрии ЦОДов – развитие пограничных вычислений (Edge Computing). Как уже отмечалось, ДИБП более выгодны для мегаваттных проектов. Но гибридные системы, в которых маховики используются в качестве устройства накопления энергии, могут оказаться вполне востребованными и в небольших Edge-ЦОДах.

В целом, по оценкам «ИКС-Медиа», суммарная емкость ДИБП, уже установленных в ЦОДах в России, составляет порядка 300 МВт. Серьезным конкурентом таких ИБП являются набирающие популярность литий-ионные аккумуляторы. Кроме того, возможность оперативно перекинуть ИТ-нагрузку в другой ЦОД снижает потребность в долгосрочных системах резервного энергоснабжения (читай – ДГУ). Вместе с тем маховики выглядят перспективным средством сглаживания кратковременных перебоев электропитания. Поэтому гибридные системы ждет большое будущее, что показывают, в частности, инновационные системы электропитания в ЦОДах «Яндекса». ИКС

«От нового игрока всегда ждут выгодных предложений»

Светлана Ниязова

В 2018 г. на карте коммерческих центров обработки данных России появился новый объект. ЦОД GreenBushDC, рассчитанный на общую мощность 21 МВА и размещение 2280 стоек, – один из крупнейших в стране. Об особенностях ЦОДа и общей ситуации на рынке рассказывает Светлана Ниязова, генеральный директор ООО «ГДЦ ЭНЕРДЖИ ГРУПП», работающего под брендом GreenBushDC.

– Как вы видите общую ситуацию на российском рынке коммерческих ЦОДов? Какие категории заказчиков в первую очередь заинтересованы в услугах GreenBushDC?

– Данные аналитиков iKS-Consulting, постоянно отслеживающих ситуацию на рынке, свидетельствуют о его стабильном росте. Этому способствует интерес заказчиков к модели аутсорсинга при одновременном повышении уровня доверия к КЦОДам. Государственные инициативы, такие как принятие закона о хранении персональных данных на территории России и программы «Цифровая экономика РФ», также стимулируют развитие рынка.

При этом хочу отметить, что на данный момент активность заказчиков невысока. Основные наши потенциальные клиенты – те, кто развивает электронные сервисы. Такие компании и организации, как правило, уже пользуются услугами внешних ЦОДов и заинтересованы в масштабировании и резервировании своих мощностей. При выходе нового игрока на рынок заказчики всегда надеются получить у него более гибкие, выгодные условия.

Если говорить об отраслевой специфике, то интерес к услугам КЦОДов в первую очередь проявляют банковский сектор и ритейл.

– Насколько ЦОДу GreenBushDC в качестве клиентов интересны майнеры?

– Мы с большим вниманием относимся ко всем категориям обращающихся к нам клиентов, но надо понимать, что ЦОДы уровня Tier III чрезмерно дороги для майнеров. Их не интересуют вопросы сертификации инженерных систем, основной критерий – стоимость электричества. В этом году у меня были встречи с несколькими владельцами больших ферм, но экономический расчет показал, что рентабельность сотрудничества с ними для нас нулевая.

Следует учитывать и то, что курс криптовалют имеет тенденцию к снижению, а стоимость электроэнергии нет. Возможно, когда курс пойдет вверх, ситуация поменяется. Если помимо стоимости электричества майнеры будут готовы оплачивать еще и высокий уровень надежности ЦОДа, мы будем рады сотрудничать с ними.

Впрочем, есть еще один вариант возможного сотрудничества с майнерами. Их оборудование может использоваться как временная нагрузка для проверки качества работы службы эксплуатации. Может получиться хорошая опытная площадка для тестирования новых сервисов и процедур с минимальным риском.

– Вы упомянули программу «Цифровая экономика». Как ее реализация скажется на индустрии КЦОДов?

– Эта программа предусматривает, в частности, перевод государственных информационных систем в профессиональные высоконадежные ЦОДы. Идея очень хорошая, ее реализация позитивно повлияет на рынок и придаст ему мощный импульс для дальнейшего развития. Мы готовы конкурировать за размещения ИС государственных структур. Главное, чтобы при выборе площадки проводились открытые тендеры без монополизма и демпинга со стороны государственных провайдеров.

Надо понимать, что построить и сертифицировать объект уровня Tier III – это очень непростая задача как в финансовом, так и в техническом плане. Практика показывает, что коммерческие организации строят быстрее, сертифицируют быстрее, во многих вопросах они более оперативны. Поэтому коммерческие ЦОДы могут стать эффективными площадками для размещения государственных ИТ-ресурсов.

– Традиционно большинство коммерческих ЦОДов в Москве строились в пределах МКАД. ЦОД GreenBushDC находится за МКАД. В чем преимущества такого расположения?

– У многих российских заказчиков имеется стереотип о том, что КЦОД должен находиться в центре города. Это, в общем, противоречит мировой практике – с учетом серьезных ограничений по площади и энергоресурсам, а также проблем с размещением внешнего инженерного оборудования. Наконец, услуги такого КЦОДа существенно дороже.

ЦОД GreenBushDC находится в административном округе Зеленоград в особой экономической зоне г. Москвы «Технополис Москва». Объект характеризуется отличной транспортной доступностью: проезд на автомобиле удобен по Ленинградскому и Пятницкому шоссе, наличие платной трассы гарантирует возможность избежать пробок. Кроме того, Зеленоград – это наукоград,

в нем проживают много специалистов по ИТ и инженерным системам, мечтающих работать рядом с домом. Это позволяет нам получить высококвалифицированный персонал, потратив меньше средств, чем в случае, если бы ЦОД находился в пределах МКАД.

Пожалуй, самое главное: ООО «ГДЦ ЭНЕРДЖИ ГРУПП» – резидент особой экономической зоны города Москвы. Данный статус дает нам существенные экономические преимущества: нулевые таможенные пошлины и нулевой НДС на ввозимое на территорию компании импортное оборудование, пониженную ставку на прибыль, льготы по налогам на фонд оплаты труда, налогу на имущество. Например, инженерные системы обошлись нам значительно дешевле, чем аналогичное оборудование для ЦОДа за пределами ОЭЗ. Все это позволяет значительно снизить себестоимость услуг, что, в свою очередь, положительно влияет на формирование цены наших предложений.

– В ЦОДе GreenBushDC используются энергоэффективные инженерные системы, в частности, динамические ИБП и адиабатические системы охлаждения. Ставили ли вы изначально целью построить «зеленый» ЦОД? Или все дело в экономике?

– Еще на стадии утверждения концепции ЦОДа мы просчитывали совокупную стоимость владения (ТСО) с 10-летним горизонтом планирования. И оказалось, что энергоэффективные решения более выгодны. Да, при заключении контрактов на поставку они несколько дороже, но при хорошей загрузке ЦОДа окупят себя достаточно быстро. Мы на это рассчитываем. Ну и, конечно, использование самых современных «зеленых» технологий – дополнительный плюс к репутации ЦОДа, который, надеюсь, оценят наши заказчики.

– Вы начали с базовой услуги colocation. Какие тенденции вы видите в области предоставления таких услуг?

– Некоторые заказчики заинтересованы в заключении договоров не на сервисы, а на долгосрочную аренду выделенных машзалов. Мы будем предоставлять нашим клиентам такую возможность. Причем речь не идет об обязательном выделении целого зала, заказчиков вполне устраивают обычные выгородки, но с подготовкой техплана и регистрацией права аренды на образованную часть помещения с указанием отдельного кадастрового номера.

Важна для заказчиков и помощь в процессе перевода ИТ-инфраструктуры в коммерческий ЦОД. Мы готовы оказывать такую помощь, а также предоставлять арендные каникулы при переезде. За время развертывания, настройки и тестирования ИТ-систем арендная плата может не взиматься. Эти условия, конечно, зависят от специфики требований конкретного заказчика и продолжительности периода миграции.

– Как планируется развивать облачные сервисы: будете сами внедрять облачные платформы или просто предоставлять площади под решения, которые будут развертывать облачные провайдеры?

– Оба варианта. Сторонних облачных провайдеров мы рассматриваем в качестве потенциальных клиентов услуги

colocation. Кроме того, у нас есть собственная облачная платформа, которая сейчас находится в стадии тестирования. Решение построено на платформе OpenStack и может быть использовано для создания клиентских инфраструктурных облачных сервисов и облачных хранилищ, как публичных, так и частных.

– Как вы оцениваете перспективы GreenBushDC на рынке?

– Итоги 2017 г. отражают в целом позитивное развитие отечественного рынка коммерческих дата-центров и преодоление им сложного этапа, обусловленного глобальным финансовым кризисом. В наиболее выигрышном положении – как в плане гибкости по отношению к клиентам, так и с точки зрения собственной жизнеспособности – оказались большие, сертифицированные дата-центры, которые располагают ресурсами для формирования конкурентоспособных предложений. Уверена, мы займем достойную нишу на этом рынке.

Говорим 5G, подразумеваем транспортные сети

Андрей Абрамов, независимый эксперт

Построение сетей 5G потребует серьезного пересмотра принципов организации транспортного домена сетей радиодоступа.

К централизованной архитектуре RAN

До недавнего времени развитие подсистемы радиодоступа (Radio Access Network, RAN) определялось поступательным внедрением радиоинтерфейсов для новых мобильных стандартов и расширением ассортимента радиооборудования для соответствующих частотных диапазонов на основе распределенной архитектуры (рис. 1, а). Но требования к емкости, гибкости и эффективности сетей 5G настолько масштабны, что предполагают пересмотр существующих функциональных и топологических принципов построения сети RAN. Отправными точками для такого пересмотра являются неэффективность протокола общего открытого радиоинтерфейса (Common Public Radio Interface, CPRI) с точки зрения транспорта и переход к централизованной архитектуре.

Протокол CPRI используется между радиомодулем выносного блока (RRH) и цифровым модулем (BBU) базовой станции. Он предполагает реализацию на транспортном канале принципа D-RoF (Digital Radio over Fiber), при соблюдении которого QAM-модулированный радиосигнал передается между BBU и RRH по двум несущим в оцифрованном виде (IQ data). Поэтому, в частности, при работе в рамках технологии LTE с шириной канала 20 МГц, обеспечивающей скорость до 150 Мбит/с, для транспорта CPRI необходима полоса 2,5 Гбит/с. При внедрении технологий 5G с ростом скорости требования к полосе в транспортной сети возрастают многократно. Кроме того, CPRI предполагает наличие отдельного соединения для каждой антенны. А это означает, что при внедрении в сетях 5G решения Massive MIMO, например для MIMO 64 x 64, будут нужны 384 отдельных волокна или DWDM-несущие.

Как полагает большинство экспертов, для 5G RAN оптимальной является централизованная архитектура (рис. 1, б). При этом наилучшим вариантом станет построение BBU с использованием технологий виртуализации и облачных вычислений.

Централизованная архитектура RAN (Centralized RAN, C-RAN) предполагает, что BBU нескольких базовых станций объединены в хабы и расположены на одной площадке. Это позволяет применять более эффективные алгоритмы цифровой обработки, которые значительно увеличивают емкость сети за счет уменьшения интерференции и более оптимального использования радиоресурсов. Кроме того, сокращается число единиц вспомогательного оборудования (кондиционеры, маршрутизаторы и т.д.), поскольку уменьшается количество площадок их размещения. Соответственно, снижаются капитальные затраты.

Если при строительстве хабов BBU задействовать технологии виртуализации и облачных вычислений, то стоимость решения можно снизить благодаря объединению вычислительных мощностей в пулы и повышению КПД их использования из-за неравномерной нагрузки в сети. Заметим, что сети RAN, построенные на основе указанных технологий, часто называют C-RAN, под «C» подразумевая «Cloud».

Смягчение требований к полосе на транспортном канале между RRH и BBU достигается использованием «улучшенного» протокола CPRI (enhanced CPRI, eCPRI). Ожидается, что его внедрение благодаря переносу части функций циф-

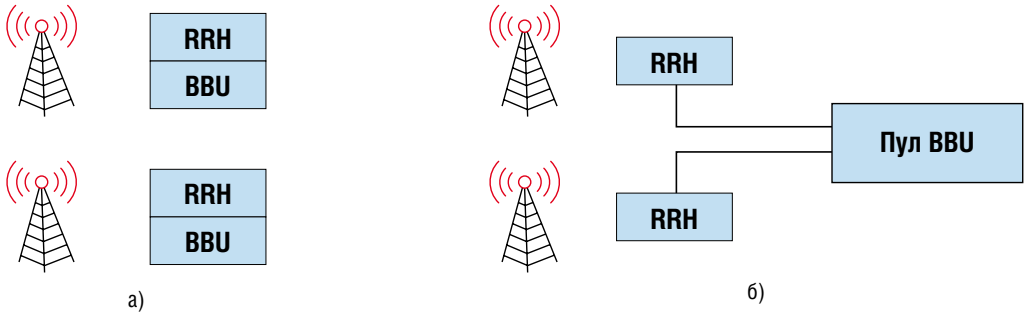


Рис. 1. Распределенная (а) и централизованная (б) архитектуры RAN

ровой обработки в RRH (new RRH/BBU functional split) позволит снизить требования к полосе пропускания более чем в 10 раз. Коммерческое применение новых аппаратных платформ BBU и RRH с поддержкой eCPRI уже началось.

Новый статус Fronthaul

Следует подчеркнуть, что существующие решения для транспорта между RRH и BBU не могут быть автоматически перенесены на новую централизованную архитектуру RAN. До недавнего времени термин Fronthaul, обозначающий транспортный домен между RRH и BBU, использовался редко, поскольку он рассматривался как составная часть базовой станции (успешные пилотные проекты использования для CPRI-транспорта решений сторонних поставщиков известны, однако коммерческого распространения такие системы не получили). С внедрением централизованной архитектуры RAN и 5G ситуация в корне меняется.

Во-первых, к Fronthaul предъявляются новые функциональные требования: более низкие задержки, ограничения на допустимый джиттер, особенности синхронизации, поддержка новых протоколов (работающих поверх транспортного уровня), масштабирование полосы под конкретную пользовательскую услугу, поддержка выделенных виртуальных сетей с требуемой функциональностью на единой сетевой инфраструктуре (Network Slicing) и т.д.

Во-вторых, централизация топологии позволяет повысить загрузку транспортных каналов за счет их агрегации. Появление функций цифровой обработки в модулях RRH открывает возможности использования пакетных Ethernet-сетей.

В-третьих, ужесточается требование экономической эффективности внедрения микро- и пикосот. До сих пор применение таких сот в мобильной связи носит нишевой характер в силу более высокой себестоимости трафика. Понятно, что микро- и пикосоты дают в среднем меньше дохода вследствие меньшего покрытия. Добиться же пропорционального уменьшению доходов снижения стоимости микросот до сих пор не удалось (рис. 2). Однако в силу нишевого характера внедрения на результирующую экономическую эффективность это влияния не оказывает.

Отсутствие эластичности стоимости транспортных решений – одна из основных проблем экономики малых сот. В 5G архитектура малых сот является основной, и от того, удастся ли обеспечить коммерческую эффективность их использования, зависит будущее бизнеса мобильных операторов.

Рассмотрим подробнее структуру стоимости системы 5G RAN. Подсистема Fronthaul может быть построена разными способами: например,

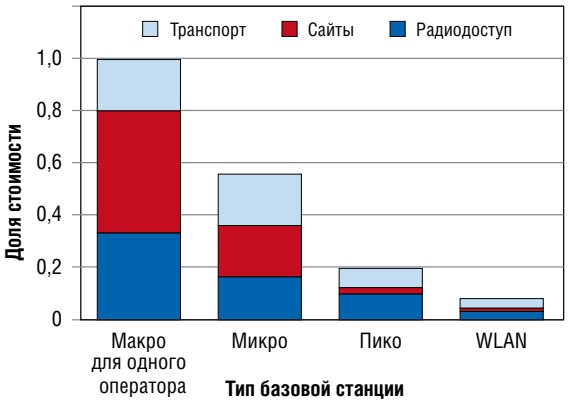


Рис. 2. Структура относительной стоимости различных типов базовых станций

По материалам Academic Press Library in Mobile and Wireless Communications (2016, Chapter 18)

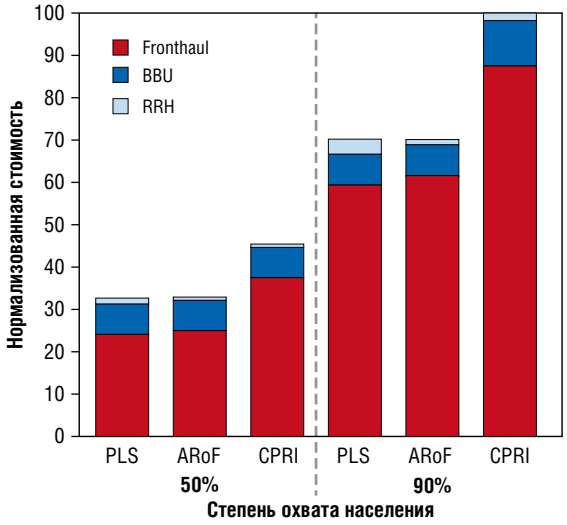


Рис. 3. Структура стоимости внедрения 5G RAN

Источник: Melbourne Networked Society Institute, 2017

с использованием CPRI или двух различных вариантов распределения функций цифровой обработки сигнала между RRH и BBU. Вариант PLS (Physical Layer Split) предполагает перенос в RRH функций цифровой обработки для MIMO, а вариант ARoF (Analog Radio over Fiber), напротив, – перенос всех функций цифровой обработки в BBU (в том числе функции аналого-цифрового преобразования и цифровых функций предискажения сигнала для максимизации линейного диапазона усиления). Расчеты стоимости сети 5G RAN с учетом инсталляционных работ, сделанные для разной степени охвата населения (50% и 90%), показывают (рис. 3), что на долю Fronthaul приходится более 70% всех затрат. Следовательно, Fronthaul не может рассматриваться как «составная часть» базовой станции и является в централизованной сети 5G RAN самостоятельным ключевым сетевым доменом.

Стандартизация обеспечит независимость от поставщиков

Здесь следует вспомнить о зависимости операторов от существующих поставщиков RAN при

внедрении 5G. Стремление операторов к свободному выбору поставщика базовых станций 5G наталкивается на отсутствие стандартов на уровне протоколов RAN при взаимном управлении радиоресурсами базовых станций LTE и 5G. В конце 2017 г. был согласован вариант неавтономной (non-standalone) архитектуры 5G (так называемый вариант Option 3 в классификации 3GPP). Он фактически свел задачу внедрения 5G к «расширению» существующей базовой станции LTE. Это решение, оптимальное в условиях отсутствия стандартов для внедрения 5G, может быть реализовано только существующими поставщиками инфраструктуры сетей LTE в соответствующих регионах.

Очевидно, традиционные поставщики RAN рассматривают домен 5G Fronthaul как часть базовой станции, пытаясь выстроить вертикально интегрированное закрытое решение и тем самым закрепить свое монопольное положение на радиосети оператора.

Однако в отличие от взаимодействия «LTE – 5G» на уровне протоколов RAN, где инициатива в формировании политики технологического развития отдана в руки малого числа производителей, развитием транспортной сети занимаются значительно больше игроков, которые становятся все активнее. На сегодняшний день существует понимание, что целевая архитектура транспортной сети 5G является самостоятельным доменом (так называемым Xhaul), который интегрирует функции Fronthaul (транспорт между центральным узлом и радиосайтами) и Backhaul (транспорт между узлами опорной сети). Домен Xhaul, включающий в себя уровни управления (control plane) и пользовательского трафика (user plane), взаимодействует с другими доменами сети по сервисной модели. Работы по стандартизации ведутся, в том числе в рамках международных проектов (например, программы 5G-PPP Horizon 2020 с участием операторов и производителей транспортной инфраструктуры).

С внедрением 5G и централизованной архитектуры RAN система Fronthaul становится самостоятельным сетевым доменом, имеющим ключевое значение для будущего развития мобильного бизнеса. У операторов есть все возможности добиться максимальной экономической эффективности строительства транспортной сети 5G за счет централизации функций BBU и использования технологий виртуализации, а стандартизация транспортных решений между RRH и BBU позволит избавиться от монопольного доминирования небольшого числа производителей при гарантии мультивендорной совместимости и сохранении единой концепции развития сети. ИКС

HDD и SSD: будущее систем хранения

Флеш-память, производство которой переживает революцию, все чаще применяется в устройствах разных классов, но и жесткие диски продолжают совершенствоваться. Какую роль в отрасли хранения данных будут играть оба типа накопителей?

Сергей Орлов, независимый эксперт

С каждым годом объем обрабатываемых и хранимых данных увеличивается. Так, IDC прогнозирует, что общее количество создаваемых в мире данных с 2018 по 2025 гг. вырастет с примерно 33 до 160 зеттабайт. Поэтому необходимо также постоянно наращивать производительность ИТ-систем и емкость хранилищ. Таким требованиям отвечают две технологии: твердотельные накопители (SSD) с высокой скоростью доступа к данным и емкие жесткие диски (HDD). Если для одних приложений лучше подойдет SSD, то для других традиционные жесткие диски остаются предпочтительным вариантом. И, похоже, такое положение дел сохранится в обозримом будущем.

HDD против SSD

В новые ноутбуки, исключая, может быть, самые дешевые модели, уже давно устанавливают накопители SSD (рис. 1). Их преимущества очевидны: они компактнее, чем жесткий диск, быстрее, тише, долговечнее, не подвержены отказам из-за магнитных полей и ударов. Ударостойкость SSD-накопителей как в рабочем, так и в нерабочем состоянии достигает 1500 г, в то время как HDD в нерабочем состоянии могут выдержать удар силой 350 г, а при работе – всего 55 г. SSD также характеризуются значительно меньшей задержкой (латентностью) и малым временем доступа к данным. Но они заметно дороже. Сегодня типичная цена 2,5-дюймового накопителя SSD на 512 Гбайт – $140–170, в то время как 3,5-дюймовый накопитель HDD емкостью 512 Гбайт обойдется в $44–65.

Разница довольно существенная, но поскольку SSD-накопитель помогает сделать ноутбук легче и устойчивее к неизбежным ударам, обеспечивает более быструю загрузку и запуск приложений, а также увеличивает скорость работы с большими файлами, он своих денег стоит. Высокая скорость работы с данными важна и для настольных ПК, поэтому их тоже все чаще оснащают SSD.

Центры обработки данных – совсем другая история. Наиболее важные параметры хранения данных в ЦОДе – надежность, плотность хранения и стоимость. SSD сильны в первых двух областях, но в последней пока проигрывают.

Накопители с более высокой емкостью обеспечивают большую плотность хранения, уменьшают расходы за счет менее частого обслуживания и снижения энергопотребления. В настоящее время в ЦОДах используются диски емкостью до 10–12 Тбайт. SSD сопоставимой емкости обойдутся примерно в $1000 за 1 Тбайт, т.е. значительно дороже соответствующего жесткого диска. Стоимость SSD еще не достигла того уровня, который сделал бы их применение безусловно выгодным с учетом предоставляемых преимуществ, поэтому можно предположить, что в ближайшем будущем в качестве основных накопителей будут использоваться жесткие диски. По данным IDC, более 90% поставок накопителей корпоративного класса сегодня приходится на HDD. К 2025 г. доля SSD составит почти 20% объема поставок (рис. 2).

Производители ожидают, что в обозримой перспективе жесткие диски и твердотельные накопители будут сосуществовать во всех областях – дома, в системах корпоративного класса и в ЦОДах. При этом клиенты будут выбирать, какие именно технологии и продукты лучше всего подходят для тех или иных задач.

По мере роста объемов продаж HDD и SSD будет увеличиваться емкость накопителей обоих типов. Поскольку для многих приложений ис-

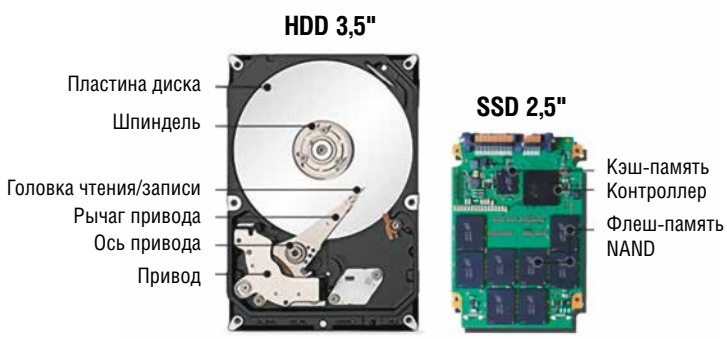


Рис. 1. Основные компоненты HDD и SSD

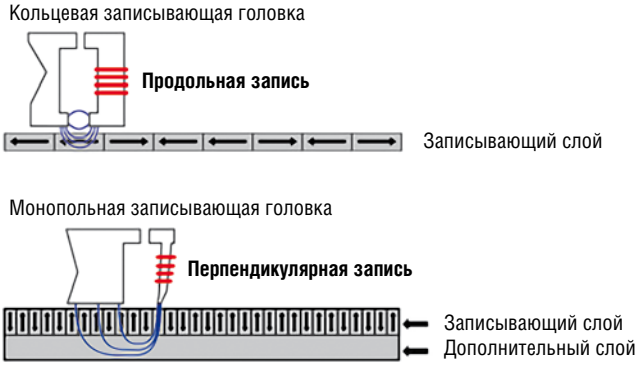
Источник: www.backblaze.com

Источник: IDC Data Age 2025, 2017

Рис. 2. Структура поставок накопителей корпоративного класса

пользование SSD дает преимущества, флеш-накопители станут постепенно заменять жесткие диски во всех сценариях, кроме тех, где требуется большая емкость хранилища. Доля SSD в объеме продаж накопителей увеличится, однако общий рост объемов данных приведет к повышению спроса как на SSD, так и на жесткие диски.

Будущее HDD



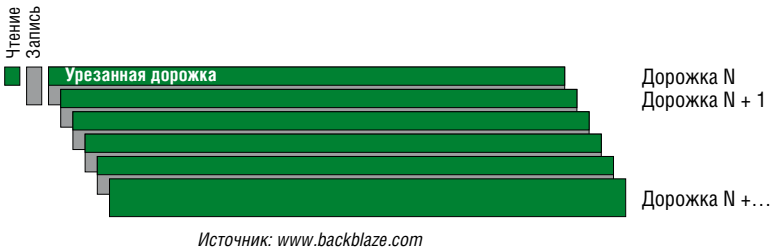
Источник: www.backblaze.com

Рис. 3. Технологии записи

История HDD – это история усовершенствований и инноваций. С момента своего создания в 1956 г. жесткий диск уменьшился в размерах в 57 тыс. раз, емкость хранения выросла в 1 млн раз, а стоимость снизилась в 2 тыс. раз. Цена за 1 Гбайт за 60 лет упала в 2 млрд раз.

Производители жестких дисков добились значительных успехов, уменьшив размер пластин и, следовательно, время поиска, увеличив плотность записи, усовершенствовав технологии чтения/записи. Увеличилось количество головок чтения/записи, появились новые интерфейсы шины, благодаря заполнению корпуса гелием уменьшилось трение.

Рис. 4. Интервал между дорожками при использовании технологии SMR



Источник: www.backblaze.com

В 2005 г. была внедрена технология перпендикулярной записи, которая позволила достичь плотности более 100 Гбит на 1 кв. дюйм (рис. 3). Технология размеченного хранения данных (Bit Patterned Media Recording, BPMR), предложенная компанией Toshiba в 2010 г., также способствовала повышению плотности записи. BPMR с помощью нанолитографии разбивает магнитную среду, уменьшая «размеры» бита. Ожидается, что к 2025 г. благодаря использованию технологий BPMR и HAMR удастся довести плотность записи до 10 Тбайт на 1 кв. дюйм.

Увеличению плотности хранения и общей емкости накопителя служит и технология черепичной магнитной записи (Shingled Magnetic Recording, SMR). Суть технологии в том, что новая записываемая дорожка перекрывает часть ранее записанной дорожки (рис. 4). Предыдущая дорожка сужается, т.е. плотность записи повышается. Этот подход был выбран потому, что из-за физических ограничений записывающие головки нельзя сузить настолько же, насколько считывающие головки.

Еще в 2002 г. компания Seagate успешно продемонстрировала магнитную запись с нагревом носителя (Heat-Assisted Magnetic Recording, HAMR), которая осуществляется с помощью лазера. Это увеличивает плотность и в итоге может привести к созданию к 2019 г. 20-терабайтного диска.

Western Digital заявляет, что ее конкурирующая технология микроволновой магнитной записи (Microwave-Assisted Magnetic Recording, MAMR) позволит к 2025 г. довести емкость диска до 40 Тбайт. Некоторые эксперты отрасли и производители дисков прогнозируют еще большее повышение плотности записи, что обеспечит в следующем десятилетии создание дисков емкостью до 100 Тбайт. Помимо тепла и микроволн, для увеличения плотности записи предполагается использовать экстремальное охлаждение.

Так что жесткие диски – вполне перспективные устройства хранения, ставить на них крест рано. В ближайшем будущем должно появиться новое поколение гибридных дисков (использующих SSD в качестве кэш-памяти HDD) с улучшенными показателями цена/производительность, расширится применение герметизированных гелиевых дисков. Гибридизация даст возможность двум типам накопителей сосуществовать и дополнять друг друга.

Многие перечисленные выше технологии HDD появились достаточно давно, но еще не дошли до стадии массового внедрения, а накопители SSD тем временем сделали огромный скачок по всем характеристикам.

Перспективы твердотельных накопителей

В накопителях SSD используется, как правило, флеш-память типа NAND трех основных разновидностей – SLC, MLC и TLC. Память SLC (одноуровневая ячейка) хранит один бит данных, MLC (многоуровневая ячейка) – два бита, TLC (трехуровневая ячейка) – три. Есть еще 3D NAND, которая хотя и отличается компоновкой, работает по тем же принципам. Одна из тенденций в технологии флеш-памяти – четырехуровневая (quad-level-cell, QLC) NAND. Ее ячейки имеют 16 уровней заряда, т.е. могут хранить четыре бита данных.

Когда-то память QLC NAND считалась практически нереализуемой из-за малого срока службы ячеек. Переход с плоской структуры QLC NAND (2D) на 3D NAND позволил использовать старые технологии, в которых ячейки памяти были крупнее. Это привело к созданию нового, более надежного типа ячеек с большим количеством циклов перезаписи. QLC NAND в 3D-версии дает возможность изготавливать более быстрые и емкие SSD. В результате стоимость SSD-накопителя емкостью 512 Гбайт может опуститься ниже $100.

По пути создания многослойных структур 3D NAND для увеличения емкости накопителей на основе флеш-памяти пошли многие производители, включая Intel, Samsung и Toshiba. Они стараются сделать ячейки многоуровневыми для увеличения плотности записи. В 2013 г. производственные процессы позволяли создавать лишь 24 слоя, в 2014-м – 36, в 2015-м – 48, затем – 64. Например, первые микросхемы 3D QLC NAND компании Toshiba, анонсированные в 2017 г., имеют емкость 96 Гбайт и используют 64 слоя. Память, созданная по технологии 3D NAND, доказала свою работоспособность и эффективность.

SSD в ЦОДе

Оборудование, используемое в дата-центрах, должно быть способно бесперебойно работать в режиме 24×7, обеспечивать высокую производительность, легко масштабироваться, настраиваться и управляться, а также отличаться адекватной стоимостью владения. Применение в ЦОДах накопителей SSD отвечает практически всем этим требованиям (см. таблицу).

В серверах с транзакционной нагрузкой на смену накопителям HDD корпоративного класса постепенно приходят SSD. Вместе с тем HDD продолжают занимать свою нишу в сегменте хранения «холодных», редко используемых или архивных данных. Флеш-память становится необходимым звеном в инфраструктуре хранения и ключевым компонентом гиперконвергентных решений, помогает эффективнее перемещать и хранить данные.

Например, компания HPE рекомендует для увеличения производительности аналитических приложений применять «ускорители ввода-вывода» – флеш-накопители, устанавливаемые в слот расширения PCIe, а также флеш-массивы и гибридные системы хранения с накопителями обоих типов. Это ускорит обработку больших данных и бизнес-аналитику.

Уменьшить задержки и свести к минимуму издержки протоколов, связанные с хранением, помогает технология NVMe (Non-Volatile Memory Express). Она позволяет повысить общую производительность системы, особенно в таких ресурсоемких задачах, как виртуализация, обработка больших данных и высокопроизводительные вычисления.

SSD и СХД

Цифровая трансформация предприятий ставит новые задачи быстрой обработки больших объемов данных. Существенно измениться должна и архитектура приложений, работающих с такими системами хранения. Последние два года вендоры отмечают быстрый рост спроса на комплектацию СХД накопителями SSD.

Это закономерно. Ведь для построения СХД производительностью 500 тыс. IOPS потребуется 2500 жестких дисков со скоростью вращения 15K об/мин – или всего один флеш-массив. Такие массивы хорошо подходят для систем виртуализации и облачных сервисов, а технологии дедупликации и сжатия данных приближают стоимость хранения данных на SSD к показателям HDD.

Внедрение твердотельных накопителей – одна из основных тенденций на рынке систем хранения данных. Все ведущие производители таких систем включили в свои линейки бездисковые

Основные преимущества применения SSD в ЦОДе

Характеристика	Пояснение
Низкое энергопотребление	При большом числе накопителей применение SSD существенно снижает плату за электроэнергию
Высокая скорость	Для ускорения доступа к данным можно использовать кэширование БД и других данных, что влияет на общую производительность приложений или системы
Отсутствие вибрации	Уменьшение вибрации повышает надежность, снижает требования к жесткости конструкции стоек
Низкий уровень шума	По мере развертывания все большего количества SSD ЦОДы будут становиться более тихими
Малое тепловыделение	Чем меньше выделяется тепла, тем ниже требования к охлаждению и мощности, потребляемой в ЦОДе
Быстрая загрузка	Чем быстрее будет загружаться система хранения данных или сервер, тем лучше
Высокая плотность	ЦОДы смогут хранить больше данных в меньшем пространстве, что повышает эффективность во всех областях (мощность, охлаждение и т.д.)
Оптимальное соотношение производительность/стоимость хранения	Применение SSD для «горячих», а HDD для «холодных» данных в сочетании с механизмами их автоматического перемещения по уровням хранения повышает эффективность ИТ-инфраструктуры

Рис. 5. Массивы Dell EMC SCv3000

массивы (All-Flash Array, AFA), построенные на SSD. Твердотельные накопители корпоративного класса – значимый драйвер роста отрасли СХД.

По данным IDC, на мировом рынке СХД в 2017 г. первое место по объему продаж заняла компания HPE, опередив прежнего лидера рынка Dell EMC. Росту рынка (впервые за несколько кварталов) способствовал спрос на флеш-массивы и конвергентные/гиперконвергентные системы. Новые решения наглядно демонстрируют эту тенденцию.

В ноябре прошлого года Dell EMC анонсировала новые системы хранения начального уровня – массивы SCv3000 (рис. 5) с новыми шестиядерными процессорами Intel, удвоенной емкостью оперативной памяти и утроенной пропускной способностью. Производительность СХД выросла на 50% – до 270 тыс. IOPS. Технология Data Progression позволяет использовать в этих гибридных системах на флеш-памяти автоматическое многоуровневое хранение (тиринг) с гибкой настройкой конфигурации, уменьшает требуемую для хранения данных емкость на 90%. Технология Live Migrate обеспечивает миграцию данных и балансирование нагрузки, а Live Volume – автоматическую обработку отказов и восстановление на уровне тома, что дает возможность без прерывания продолжать работу в случае сбоев или отказов.

Рис.6. Система хранения Huawei OceanStor Dorado18000 V3

Наряду с аппаратной платформой производители СХД совершенствуют и программное обеспечение. Например, новое ПО NetApp ONTAP 9.3 благодаря оптимизации полосы пропускания с целью повышения IOPS и снижения латентности обеспечивает 40%-ное повышение производительности по сравнению с предыдущей версией и 30%-ную экономию емкости за счет усовершенствованной дедупликации.

Этим инновации вендоров не ограничиваются. Как сообщает компания Huawei, в ее новой системе хранения OceanStor Dorado18000 V3 (рис. 6), которая разработана для высоконагруженных критически важных сервисов, используются технология Flash-Ice на основе графенового рассеяния (Graphene Dissipation Technology, GDT) и динамический алгоритм теплового баланса (Dynamic Heat Balance Algorithm), что позволяет повысить рассеивание тепла и продлить срок службы твердотельных накопителей на 20%. Максимальная производительность этой СХД составляет 7 млн IOPS, а постоянное значение задержки – 0,5 мс.

Huawei также идет по пути упрощения управления СХД. Для этого в OceanStor Dorado18000 V3 применяются средства интеллектуального управления eService. Они оптимизируют процессы управления СХД на основе технологий искусственного интеллекта (ИИ) и больших данных, реализуя автоматическое развертывание и диагностическое обслуживание. В частности, система может предвидеть ограничения по производительности и емкости и подсказывать оптимальные решения.

В 2017 году компания Fujitsu обновила свою линейку систем хранения Eternus (рис. 7). Гибридные массивы Eternus DX60 S4, DX100 S4 и DX200 S4 предназначены для малого и среднего бизнеса, обеспечивают вдвое большую масштабируемость емкости (до 4 Пбайт) и способны обрабатывать втрое больше транзакций. По заявлению производителя, они гарантируют доступность данных на уровне «шести девяток» (99,9999%). Новинки поддерживают функции мгновенных снимков, дедупликации, синхронной и асинхронной репликации, многоуровневого хранения с использованием SSD и HDD, управления качеством обслуживания (QoS).

Компания Lenovo представила в 2017 г. новинку иного класса. Ее система Distributed Storage Solution рассчитана на хранение большого объема как структурированных, так и неструктурированных данных и предназначена для программно определяемых ЦОДов. Особенности СХД – простая масштабируемость, технологии высокоскоростного (до 100 Гбит/с) доступа, включая Infiniband и Ethernet.

На отечественном рынке СХД, конечно, представлены и российские разработки. Например, на основе программно-аппаратного комплекса «Полибайт» (рис. 8) компании RCNTEC можно создать облачное хранилище емкостью до сотен петабайт с трехкратным резервированием. Комплекс ориентирован на крупные корпорации, частные и государственные проекты, нуждающиеся в надежном хранении неограниченных объемов данных. Он может содержать диски различного типа, что позволяет решать разные задачи. ПО «Полибайт» создано в RCNTEC, а производится система в России.

Система не имеет традиционных централизованных контроллеров, которые обрабатывают данные. Клиенты СХД взаимодействуют напрямую с модулями хранения. Модульная архитектура дает возможность создать систему с массовым параллелизмом, в которой операции ввода-вывода выполняются в распределенной среде, а с увеличением емкости линейно растет производительность.

Другая российская компания, Aerodisk, предлагает хранилища Aerodisk Engine, предназначенные для систем виртуализации, баз данных, видеонаблюдения и высоконагруженных корпоративных систем. Эти СХД поддерживают многоуровневое хранение, кэширование на SSD, дедупликацию, локальную и удаленную репликацию, а также интеграцию с ПО VMware. Масштабируемые СХД Aerodisk Engine выпускаются в конфигурации только на твердотельных накопителях или в конфигурации гибридного хранилища.

SSD, облака и ИИ

В условиях стремительного роста объемов данных хорошим выходом становятся облачные хранилища. Использование в них накопителей SSD позволяет провайдеру гарантировать параметры IOPS в SLA. Облачные хранилища для бизнеса дают возможность достаточно надежно и недорого хранить данные, обеспечивать доступ к ним вне зависимости от местонахождения пользователя, легко масштабировать ресурсы. Сокращаются затраты на создание и техническое обслуживание ИТ-инфраструктуры. Нет необходимости приобретать собственные СХД и прочее инфраструктурное оборудование, нести расходы по его администрированию, обновлению, обеспечению безопасности.

Продукты накопительного класса – SCM (Storage-Class Memory) могут сделать массивы хранения быстрее и эффективнее, а благодаря поддержке интерфейса NVMe в серверах и системах хранения можно будет задействовать более эффективный стек аппаратного и программного обеспечения. Суть решений SCM в использовании флеш-памяти в качестве ОЗУ или ее дополнения.

Предпринимаются попытки объединить хранилища данных с возможностями автоматизации, искусственного интеллекта и машинного обучения. Эти перспективы демонстрирует новый облачный сервис Oracle Autonomous Data Warehouse Cloud Service. Этот сервис избавляет администратора баз данных от целого ряда задач: планирования параметров оборудования, организации резервного копирования, применения патчей, организации защиты данных и аварийного восстановления. Все это делается автоматически и автономно, утверждают в Oracle. Кроме того, Autonomous Data Warehouse Cloud

Рис. 7. Гибридный массив Fujitsu Eternus

постоянно оптимизирует ресурсы системы на основе входящих запросов, что обеспечивает высокую производительность без какой-либо настройки вручную или вмешательства администраторов.

Не забывает об облаках и NetApp. Совместно с Microsoft в облаке Azure ею реализован сервис выделения томов файловой системы NFS с заданными параметрами готовности, производительности и защиты данных, причем возможна репликация подобных томов из облака на площадку клиента.

По прогнозам NetApp, благодаря механизмам метаданных вскоре можно будет принимать решения по их транспортировке, категоризации, анализу и защите, автоматически определять права доступа и способы обработки, что даст возможность выстраивать процессы без участия человека. Тиринг станет более интеллектуальным, многоуровневое хранение данных – более детализированным.

Рис. 8. Система «Полибайт» компании RCNTEC

В том же направлении продвигается HPE. Ее технология выработки рекомендаций InfoSight нацелена на создание «автономных дата-центров». Сначала она будет применяться в системах хранения HPE 3Par на основе флеш-памяти, а затем появится и в других решениях компании. В платформе прогнозной аналитики InfoSight задействована технология выработки рекомендаций с помощью ИИ. Предполагается, что такой подход приведет к созданию автономных ЦОДов, способных самостоятельно модифицироваться и оптимизироваться.

Dell EMC адаптирует и внедряет новейшие разработки в области микропроцессоров, такие как графические процессоры, тензорные процессоры или программируемые вентильные матрицы, чтобы создать автономное самоуправляемое хранилище.

Цель подобных разработок – упростить и автоматизировать управление ИТ-инфраструктурой, прогнозирование возможных проблем и получение рекомендаций по увеличению производительности, а также сократить операционные затраты. ИКС

Практический взгляд на автоматизацию сетей и SDN

Нарек Татевосян, руководитель отдела тестирования и анализа средств защиты, BI.ZONE

Перевод сети современных ЦОДов, ориентированных на предоставление облачных услуг, на принципы Software-Defined Network позволит автоматизировать и ускорить процесс внесения сложных изменений на большой парк оборудования разных производителей.

Центры обработки данных повсеместно переходят к предоставлению услуг по облачной модели. Не важно, используются ли публичные облака, частные или гибридный подход, главная особенность облака – это высокая скорость внесения изменений в услуги, причем автоматически, по «нажатию кнопки» на портале самообслуживания. Такая автоматизация требует кардинального изменения метода управления сетями передачи данных. Если раньше как корпоративные, так и коммерческие ЦОДы могли себе позволить полностью ручное управление сетями и работу по запросу (многие так делают до сих пор), то теперь это с каждым днем становится все менее и менее допустимым.

Основные требования к сетям для облаков

Скорость внесения изменений. Сегодня это одна из наиболее важных метрик для компаний. Современные ИТ-проекты, с одной стороны, очень сложны, а с другой – имеют жесткие временные рамки. Проектные команды просто не в состоянии заранее предусмотреть все требования к инфраструктуре и вынуждены их менять. Если собственная ИТ-служба медленно реагирует на запросы бизнес-пользователей, то последним приходится обращаться к внешним сервис-провайдерам, «теневым» ИТ или прибегать к разным IaaS- и PaaS-сервисам, которые позволяют им самим быстро и легко работать с сетевыми сервисами.

Качество внесения изменений. Ключевые показатели качества – это высокий уровень доступности (внесение изменений без простоя сервисов), конфиденциальности (сохранение необходимого контроля доступа) и управляемости (изменения состоят из понятных «кубиков», которые легче эксплуатировать). Для обеспечения доступности сервисов мало построить сеть правильно (сейчас это требование обычно соблюдается, поскольку строительством сетей занимаются высококвалифицированные специалисты), нужно грамотно ее эксплуатировать. И вот это часто бывает проблемой из-за более низкой квалификации работающего с сетью персонала, а также из-за необходимости быстро вносить изменения на множество устройств. Скорость изменений всегда имеет приоритет перед качеством, так как скорость – это понятная для бизнеса метрика, проблемы же с качеством вскроются только при массовом сбое или внешнем аудите. А сбой на сети – это, как правило, приостановка большого количества сервисов.

Сложность и массовость изменений. Сегодня даже тривиальная ранее операция может потребовать изменений в большом числе единиц оборудования и ПО разных поставщиков. Например, чтобы добавить новый внешний VLAN-канал в обычной сети облака (скажем, для подключения клиентов друг к другу или к MPLS-сети), потребуется настроить его в CE-устройствах, edge-коммутаторах, гипервизорах серверов, облачной платформе. Риск ошибки повышается, каждая ошибка может обернуться сбоем сервиса, поэтому важно грамотно протестировать влияние изменений на работу сервисов.

Мультитенантность. Под мультитенантностью подразумевается возможность разделения системы на разные среды, не мешающие друг другу. Публичным сервис-провайдерам такая возможность нужна для предоставления услуг разным клиентам, службам ИТ – для разных проектов, сред (разработки, тестирования, бизнес-систем), сегментов сети или разных подразделений в компании. Разделять все на физическом уровне слишком затратно с финансовой точки зрения, а производительность и уровень развития сетей уже давно позволяют решать эту задачу на базе стандартных технологий (VLAN, MPLS, EVPN).

Мультивендорность. Большинство серверов в настоящее время построено на базе стандартной архитектуры x86 от Intel или AMD с использованием одних и тех же компонентов. Разница

между ними только в цене, качестве сборки и поддержки. Та же ситуация с коммутаторами и маршрутизаторами: по сути, они строятся на одних тех же чипсетах, производимых компаниями Broadcom или Mellanox, а различие в качестве ПО постепенно сходит на нет, поскольку от устройств требуется поддержка стандартных протоколов. Однако решения класса IPS (Intrusion Prevention System), NGFW (Next-Generation Firewall) и WAF (Web Application Firewall) сильно отличаются друг от друга функциональностью, производительностью и защищенностью. С экономической точки зрения сейчас невыгодно «зацикливаться» на одном производителе или альянсе компаний. В одних случаях важнее ценовой фактор (когда функциональность практически идентична), в других требуется выбрать наиболее производительное решение при той же цене или функциональности и т.д. Желательно предварительно протестировать решения, а не слепо доверяться их поставщикам. И службы ИТ должны быть к этому готовы.

Разделение задач между персоналом разной квалификации. С одной стороны, сеть – это критически важная инфраструктура, работа с которой подразумевает наличие персонала высокой квалификации, выделенных временных окон для внесений изменений и тестирование их корректности. С другой стороны, жизнь и бизнес требуют высокой скорости внесения изменений при известных ограничениях рынка труда. Выходом из такой ситуации зачастую становится перекладывание части обязанностей на сотрудников более низкой квалификации с сужением круга выполняемых ими действий для минимизации возможного вреда.

Соответственно, для современных сетей необходимо решение, которое обеспечит персоналу разной квалификации возможность быстро и качественно вносить изменения в мультивендорную сеть, учитывая специфику бизнеса компании. При этом необходимо проверять, что изменения не затрагивают сервисы компании, а если затрагивают, то должна быть предусмотрена процедура отката. Конечно, если позволяют финансы, ничто не мешает задействовать для этих целей большой штат высококвалифицированных сотрудников: есть примеры, когда компании держат целые команды просто для внесения записей в списки контроля доступа. Но, во-первых, высококвалифицированных кадров в России и СНГ для подобных работ недостаточно, во-вторых, таких специалистов задачи эксплуатации зачастую не привлекают: эксперты, как правило, хотят развития и новых интересных задач. Для сервис-провайдеров эффективность персонала – это важное конкурентное преимущество, так как от нее зависит себестоимость услуг. Поэтому все больше компаний осознают необходимость автоматизировать управление сетью.

Раньше для такой задачи создавались различные системы управления сетью (Network Management System), но почти все такие проекты провалились, потому что в основном они были «заточены» под одного поставщика, закрыты для расширения (или расширение было очень сложным для сетевиков), часто позволяли только управлять конфигурациями отдельных устройств через единый интерфейс и не содержали в себе какого-либо слоя абстракции для управления сервисами. Ситуация изменилась с появлением концепции Software-Defined Network. Сначала был разработан протокол OpenFlow, но он не получил широкого распространения из-за архитектурных особенностей, которые не вполне соответствовали сложившимся алгоритмам работы сети (см. ниже). Однако базовые принципы концепции дали развитие большому числу решений для программно определяемых сетей, которые решают задачи автоматизации.

Принципы SDN

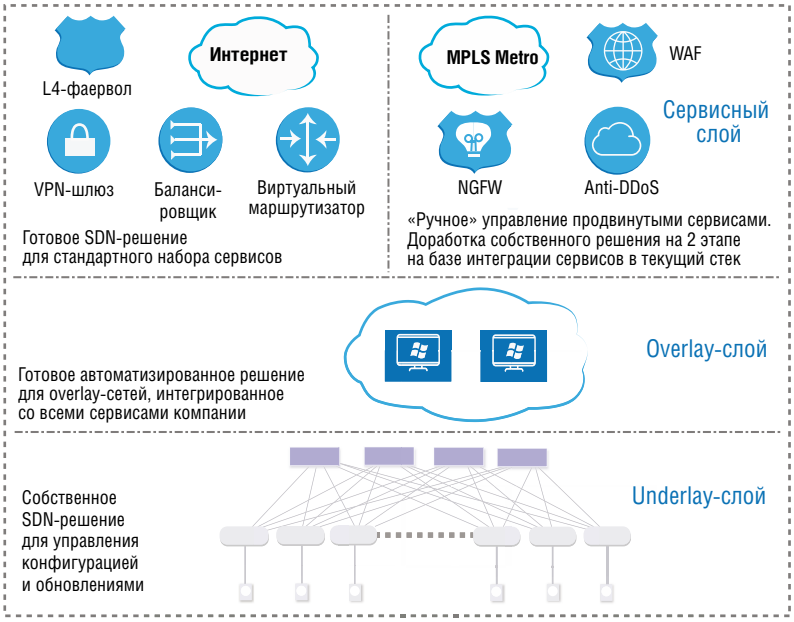
Базовый принцип SDN – это декомпозиция сети на три плоскости (plane):

- Management Plane – плоскость управления конфигурацией сети. В случае одного устройства это непосредственно его конфигурирование, в случае SDN – конфигурирование всех составляющих сети (underlay, overlay, сервисы).
- Control Plane – плоскость оперативной информации о состоянии сети. Для одного устройства это, например, таблица маршрутизации, в сети SDN – таблицы маршрутизации всех устройств на разных уровнях (underlay, overlay, сервисы).
- Data Plane – плоскость, в которой осуществляется непосредственная передача пакетов с одного порта устройства на другой порт.

При реализации этого принципа на практике важен вопрос выбора архитектуры: централизованная или распределенная. С Management Plane и Data Plane все понятно: управление должно быть централизованным (в этом отчасти смысл SDN), а коммутация пакетов на каждом отдельном устройстве – распределенная функция. В случае Control Plane индустрия пошла разными путями: одни производители выбрали централизованную архитектуру (VMware, Nuage, Google), а другие пошли по пути реализации распределенной или частично распределенной архитектуры (Cisco, Juniper, Facebook).

Конечно, можно спорить о том, какой путь лучше, но в целом различие подходов обусловлено особенностями бизнеса компаний. Cisco, Juniper и другим сетевым вендорам нет смысла заниматься новой реализацией Control Plane, потому что у них накоплена большая экспертиза по работе с протоколами маршрутизации, MPLS и т.д. Новые игроки на рынке сетевых технологий, такие как VMware, свои решения, которые являются исключительно программными и работают в тесной интеграции с гипервизорами, создавали с нуля, поэтому они пошли по пути развития централизованной архитектуры Control Plane. А Google, реализуя свою концепцию Site Reliability Engineering, выбрала централизацию для более гранулярного управления путями маршрутизации и полосой пропускания, что важно для сетей масштаба этой компании. В итоге получается, что правильный путь – тот, который больше соответствует накопленной экспертизе компании.

Рис. 1. Архитектура сети, реализованной для одного из сервис-провайдеров СНГ



Эволюция сетей в центрах обработки данных при внедрении принципов SDN во многом определялась возможностью растягивания L2-домена на весь ЦОД и предоставления разных сервисов. Это привело к следующей архитектуре сети:

- Underlay – сеть, обеспечивающая связность между компонентами, на основе которых строится сетевая инфраструктура SDN. Это обычный IP-транспорт. По сути, чтобы реализовать этот уровень, достаточно протокола маршрутизации OSPF (Open Shortest Path First) и поддержки балансировки по маршрутам ECMP (Equal-Cost Multi-Path).
- Overlay – виртуализированная сеть, которая позволяет предоставлять распределенные сервисы L2. Для реализации этого уровня используются разные механизмы: например, архитектура EVPN (BGP + VXLAN) для аппаратных коммутаторов или технология VMware NSX.
- Сервисы. Реализация сервисов сильно зависит от выбранного решения для Underlay и Overlay. В облачной сети можно выделить следующие сервисы: маршрутизация для виртуальных машин облака, выход во внешний мир (интернет, MPLS), обеспечение сетевой безопасности (межсетевой экран, WAF, IPS и пр.).

Резюмируем принципы, которых следует придерживаться при построении сети SDN:

1. SDN – это централизованное управление конфигурацией сети (Management Plane) и распределенная передача пакетов данных (Data Plane).
2. Архитектура Control Plane должна опираться на специфику бизнеса. С учетом того, что сети строились по принципу распределенной системы, в большинстве случаев подойдет распределенный вариант.
3. Специфика бизнеса и стек уже используемых в компании технологий также влияют на целесообразность развертывания собственного SDN-решения на каждом уровне эталонной архитектуры. Например, если уже закуплен парк оборудования Arista или Juniper и используется архитектура BGP EVPN, то есть смысл автоматизировать сети Underlay и Overlay. А если сервис-провайдер работает полностью по программе VMware vCAN, то целесообразно задуматься об автоматизации сети Underlay и сервисов, задействовав в сети Overlay технологию NSX и сделав упор на интеграцию своего решения с NSX.
4. Стек технологий, на котором будет разрабатываться решение автоматизации, должен быть написан на языке программирования, доступном широкому кругу лиц. Сегодня можно смело говорить, что наиболее приемлемым языком для автоматизации сетей является Python ввиду быстроты освоения, наличия большого числа библиотек и решений и отсутствия требований к высокой производительности для системы автоматизации.

От теории – к практике

Примером применения подхода SDN для автоматизации сети может служить проект, осуществленный нашей компанией для одного из сервис-провайдеров СНГ. Провайдер намеревался на базе решения VMware предоставлять услуги IaaS, а также сервисы безопасности, такие как NGFW, WAF и Anti-DDoS. В проекте

было задействовано 80 единиц коммутаторов и маршрутизаторов. Важно было обеспечить быстроту выхода на рынок и высокое качество реализации, поскольку первые и одновременно ключевые заказчики провайдера внедряли систему SAP HANA. Команда инженеров, выполняющих проект, состояла всего из трех человек.

Мы пошли по следующему пути. Сеть Overlay и базовые сетевые сервисы IaaS были реализованы полностью на стеке VMware NSX с использованием vCloud Director. Помочь обосновать такое решение нам помогло то, что заказчик подпадал под операторскую программу vCAN, условия которой были экономически привлекательны. Если бы заказчик создавал себе частное облако или внедрял исключительно услугу NFV, то, скорее всего, следовало бы выбрать другое решение.

Для провайдера была реализована единая платформа управления Underlay-сетью облака, сетью управления облака и сетью предоставления внешних услуг (edge-сеть), построенной на базе оборудования Juniper (рис. 1). В первую очередь мы решили добиться единого управления конфигурацией сети, которое позволило бы нам быстро и качественно внедрить систему, и уже на этой базе наладить эксплуатацию сети, развернув управление сервисами заказчика. Первыми пользователями сети стали сетевые инженеры, которые благодаря проекту смогли повысить свою эффективность в деле управления сетью. Этап передачи централизованного управления сетью инженерам поддержки мы решили отложить до следующего проекта, когда конфигурация сети полностью стабилизируется.

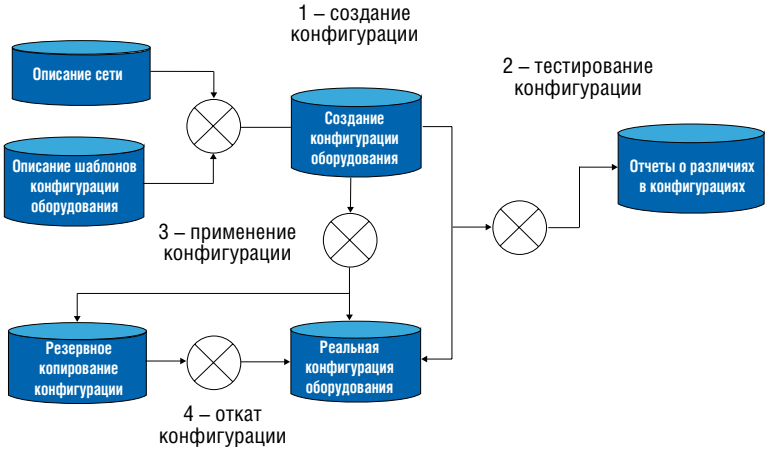
Слой Underlay был создан в кратчайшие сроки. При проектировании сети leaf-spine были сделаны некоторые допущения о возможностях leaf-коммутаторов, которые оказались ошибочными, из-за чего пришлось на ходу перепроектировать и внедрять новую конфигурацию. Но благодаря выбранному решению для этого было достаточно внести незначительные изменения в базу шаблонов.

Автоматизация сети позволила обеспечить выполнение основных задач администратора сети – настройку системных сервисов (аутентификацию, авторизацию, мониторинг, системное время, логирование), портов и протоколов маршрутизации – в соответствии с едиными шаблонами, построенными на базе лучших практик.

Процесс обновления конфигурации (рис. 2) стал масштабируемым и безопасным. Упрощенно этот процесс можно представить следующим образом:

1. Создание конфигурации. На базе описания сети и комбинации шаблонов собирается полная конфигурация устройства.
2. Тестирование конфигурации. Созданная конфигурация сравнивается с текущей. Это позволяет «выловить» ошибки синтаксиса конфигурации и увидеть различия между текущей конфигурацией и созданной. Анализ различий также дает возможность выявить и исправить ошибки.
3. Применение конфигурации. Текущая конфигурация сохраняется, новая конфигурация устанавливается на устройства.
4. Откат конфигурации. В случае неуспеха (появились проблемы в сети, не удалось достичь желаемого результата) делается откат и ищется причина.

Рис.2. Процесс обновления конфигурации



Реализованное решение позволило с легкостью управлять конфигурационными файлами большого числа устройств, а исправления в конфигурации, скажем, из-за ошибок ПО коммутаторов, вносились очень быстро. Например, мы обнаружили серьезную проблему, которая не позволила сформировать кластер leaf-коммутаторов, и для объединения коммутаторов нам пришлось задействовать стандартную технологию MC-LAG (Multi-Chassis Link Aggregation Group). Потребовалось изменить шаблоны конфигурации.

В результате осуществления проекта заказчик начал предоставлять своим клиентам полностью самоуправляемую услугу IaaS, в которую входит возможность управлять сетевыми сервисами балансировщика нагрузки, выхода в интернет, IPsec, межсетевого экрана L4.

Получить представление о системе можно, обратившись к репозиторию https://github.com/nar3k/vagrant-net-lab, который мы использовали, проверяя правильность первоначальной концепции, а затем расширили для работы с реальным проектом. ИКС

ЦОДы – приоритетное направление развития ДКС

Компания ДКС может предложить заказчикам практически весь спектр продукции для создания инженерной инфраструктуры ЦОДа, уверен заместитель генерального директора компании Руслан Фаррахов.

Руслан Фаррахов

– Руслан Раифович, в августе компании ДКС исполнилось 20 лет. Расскажите, как все начиналось?

– Решение о создании компании было принято еще в 1997 г. Полгода мы изучали потребности рынка, на котором тогда доминировало импортное оборудование. Начали производство с простого – с пластиковой гофрированной трубы. 14 августа 1998 г., в пятницу, наш завод в Твери выпустил первую трубу, а в понедельник произошел дефолт. Курс рубля упал в три раза, и рынок сразу заинтересовался нашими ценами.

Условия для старта были благоприятными, но дело не только в них. Например, пластиковые трубы завозились из-за рубежа маленькими партиями, а наша компания предлагала дистрибьюторам любые объемы поставок непосредственно из России. Кроме того, мы тщательно проанализировали существующую на рынке продукцию и выпустили максимально качественное изделие. Внимание к мелочам, изучение потребностей всех участников бизнес-процессов от производства и поставки до итогового монтажа – подход, который привел нас к успеху тогда и помогает выводить на рынок новые продукты по сей день.

Инсталляция шинопровода и системы распределения электроэнергии в ЦОДе

– Как развивалась продуктовая линейка компании?

– Следующим этапом развития стал запуск производства пластиковых кабель-каналов. Такое производство сложнее, так как требуется выпускать разнообразную номенклатуру соединительных и крепежных элементов. В 2001 г. компания предложила рынку кабельные каналы с силовыми розетками и ИТ-разъемами RJ-45 и RJ-11 для организации рабочих мест, что было качественным скачком для российского рынка, на котором у западных решений не было конкурентов. Помогло традиционное внимание к мелочам. Например, мы начали наклеивать на короба пленку для защиты от пыли во время строительства, что тогда было для рынка новшеством. Это был наш первый выход на рынок систем для ИТ.

В 2003 г. компания ДКС предложила рынку металлические кабельные каналы. Технологию производства этого востребованного продукта мы перенесли из Италии. Сейчас наши металлические лотки активно используются в дата-центрах. В ЦОД Сбербанка в Сколково мы поставили лотки и короба разных типоразмеров общей протяженностью 400 км. Сегодня наша доля на российском рынке лотков для ЦОДов, по оценкам специалистов, составляет порядка 50–70%.

– Как разворачивалась международная экспансия компании?

– Глобализация вытекает из логики бизнеса. Первое наше зарубежное предприятие появилось в 2000 г. на Украине. Когда компании исполнилось 10 лет, мы задумались о широкой международной экспансии.

Мы начинали сотрудничать с зарубежными компаниями, потом становились их крупнейшими заказчиками. Понимая преимущества партнерства, владельцы зачастую сами предлагали продажу бизнеса, и их предприятия вливались в нашу группу ДКС. По такой схеме мы вывели на российский рынок металлические корпуса, кабельные каналы, металлические трубы, ИБП, кондиционеры для электротехнических шкафов и силовые трансформаторы. Параллельно мы сформировали соответствующий единый монобрендовый продуктовый портфель и для рынков Европы.

Приобретя в 2015 г. две сильные бразильские компании в области производства кабельных систем и комплексных ре-

шений для распределения электроэнергии, ДКС вышла на перспективный рынок Южной Америки. Для продвижения на рынки Северной Африки была образована компания в Тунисе. Помимо этого, у нас появилась компания «ДКС Азия Пасифик» в Сингапуре, так как в Юго-Восточной Азии на наши шинопроводы сразу сформировался повышенный спрос.

– ДКС стала глобальной компанией. Как это отразилось на производстве в России?

– Мы не только локализовали производство итальянских шкафов в России, но и доработали технологические процессы, перешли к использованию российских компонентов, например, стали и красок. На нашем заводе в Твери освоены передовые процессы обработки металлов. Введены в строй линии покраски и цинк-ламельного покрытия элементов шкафов. Осенью мы запускаем цех горячего цинкования. Недавно установили первый в России аппарат сварки трением. Наша локализация – не отверточная сборка, а разработка и производство на основе самых современных технологий.

– Когда компания начала уделять особое внимание развитию ИТ-направления?

– В 2012 г. мы выделили три линейки шкафов: электрические, для систем автоматизации, а также шкафы и стойки ИТ. В 2018 г. мы провели глубокую модернизацию линейки ИТ-шкафов и усовершенствовали технологию производства. Теперь шкафы производятся на полностью роботизированной линии. Данную серию ДКС представит на осенней конференции ИКС-Медиа «ЦОД-2018» в Москве.

В 2013 г. мы инвестировали в разработку полной линейки шинопроводов, а в 2017 г. на одной из крупнейших площадок дата-центра «Алабушево» осуществили первую инсталляцию решений на шинопроводах ДКС. Благодаря растущему спросу мы локализовали производство шинопроводов в России, Бразилии и Сингапуре. Наши инновации в производстве позволяют повысить оперативность работ и удовлетворить все потребности клиентов, а также планомерно сокращать сроки поставки.

В 2014 г. компания ДКС ввела в ассортимент источники бесперебойного питания. Этот продукт позволил компании выйти на новый качественный уровень производства и продаж сложного оборудования. Два стадиона, построенные для Чемпионата мира по футболу, были полностью укомплектованы нашими ИБП, которые выполняли одни из самых ответственных задач. В планах на 2020 г. – выпуск ИБП мощностью до 1,2 МВт.

– Продолжаете ли вы развивать линейку кабеленесущих систем?

– Да, конечно. Мы не только ведем непрерывную работу по модернизации конструктивных решений, но и выпускаем новые продукты. Недавно у нас появилась система жестких и гибких металлических труб, которые используются для защиты кабелей от агрессивных сред. Важной особенностью данной системы является ускорение прокладки кабелей и снижение издержек при монтаже. Значительную долю роста их продаж обеспечили ЦОДы.

– Многие вендоры сейчас предлагают комплексные решения, которые позволяют заказчику строить ЦОДы на оборудовании одного производителя. Есть ли у компании ДКС комплексные решения для дата-центров?

Кабеленесущая система в ЦОДе компании «Мегафон»

– ЦОДы – приоритетное направление в нашей работе. Оборудование и материалы ДКС могут применяться в дата-центрах любых масштабов: от серверных на две-три стойки до мегаЦОДов.

Еще 20 лет назад мы стали придерживаться принципа полной совместимости наших продуктов. В результате такого подхода сегодня мы можем предложить комплексные решения не только для небольших проектов, но и для крупных промышленных комплексов и ЦОДов.

Наши системы универсальны: для базовых станций (по сути это микроЦОДы) мы разработали всепогодные шкафы с кондиционированием, которые работают в диапазоне –50…+50°С, они уже устанавливаются на магистральных автотрассах.

В 2018 г. мы начали выпускать медные компоненты СКС, благодаря которым предлагаем полностью законченную систему кабельной инфраструктуры.

В прошлом году компания ДКС ввела в ассортимент силовые трансформаторы, в 2018 г. запустила производство системы RAM power, которая предназначена для шкафов распределения электроэнергии на токи до 6300 А. ДКС – единственная российская компания, предлагающая такое решение.

Мы очень гордимся тем, что к нам в команду приходят специалисты с огромным опытом, компетенциями и идеями, которые ДКС реализует при разработке и производстве решений.

Подводя итоги 20-летней работы, можно с уверенностью сказать, что ДКС стала компанией, поставляющей комплексные решения, которые практически полностью закрывают потребности инженерной инфраструктуры дата-центров. ЦОДы, построенные на системах ДКС, в России уже есть.

Наши клиенты успешно развиваются, а вместе с ними развиваемся и мы. И следующие 20 лет обещают быть для всех нас не менее интересными.

«Длинный» Ethernet: возможности и перспективы

Андрей Семенов, профессор, МТУСИ

Евгений Кандзюба, аспирант, МТУСИ

Предоставление современных телекоммуникационных сервисов может быть облегчено использованием линий Ethernet увеличенной по сравнению с привычными 100 м протяженности.

Основная масса электронных сервисов, которые появились в последнее время, не предъявляют высоких требований к пропускной способности канала связи между центральным и терминальным устройствами. Даже при работе с видеоинформацией благодаря применению эффективных алгоритмов сжатия и устранению избыточности в потоке данных приемлемое для большинства практически важных случаев качество обеспечивается каналом связи с пропускной способностью чуть выше 10 Мбит/с. Однако зачастую для этих сервисов, особенно для передачи изображения в реальном масштабе времени, критична малая задержка передаваемых данных.

Поэтому информационные подсистемы для предоставления новых сервисов целесообразно реализовывать по централизованной схеме. Во-первых, централизованные системы обеспечивают минимальное и, главное, стабильное время задержки всех передаваемых пакетов. Во-вторых, размещение дополнительных коммутационных узлов новых сервисов – задача во многих случаях трудноразрешимая, и отказ от них в централизованных структурах сам по себе выгоден.

Построение централизованной структуры существенно упрощается в случае наличия линий связи максимальной протяженности, которые применительно к информационно-телекоммуникационным системам (ИТС) часто называют «длинным» Ethernet.

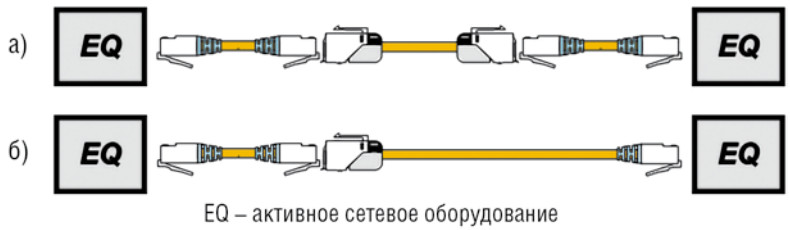
Варианты организации трактов увеличенной протяженности

Для повышения технико-экономической эффективности линии «длинного» Ethernet целесообразно строить на основе существующей элементной базы. При этом могут быть использованы и волоконно-оптические, и симметричные электропроводные линии.

Волоконно-оптическая техника демонстрирует здесь такие известные достоинства, как большая дальность действия (в случае даже многомодовой техники штатно достигается 2 км на скоростях 100 Мбит/с, и есть возможность увеличения дальности до 5 км) и отсутствие необходимости в новых разработках.

Однако массовому внедрению оптических линий во вновь создаваемые ИТС препятствует сложность обеспечения дистанционного питания одиночных терминальных устройств. Такое питание требует применения комбинированных волоконно-оптических кабелей с интегрированными в них выделенными медными жилами. Определенное значение имеют также более высокая стоимость и меньшая надежность оптических линий из-за неизбежного появления в цепи передачи двух дополнительных преобразований сигналов – из электрической формы в оптическую на передаче и обратно на приеме. Поэтому основным кандидатом на формирование линейной части «длинного» Ethernet становятся симметричные кабели.

Структура симметричного тракта: а) классическая, со схемой подключения interconnect; б) direct connection



Пути наращивания дальности действия симметричных линий

Классическая техника СКС создается исходя из требований обеспечения 100-метровой протяженности тракта, но для новых областей применения этого недостаточно. Главным фактором, ограничивающим предельную дальность связи, является отношение сигнала к шуму. Для сетевых интерфейсов Fast Ethernet этот параметр полностью определяется защищенностью ближнего конца. Предельную дальность связи с сохранением качества передачи информации можно увеличить несколькими основными способами:

- наращиванием параметра NEXT (переходного затухания на ближнем конце);
- сокращением «электрической» длины тракта;
- уменьшением коэффициента затухания.

Значимое для практики увеличение NEXT (на 10 дБ и более) возможно при переходе на экрани-

рованную технику или применении элементной базы категории 6 и выше. Однако и то и другое приводит к росту коэффициента затухания вследствие неизбежных дополнительных потерь в металле структур типа x/FTP в первом случае и роста активного сопротивления из-за уменьшения шага скрутки неэкранированных кабелей высоких категорий – во втором. Таким образом положительный эффект заметно нивелируется.

Типовой прием уменьшения «электрической» длины тракта основан на изменении его структуры и применении схемы direct connection (см. рисунок). Необходимый эффект в данном случае достигается за счет уменьшения общей длины шнуров, которые имеют в 1,2–1,5 раза большее погонное затухание, а также за счет сокращения до одного количества разъемных соединителей в тракте (левый и правый разъемы на рисунке в части б, согласно стандартам, считаются частью аппаратуры и не учитываются при формировании требований норм).

К сожалению, возможности этого способа крайне ограничены. Поэтому целесообразно в первую очередь уменьшать коэффициент затухания.

Расчетные величины коэффициента затухания и дальности связи сетевых интерфейсов Fast Ethernet

Параметры сетевых интерфейсов Fast Ethernet	Диаметр жилы, мм				
	0,5	0,52	0,55	0,6	0,64
Zв = 100 Ом					
Коэффициент затухания	21,5	20,0	18,2	15,6	14,0
Длина, м	185	202	226	258	288
Zв = 120 Ом					
Коэффициент затухания	18,3	16,3	14,8	12,8	11,5
Длина, м	221	251	268	311	345
Zв = 150 Ом					
Коэффициент затухания	15,1	13,8	12,6	10,9	9,9
Длина, м	263	293	315	366	402

Способы снижения затухания

Коэффициент затухания симметричного тракта, представляющий собой потери в окружающих металлических элементах, в том числе в экранирующих покрытиях, минимизируется увеличением диаметра провода и наращиванием волнового сопротивления (Zв). Допустимо применение обоих приемов одновременно. Кроме того, для снижения коэффициента затухания необходимо отказываться от экранированных конструкций в пользу структур U/UTP.

Увеличение диаметра провода имеет большие перспективы за счет того, что современные высокочастотные IDC-контакты дают возможность подключать проводники диаметром до 0,8 мм, что уменьшает активное сопротивление и соответственно коэффициент затухания примерно в 2 раза по сравнению с широко распространенными кабелями СКС с диаметром жилы 0,51–0,52 мм.

На этом фоне уменьшение коэффициента затухания через наращивание Zв выглядит менее предпочтительным (волновое сопротивление можно увеличить примерно до 150 Ом, т.е. в 1,5 раза). Кроме того, эффективность этого приема снижается из-за дополнительных потерь рассогласования Zв с импедансом передатчика и приемника сетевого интерфейса, а также неизбежного роста потерь в изоляции по мере увеличения волнового сопротивления.

Предельная дальность связи

Предельная дальность действия сетевых интерфейсов Fast Ethernet определялась расчетным путем. Результаты расчетов приведены в таблице.

Для проверки теоретических расчетов и выявления дополнительных ограничений проводились также натурные эксперименты на опытных образцах кабелей. Цифровой сигнал IP-камеры видеонаблюдения удалось передать на расстояние:

- 230 м – по кабелю с Zв = 100 Ом и диаметром жилы 0,69 мм, образец № 1;
- 200 м – по кабелю с Zв = 150 Ом и диаметром жилы 0,52 мм, образец № 2;
- 270 м – по кабелю с Zв = 100 Ом и диаметром жилы 0,644 мм, образец № 3.

Во всех экспериментах для построения линии была использована схема direct connection, подключение коммутатора производилось шнуром длиной 1,5–2,0 м категории 5e с жилами диаметром 0,52 мм.

Существенные различия в максимально допустимой длине тракта, которые показали 100-омные кабели с близкими сечениями жил (образцы №№ 1 и 3), обусловлены тем, что в образце № 1 витые пары имели изоляцию из сплошного полиэтилена, тогда как в образце № 3 применялся вспененный полиэтилен, уменьшающий емкость пары и тем самым снижающий коэффициент затухания.

Большое расхождение между реально полученными и теоретически рассчитанными максимальными длинами тракта объясняется тем, что при протяженности тракта заметно меньше предельной сетевой интерфейс отключался из-за слишком большого шлейфового сопротивления витой пары.

В связи с такой особенностью серийных систем Fast Ethernet дальнейшее наращивание протяженности тракта возможно при установке промежуточных репитеров. Перспективы применения этой техники расширяет возможность дистанционного питания подключаемых устройств в сочетании с малой потребляемой мощностью их управляющих контроллеров.

■ ■ ■

Использование кабелей из витых пар при условии выполнения достаточно мягких дополнительных ограничений позволяет значительно (в два раза и более) увеличить предельную дальность связи сетевых интерфейсов Fast Ethernet. Для максимизации дальности связи без переприема целесообразно применять модернизированный кабель, а сам тракт передачи формировать по схеме direct connection. С учетом того, что главным фактором ограничения дальности связи является коэффициент затухания, линейные кабели «длинного» Ethernet должны иметь структуру U/UTP. ИКС

Куда плывут облака

Александр Барсков

От простого выноса имеющихся приложений в облака компании переходят к их переработке с учетом облачной специфики. Набирают популярность гибридные решения и услуги, предоставляемые по модели «платформа как сервис», появляются услуги «контейнеры как сервис».

Казалось бы, облака уже распространились повсеместно и не осталось ни одной современной компании или организации, которая не использовала бы облачные сервисы. Но, по данным ABC Data, 82% текущих ИТ-бюджетов организаций все еще направляется на локальную инфраструктуру и приложения. Однако уже к 2020 г. как минимум 50% ИТ-расходов будет связано с облачными решениями. Так что тенденция к переводу в облака все большего числа ИТ-сервисов очевидна. Эта тенденция стала, в частности, одной из основных тем обсуждения на проведенной «ИКС-Медиа» конференции Cloud & Digital Transformation 2018.

Первый этап: снижение затрат

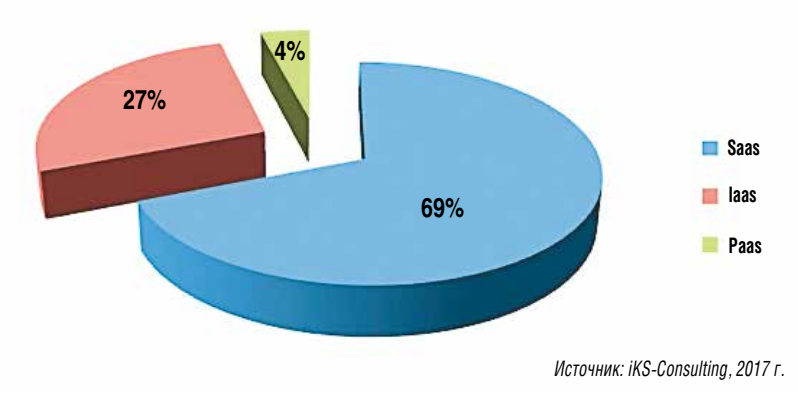
Изначально облака применялись главным образом для оптимизации стоимости получения ИТ-сервисов – читай, для сокращения затрат. На этом этапе спросом в основном пользовались базовые модели «ПО как сервис» (SaaS) и «инфраструктура как сервис» (IaaS), которые и сегодня доминируют на рынке. Так, по данным iKS-Consulting, в 2017 г. 69% доходов на рынке облачных услуг России пришлось на сервисы SaaS, а еще 27% – на IaaS (рис. 1).

В большинстве случаев использование моделей SaaS и IaaS на начальном этапе не требовало сколько-нибудь существенного изменения ИТ-менталитета заказчиков. В случае покупки самой популярной в IaaS-портфеле услуги «виртуальный сервер» заказчик получал возможности, к которым привык при работе с обычными серверами. Он так же мог устанавливать операционную систему и приложения, работать с файлами – но со всеми преимуществами облачной модели, включая гибкое масштабирование и оплату только задействованных ресурсов.

Второй этап: учет специфики

Новые возможности, включая гибкое масштабирование ресурсов и реализацию новых бизнес-моделей, стали катализаторами роста интереса к облачной модели. Если на первом этапе эволюции облаков корпоративные приложения, по сути, не менялись, то на втором этапе заказчики начали перерабатывать свои приложения с учетом облачной специфики. Как отмечает Константин Юров, руководитель технической экспертизы гибридных облачных решений IBM, на этом этапе растет популярность гибридных решений, а также услуг, предоставляемых по модели «платформа как сервис» (PaaS). Появляются и новые услуги, такие как «контейнеры как сервис» (CaaS).

Если в 2017 г. в России услуги PaaS занимали скромные 4%, то в мире – около 10%. В 2020 г. объем этого сегмента, по прогнозу Gartner, увеличится до $14,7 млрд (рис. 2). В числе драйверов роста Илья Летунов, руководитель b2b-облаков Mail.Ru Group, называет достигаемое благодаря использованию этих сервисов существенное сокращение стоимости разработки и вывода новых продуктов и услуг на рынок.



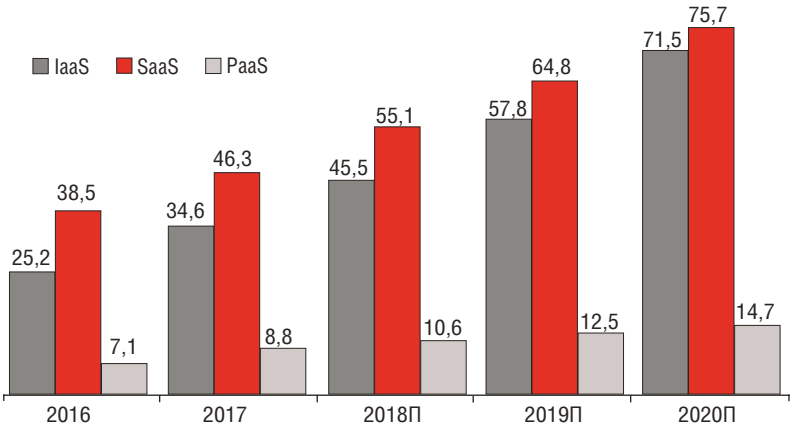
Источник: iKS-Consulting, 2017 г.

Рис. 1. Доли основных типов облачных сервисов на рынке России

Почему Россия по уровню проникновения PaaS серьезно отстает? Одна из причин – общее отставание в части использования облачных моделей. Как уже говорилось, в нашей стране до сих пор доминируют концептуально более простые сервисы SaaS и IaaS. Однако, возможно, здесь сказываются и различия в методике классификации. Некоторые услуги однозначно классифицируются как PaaS. Это, скажем, доступ к платформам баз данных, средства визуализации, инструменты для разработчиков, сервисы мониторинга, безопасности и пр. Но есть сервисы, с классификацией которых пока не все ясно. Это, например, CaaS.

«Контейнеры как услуга»

Как известно, контейнер представляет собой изолированную и переносимую среду выполнения приложений или процессов, которые поставляются вместе со всеми необходимыми компонентами и файлами конфигурации. Все нужные для работы приложения находятся внутри контейнера, поэтому его можно легко переносить в разные операционные среды. Он может



Источник: Gartner

Рис. 2. Рост мирового рынка услуг xaaS, $ млрд

функционировать как поверх виртуальной машины, так и на физическом сервере.

Помимо отличной переносимости, другим важным преимуществом программных контейнеров является экономное использование ИТ-ресурсов. Контейнеры позволяют уместить на одном физическом сервере гораздо больше приложений, чем виртуальные машины. Дело в том, что виртуальные машины требуют много системных ресурсов (оперативной памяти и процессорных циклов), поскольку каждая такая машина содержит не только операционную систему, но и необходимое для работы виртуальное оборудование. Контейнерам «своя» ОС не нужна.

Но вернемся к вопросу классификации CaaS. Ресурсным элементом в данном случае служит не виртуальный или физический сервер, а контейнер. Хотя большинство экспертов склонны рассматривать CaaS как подмножество IaaS, некоторые считают, что эти услуги находятся между IaaS и PaaS (рис. 3).

Пользователям услуги CaaS предоставляется возможность производить различные операции с контейнерами (загружать, организовывать, запускать, останавливать), оплачивая только используемые объемы ресурсов. Эти услуги могут оказаться чрезвычайно привлекательными для оптимизации процессов разработки и вывода новых решений на рынок. При этом контейнеризация позволяет осуществлять собственно разработку и тестирование, например, в публичном облаке, а потом, при необходимости, легко переносить приложения в частное облако. В целом контейнерные технологии помогают мигрировать между различными вариантами размещения: on-premise, частное облако, публичное облако.

Третий этап: переосмысление

Следующий шаг связан с переосмыслением компаниями всей своей ИТ-инфраструктуры и бизнес-процессов с учетом применения облачных, а фактически мультиоблачных сред. На этом этапе все больше решений создается для облаков с нуля – они становятся cloud native.

Мультиоблачный подход дает новые возможности, в том числе в части дальнейшей оптимизации ИТ. Но здесь не все однозначно. Дело в том, что при реализации мультиоблачной модели могут существенно вырасти расходы на интеграцию и управление, что сведет на нет экономические выгоды. Многие поставщики облачных сервисов рассматривают друг друга в качестве конкурентов, а потому не стремятся помогать заказчикам в вопросах интеграции.

Важен и вопрос безопасности. Чем больше облаков вы используете, тем больше существует потенциальных угроз безопасности, для ликвидации которых опять-таки потребуются дополнительные средства. Следует учитывать, что большинство облачных приложений и сервисов не обеспечивают выполнения требований корпоративной безопасности по умолчанию.

Произошедшие в апреле 2018 г. события, связанные с попытками блокировки сервиса Telegram в России, также показали риск использования популярных западных облаков. В условиях, когда этот сервис начал «скакать» с одной подсети на другую, российскому регулятору ничего не оставалось, как заставлять операторов блокировать все новые и новые миллионы IP-

В копилку строителей гибридного облака

Сегодня компании среднего и крупного бизнеса во всем мире склоняются к построению виртуальной инфраструктуры по гибридной модели. В ее рамках использование вычислительных ресурсов, расположенных в корпоративных дата-центрах, сочетается с размещением вычислительных мощностей на площадках провайдеров публичных облачных сервисов. По оценке Василия Лизунова, менеджера по развитию бизнеса Intel, в публичных облаках находятся 30–40% всех приложений, а 60–70% компании держат в частном облаке.

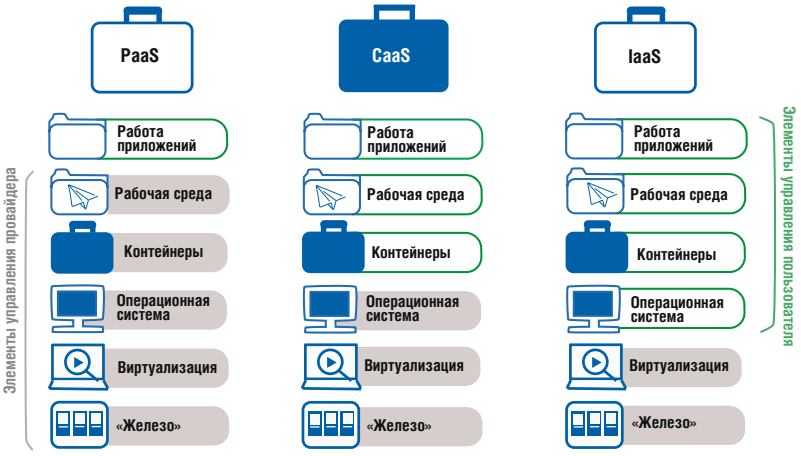
Вариантов «гибридизации» облачных сред множество: можно прибегнуть к моновендорным облачным решениям (например, на платформах VMware или Microsoft), можно создавать решения «своей» конфигурации с использованием систем open source.

Поскольку Intel работает со всеми ведущими облачными провайдерами, а также со всеми значимыми open source-проектами, у вендора есть собственное видение тактики построения гибридного облака. По словам В. Лизунова, начать стоит с ревизии ИТ-сервисов компании, чтобы по ее результатам составить план их постепенного перевода в облако. Следующий шаг предполагает выбор отвечающей задачам компании SDI-модели (Software-Defined Infrastructure) из трех возможных: традиционной, конвергентной и гиперконвергентной. К преимуществам последнего варианта можно отнести лучшую совместимость компонентов решения, большие производительность, гибкость и масштабируемость.

Цифровая трансформация бизнеса, которая базируется на использовании облачных технологий, предполагает наличие в компании приложений, от работоспособности которых напрямую зависит ее бизнес. Понятно, что подобные программные продукты полностью адаптированы к потребностям компании и

адресов, в том числе популярных облачных сервисов Google Cloud, AWS, Digital Ocean, Azure. Из-за этого пострадали ни в чем не повинные сервисы – от мессенджера Viber до электронных касс одной из ритейловых сетей.

Тем не менее при всех сложностях мультиклауд – будущее облачной модели. Но для ее успешной реализации необходима безопасная интеграция приложений и данных, задействованных в разных облачных средах. Заказчикам следует требовать обеспечения такой интеграции непосредственно от сервис-провайдеров, которым в условиях все более острой конкуренции неизбежно придется осваивать новые для многих компетенции.



Источник: Atlex

Рис. 3. Варианты классификации PaaS, CaaS и IaaS

Курс на гиперконвергенцию

Наряду с самими облачными сервисами развиваются и технологические платформы, на которых они предоставляются. Здесь тоже можно выделить три этапа. На первом для предоставления облачных сервисов использовалась традиционная (распределенная) мультивендорная ИТ-инфраструктура, в состав которой, помимо объединенного локальной сетью (Ethernet) серверного комплекса, как правило, входила сеть средств хранения (SAN на базе Fibre Channel).

В качестве следующего шага некоторые ведущие производители предложили интегрированные (конвергентные) комплексы, укомплектованные проверенными на совместимость компонентами, которые реализуют комплексное решение. В состав конвергентных решений входят продукты двух-трех производителей, скажем, сетевые компоненты и серверы одной компании, а СХД – другой. Но в таких решениях, пусть и упакованных в одну стойку, серверы и СХД остаются отдельными элементами.

Третий шаг – выпуск гиперконвергентных решений как ответ на желание заказчиков сэкономить за счет отказа от дорогостоящих выделенных систем хранения данных и сетей SAN. Такие решения состоят из универсальных узлов, реализующих как вычислительные функции, так и функции хранения данных. Кроме того, внутри такого узла имеются все необходимые средства сетевого взаимодействия (рис. 4). Часто за основу гиперконвергентного узла берется обычный сервер x86, который оснащается необходимым числом накопителей. Но это не есть возврат в 90-е годы прошлого столетия, когда активно использовались напрямую подключаемые системы хранения (Direct-Attached Storage, DAS). В отличие от архитектуры DAS, которая

уникальны с точки зрения функциональности. Их невозможно купить, а приходится создавать и развивать собственными силами.

При переводе бизнеса на «цифровые рельсы» скорость изменений в продуктах и сервисах компании возрастает, требуется чуть ли не ежедневное обновление соответствующих ключевых приложений. Этого невозможно добиться при классическом подходе к разработке ПО, поэтому сегодня на повестку дня выходит применение гибкой методологии разработки (Agile) и набора практик DevOps, описывающего технологический подход к организации инфраструктуры для ее реализации, констатирует Андрей Николаев, специалист по облачным платформам компании Dell EMC.

Кроме того, изменения затрагивают саму архитектуру бизнес-приложений. На смену монолитной архитектуре все чаще приходит архитектура микросервисная. Вся функциональность в ней делится на отдельные блоки, каждый из которых «живет» в инфраструктуре как независимый сервис и обращается к своей собственной локальной базе данных. Такая архитектура позволяет разработчикам при необходимости вносить изменения в код отдельного блока, не влияя на работоспособность остальных. Тем самым складываются предпосылки для того, чтобы процесс производства ПО в компании становился непрерывным и автоматизированным.

Правда, при этом важно позволить разработчику сфокусироваться на своей основной задаче – написании кода, освободив его от решения инфраструктурных задач и необходимости думать о том, как работает и настраивается инфраструктура, в которой запускаются его приложения. Как этого добиться? Один из вариантов – использование специализированного PaaS-решения, которое обеспечивало бы автоматическое размещение кода в среде исполнения.

Александра Крылова

приводит к образованию изолированных островков хранения, в гиперконвергентных системах каждый сервер может воспользоваться ресурсами хранения на других серверах. Фактически в них реализуется виртуальная сеть хранения (VSAN).

Например, об использовании систем, в которых вычислительные ресурсы и СХД были бы реализованы в одном блоке, в Cloud4Y задумывались еще девять лет назад. Но, по словам Евгения Бессонова, директора по маркетингу этой компании, удовлетворительных (по технико-экономическим показателям) решений тогда не оказалось. Этот провайдер изначально пробовал использовать сеть SAN на базе протокола Fibre Channel, но выявленные недостатки (отсутствие необходимой гибкости, невозможность построить metro-инфраструктуру между двумя ЦОДами) заставили отказаться от этого решения и сделать выбор в пользу iSCSI. Но, похоже, время гиперконвергенции наступает. Все больше сервис-провайдеров устанавливают такие решения и рапортуют об их многочисленных преимуществах.

Одним из пионеров этой тенденции стала компания Linxdatacenter, которая первой среди поставщиков услуг коммерческих ЦОДов в России развернула для предоставления сервисов IaaS гиперконвергентное решение, а именно Cisco HyperFlex. Это решение построено на основе серверов Cisco UCS, к которым добавлена платформа HX Data, объединяющая твердотельные и дисковые накопители в единое распределенное многоуровневое объектное хранилище данных. Облачные платформы, установленные в других ЦОДах Linxdatacenter – в Варшаве (2012 г.) и Санкт-Петербурге (2013 г.), – построены на основе конвергентного решения FlexPod. В 2017-м, когда было запущено облако в Москве, выбор был сделан уже в пользу гиперконвергентной платформы. Главным результатом развертывания гиперконвергентного решения, по словам Константина Андреенко, технического консультанта Linxdatacenter, стало увеличение прибыли, получаемой с 1 кв. м площади ЦОДа, что особенно важно для объекта, расположенного в центральной части Москвы.

Еще один сервис-провайдер, Orange Business Services, решил отказаться от классической архитектуры (отдельно серверы, отдельно СХД) и тоже строит свое «облако 2.0» на базе гиперконвергентных решений. В России компания использует для этого серверы Huawei и программное хранилище VMware vSAN. Как сообщил Алексей Кречетов, менеджер по развитию бизнеса Orange Business Services, в Москве будет реализовано metro-облако, «растянутое» на две площадки. «Классических СХД в нем не будет – только рэк-серверы, «набитые» дисками, виртуальная СХД. Это решение дешевле, надежнее и гибче. Его очень просто расширять, – рассказывает А. Кречетов. – Задержка между площадками меньше 2 мс, поэтому репликация будет синхронной».

Рис. 4. Традиционная и гиперконвергентная ИТ-инфраструктура

Источник: Orange Business Services

Облака становятся распределенными

Ввиду большой протяженности производственных мощностей и офисов многих компаний в России и их удаленности друг от друга сетевые задержки зачастую критически влияют на бизнес вплоть до того, что не все приложения можно развернуть в облаке и надо делать локальное решение. Поэтому, например, Orange Business Services в рамках описанного выше проекта планирует разворачивать региональные облака-сателлиты с резервированием в центральных хабах. К таким хабам – первый из них создается в Москве – предъявляются особые требования по отказоустойчивости и гибкости.

Тема децентрализации облаков и пограничных вычислений неразрывно связана с так называемыми туманными вычислениями – fog computing. Компания SONM, по словам ее технического директора Игоря Лебедева, собирается создать платформу, которая позволит использовать узлы fog computing для предоставления облачных сервисов. Этими узлами могут служить бытовые компьютеры обычных пользователей, незадействованные ресурсы которых можно направить на обработку задач внешних заказчиков. Такой подход обещает существенное снижение стоимости облачных сервисов. К осени 2018 г. SONM планирует вывести на рынок решение для предоставления услуг IaaS и CaaS, а к концу года – PaaS.

■ ■ ■

Что ж, облачные модели становятся все интереснее для специалистов и привлекательнее для заказчиков. Вопрос в обеспечении SLA и безопасности – но это уже тема для отдельного разговора. ИКС

Реальность дополненной стоимости

AR- и VR-инструменты помогают увеличивать продажи и обучать промышленный персонал без остановки производства.

Илья Симонов, директор Центра виртуальной реальности, КРОК

От фантастики к инструменту для бизнеса

Виртуальная и дополненная реальность перестают быть просто трендом и все больше осознаются бизнесом и промышленностью как один из инструментов, на которых будут строиться цифровая экономика и обновляться реальный сектор. В компаниях появляются целые подразделения, заинтересованные в инструментах виртуальной реальности. Уже сейчас в крупном бизнесе создаются позиции CDO (Chief Digital Officer), отвечающих за внедрение цифровых технологий и digital-трансформацию. Главной целью компаний становятся формирование платформы для изменений, обусловленных цифровым развитием, и понимание нового места технологий в бизнесе.

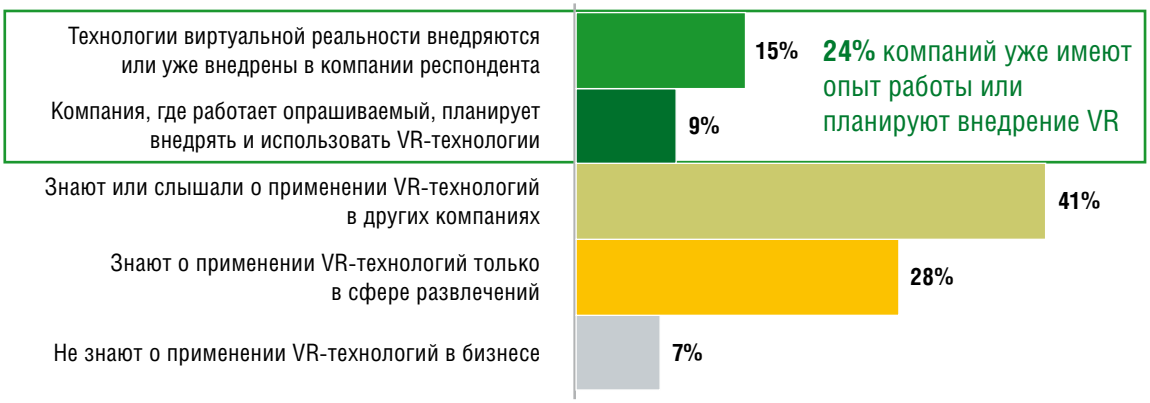
В 2017 г. Центр виртуальной реальности КРОК и Институт современных медиа (Modern Media Research Institute, MOMRI) провели совместное исследование заинтересованности крупнейших российских компаний и отраслей в применении технологий виртуальной реальности в бизнесе. В исследовании приняли участие 247 руководителей и специалистов различного профиля, представляющих более 200 крупнейших компаний России. Согласно данным исследования, почти две трети (65%) опрошенных знают о перспективах использования технологий VR и AR на предприятиях (рис. 1 и 2). Причем уровень осведомленности одинаково высок как в реальном секторе, так и в сфере услуг. О примерах успешного внедрения VR в технологические и бизнес-процессы слышали в металлургии, машиностроении, строительном бизнесе, энергетике, транспортной отрасли, а также в банковском и телеком-секторах.

Более 40% опрошенных сообщили, что знакомы с примерами внедрения виртуальной реальности в других компаниях. Участники исследования называли решения для промышленного, строительного и инженерного проектирования, продаж жилой недвижимости, виртуальные обзоры производственных объектов, применение VR в обучении сотрудников (тренажеры и симуляторы). Почти четверть – 24% – представителей российского бизнеса заявили, что в их компаниях VR-технологии уже внедрены или их внедрение планируется.

Отраслевое применение AR/VR-технологий

На международных технологических конференциях, говоря о виртуальной и дополненной реальности, все чаще прибегают к термину XR, объединяющему все виды «реальностей» и смежных технологий, связанных с компьютерной графикой. Несмотря на ажиотаж вокруг этих технологий, не стоит считать AR и VR универсальным средством решения проблем в бизнесе. Задумываясь о внедрении инструментов виртуальной и дополненной реальности, нужно четко понимать, в каких сценариях их планируется использовать.

В начале перехода к VR и AR необходимо разработать критерии оценки результатов внедре-



Источник: исследование Центра виртуальной реальности КРОК и MOMRI, 2017 г.

Рис. 1. Применение технологий VR в бизнесе: опыт компаний и осведомленность о бизнес-кейсах

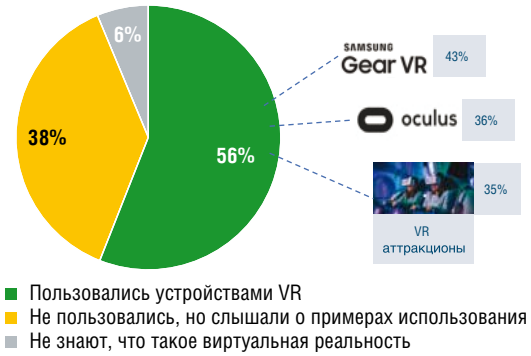


Рис. 2. Наличие у руководителей предприятий опыта использования VR-устройств

Источник: исследование Центра виртуальной реальности КРОК и MOMRI, 2017 г.

ния и осознать, что эффект не будет сиюминутным и окупаться такие проекты будут достаточно долго. Определяющим фактором при принятии решений о внедрении XR остаются технологическая готовность предприятий и зрелость самих технологий. В России драйверами корпоративного AR/VR-рынка выступают строительные компании, ритейл, промышленные предприятия и крупные музеи. Для более широкого промышленного применения этих технологий необходимы инфраструктура XR-ready, достаточное количество пользователей и доступных устройств с поддержкой AR- и VR-приложений. Отставание нашей страны во внедрении VR и AR от западных рынков составляет сейчас полтора-два года.

В числе сценариев, где технологии виртуальной и дополненной реальности себя уже зарекомендовали, можно назвать обучение, проектирование, строительство, продажи и музейное дело.

На промышленных предприятиях VR-тренажеры и AR-приложения применяются для отработки технологических процедур, связанных с обслуживанием производственных активов и действий в нештатных ситуациях. Они полезны и в ходе практического освоения новых навыков. В России уже есть пилотные проекты по работе с промышленным оборудованием с помощью AR. При обслуживании технических активов с помощью AR можно создавать подсказки и инструкции для производственного персонала для работы в «поле». Например, при наведении камеры планшета с установленным приложением на то или иное оборудование сотрудник будет видеть интерактивные подсказки, инструкции по работе на станке или порядок действий при замене какого-либо компонента. Такие приложения достаточно широко используются в логистике, помогая сотрудникам складов повысить эффективность складских операций и быстрее ориентироваться в помещении склада.

В международной компании Royal Dutch Shell перешли к виртуальным интерактивным тренингам для персонала. Это позволило на 90% сократить расходы на дорогостоящие обучающие программы. В России для обучения и тестирования персонала крупной газораспределительной компании Центр виртуальной реальности КРОК разработал AR-приложение, которое помогает сотрудникам осваивать последовательность операций при переключении режимов газораспределительного оборудования (рис. 3). Используя AR/VR-приложения, в том числе в «полях», можно отрабатывать навыки обслуживания инфраструктуры и изучать порядок действий. Такой подход помогает производственному персоналу в регионах обучаться без посещения учебного центра и

МНЕНИЕ ЭКСПЕРТА

7 вещей, которые надо знать про XR

Эрик Вандербург, специалист по безопасности и технологиям

В последнее время много говорят о виртуальной реальности. Но что действительно способно расширить наши возможности и позволить взаимодействовать с технологиями в более интуитивной манере – это дополненная и смешанная реальности.

В виртуальной реальности вы погружаетесь в вымышленный мир, а в дополненной реальности виртуальные или искусственные элементы накладываются на мир вокруг вас, хотя вы не можете взаимодействовать с этим контентом. Поэтому дополненная реальность имеет преимущественно информационное назначение. Смешанная реальность похожа на дополненную, но отличается от нее тем, что позволяет взаимодействовать с виртуальными и реальными объектами.

Дополненная реальность

1. Дополненная реальность дает возможность человеку, оставаясь в реальном мире, пользоваться интернетом и специально разработанными приложениями и сервисами. Так, сотрудники, находящиеся на заводе, должны взаимодействовать с реальной средой, а не с виртуальным миром.

2. Дополненная реальность освободит руки. Рабочие смогут действовать свободно, оставаясь при этом подключенными к интернету. Более того, системы дополненной реальности можно использовать в любом положении: лежа (например, под автомобилем), стоя и даже в движении. Эта технология расширяет диапазон наших обычных действий и в то же время не отвлекает. Согласно исследованию Future Workforce Study, проведенному Dell и Intel, 77% молодых людей и 47% людей старшего поколения готовы использовать дополненную реальность в профессиональной деятельности.

3. Дополненная реальность оптимизирует наши бизнес-процессы. Она упрощает доступ к под-

не требует инвестиций в создание филиалов учебных центров. Благодаря высокой степени погружения в моделируемые сценарии сотрудники получают практический опыт, который сложно воссоздать в реальной жизни без остановки производственных мощностей. Подобный проект есть в компании СИБУР, которая обучает сотрудников на виртуальном компрессоре. В оборонном комплексе на VR для обучения переходят Королевские военно-морские силы Норвегии. Внедрение носимых VR-тренажеров дает возможность воспроизводить полетные палубы и наземные аэродромные среды для освоения процедур обработки воздушных судов.

В учебном центре Центральной пригородной пассажирской компании установлен VR-тренажер для тестирования и обучения сотрудников при приеме на работу и в ходе их переаттестации. Внедрение виртуальной реальности в подготовку персонала улучшило ответы на профессиональные вопросы почти на 65%. Концерн Boeing при помощи VR и AR на 75% сократил время, затрачиваемое на обучение сотрудников тому, как правильно соединять кабели при сборке сложнейших систем самолетов.

В сфере промышленного проектирования VR-технологии применяются для детальной технической визуализации инженерных данных. Польза заключается в своевременном обнаружении ошибок и их устранении на конвейере еще до запуска изделия в серию. Применение VR-технологий ускоряет принятие конструкторских и инвестиционных решений. В строительстве визуализация полезна в связке с технологией BIM. Она позволяет ускорить работу над проектами, упростить процесс согласования и избежать ошибок на ранних этапах проектирования зданий и сооружений.

Рис. 3. AR-приложение для отработки последовательности операций при переключении режимов газораспределительного оборудования

В нефтедобывающей индустрии один из сценариев, получающих распространение в России, – применение VR-технологий для контроля и управления рисками на всех этапах работ на месторождениях. С помощью VR можно наглядно визуализировать информацию, полученную в ходе исследований шельфа, моделировать скважины и технологические процессы, применять визуализацию при проектировании и строительстве буровых платформ. VR-симуляторы дают персоналу нефтеперерабатывающих заводов и буровых платформ возможность лучше усвоить действия в нештатных ситуациях и позволяют более эффективно управлять рисками.

МНЕНИЕ ЭКСПЕРТА

держке, поскольку технический ассистент в удаленном центре может видеть, над чем вы работаете в данный момент, и давать конкретные подсказки. Такая технология также представляет большую ценность для обучения. Указания или демонстрации во время выполнения задачи могут быть наложены прямо на реальный мир.

4. Дополненная реальность открывает массу возможностей. Скажем, можно «просветить» оборудование с помощью внутренних сенсоров или наложить инфракрасные сигнатуры на привычное поле зрения. Вы можете видеть навигационные подсказки во время прогулки или контактные данные человека, когда на него смотрите (с помощью функции распознавания лиц).

Смешанная реальность

5. В смешанной реальности возможность взаимодействовать с виртуальными и реальными объектами используется, в частности, для управления устройствами интернета вещей. Данные от датчиков и устройств, проецируемые соответствующим оборудованием, могут окружать пользователя в пространстве. Например, дежурный на насосной станции может таким образом наблюдать за давлением в системе. С помощью технологии смешанной реальности он может вносить коррективы в рабочий процесс, не прекращая обхода и не прибегая к помощи компьютера в центре управления.

6. Смешанная реальность также может сочетаться с системами безопасности. Представьте, к примеру, дверь, оборудованную камерой. Когда человек подходит к этой двери, надетая на него система смешанной реальности отображает перед его глазами серию картинок. Передвигая их в пространстве, пользователь вводит код доступа. Камера в двери узнает текущий код, связываясь с оборудованием пользователя.

7. Смешанная реальность способна помочь в создании контента. Представьте рисование с помощью виртуальных кистей, манипулирование 3D-объектами, которые можно обойти со всех сторон, или общий письменный стол для двух человек, каждый из которых находится в своем офисе.

▲
Рис. 4. Использование AR/VR-технологий позволяет получить дополнительную информацию об экспонатах

Ведущие российские музеи, несмотря на консервативность, также видят перспективы во внедрении VR и AR. Здесь потенциал технологий виртуальной реальности заключается в создании нового опыта посещения музея и сохранении музейных ценностей в формате цифровых копий, а также в расширении экспозиционных возможностей. Первым из российских музеев заинтересовался такими проектами Государственный Эрмитаж. В ходе совместного с музеем проекта специалистами Центра виртуальной реальности КРОК создана виртуальная копия зала Юпитера, полностью повторяющая его интерьер и 46 экспонатов (рис. 4). Теперь с помощью технологий виртуальной реальности можно познакомиться с богатейшей коллекцией античного искусства, не посещая Эрмитажа.

Виртуальная и дополненная реальность хорошо работают в продажах технически сложной продукции и маркетинге. Например, компания DeLaval, производитель оборудования для оснащения ферм, с помощью AR-приложения демонстрирует высокотехнологичные комплексы для молочного животноводства, которые практически невозможно привезти потенциальному покупателю (рис. 5). Для поддержки выставочных мероприятий компания использует столы виртуальной голографии для наглядной демонстрации работы «умных» ферм. Сеть Leroy Merlin с помощью приложений дополненной реальности дает возможность «примерить» мебель и декоративные товары к реальному интерьеру — через камеру iPhone или iPad. Продукцию можно не только тщательно рассмотреть, но и купить тут же, не закрывая приложение. Компания Gilette для демонстрации новых лезвий запустила в ряде магазинов ролик с VR для потенциальных покупателей. В результате продажи Gillette ProShield в этих точках увеличились на 30%. Amazon внедрила поддержку AR в своем iOS-приложении. Благодаря этому появилась функция AR View, которая активизируется нажатием на значок камеры в приложении Amazon и помогает выбрать любой товар из соответствующих категорий: мебель, кухонная посуда, домашний декор.

Рис. 5. AR-приложение для демонстрации высокотехнологичных комплексов в сфере молочного животноводства ▼

Телекоммуникационные операторы заинтересованы в VR и AR не меньше ритейла. В первую очередь эти технологии могут использоваться при запуске маркетплейсов и лечь в основу новых контентных сервисов для абонентов. В условиях трансформации бизнес-моделей телекомоператоров ставка на эти технологии позволит в будущем увеличить выручку за счет дополнительных услуг.

Перспективы внедрения AR/VR-решений

В 2018 г. на фоне роста интереса к AR/VR-технологиям увеличивается количество проектов с предсказуемым экономическим эффектом. Однако пока существует дисбаланс между ценой решений виртуальной реальности и потребностями предприятий в их внедрении. Главный вопрос: как оценить стоимость проекта или хотя бы ее порядок? У VR-проектов довольно длительный срок окупаемости, а их экономический эффект станет ощутимым через три–пять лет.

Массовое использование AR в бизнес-сегменте тесно связано с коммерческим запуском сетей 5G, который в 2018 г. не планируется. Несмотря на это, крупный ритейл уже осознал пользу AR/VR-технологий. Так, дополненная реальность меняет способ взаимодействия с потребителем и в этом смысле очень перспективна для создания новых сервисов и формирования пользовательского опыта совершенно нового типа за счет возможности увидеть товар или объект в деталях. С помощью VR можно показать тысячи наименований товаров в магазине небольшой площади. Промышленные компании тоже поняли, что

технологии AR/VR работают, но у них пока нет подходящей инфраструктуры, например, достаточного покрытия скоростного Wi-Fi.

Усложняет внедрение профессиональных XR-систем отсутствие в штате компаний квалифицированных специалистов, способных их разворачивать и обслуживать. Промышленные предприятия только начинают нанимать компетентный в применении VR- и AR-инструментов персонал.

Еще одно препятствие широкому проникновению технологий дополненной и виртуальной реальности в бизнесе (рис. 6) – отсутствие отечественных AR-очков для промышленного применения, надежных и обладающих сертификатами. С другой стороны, появление смартфонов с поддержкой мобильных AR-приложений, ARKit и ARCore способствует массовому проникновению AR на российский рынок.

Полноценный опыт погружения в виртуальную реальность обеспечивают наголовные (HMD) устройства, которые пока дороги и не нашли широкого применения в бизнесе. Это один из сдерживающих факторов массового внедрения VR. Производители недорогих HMD-гарнитур из Китая, предлагая пользователям свои разработки, поддерживают распространение VR-технологий.

Оценка по 5-балльной шкале, где 1 балл – не является препятствием, 5 баллов – является очень серьезным препятствием

Источник: исследование Центра виртуальной реальности КРОК и MOMRI, 2017 г.

▲ **Рис. 6. Препятствия внедрению VR-технологий**

Пути внедрения AR/VR-технологий

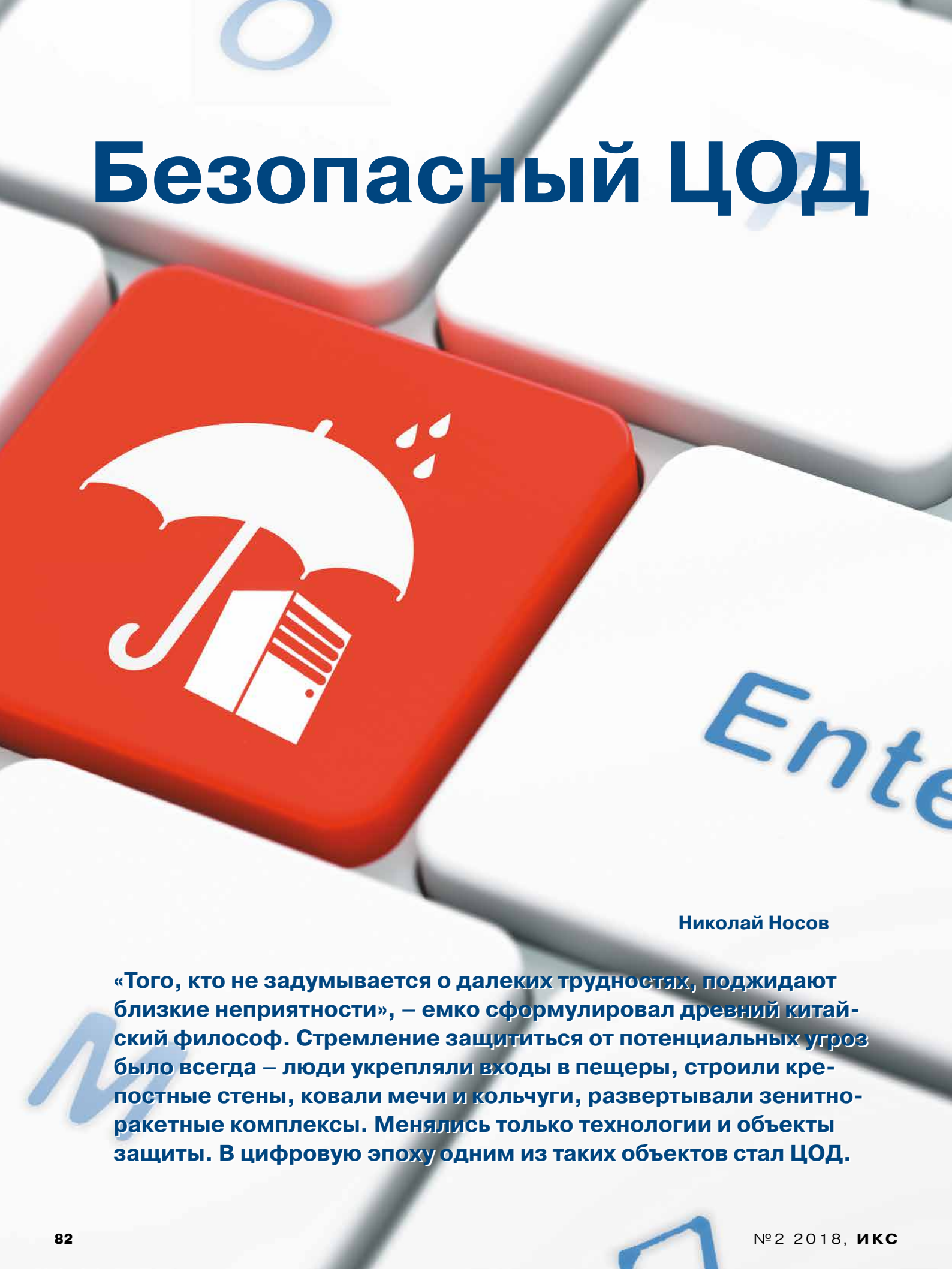
Оптимальным сценарием при переходе к AR/VR может стать аутсорсинг. Идеально начать с аудита производственных операций, поскольку для внедрения необходимо разработать регламенты, разработать или закупить симуляторы (при необходимости), разработать 3D-интерфейсы для приложений персональных или планшетных ПК (3D-приложений) и только потом создавать VR-интерфейсы. Без аудита практически невозможно рассчитать эффективность будущего проекта. Поэтому переход к VR должен быть поэтапным и максимально подготовленным на всех уровнях. Начав с внешнего консалтинга и аудита перед внедрением виртуальных тренажеров в производственные процессы, можно далее получать весь цикл сервисной поддержки вплоть до обучения персонала работе с системами виртуальной реальности.

Один из главных вызовов, стоящих перед предприятиями, – наличие XR-ready инфраструктуры, среды, полностью готовой к внедрению VR- и AR-приложений. Значительная доля стоимости проекта приходится на вычислительные ресурсы и производительные графические процессоры. На их основе создается среда для работы с VR-контентом, который требователен к быстродействию серверов и пропускной способности каналов связи. Например, при коллективном обучении важен быстрый отклик оборудования, чтобы изображение без задержки перемещалось по мере движения пользователя. Для конструкторов и инженеров нужны производительные рабочие станции для работы с 3D-моделями и одновременного доступа к ним. Это создает большие вычислительные нагрузки, влияя на общую производительность инфраструктуры. Поэтому еще на этапе планирования необходимо рассчитать допустимый предел нагрузок и подготовить инфраструктуру к работе с графикой, обеспечив надежное резервирование ИТ-мощностей.

Уже на этапе пилотов важно получать метрики для оценки целесообразности развертывания XR-инструментов. Эти метрики должны отражать влияние технологий на скорость, качество исполнения, упрощение технологических или бизнес-операций. Например, в обучении промышленного персонала помимо самой разработки учебной программы нужно создавать методику ее испытаний, включая KPI по срокам обучения, контролю остаточных знаний, проведению тестирований. Важно понимать, какого результата мы хотим добиться: снижения травматизма на опасных производствах, сокращения затрат на обучение или формирования нового клиентского опыта. От этого будет зависеть целесообразность внедрения VR и AR на том или ином этапе производства или бизнес-процесса.

AR/VR-инструменты для обучения персонала не только позволяют сотрудникам погрузиться в виртуальную среду, но и увеличивают их вовлеченность в процесс обучения благодаря возможности пройти тренинг на рабочем месте. Причем в два раза сокращаются и время на изучение учебных материалов, и затраты на обучение, более эффективным становится планирование ресурсов сотрудников. В результате AR/VR-технологии помогают снизить технические риски, отработать последовательность любых операций, уменьшить количество ошибок персонала и сделать обучение сотрудников работе с новыми техническими средствами более наглядным. ИКС

Безопасный ЦОД



Николай Носов

«Того, кто не задумывается о далеких трудностях, поджидают близкие неприятности», – емко сформулировал древний китайский философ. Стремление защититься от потенциальных угроз было всегда – люди укрепляли входы в пещеры, строили крепостные стены, ковали мечи и кольчуги, развертывали зенитно-ракетные комплексы. Менялись только технологии и объекты защиты. В цифровую эпоху одним из таких объектов стал ЦОД.

Политики информационной безопасности

Для злоумышленников наиболее привлекательны информационные системы банков, и не удивительно, что именно банки стали лидерами в деле защиты информации, а разработанные ими стандарты безопасности – ориентиром для других отраслей.

В 2010 г. Банком России был принят первый отраслевой стандарт обеспечения информационной безопасности СТО БР ИББС-1.0-2010, который распространялся и на дата-центры коммерческих банков. Предложенные принципы построения системы нормативных документов безопасности можно сравнить с подходом к управлению государством.

На первом (верхнем) уровне – в общей политике (концепции) ИБ, как и в конституции страны, прописываются общие задачи, которые конкретизируются в частных политиках (второй уровень), таких как «Политика физической защиты информационных систем», «Политика управления доступом и регистрацией», «Политика использования средств криптографической защиты информации» и т.п. Третий уровень представляют регламенты, процедуры и инструкции, подробно описывающие способы применения средств защиты, порядок и частоту выполнения процедур. Примером могут служить положения о персональных данных, о проведении аварийного восстановления, регламент контроля состояния систем информационной безопасности. Нижний уровень – журналы учета предоставления доступа, сообщений об инцидентах ИБ, аудита систем.

Основными объектами защиты при обеспечении информационной безопасности ЦОДа являются: информационные ресурсы (данные); процессы сбора, обработки, хранения и передачи информации; пользователи системы и обслуживающий персонал; информационная инфраструктура, включающая технические и программные средства обработки, передачи и отображения информации, в том числе каналы информационного обмена, системы защиты информации и помещения. Зона ответственности ЦОДа зависит от модели предоставляемых услуг (табл. 1).

Важнейшая часть разработки политики информационной безопасности – построение модели угроз и нарушителей (табл. 2).

Анализ рисков – выявление потенциальных угроз и оценка масштабов последствий их реализации – поможет правильно выбрать первоочередные задачи, которые должны решать специалисты по информационной безопасности ЦОДа, спланировать бюджеты на покупку технических и программных средств.

Обеспечение безопасности – непрерывный процесс, который включает этапы планирования, реализации и эксплуатации, мониторинга, анализа и совершенствования системы ИБ. Для создания систем менеджмента информационной безопасности используют так называемый цикл Деминга.

Важной частью политик безопасности является распределение ролей и ответственности персонала за их выполнение. Следует постоянно пересматривать политики с учетом изменений законодательства, новых угроз и появляющихся средств защиты. И, конечно, доводить требования к информационной безопасности до персонала и проводить его обучение.

Colocation	IaaS	Paas	SaaS
Помещение	Помещение	Помещение	Помещение
Персонал	Персонал	Персонал	Персонал
Каналы связи	Каналы связи	Каналы связи	Каналы связи
Инженерная инфраструктура	Инженерная инфраструктура	Инженерная инфраструктура	Инженерная инфраструктура
Сеть	Сеть	Сеть	Сеть
Хранилища	Хранилища	Хранилища	Хранилища
ОС	ОС	ОС	ОС
Виртуализация	Виртуализация	Виртуализация	Виртуализация
Серверы	Серверы	Серверы	Серверы
Данные	Данные	Данные	Данные
Платформы	Платформы	Платформы	Платформы
Приложения	Приложения	Приложения	Приложения
Зона ответственности ЦОДа		*Зона ответственности клиента*	

Таблица 1. Область действия политики безопасности ЦОДа в зависимости от модели предоставляемых сервисов

Организационные меры

Некоторые эксперты скептически относятся к «бумажной» безопасности, считая главным умение взламывать системы. Практический опыт работы по обеспечению информационной безопасности в банках говорит об обратном. Специалисты по ИБ могут иметь отличную экспертизу в деле выявления и снижения рисков, но если персонал ЦОДа не будет выполнять их указания, все будет напрасным.

Таблица 2. Модель угроз и нарушителей ИБ

1	Неблагоприятные события природного, техногенного и социального характера
2	Террористы, криминальные элементы и др.
3	Зависимость от поставщиков, провайдеров, партнеров, клиентов
4	Сбои, отказы, разрушения, повреждения программных и технических средств
5	Сотрудники ЦОДа, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ)
6	Сотрудники ЦОДа, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не относящиеся к персоналу ЦОДа, но осуществляющие попытки несанкционированного доступа и неразрешенных действий (внешние нарушители ИБ)
7	Несоответствие требованиям надзорных и регулирующих органов, действующему законодательству

Чтобы попасть в машзал в ЦОДе Сбербанка в Сколково, нужно пройти через сканирующую кабину

Безопасность, как правило, не приносит денег, а лишь минимизирует риски. Поэтому к ней часто относятся как к чему-то мешающему и второстепенному. Требования специалистов по безопасности нередко приводят к конфликтам с персоналом и руководителями эксплуатационных подразделений.

Наличие отраслевых стандартов и требований регуляторов помогает безопасникам отстаивать свои позиции на переговорах с руководством, а утвержденные политики ИБ, положения и регламенты позволяют добиваться от персонала выполнения изложенных там требований, подводя базу под проведение зачастую непопулярных решений.

Защита помещений

При предоставлении ЦОДом услуг по модели colocation на первый план выходит обеспечение физической безопасности и контроля доступа к оборудованию клиента. Для этого используются выгородки (огороженные части зала), которые находятся под видеонаблюдением клиента и к которым доступ персонала ЦОДа крайне ограничен.

В государственных вычислительных центрах с физической безопасностью и в конце прошлого века дела обстояли неплохо. Был пропускной режим, контроль доступа в помещения, пусть без компьютеров и видеокамер, системы пожаротушения – в случае возгорания в машинный зал автоматически пускался фреон.

В наше время физическая безопасность обеспечивается еще лучше. Системы контроля и фотоуправления доступом (СКУД) стали интеллектуальными, внедряются биометрические методы, например контроль входа в машзал по руке человека в ЦОДе IXcellerate или специальная кабинка, сканирующая человека при доступе в машзал ЦОДа Сбербанка в Сколково.

Более безопасными для персонала и оборудования стали системы пожаротушения, среди которых можно выделить установки пожаротушения тонкораспыленной водой. Наряду с обязательными системами противопожарной защиты в ЦОДах часто используется система раннего обнаружения пожара аспирационного типа.

Для защиты дата-центров от внешних угроз – пожаров, взрывов, обрушения конструкций здания, затопления, коррозийных газов – стали использоваться комнаты и сейфы безопасности (см. «ЦОДу и стены помогают»), в которых серверное оборудование защищено практически от всех внешних повреждающих факторов.

Слабое звено – человек

«Умные» системы видеонаблюдения, датчики объемного слежения (акустические, инфракрасные, ультразвуковые, микроволновые), СКУД снизили риски, но не решили всех проблем. Эти средства не помогут, например, когда правильно допущенные в ЦОД люди с правильно пронесенным инструментом что-нибудь зацепят («Из чего состоит безопасность», с. 89).

На работе дата-центра может сказаться нецелевое использование персоналом его ресурсов, например нелегальный майнинг («Как бороться с нелегальным майнингом в ЦОДах?», с. 41).

МНЕНИЕ ЭКСПЕРТА

Александр Нилов, старший менеджер по продуции для ИТ-инфраструктуры, Rittal

ЦОДу и стены помогают

Центры обработки данных могут пострадать от пожара, возникшего в других помещениях или зданиях, а в случае аварии в системе водоснабжения – подвергнуться затоплению из расположенных выше помещений. Нередко присутствуют и риски воздействия внешних коррозийных газов, а также взрыва и обрушения здания – например, на химических производствах.

Проблему могут решить комнаты безопасности, которые создаются внутри уже существующих помещений. В такой защищенной от внешних угроз комнате располагается машинный зал, а мини-ЦОД из нескольких стоек с критически важной инфраструктурой можно разместить в сейфе безопасности.

Особенно актуально использование подобных решений на вновь строящихся заводах, поскольку они подпадают под действие приказа Ростехнадзора № 96 от 11.03.2013, утверждающего общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств. Согласно этому приказу, все оборудование, которое отвечает за технологические процессы, должно располагаться в помещениях, выдерживающих взрывную волну в 21 кПа. Так что взрыв такой силы должно вы-

Помочь в этих случаях могут системы управления инфраструктурой ЦОДа (DCIM).

Защиты требует и сам персонал. Целевые атаки профессиональных преступников чаще всего начинаются с использования методов социальной инженерии. Олег Наскидаев (DEAC) напоминает, что подобные риски можно минимизировать, обучая персонал и внедряя лучшие мировые практики в области информационной безопасности.

Защита инженерной инфраструктуры

Традиционные угрозы функционированию дата-центра – сбои электропитания и отказы систем охлаждения («Безопасность инженерной инфраструктуры – основа жизнедеятельности ЦОДа», с. 90). К таким угрозам уже привыкли и научились с ними бороться.

Новой тенденцией стало повсеместное внедрение «умного» оборудования, объединенного в сеть: управляемые ИБП, интеллектуальные системы охлаждения и вентиляции, разнообразные контроллеры и датчики, подключенные к системам мониторинга. При построении модели угроз ЦОДа не стоит забывать о вероятности атаки на сеть инфраструктуры (а, возможно, и на связанную с ней ИТ-сеть ЦОДа). Усугубляет ситуацию то, что часть оборудования, например чиллеры, может быть вынесена за пределы ЦОДа, скажем, на крышу арендуемого здания.

Защита каналов связи

Если дата-центр предоставляет услуги не только по модели colocation, то придется заниматься защитой облаков. По данным Check Point, только в прошлом году 51% организаций по всему миру столкнулись с атаками на облачные структуры. DDoS-атаки останавливают бизнес, вирусы-шифровальщики требуют выкуп, целевые атаки на банковские системы

> Не секрет, что в российском бизнесе, покупая сотрудника конкурентов, покупают и имеющуюся у него информацию. Люди скачивают архивы и уносят с собой, и только очень крупные компании занимаются этой проблемой.

Алексей Карпинский, заместитель гендиректора, ИТ-компания iCore

приводят к хищению средств с корсчетов. Угрозы внешних вторжений беспокоят и специалистов по информационной безопасности дата-центров. По мнению Артема Гавриченкова (Qrator Labs), наиболее актуальны для ЦОДов распределенные атаки, нацеленные на прекращение предоставления услуг, а также угрозы взлома, кражи либо изменения данных, содержащихся в виртуальной инфраструктуре или системах хранения.

Для защиты внешнего периметра ЦОДа служат современные системы с функциями выявления и нейтрализации вредоносного кода, контроля приложений и возможностью импорта технологии проактивной защиты Threat Intelligence. Некоторые пользователи разворачивают системы с функционалом IPS (предотвращения вторжений) с автоматической подстройкой сигнатурного набора под параметры защищаемого окружения.

Для защиты от DDoS-атак российские компании, как правило, используют внешние специализированные сервисы, которые уводят трафик на другие узлы и фильтруют его в облаке. Защита на стороне оператора выполняется гораздо эффективнее, чем на стороне клиента, а ЦОДы выступают в качестве посредников по продаже услуг.

В ЦОДах возможны и внутренние DDoS-атаки: злоумышленник проникает на слабо защищенные серверы одной компании, размещающей свое обо-

МНЕНИЕ ЭКСПЕРТА

держивать здание с мини-ЦОДом для АСУ ТП, обеспечивающей работу инфраструктуры предприятия. Кроме того, помещение с оборудованием должно быть способно противостоять внешнему пожару не менее 120 мин.

В сейфах и комнатах безопасности используются пожаростойкие вводы кабельных систем, уплотнители, специальная краска. В сейфах безопасности системы пожаротушения размещаются локально внутри стоек. В комнатах безопасности применяются стандартные для больших ЦОДов решения, но есть и специфика, заключающаяся в герметичности помещений. Если в соседнем помещении сработала пожарная сигнализация – в комнате автоматически закрываются и герметизируются все двери и вентиляционные люки.

Если в это время срабатывает система пожаротушения ЦОДа, например происходит пуск хладона, то в защищенном контуре создается избыточное давление. Для его регулирования имеются люки стравливания. Двери комнаты безопасности оснащаются замками «антипаника». Их всегда можно открыть изнутри, и человек сможет покинуть помещение, даже если в аварийной ситуации в ЦОДе сработала защита и двери автоматически закрылись.

Такие решения стали особенно популярны в связи с принятием закона «О персональных данных». Операторы персональных данных должны хранить их в местах с ограниченным физическим доступом персонала. Сейфы безопасности, являющиеся по сути несгораемым шкафом, идеально подходят под эти требования: они ограничивают доступ персонала, обеспечивают физическую защиту и полностью автономны.

Дмитрий Гуляев, руководитель направления инфраструктуры ЦОД, Delta Electronics

Специалисты по безопасности, как правило, воспринимают инженерную инфраструктуру как некую изолированную сущность, по умолчанию защищенную от действий злоумышленников, а сотрудники, занимающиеся эксплуатацией инженерной инфраструктуры, не разбираются в вопросах безопасности.

рудование по модели colocation, и с них по внутренней сети проводит атаку «отказ в обслуживании» на других клиентов этого дата-центра.

Внимание виртуальным средам

Нужно учитывать специфику защищаемого объекта – использование средств виртуализации, динамичность изменения ИТ-инфраструктур, взаимосвязанность сервисов, когда успешная атака на одного клиента может угрожать безопасности соседей. Как отмечает Нарек Татевосян (BI.Zone), взломав front-end докер при работе в PaaS на базе Kubernetes, злоумышленник сразу может получить всю парольную информацию и даже доступ к системе оркестрации.

Продукты, предоставляемые по сервисной модели, имеют высокую степень автоматизации. Чтобы не мешать бизнесу, не меньшую степень автоматизации и горизонтального масштабирования должны иметь наложенные средства защиты информации. Масштабирование должно обеспечиваться на всех уровнях ИБ, включая автоматизацию контроля доступа и ротацию ключей доступа. Особняком стоит задача масштабирования функциональных модулей, осуществляющих инспекцию сетевого трафика. По мнению Александра Власова (BI.Zone), фильтрация сетевого трафика на прикладном, сетевом и сеансовом уровнях в ЦОДах с высокой степенью виртуализации должна выполняться на уровне сетевых модулей гипервизора (например, Distributed Firewall компании VMware) либо путем создания цепочек сервисов (виртуальные межсетевые экраны от Palo Alto Networks).

Андрей Акинин, генеральный директор, Web Control

Устанавливать систему обнаружения вторжений на весь внутренний трафик, как правило, экономически не оправданно. Оптимальный вариант – сбор и анализ сетевой статистики в узловых точках (flow monitoring) с целью обнаружения сетевых аномалий и смягчения DDoS-атак.

При наличии слабых мест на уровне виртуализации вычислительных ресурсов усилия по созданию комплексной системы информационной безопасности на уровне платформы будут затрачены впустую.

Уровни защиты информации в ЦОДе

Общий подход к защите – использование интегрированных, многоуровневых систем обеспечения ИБ, включающих макросегментацию на уровне межсетевого экрана (выделение сегментов под различные функциональные направления бизнеса), микросегментацию на базе виртуальных межсетевых экранов или маркирования метками трафика групп (ролей пользователей или сервисов), определенных политиками доступа.

Следующий уровень – выявление аномалий внутри сегментов и между ними. Анализируется динамика трафика, которая может свидетельствовать о наличии вредоносных активностей, таких как сканирование сети, попытки DDoS-атак, скачивание данных, например путем нарезки файлов базы данных и вывода их периодически появляющимися сессиями через длительные промежутки времени. Внутри ЦОДа проходят гигантские объемы трафика, так что для выявления аномалий нужно использовать продвинутые алгоритмы поиска, причем без пакетного анализа. Важно, чтобы распознавались не только признаки вредоносной и аномальной активности, но и работа вредоносного ПО даже в зашифрованном трафике без его расшифровки, как это предлагается в решениях Cisco (Stealthwatch).

Последний рубеж – защита оконечных устройств локальной сети: серверов и виртуальных машин, например, с помощью агентов, устанавливаемых на оконечные устройства (виртуальные машины), которые анализируют операции ввода-вывода, удаления, копирования и сетевые активности, передают данные в облако, где и проводятся требующие больших вычислительных мощностей расчеты. Там производится анализ с помощью алгоритмов Big Data, строятся деревья машинной логики и выявляются аномалии. Алгоритмы самообучаются на базе огромного количества данных, поставляемых глобальной сетью сенсоров.

Можно обойтись и без установки агентов. Так, Юрий Бражников из 5nine Software считает, что современные средства защиты информации должны быть безагентными и интегрироваться в операционные системы на уровне гипервизора («Как защитить гибридную инфраструктуру предприятия», с. 91).

Перечисленные меры значительно снижают риски информационной безопасности, но это-

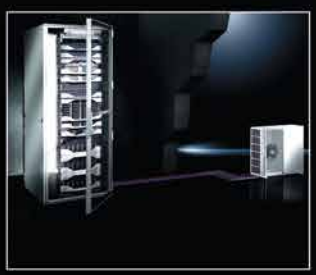
Rittal – The System.

Faster – better – everywhere.

Самая компактная установка IT-охлаждения Rittal в своём классе

- Расположение непосредственно внутри шкафа
- Оптимальное движение воздуха «спереди-назад»
- Два класса мощности в одном типоразмере
- Возможность резервирования
- Инверторные и EC технологии
- Выносной наружный блок

Обеспечение необходимого для IT потока воздуха «спереди-назад». Инверторное управление компрессором и EC вентиляторы для достижения максимальной энергоэффективности и точности поддержания параметров.



«Сплит» исполнение без нагрева внутреннего воздуха. Гибкое расположение наружного блока. Максимальное расстояние до 50 метров.

ENCLOSURES | POWER DISTRIBUTION | CLIMATE CONTROL | IT INFRASTRUCTURE | SOFTWARE & SERVICES

RITTAL

FRIEDHELM LOH GROUP

www.rittal.ru

МНЕНИЕ ЭКСПЕРТА

Павел Новожилов, ведущий консультант Центра информационной безопасности, «Инфосистемы Джет»

Является ли субъектом КИИ облачный провайдер?

В настоящий момент четкие критерии отнесения организаций к субъектам КИИ в соответствии с ФЗ-187 отсутствуют. Для того чтобы определить, является ли дата-центр облачного провайдера субъектом КИИ, нужно руководствоваться уставом, лицензиями на оказание услуг, а также классификатором деятельности ОКВЭД-2 (размещен на сайте http://оквэд-2.рф).

Облачный провайдер, являющийся оператором связи, к субъектам КИИ относится однозначно. В случае с операторами IaaS-, PaaS- и SaaS-услуг нужно обратить внимание на код ОКВЭД-2 63.11 «Деятельность по обработке данных, предоставление услуг по размещению информации и связанная с этим деятельность», который входит в раздел «Деятельность в области информации и связи». Использование кода ОКВЭД-2 может быть основанием для отнесения облачного провайдера к субъектам КИИ. Дата-центры, ориентированные на colocation-сервисы, могут быть операторами связи либо размещать у себя оборудование клиентов без предоставления дополнительных услуг – в первом случае они являются субъектами КИИ, во втором – нет.

Однако такой подход нельзя назвать однозначно верным. Сам закон ФЗ-187 и подзаконные акты к нему появились не так давно, и правоприменительная практика еще не сформирована. В частности, проблемы возникают у организаций, деятельность которых находится на границе отраслей, описанных в ФЗ-187.

го может быть недостаточно для дата-центров, обеспечивающих автоматизацию производственных процессов повышенной опасности, например, атомных станций.

Эксперты «Московского завода «Физприбор», разрабатывающего аппаратные системы противоаварийной защиты (ПАЗ) для атомных станций, предлагают отделить автоматизированную систему безопасности от системы АСУ ТП. Системы верхнего уровня могут использовать программно определяемые устройства, гиперконвергентные системы – в общем, все возможности современных информационных технологий. А система ПАЗ, не позволяющая ни при каких условиях произойти аварии, будет работать по жестко заданному неизменяемому алгоритму, задействуя максимально упрощенные и надежные контроллеры.

Требования регуляторов

В зависимости от обрабатываемой информации физические и виртуализованные инфраструктуры дата-центра должны удовлетворять разным требованиям по безопасности, сформулированным в законах и отраслевых стандартах.

Денис Дубцов, директор центра компетенций информационной безопасности, ГК «Рамакс»

Позиция регулятора неоднозначная. ФСТЭК не готова отнести к субъектам КИИ ни облачных провайдеров, ни дата-центры и предлагает смотреть на конкретные предоставляемые услуги. В целом 187-ФЗ похож на попытку разобраться с деятельностью хозяйствующих субъектов с их же помощью.

К таким законам относится закон «О персональных данных» (152-ФЗ) и вступивший в этом году в силу закон «О безопасности объектов КИИ РФ» (187-ФЗ) – прокуратура уже стала интересоваться ходом его выполнения. Споры о принадлежности ЦОДов к субъектам КИИ еще идут («Является ли субъектом КИИ облачный провайдер?», с. 88), но, скорее всего, дата-центрам, желающим предоставлять услуги субъектам КИИ, придется выполнять требования нового законодательства.

Непросто придется ЦОДам, размещающим у себя государственные информационные системы («ЦОДы и безопасность ГИС», с. 93). Согласно Постановлению Правительства РФ от 11.05.2017 № 555 вопросы информационной безопасности следует решить до ввода ГИС в промышленную эксплуатацию. Соответственно ЦОД, который хочет размещать у себя ГИС, заранее должен соответствовать требованиям регуляторов.

■ ■ ■

За последние 30 лет системы обеспечения безопасности ЦОДов проделали огромный путь: от простых систем физической защиты и организационных мер, не потерявших, впрочем, своей актуальности, к сложным интеллектуальным системам, в которых все чаще используются элементы искусственного интеллекта. Но суть подхода при этом не поменялась. Самые современные технологии не спасут без организационных мер и обучения персонала, а бумаги – без программных и технических решений. Безопасность ЦОДа нельзя обеспечить раз и навсегда, это постоянный ежедневный труд по выявлению первоочередных угроз и комплексному решению возникающих проблем. ИКС

Из чего состоит безопасность

Безопасность – не бумаги, не программы и не «железо». Это комплекс, состоящий из технических средств и организационных мероприятий. Это круглосуточная работа, включающая постоянный анализ угроз и обучение сотрудников.

Богдан Колодий, советник по техническим вопросам дата-центра IXcellerate

Безопасность имеет много составляющих. Это и физическая безопасность, и информационная (включая безопасность данных), и режим обеспечения сохранности носителей информации, в том числе таких архаических, как бумаги с коммерческой тайной, и пр. Можно вспомнить и о десятках определяющих стандартов и положений, о сложном оборудовании и рубежах безопасности. Но мое искреннее убеждение – все это не более 20% успеха. Чаще всего, рассматривая любую из вышеперечисленных «безопасностей», выделяют две компоненты: техническую и организационную.

О технической компоненте физической безопасности много говорят и пишут. В рамках эксплуатации дата-центров накоплен огромный опыт по ее проектированию и строительству. Предлагается ряд высококлассных средств защиты, таких как СКУД, биометрические системы, датчики присутствия, средства видеонаблюдения. Используются совершенные системы пожаротушения, датчики противопожарной безопасности разного уровня (сверхраннего предупреждения, противодымные, инфракрасные). В ответ на появившиеся террористические угрозы ЦОДы оснащаются рамками металлодетекторов и химическими датчиками, проверяющими наличие отравляющих веществ.

Разработано множество инструкций, положений и политик. Действуют прекрасные системы сертификации. Однако оборудование и методология – это только база. Реальную безопасность обеспечивают люди, которые правильно обучены, имеют технические средства и политики, предписывающие, как действовать в тех или иных ситуациях. А самое главное – имеют наработанную матрицу возможных рисков и по ней постоянно тренируют свои навыки.

Важно иметь в виду: никто не припомнит, чтобы «злоумышленники» и «диверсанты» взламывали какой-либо ЦОД в попытке выкрасть и продать серверы или стойки... А вот работы с оборудованием, посещения залов существующими и будущими клиентами проводятся ежедневно, и это серьезная угроза. Большинство аварий, потерь оборудования и информации связано именно с такими инцидентами.

Настоящие риски начинаются в момент эксплуатации. Все организовано, все под контролем, ненужных людей в зале нет, вот только монтажник с трехметровой стремянкой неловко развернулся... Все прошли через СКУД с самой сложной идентификацией, камеры видеонаблюдения и объемные датчики контролируют процессы выполнения работ, но они не помогут, когда правильно допущенные люди с правильно пронесенным инструментом что-нибудь заденут.

Кроме допуска нужно организовать правильное и безопасное выполнение работ, подготовку бригады, рабочего места для проведения работы, оценить угрозы, которые могут возникнуть при выполнении ремонта и модернизации устройств, при вносе и выносе тяжелого или крупногабаритного оборудования.

> Реальную безопасность обеспечивают люди, которые правильно обучены, имеют технические средства и политики, предписывающие, как действовать в тех или иных ситуациях

Для каждого вида работ должны быть заранее определены риски, составлена матрица угроз и на ее основе сформирован план работ на объекте обязательно с привлечением специалистов по безопасности проведения работ и поведения. Начинать надо с элементарных вещей – в нужном месте поставить оградительную решетку, оборудовать стремянку противоскользящими башмаками, подложить диэлектрические резиновые коврики.

Сегодня во всех ЦОДах внедрены серьезные системы физической, информационной и «бумажной» безопасности: установлено совершенное оборудование, разработаны документы в соответствии с требованиями регуляторов. Но эти виды безопасности будут бесполезны без персонала, который знает, что делать в той или иной ситуации. ИКС

Безопасность инженерной инфраструктуры – основа жизнедеятельности ЦОДа

Кирилл Сольев, технический эксперт департамента развития корпоративных продаж, ГК Softline

Сбои электропитания и отказы систем охлаждения – главные угрозы для функционирования дата-центра.

Риски для ЦОДов в первую очередь связаны с инженерной инфраструктурой – это сбои в электропитании, неисправность или полный отказ системы охлаждения. Риск проникновения в дата-центр извне значительно ниже, – я давно не слышал, чтобы подобная угроза реализовывалась. Это означает, что физическая безопасность ЦОДов с точки зрения диверсий находится на достаточно высоком уровне. С точки зрения человеческого фактора главную угрозу представляют инсайдеры – люди, работающие внутри периметра дата-центра и имеющие доступ либо к вычислительному оборудованию, либо к оборудованию инженерной инфраструктуры (тем же системам электроснабжения и охлаждения).

> Публичный ЦОД высокой степени надежности не рекомендуется строить в местах, где затопления были в последние 100 лет

Инженерная структура – уязвимое место и для контейнерных ЦОДов. Такие ЦОДы, если они размещаются на неохраняемой территории, например на промысле или месторождении, могут подвергнуться актам вандализма. Мини- и микроЦОДы тоже могут эксплуатироваться в значительном отдалении от крупных населенных пунктов. Помимо угроз физической безопасности это влечет за собой невозможность быстро решить какую-либо техническую проблему, – соответствующего специалиста придется везти с «большой земли», на что требуется время. Эксплуатанту следует продумать способы снижения подобных рисков, например, резервировать ключевые подсистемы ЦОДа, перенести часть продуктивных систем в облако или обеспечить присутствие на объекте сотрудника, который будет следить за его работоспособностью.

Если ЦОД расположен в городе, то основная угроза – перебои в электроснабжении. Например, один крупный банк оплатил строительство отдельной линии от энергоблока тепловой электростанции, но все равно у него регулярно происходят сбои электропитания длительностью 1–3 с. Вероятно, это особенность конкретной ТЭС.

В регионах, где случаются стихийные бедствия, к строительству ЦОДов надо подходить с осторожностью. Скажем, если в регионе за прошедшие 50 лет происходили затопления, то дата-центр там не рекомендуется строить вообще. Если речь идет о публичном ЦОДе высокой степени надежности, то его не рекомендуется строить в местах, где затопления были в последние 100 лет.

ЦОД, находящийся рядом с крупными магистралями или аэропортами, не пройдет сертификацию по стандартам Uptime Institute. С аэропортами связан интересный кейс. Одна компания собиралась строить частный ЦОД (не для сертификации) за чертой города. Нашла подходящий земельный участок, но насторожила его низкая цена. Выяснилось, что участок находится на территории, которая отведена под аварийный сброс топлива самолетами. Продавец земли потенциального покупателя об этом не предупредил. И если бы участок был куплен, вполне вероятно, что строить на нем такой объект, как ЦОД, ему бы не разрешили.

Крупные заказчики, которые строят частные ЦОДы, где хранится особо ценная информация – скажем, данные о банковских транзакциях, – к требованиям стандартов особо не прислушиваются. Они делают акцент на физическую безопасность и создают до трех рубежей физической защиты, а также нередко применяют резервирование ключевых подсистем дата-центра по схеме 2N + 1, поскольку цена простоя в случае сбоя несравнимо выше затрат на создание многократного резервирования. Финансовые организации – пожалуй, единственная категория эксплуатантов, которая знает стоимость часа простоя своих продуктивных систем.

Заказчики не из банковской сферы обычно оперируют не вероятными потерями, а временем простоя. И тех, кто называет конкретные цифры, говоря, что для них критичны час, три часа или один день простоя, уже большинство. ИКС

Как защитить гибридную инфраструктуру предприятия

Современные средства защиты информации должны быть безагентными и интегрироваться в операционные системы на уровне гипервизора.

Юрий Бражников, генеральный директор по России и СНГ, 5nine Software

Почему гибрид?

Сегодня все больше корпоративных информационных систем переносится в облако или потребляется в виде сервисов. В то же время соображения безопасности побуждают крупные предприятия выбирать гибридный вариант построения ИТ-инфраструктуры, когда наиболее критичные ресурсы размещаются в собственном ЦОДе, а остальные переносятся в облако по моделям IaaS или SaaS. Но и такой вариант не всегда устраивает службу информационной безопасности компании, поскольку она теряет прямой контроль над данными, вынуждена полностью доверять средствам защиты информации, архитектуре облака и персоналу провайдера, а выполнение корпоративных политик безопасности затрудняется. Поэтому многие предприятия, не готовые идти на подобные риски, не используют огромный потенциал облачных технологий, которые верно служат их конкурентам. Им приходится переплачивать за временно необходимые ресурсы, а стоимость и сроки развертывания новых систем увеличиваются. Как же разрешить противоречие между гибкостью и безопасностью, экономией и рисками?

На выручку приходят современные технологии, которые позволяют объединить контроль и защиту своих ресурсов как в собственном ЦОДе, так и в облаке хостинг-провайдера за счет интеграции в платформу виртуализации средства защиты информации и управления инфраструктурой. Провайдеры облаков, не желая терять крупных клиентов, идут навстречу клиентам, предлагая новую услугу «Безопасность как сервис» (SECaaS). Эта услуга помогает клиенту поддерживать консистентные политики безопасности в своем ЦОДе и в облаке, управляя не только виртуальными машинами и сетями, но и их изоляцией, антивирусной защитой и отражением атак на уровне приложений.

Вирусы опережают

Печально знаменитые атаки прошлого года – WannaCry, Petya и другие – продемонстрировали прорехи в защите ИТ-инфраструктуры даже у таких крупных мировых компаний, как Maersk, «Роснефть», Mars, Nivea и т.п. Эти атаки выявили ряд важных проблем в обеспечении информационной безопасности предприятий, и нужно учесть их негативный опыт, чтобы построить современную систему защиты своих ресурсов.

В чем причины крупных масштабов инцидентов? Их много, но одна из важных – несоответствие применяемых средств защиты информации существующей инфраструктуре компаний. За последние пять лет виртуализация и использование облачных ресурсов стали общей практикой для большинства пользователей. По данным Gartner, доля виртуализированных ресурсов в крупных компаниях достигла 75%, а облачные решения, по данным RightScale, в 2017 г. применяли 89% предприятий. В то же время решения для защиты информации у многих вендоров разрабатываются на базе устаревшей модели endpoint security, которая уже неактуальна в современной архитектуре, где нагрузки разворачиваются на серверах или в ЦОДах провайдера, а не на рабочих местах сотрудников. Устаревшие средства защиты информации требуют установки агента на каждом рабочем месте, если даже оно виртуализировано, но это дает возможность блокировки агента или его удаления, увеличивает нагрузку на серверы и усложняет процесс обновления программных решений.

Гибридной инфраструктуре – гибридную защиту

Современные средства защиты информации (СЗИ) должны быть безагентными и интегрироваться в операционные системы на уровне гипервизора. Это позволяет защищать рабочие места без установки дополнительного программного обеспечения, уменьшает влияние персонала на процесс защиты ресурсов и усложняет доступ злоумышленникам. Такие средства защиты потребляют до 30% меньше ресурсов серверов и обладают меньшей площадью атаки, так как не требуют открытия дополнительных портов в межсетевом экране для управления.

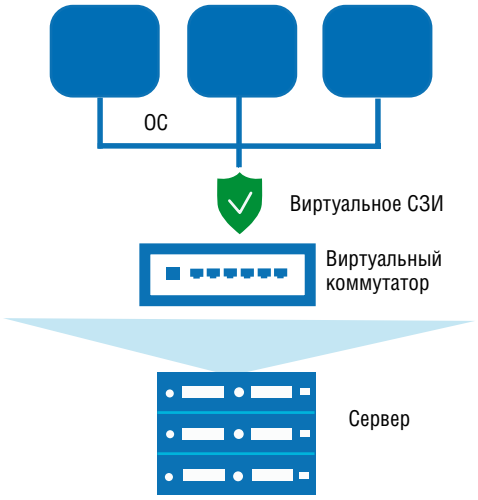


Рис. 1. Использование МСЭ нового поколения

Интеллектуальный межсетевой экран (МСЭ) нового поколения, интегрированный в гипервизор (рис. 1), помогает сегментировать среду виртуализации и избежать одновременного заражения многих виртуальных машин вирусами, как происходило в случае с WannaCry и другими зловредами, которые вывели из строя сотни и тысячи рабочих мест практически одновременно. Кроме того, правильная настройка межсетевого экрана в соответствии с широко распространенной архитектурой клиент–сервер тоже повысит защищенность от современных атак.

Антивирусная защита на базе сигнатурного метода перестала быть главной для борьбы с современными угрозами. Последние атаки были произведены вирусами, которых не было ни в одной базе сигнатур мировых разработчиков. К тому же базы сигнатур стали громоздкими и существенно влияют на производительность ресурсов. И хотя споры о том, не устарели ли антивирусы, продолжаются, лучшей практикой на сегодня является применение и сигнатурного, и поведенческого методов защиты от злоумышленников.

Вернемся к упомянутым инцидентам. В период между инфильтрацией и началом активности вирусы сканировали внутренние ресурсы и обращались к внешним для определения возможности атаки. Эту активность могли отследить анализаторы трафика, сравнить его профиль с обычным и дать сигнал администратору безопасности о подозрительной активности. Своевременное вмешательство сохранило бы ценную информацию и ресурсы пострадавших компаний. Поэтому еще одной важной чертой современных средств защиты информации является сочетание сигнатурных и когнитивных средств определения угрозы, в том числе искусственного интеллекта, как для антивирусной защиты, так и для систем обнаружения вторжений на уровне приложений.

Конечно, все эти системы должны работать в среде, в которой запускаются клиентские приложения, т.е. на уровне гипервизора операционной системы.

Поскольку ресурсы предприятия сегодня располагаются как в корпоративном ЦОДе, так и в облаке, современные средства защиты информации должны интегрироваться не только в инфраструктуру клиента, но и в облако провайдера (рис. 2). Они должны прежде всего изолировать ресурсы клиентов друг от друга и давать возможность анализа логов системами SIEM/UEBA для выявления комплексных многовекторных атак.

Средство защиты информации само должно быть отказоустойчивым к авариям, чтобы при выходе из строя хоста виртуализации или виртуальной машины, на которой оно установлено, сохранились все настройки и правила и защита работала без остановок, даже при миграции ресурсов из одного ЦОДа в другой. Для этого управляющие сервисы и базы данных решающих правил должны быть кластеризованы и являться ресурсами с высокой доступностью.

Важной частью комплекса мер безопасности является поддержка ролевой модели управления, что повышает защищенность информационных систем компании от инсайда.

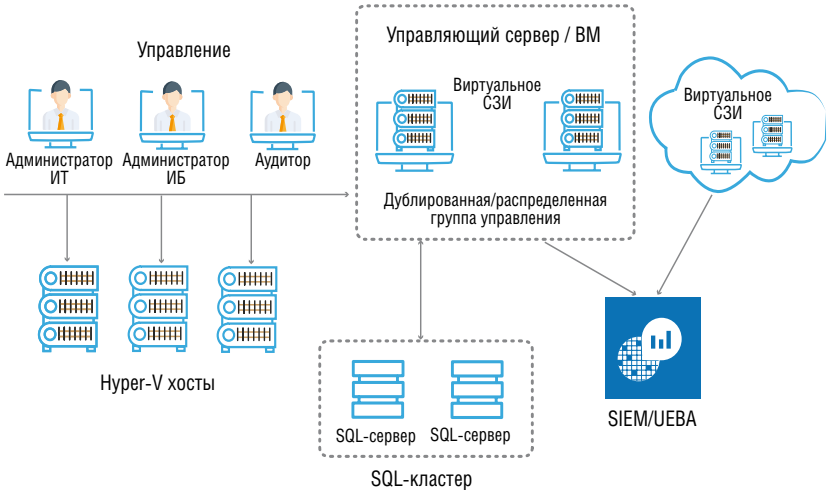


Рис. 2. Схема защиты гибридной ИТ-инфраструктуры

Таким образом, современное средство защиты информации должно включать в себя весь комплекс существующих защитных мер: межсетевой экран, безагентный антивирус, систему обнаружения вторжений. Оно должно интегрировать защиту ресурсов в облаке и в ЦОДе пользователя, давать возможность анализа логов событий безопасности для обнаружения сложных многовекторных атак и аудита. Что еще? Конечно, все эти системы должны соответствовать требованиям законодательной базы РФ и мировых стандартов информационной безопасности, таких как PCI DSS, требования которых обязательны и для российских компаний. ИКС

ЦОДы и безопасность ГИС

О задачах ЦОДов, предоставляющих услуги государственным структурам, – Булат Гузаиров, руководитель отдела серверных технологий компании «ICL Системные Технологии».

– Появление облачных технологий позволило перенести заботы о поддержании работоспособности вычислительной инфраструктуры на провайдера предоставляемых услуг. В сторону централизованного получения услуг по сервисной модели движется развитие информационных систем по всему миру и в том числе в России.

– С какими задачами информационной безопасности сталкивается ЦОД, размещающий у себя государственные информационные системы?

– В прошлом году было принято Постановление Правительства РФ от 11.05.2017 № 555, которое предписывает, что вопросы информационной безопасности должны быть решены до ввода ГИС в промышленную эксплуатацию. Соответственно, ЦОД, который хочет размещать у себя ГИС, заранее должен соответствовать требованиям безопасности.

В частности, он должен быть аттестован на соответствие требованиям приказа ФСТЭК России от 11.02.2013 № 17 для размещения ГИС. Это не так просто – методики аттестации не сформированы. Есть новые указания ФСТЭК России о том, что аттестацию ЦОДа, в котором размещается ГИС, проводить надо, но как конкретно это делать, точно не определено.

Новая проблема – вступивший в этом году в силу Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» (от 26.07.2017 № 187-ФЗ). Если информационная система клиента – субъекта КИИ развернута в ЦОДе и предоставляется ему по сервисной модели, то она является объектом КИИ и на нее распространяются все требования 187-ФЗ.

– Какие сложности возникают при предоставлении облачных услуг?

– В случае ГИС надо учитывать, что приказ ФСТЭК России от 11.02.2013 № 17 содержит требования, которые применяются не только к ЦОДу до уровня виртуализации, но и к прикладным системам. ЦОДу трудно выполнить требования, предъявляемые ко всем системам, которые потенциально могут в нем быть размещены.

ЦОД может выбрать два пути. Самый простой – обеспечивать информационную безопасность уровня IaaS, а все, что «выше», оставлять в зоне ответственности заказчика. И заключить с ним договор, в котором подробно разграничиваются зоны ответственности.

Если коммерческий ЦОД обладает возможностями центра обнаружения и предотвращения компьютерных атак (Security Operation Center, SOC) и соответствующими лицензиями ФСТЭК и ФСБ, то может взяться за проектирование системы безопасности клиента, ее реализацию и эксплуатацию.

> ЦОД, который хочет размещать у себя государственную информационную систему, заранее должен соответствовать требованиям безопасности

– Какие проблемы создает требование об использовании сертифицированных средств защиты?

– Согласно приказу ФСТЭК России от 11.02.2013 № 17, системы безопасности ГИС должны быть реализованы на сертифицированных средствах защиты. Это накладывает серьезные ограничения на перечень используемых средств. В частности, они должны проходить сертификацию на отсутствие недекларированных возможностей. Проверка требует раскрытия кода, к чему не готовы многие западные компании.

Срок действия сертификатов рано или поздно истекает. У средства защиты сертификат действует три года, а потом может случиться так, что производитель «разочаровался» в рынке России и дальше сертифицировать продукт не будет. Поддержка продолжает предоставляться, патчи выпускаются, а срок действия сертификата истек. Безопасность обеспечивается, но, в соответствии с требованиями регуляторов, нужно искать другое средство защиты с действительным сертификатом. А это большие капитальные затраты.

Беседовал Николай Носов

Напольный всепогодный укомплектованный шкаф

Шкафы укомплектованные серии ШТВ-1 и ШТВ-2, выпускаемые производственной группой Remer, предназначены для размещения автономно функционирующего активного и пассивного телекоммуникационного оборудования. Они обеспечивают защиту от воздействия окружающей среды и несанкционированного доступа, а также поддерживают требуемый температурный режим во внутреннем пространстве. Степень защиты, обеспечиваемая оболочкой по ГОСТ 14254, не ниже IP54.

В основании шкафов предусмотрены отверстия для ввода кабелей. В дне каркаса и стенке между отсеками модели ШТВ-2 может быть разное количество отверстий разного диаметра для установки кабельных вводов по требованию заказчика. В комплект поставки входят два кабельных ввода с гайкой М32 (типа MG32A-25G), 10 резиновых заглушек для отверстий под ввод кабеля, а также набор для блокировки задней двери изнутри шкафа.

Система климат-контроля REM, установленная на передней двери шкафа, представляет собой кондиционер мощностью от 1000 до 2000 Вт с нагревателем, имеющим мощность по теплу от 500 до 1000 Вт.

Предусмотрен широкий ряд аксессуаров для дополнительной защиты и удобства обслуживания в процессе эксплуатации (дополнительные цоколи 300 и 600 мм с дверцами для обслуживания, крыша с выдвижным козырьком, усиленный замок и т.д.).

Питание изделий осуществляется от электрической сети переменного тока с напряжением 220 В и частотой 50 Гц. Для шкафов ШТВ-2 предусмотрена возможность подключения резервного питания через розетку (вилку) 32 А типа DEKraft серии ВЩ-102 (или аналогичную) от внешнего источника с номинальным напряжением 220 В частотой 50 Гц.

Изделия имеют I класс защиты от поражения электрическим током в соответствии с ГОСТ 12.2.027.0-96. В части стойкости к механическим внешним воздействиям шкафы соответствуют группе М1 по ГОСТ 17516.1.

Шкафы выпускаются в климатическом исполнении У1 по ГОСТ 15150 и предназначены для уличной эксплуатации при температуре –50...+45°С и относительной влажности воздуха не более 80% при 20°С. Допустимая распределенная статическая нагрузка – до 800 кг.

www.cmo.ru

Однофазный ИБП с двойным преобразованием энергии

Eaton 9SX – флагманская модель в линейке однофазных ИБП компании Eaton, которая является следующим поколением серии 9130. Новые ИБП представлены мощностным рядом от 0,7 до 6 кВА в двух формфакторах – башенном и стоечном.

Выходной коэффициент мощности Eaton 9SX равен 0,9. Благодаря топологии двойного преобразования ИБП выполняет постоянный мониторинг электропитания внешней сети и регулирует напряжение и частоту. Внутренний байпас обеспечивает непрерывность работы, в качестве опции также доступен внешний сервисный байпас, с помощью которого можно производить замену батарей и осуществлять обслуживание ИБП без отключения питания нагрузки.

Технология управления батареями Eaton ABM использует трехступенчатую систему зарядки, которая продлевает срок службы батареи на величину до 50%. Встроенный счетчик ИБП 9SX показывает рекомендованную дату замены батарей. При необходимости время автономной работы может быть увеличено за счет подключения четырех дополнительных внешних батарейных модулей с возможностью «горячей» замены, которые смогут обеспечить работу нагрузки в течение нескольких часов. Подключение дополнительных батарейных модулей ИБП определяет автоматически.

Графический ЖК-дисплей отображает на одном экране информацию о состоянии ИБП и результаты измерений параметров. Также доступны расширенные возможности настройки. 9SX оснащен последовательным и USB-портами и слотом для подключения опциональной карты сетевого управления.

С помощью программного обеспечения Intelligent Power возможна интеграция с ведущими системами виртуализации и инструментами оркестровки облачных приложений, а также управление сегментами нагрузки, которое позволяет определять приоритетность отключения второстепенного оборудования для максимального увеличения времени работы от батарей критически важной нагрузки.

www.eaton.ru

Межрядные прецизионные кондиционеры с инверторными компрессорами

Компания «Вайбос» начала выпуск межрядных прецизионных кондиционеров серии BP с инверторными компрессорами. Устройства предназначены для установки в серверных и ЦОДах, а также в производственных, лабораторных и других помещениях, где нужно непрерывно поддерживать определенный микроклимат. Межрядные прецизионные кондиционеры обеспечивают непрерывное нахождение в заданных пределах температуры, влажности и чистоты воздуха.

Холодопроизводительность кондиционеров составляет от 15 до 50 кВт. Применение инверторных компрессоров позволяет плавно регулировать этот параметр в зависимости от потребности. В устройствах используется экологически безопасный фреон (R410a).

Серия инверторных межрядных кондиционеров комплектуется контроллерами Carel pCO5+, электронно-коммутируемыми вентиляторами EBMpapst, автоматикой Carel и ABB и другими агрегатами ведущих производителей. В частности, инверторные компрессоры изготавливаются компанией Danfoss (используются герметичные спиральные инверторные компрессоры со встроенной тепловой защитой и виброопорами).

Металлический корпус кондиционеров серии BP и его внутренние элементы выполнены из оцинкованной листовой стали со звуко- и теплоизоляционными панелями. Из оцинкованной листовой стали выполнены и внутренние панели, разделяющие кондиционер на отсеки. Испаритель изготовлен из медных труб с алюминиевым оребрением, поддон – из нержавеющей стали.

Варианты подачи воздуха: фронтально вперед, фронтально в стороны.

Кондиционеры комплектуются низкотемпературными комплектами (увеличенный ресивер, трехходовой (байпасный) клапан, вентили Rotalock, обратный и предохранительный клапаны), позволяющими оборудованию эффективно работать при температурах наружного воздуха –40...+40°C. В низкотемпературном исполнении скорость вращения вентиляторов наружного блока плавно регулируется.

Кондиционеры оснащены интеллектуальным контроллером и имеют русифицированный дисплей.

Ширина кондиционеров серии BP составляет 300 или 600 мм (такие габариты наиболее удобны для установки кондиционеров в ряды вместе с ИТ-стойками), вес – от 220 до 640 кг.

www.vybos.ru

ИБП для небольших нагрузок

Серия Easy UPS 3S, выпускаемая компанией Schneider Electric, пришла на смену продуктовой линейке ИБП Galaxy 300. Новые устройства предназначены для защиты небольших объектов гражданского строительства, отдельных инженерных систем различных зданий, промышленных нагрузок без повышенных требований по защите от внешних факторов среды, а также в ИТ-секторе.

Серия Easy UPS 3S представлена моделями мощностью 10–40 кВА. Ее отличительными характеристиками в сравнении с Galaxy 300 являются:

- выходной коэффициент мощности, равный 1, что при той же полной мощности системы, измеряемой в кВА, дает на 20% большую активную мощность, измеряемую в кВт);
- возможность использования модульных батарей для упрощения обслуживания и ускорения инсталляции;
- гораздо более высокий КПД – до 96%, что позволяет ощутимо экономить электроэнергию и снижать требования к системе кондиционирования комнаты с ИБП;
- в два раза более мощное зарядное устройство, обеспечивающее зарядку батарейных массивов большой емкости, что открывает возможность применения данной модели на объектах, где требуется многочасовое время автономной работы;
- наличие функции SPoT, которая позволяет провести нагрузочное тестирование системы без подключения реальной нагрузки;
- интуитивно понятный графический дисплей.

ИБП готовы для внедрения в не-ИТ системах: для диспетчеризации они укомплектованы интерфейсами сухих контактов и Modbus RS-485. Для ИТ-применения есть возможность дополнительного подключения SNMP-карты, благодаря которой ИБП подключается к сети Ethernet, к примеру для корректного завершения работы приложений на ИТ-нагрузке по сигналу разряда батареи при пропадании электропитания.

www.schneider-electric.ru

РЕКЛАМА В НОМЕРЕ

ДКС
Тел.: (495) 916–5262
Факс: (495) 916–5208
E-mail: info@dkc.ru
www.dkc.ru . . . . . **с. 68–69**

CYBERPOWER
Тел/факс: (495) 783-9445
www.cyberpower.com . . . . . **с. 43**

GREENBUSHDC
Тел.: (800) 350-1500
www.greendc.ru . . . . . **с. 54–55**

ITK
Тел.: (495) 542-2222
Факс: (495) 542-2224
E-mail: info@itk-group.ru
www.itk-group.ru . . . . . **с. 37**

IXCELLERATE РОССИЯ
Тел.: (499) 201-7956
E-mail: info@ixcellerate.ru
www.ixcellerate.ru . . . . . **1-я обл., вкладка**

PANASONIC
Тел.: (495) 665-4292
E-mail: office@panasonic.ru
www.panasonic.ru . . . . . **с. 15**

RITTAL
Тел.: (495) 775-0230
Факс: (495) 775-0239
E-mail: info@rittal.ru
www.rittal.ru . . . . . **с. 9, 38–39, 87**

SCHNEIDER ELECTRIC
Тел.: (495) 777-9990
Факс: (495) 777-9992
www.schneider-electric.com . . . **с. 18–19, 4-я обл.**

Указатель фирм и организаций

Учредители журнала «ИнформКурьер-Связь»:

ООО «ИКС-Медиа»:
127254, Москва,
Огородный пр-д, д. 5, стр. 3;
тел.: (495) 785-1490, 229-4978.

МНТОРЭС им. А.С. Попова:
107031, Москва, ул. Рождественка,
д. 6/9/20, стр. 1;
тел.: (495) 921-1616.

Конференция и выставка
«ЦОД-2018: модели, сервисы, инфраструктура»

ЦОД

DATA CENTER FORUM

18 октября 2018, Санкт-Петербург

Спонсоры и партнеры

RITTAL · CITRIX · PILLER Power Systems · SUSE · Complete Компания КОМПЛИТ · Hewlett Packard Enterprise · FUJITSU · socomec Innovative Power Solutions · ПРЕОРА · АККУ-ФЕРТРИБ · ИМПУЛЬС Источники бесперебойного питания · ХАЙТЕД Максимум энергии

Edge Computing - новый виток эволюции вычислений!

APC by Schneider Electric предлагает готовую инфраструктуру и компоненты для развертывания периферийных вычислительных узлов (Edge Computing), обеспечивающих безотказную работу ИТ-оборудования:

- Источники бесперебойного питания
- Шкафы-стойки APC NetShelter
- Блоки распределения питания APC Rack PDU
- Системы охлаждения различных типов, мощности и конфигураций
- Средства управления воздушными потоками
- ПО StruxureWare (DCIM) и аппаратные средства мониторинга и удаленного управления инфраструктурой
- Модульные помещения физической защиты SmartShelter
- Prefab-ЦОДы - комплексные решения высокой заводской готовности, повторяющих оснащение полноценного дата-центра.

Реклама.

Как быстро просчитать проект инфраструктуры для Edge Computing?

Воспользуйтесь конфигуратором Edge-решений уже сейчас!

www.apc.com/edge-for-partners

Life Is On

APC by Schneider Electric