

ТЕМА НОМЕРА

СЕТЕВАЯ ИНФРАСТРУКТУРА ЦОДов

ЦОД-2021:

основные тенденции

8

Стандарт EN 50600:

первое знакомство

50

Дата-центр

переезжает

67

Кибербезопасность

стремится в облака

82

ИнформКурьер-Связь

ИКС

издается с 1992 года

Андрей Аксенов

Генеральный директор
IXcellerate

Вместе — в новую цифровую эру

НАДЕЖНОЕ

решение для ИТ-провайдеров

APC

Настенный сверхкомпактный 6U микро-ЦОД EcoStruxure™ от Schneider Electric™

- Компактная конструкция
- Быстрое развертывание
- Сокращение времени простоев и сервисных затрат

apc.com/edge



EcoStruxure™
IT Expert



Настенный
сверхкомпактный
6U микро-ЦОД
EcoStruxure™

Издается с мая 1992 г.

Издатель
ООО «ИКС-Медиа»участник
АНО КС ЦОДКООРДИНАЦИОННЫЙ СОВЕТ
ПО ЦОДАМ И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

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

Обозреватель

Н.В. Носов
nikolay.nosov@iks-media.ru

Корректор

Е.А. Краснушкина

Дизайн и верстка

Е.В. Денисова

КОММЕРЧЕСКАЯ СЛУЖБА

Г.Н. Новикова, коммерческий
директор – galina@iks-media.ru
Е.О. Самохина, ст. менеджер – es@iks-media.ru
Д.А. Устинова, ст. менеджер –
ustinova@iks-media.ru
А.Д. Остапенко, ст. менеджер –
a.ostapenko@iks-media.ru
Д.Ю. Жаров, координатор – dim@iks-media.ru

СЛУЖБА РАСПРОСТРАНЕНИЯ

Выставки, конференции
expo@iks-media.ru
Подписка
podpiska@iks-media.ruЖурнал «ИнформКурьер-Связь» зарегистрирован
в Федеральной службе по надзору в сфере связи,
информационных технологий и массовых
коммуникаций 02 февраля 2016 г.;
ПИ №ФС77-64804.Мнения авторов не всегда отражают точку зрения
редакции. Статьи с пометкой «бизнес-партнер»
публикуются на правах рекламы. За содержание
рекламных публикаций и объявлений редакция
ответственности не несет. Любое использование
материалов журнала допускается только
с письменного разрешения редакции и со ссылкой
на журнал.

Рукописи не рецензируются и не возвращаются.

© «ИнформКурьер-Связь», 2021

Адрес редакции и издателя:

105082, Россия, г. Москва,
2-й Ирининский пер. д. 3
Тел./факс: (495) 150-6424
E-mail: iks@iks-media.ru
Адрес в Интернете: www.iksmedia.ruРедакция пользуется
облачными услугами 3data№3/2021 подписан в печать 20.08.21.
Тираж 8 000 экз. Свободная цена.
Формат 64x84/8

ISSN 0869-7973

12+

Цена ЦОДа*



В 2006 г. Uptime Institute опубликовал данные о стоимости ЦОДов разного уровня отказоустойчивости. Для наиболее распространенных объектов уровня Tier III она оказалась равной \$20 тыс. за 1 кВт мощности полезной (ИТ) нагрузки, для объектов уровня Tier I – в два раза ниже (\$10 тыс. за 1 кВт), а для Tier IV – на 10% выше (\$22 тыс. за 1 кВт).

Данные Uptime Institute, опубликованные в 2020 г., демонстрируют существенное снижение капитальных затрат на ЦОДы. В среднем они составили \$7–8 млн за 1 МВт для объектов мощностью свыше 20 МВт и \$8–9 млн за 1 МВт для дата-центров мощностью 5–20 МВт (все данные для ЦОДов Tier III).

Столь существенное снижение стоимости эксперты связывают с развитием индустрии ЦОДов, зрелостью технологий и переходом к массовому выпуску основных продуктов для инженерной инфраструктуры ИКТ-объектов. Следует отметить, что на общестроительные работы (создание «коробки» ЦОДа) тратится, по разным оценкам, от 20 до 30% средств, практически все остальное идет на инженерные системы. Поэтому их стандартизация, типизация и массовое производство вносят весомый вклад в уменьшение стоимости ЦОДа. Также большое значение имеют накопление опыта создания ЦОДов, проведение «работы над ошибками», что позволяет командам с каждым новым объектом оптимизировать расходы.

А что в России? Сразу заметим, что у нас, в отличие от западных стран, принято оценивать стоимость в расчете на одну стойку (хотя российские аналитики говорят о намерении перейти к расчетам за 1 кВт). По данным iKS-Consulting, «среднеотраслевой бенчмарк по России» составляет \$38 тыс. за стойку – для объекта Tier III на 2000 стоек мощностью по 5 кВт каждая. Это дает \$7,6 тыс. за 1 кВт, что полностью соответствует общемировым значениям. А компания Selectel, одна из немногих, публикующих данные о стоимости своих ЦОДов, заявила, что на новых объектах ей удалось опустить планку капитальных затрат до уровня ниже \$4 млн за 1 МВт.

Итак, за 15 лет затраты на создание ЦОДов уменьшились в среднем в три раза. Но в 2021 г. резко выросли цены на стройматериалы. Кроме того, сильно подорожали материалы (в частности, медь), используемые в инженерных системах, что увеличит и их стоимость. Насколько эта тенденция будет доминировать и победит ли она многолетний тренд снижения удельной стоимости дата-центра, покажет ближайшее время. По крайней мере строительство ЦОДов, несмотря на жалобы на дороговизну «всего и вся», идет очень активно.

С надеждой на то, что общее подорожание
не замедлит развитие отрасли ЦОДов,
Александр Барсков

*Приведенные в колонке данные были представлены на тренинге «Построение ЦОДов» АНО «Координационный совет по ЦОДам и облачным технологиям».

ТЕМА НОМЕРА

Сетевая инфраструктура в ЦОДах

с. 26

1 КОЛОНКА РЕДАКТОРА

4 ИКС-Панорама

- 4 Мощный рывок. Что дальше?
- 8 ЦОД-2021: основные тенденции
- 10 Беспилотники на МАКС-2021
- 12 Уроки от АНО КС ЦОД
- 14 ДАЙДЖЕСТ ОТРАСЛИ ЦОДов
- 15 А. Барсков. ЦОД будет определен!

16 Экономика и бизнес

- 16 И. Бакланов. Война Афины
- 18 А. Аксенов. «Время нам благоволит»
- 20 С. Анисимова. Citizen development как движущая сила автоматизации
- 22 М. Кыркунов, А. Суворов. С3 Solutions и «Новые Технологии»: синергия объединения
- 24 В. Валуев. Одной левой: как ИТ меняют работу трактористов



с. 10 Беспилотники на МАКС-2021



с. 16 И. Бакланов. Война Афины



с. 59

А. Эрлих, А. Галкина.
ЦОД без наружных систем
охлаждения



с. 74

Н. Носов. VSaaS-провайдеры:
перспективные клиенты
для ЦОДов



с. 90

А. Першин.
Пользователи зарубежных
мобильных технологий:
заложники или жертвы?

26 Инфраструктура

- 26** С. Кулаков, А. Барсков. Сетевая инфраструктура в ЦОДах. Что изменила пандемия
- 32** А. Морозов. ЦОД «Миран-2»: эстетика и функциональность
- 34** Дж. Янг, Дж. Батиста, К. Холл, М. Бальдассано. Готовимся к 400G, ждем 800G
- 38** Т. Алтышев. Schneider Electric: перестройка и ускорение
- 40** А. Барсков, Н. Носов. «Инженерка»-2021: это сладкое слово «эффективность»
- 48** М. Зиденханс. RiMatrix Next Generation: модульное решение горячих проблем
- 50** К. Королев. Стандарт EN 50600: первое знакомство
- 56** Е. Вирцер, Е. Колосков, А. Мартынюк. МегаЦОДы: когда размер имеет значение
- 59** А. Эрлих, А. Галкина. ЦОД без наружных систем охлаждения
- 62** М. Церулев, В. Морозов. Инновации ABB в ЦОДах 3data
- 64** А. Павлов, М. Матвиенко. Оцениваем площадь и состав помещений крупного ЦОДа
- 67** Л. Старикова, В. Назаренко. Дата-центр переезжает
- 72** В. Герасиков. ЦОДы, знакомьтесь: Jenbacher!

74 Сервисы и приложения

- 74** Н. Носов. VSaaS-провайдеры: перспективные клиенты для ЦОДов
- 78** В. Крылов. ИИ в медицине: тренды и примеры применения

82 Безопасность

- 82** Н. Носов. Рынок кибербезопасности стремится в облака
- 88** М. Кондрашин. Игры в песочнице
- 90** А. Першин. Пользователи зарубежных мобильных технологий: заложники или жертвы?

94 Новые продукты

Мощный рывок. Что дальше?



Рынок коммерческих ЦОДов Санкт-Петербурга наконец начал стремительно расти. Продолжится ли этот рост или динамика снова упадет ниже московской?

Эту интригу обсуждали на проведенной «ИКС-Медиа» в северной столице конференции «ЦОД: модели, сервисы, инфраструктура».

«За 10 месяцев – с сентября 2020 г. по июнь 2021 г. – рынок коммерческих ЦОДов Санкт-Петербурга вырос на рекордные 33%», – сообщил Дмитрий Горкавенко, директор по развитию бизнеса iKS-Consulting. Особенно примечательно, что такой рост был продемонстрирован после многих лет стагнации, когда не было реализовано ни одного крупного проекта.

За указанный период на рынок было выведено 1700 стоек, что увеличило его емкость до 6800 стоек. Рост обусловлен тремя крупными проектами: расширением площадок Selectel (+ 600 стоек), вводом в строй дата-центров «Ростелеком-ЦОД» (800) и «Миран-2» (300).

Аналитик также отметил, что последние крупные M&A-сделки в сфере ЦОДов связаны с питерским рынком. Как известно, недавно «Росэнергоатом» за 2 млрд руб. купил дата-центр Xelent (984 стойки), а «ЭР-Телеком Холдинг» вместе с партнерами приобрел российские активы компании Linxdatacenter, включая ЦОДы в двух столицах общей емкостью 1460 стоек. iKS-Consulting оценивает эту сделку в 6,53 млрд руб. «В рынок верят, пошли серьезные инвестиции», – утверждает Дмитрий Горкавенко, который характеризует те-

кущую ситуацию как «перезапуск рынка коммерческих ЦОДов Санкт-Петербурга».

Питерские проекты

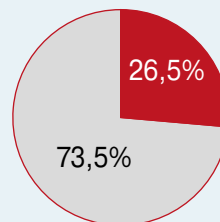
Объект «Ростелеком-ЦОД», введенный в эксплуатацию в декабре 2020 г., стал одним из крупнейших дата-центров на Северо-Западе России. ЦОД



общей емкостью 800 стойко-мест и мощностью 7,4 МВт имеет четыре машинных зала по 200 стоек каждый. Как рассказал Владислав Берзин, старший инженер-энергетик «Ростелеком-ЦОД», выбор точки дислокации площадки (на севере города, ул. Жукова, д. 43) во многом определен наличием рядом генератора электроэнергии – ТЭЦ-17, а также подстанции ПС 330 «Волхов-Северная». Это федеральный сетевой объект, поэтому электроэнергию ЦОД получает напрямую от ФСК (без посредников). Вся система энергоснабжения зарезервирована по схеме 2N, а емкость топлиохранилища (30 куб. м) обеспечит 13–14 ч непрерывной работы объекта.

Крупнейшие коммерческие ЦОДы Санкт-Петербурга на середину 2021 г. (число введенных стойко-мест)

Selectel	1351	600	1951
Xelent	984		984
Linxdatacenter	840		840
«Ростелеком»	800		800
«Миран»	261	300	561
IMAQLIQ	80		



■ Стойко-места, введенные за последние 3 года

□ Стойко-места старше 3 лет

Источник: iKS-Consulting

В качестве важных преимуществ новой площадки представитель «Ростелеком-ЦОД» отметил ее хорошую связность с дата-центрами компании в других городах и возможность прямого подключения к точке обмена трафиком MSK-IX. Все это позволяет быстро организовывать геораспределенные решения и удобную миграцию между площадками.

Открытый недавно коммерческий ЦОД «Миран-2» рассчитан на 300 стоек, которые будут введены в эксплуатацию в течение года. Расчетная мощность ИТ-нагрузки новой очереди – 1500 кВт. Клиенты получают бесперебойное электропитание с резервированием $2(N + 1)$, поддержку постоянного климата в серверных залах и возможность подключиться более чем к 50 операторам связи, а при желании – арендовать в дата-центре помещения для своих служб.



Интересно, что, по словам директора по эксплуатации и строительству ЦОДа «Миран» Виталия Николаева, клиентами дата-центра являются, в частности, компании из Владивостока и Сибири. «Вовсе не обязательно, чтобы ЦОД находился в шаговой доступности. Компании выбирают ЦОД там, где находятся их клиенты, а не головной офис», – указал он.

Отметим еще один ЦОДовский проект в Санкт-Петербурге: в начале июня 2021 г. состоялось официальное открытие дата-центра Гознака на базе Санкт-Петербургской бумажной фабрики. Проектирование и постройка этого ЦОДа сертифицированы на соответствие уровню надежности Tier III Uptime Institute. В шести машинных залах ЦОДа разместятся 470 стоек, средняя мощность на одну стойку – 8 кВт.

Как сообщил на конференции Андрей Веселов, руководитель центра продаж цифровых продуктов АО «Гознак», ЦОД предприятия в Санкт-Петербурге является коммерческим, часть стоек будет предлагаться сторонним клиентам – государственным и коммерческим заказчикам.



Москву «не догонишь»?

Анализируя перспективы дальнейшего развития рынка, Д. Горкавенко сфокусировал внимание на нескольких факторах: подтвержденном спросе (включая готовность московских/федеральных компаний размещаться на площадках Санкт-Петербурга), накопленную экспертизу в сфере строительства и эксплуатации ЦОДов, а



также гибкую ценовую политику питерских провайдеров (цены ниже столичных на 20–30%).

Некоторые особенности текущей ситуации на московском рынке могут еще больше усилить привлекательность Питера. Эксперт iKS-Consulting отметил инертность московского рынка, рост цен и одновременно желание коммерческих ЦОДов выбирать себе

заказчиков, ограниченное число профессиональных команд, который могут строить быстро, качественно и экономически эффективно, а также меньшую заинтересованность в Москве операторов связи, выходящих на рынок коммерческих ЦОДов. Вопрос в том, смогут ли питерские компании перетянуть на себя интересы инвесторов и клиентов.

По словам В. Берзина, спрос явно не удовлетворен, поэтому планы на вторую очередь (дата-центра «РТК-ЦОД») будут реализованы в ближайшее время. Планы других игроков пока скромнее.

«Миран» активно рассматривает две локации (объекты с уже подведенной электроэнергией), но начало строительства ЦОДа «Миран-3», согласно планам, о которых сообщил В. Николаев, – конец 2022 г.

«Планировали строить (новый ЦОД) в следующем году в Санкт-Петербурге, – рассказал Алексей Ерёменко, директор по инфраструктуре Selectel. – Но решили строить в Москве. При вложении тех же средств результат будет лучше».

Управляющий партнер iKS-Consulting Татьяна Толмачева обратила внимание на то, что доля Санкт-Петербурга и Ленинградской области на рынке коммерческих ЦОДов России (5–6%) примерно соответствует доле СЗФО в ВВП страны. И ожидать, что она станет существенно выше, не приходится. «Средняя доходность одной стойки в Москве выше. Проекты окупаются быстрее», – отметила она.



Госы мечтают об облаках

Серьезным дополнительным источником клиентов для коммерческих ЦОДов, в том числе в Санкт-Петербурге, могли бы стать государственные предприятия и организации. И многие из них действительно стремятся передать свои ИТ-системы на аутсорсинг. Но разные причины пока мешают им в этом.



Так, Алексей Вагин, начальник отдела технического обеспечения ИТ Балтийского завода, прекрасно понимает все экономические преимущества облачных моделей. Но пока в законодательстве отсутствует даже само понятие облачных сервисов, а провайдеры не обеспечивают требуемый такому серьезному предприятию уровень безопасности, включа-

ющая шифрование в каналах доступа в облака, Балтийскому заводу приходится держать свою ИТ-инфраструктуру «у себя».

Схожую ситуацию описал и Артем Мелешкин, начальник управления по сопровождению информационных систем, развитию и сопровождению распределенного регионального ЦОДа Комитета по информатизации и связи СПб ГУП «СПб ИАЦ». Сейчас этой организации приходится содержать три собственные ИТ-площадки, и ее ИТ-руководитель стремится к аутсорсингу, в первую очередь к использованию платформенных решений. Изучаются различные варианты, в том числе облачные услуги «Яндекса», но вариант, полностью устраивающий этого госзаказчика, пока не найден.

Заметим, что ИТ-руководители обеих названных структур говорят именно об использовании облачных сервисов, а не о размещении своих серверов в коммерческих ЦОДах. Это показывают и исследования аналитиков iKS-Consulting: облачный бизнес растет быстрее, чем colocation.

Edge в помощь

Будущее ИТ-систем большинства организаций, скорее всего, будет гибридным. Они будут использовать и облака, и классические услуги коммерческих ЦОДов, но часть ресурсов, безусловно, останется на их территории – в edge-ЦОДах.

Тема распределенных (или периферийных) вычислений широко обсуждалась на конференции в Санкт-Петербурге. И многие производители уделили отдельное внимание своим предложениям для edge-узлов.

Владимир Статуев, руководитель направления по работе с региональными за-



казчиками Schneider Electric, проанализировал недостатки централизованных архитектур: это и задержки в сети (проблемы при работе в режиме реального времени), и нехватка ее пропускной способности (проблемы передачи большого объема данных), и сложности с обеспечением локализации данных на удаленном узле (взаимодействие внутри филиала) и его автономной работы (в условиях потери связи), и, наконец, проблемы безопасности. Edge-узлы помогают решить эти проблемы, позволяя бизнесу продолжить работу даже при отсутствии связи, недостатке пропускной способности и т.д. При этом, по мнению эксперта Schneider Electric, рост использования edge-узлов никак не мешает развитию головных ЦОДов.

Современные технологии позволяют упаковать все необходимые инженерные системы в «маленький шкаф» – микроЦОД. Компания Schneider Electric представила в Санкт-Петербурге микроЦОДы С-серии на 43 и 6 юнитов, защищенный звукоизолированный шкаф NetShelter CX для развертывания микроЦОДа в офисной среде, а также микроЦОДы R-серии для складских и транспортных проектов и всепогодные периферийные ИТ-узлы.

В свою очередь, компания Rittal представила платформу нового поколения RiMatrix NG, куда входят все основные инженерные системы: электропитания (ИБП и новые PDU), охлаждения (LCP VX), размещения оборудования (новое поколение серверных шкафов VX IT), а также

обеспечения безопасности (беспроводная система контроля доступа CMC Online). На базе этих технических решений можно строить ЦОДы разного масштаба – от edge-узла до крупного коммерческого ЦОДа.



Именно шкафы и системы изоляции коридоров Rittal используются в новом ЦОДе «Миран-2». Что же касается edge-систем, то Кирилл Дмитриев, главный технический специалист компании по ИТ-проектам, привел примеры проектов на базе продуктов Rittal в металлургии (промышленные edge-узлы с уровнем защиты IP54), ритейле (компактное решение с возможностью перемещения и малым временем поставки), на транспорте (кластер на 60 кВт ИТ-нагрузки) и в других отраслях экономики.

В целом потенциал рынка ЦОДов Санкт-Петербурга велик, и он будет раскрываться по разным направлениям: это и внедрение edge-ЦОДов, и увеличение площадей коммерческих дата-центров, и рост предложений облачных сервисов. Ну а здоровая конкуренция (и кооперация) с московскими игроками должна послужить на благо как российскому рынку в целом, так и интересам конкретных заказчиков.

Александр Барсков
Санкт-Петербург – Москва



16-Я МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ И ВЫСТАВКА



Москва 8 сентября 2021

Holiday Inn Moscow Sokolniki

За свою 16-летнюю историю конференция «ЦОД» стала главным российским профессиональным событием для тех, кто проектирует, строит и эксплуатирует дата-центры. Важнейшие задачи форума – обмен знаниями и наилучшими практиками, выявление и обсуждение отраслевых и глобальных трендов, которые оказывают непосредственное влияние на развитие критически важных корпоративных информационных инфраструктур.



подробно о программе и участниках
на сайте конференции dcforum.ru



Реклама

16+

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

ОРГАНИЗАТОРЫ



ПРИ
ПОДДЕРЖКЕ
И УЧАСТИИ



Минцифры
России



КООРДИНАЦИОННЫЙ СОВЕТ
ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

UptimeInstitute®

ЦОД-2021: основные тенденции



Повышение роли человеческого фактора, автоматизация, ускорение реализации проектов, технологические инновации и периферийные вычисления – факторы, определяющие сегодня направления развития рынка ЦОДов.

Рынок растет

Рынок ЦОДов уверенно растет, и этот рост будет продолжаться – главный вывод 8-й международной конференции Data Center Design & Engineering, организованной «ИКС-Медиа» в Москве. Прошедшее наконец-то в офлайн-формате мероприятие собрало более 500 делегатов.

По данным iKS-Consulting, число стойко-мест в 2020 г. в российских ЦОДах увеличилось на 13%, достигнув почти 50 тыс., и, по прогнозу, дойдет до 76 тыс. в 2024 г. Пандемия COVID-19 не только подстегнула спрос на дата-центры, но и повысила их расходы. Так, 26% опрошенных Uptime Institute менеджеров ЦОДов сообщили о росте расходов на выплаты персоналу (в том числе из-за переработки), 29% – об увеличении затрат на системы мониторинга и управления, 36% – на инфраструктуру, 66% – на дополнительные средства обеспечения безопасности.

Пандемия наглядно продемонстрировала, что человек – самое слабое звено в системе эксплуатации ЦОДов. Поэтому, как отметил главный редактор «ИКС-Медиа» Александр Барсков, поддержание здоровья и резервирование персонала требуют пристального внимания наравне с обеспечением работоспособности основных инженерных систем. Снизить зависимость от человеческого фактора помогут повышение надежности ЦОДов, удаленное управление и использование систем автоматизации, в том числе с элементами искусственного интеллекта.

Важная тенденция – ускорение реализации проектов. Этому способствуют использование блоков высокой заводской готовности (энергомодулей, блоков охлаждения, модулей машзалов и коридоров), декомпозиция объекта на коробочные решения (модули) и распараллеливание процессов.

Среди технологических инноваций А. Барсков выделил вышедшие на уровень зрелости литий-ионные батареи, мегаваттные статические ИБП, которые теснят динамические устройства, и «холодные стены», идущие на смену классическим прецизионным кондиционерам.

От оборудования к сервисам

Пандемия ускорила процессы цифровизации. «В прошлом году мы за две недели резко перестроили все процессы и совершенно спокойно использовали удаленные места работы, бизнес не остановился», – поделился опытом перехода на режим самоизоляции технический директор подразделения Secure Power компании Schneider Electric Алексей Соловьев.



Цифровая трансформация не только перекраивает бизнес-процессы, но и меняет ИТ-инфраструктуру предприятий. Централизованная ИТ-среда трансформируется в гибридную с множеством оконечных устройств, информация с которых собирается на периферийных узлах. Собранные данные поступают в региональные опорные ЦОДы, а местом конечной обработки и хранения данных выступает головной ЦОД.

«Меняется понятие “отказ оборудования”. Теперь это не отказ отдельного устройства, а отказ в предоставлении сервиса всей системой», – пояснил А. Соловьев.

Децентрализация ИТ-инфраструктуры сопровождается централизацией контроля – решения в распределенной вычислительной среде принимаются в центре, а не на местах. Компании приходят к единой стратегии развития вычислительной среды. В центре контролируется доступность всех сервисов, анализируется эффективность системы. Централизуются и функции мониторинга работы инженерной инфраструктуры и ИТ-систем.

Интеграция инженерной инфраструктуры выходит на новый уровень – с единым дистанционным мониторингом и управлением, причем не только для оборудования, но и для сервисов. Для предотвращения простоя сервисов нужно резер-



вировать не только оборудование, но и, как показал прошедший пандемийный год, службы эксплуатации.

Инвестиционный интерес

Резкий рост спроса на услуги ЦОДов усилил внимание к этому рынку инвесторов, в том числе тех, кто ранее им не интересовался. Однако неправильный учет особенностей прединвестиционного этапа проекта коммерческого ЦОДа может сделать его «долиной смерти», предупреждает управляющий партнер iKS-Consulting Татьяна Толмачева.

Критическими условиями успеха проекта эксперт назвала адекватную оценку начальных инвестиций, доступ к дешевой электроэнергии, наличие квалифицированной команды, телекоммуникационной инфраструктуры для связности ЦОДа и административной поддержки, снижающей барьеры при решении вопросов прединвестиционного этапа. Существование базового инвестора позволит пройти этот этап эффективнее и быстрее. Якорный заказчик гарантирует генерацию денежного потока на более ранних этапах реализации проекта.

Поглощения и коллаборации

Повысившаяся привлекательность рынка дата-центров обострила конкурентную борьбу вендоров. Одни, покупая существующие компании, пытаются добиться успеха на новом для себя рынке благодаря использованию уже раскрученного бренда. Так действует Rolls-Royce, стремясь перенести на свое инженерное оборудование восприятие основного бренда – элитной, престижной, дорогой, сверхнадежной машины. Другие идут путем расширения номенклатуры решений и сервисов, в том числе за счет коллаборации с игроками, которые предлагают недостающие позиции. Так, в марте 2021 г. заключили соглашение о глобальном сотрудничестве в области индивидуальных решений для инфраструктуры ЦОДов компании Stulz и Rittal.

«Многие до сих пор считают, что Rittal – это только шкафы. Действительно, в этом году исполняется 60 лет с начала производства компанией корпусов. Но продукт – это только база, главное – услуги, сопровождение и поддержка проекта на протяжении всего жизненного цикла и построение долгосрочных партнерских отношений с заказчиком», – заявил главный технический специалист по ИТ-проектам Rittal Кирилл Дмитриев. В прошлом году компания выпустила новое поколение инженерного оборудования для ЦОДов – RiMatrix Next Generation, включающее новые серверные шкафы VX IT, обновленную линейку PDU, системы водяного и фреоновоего охлаждения.

«Объявленное глобальное партнерство с компанией Stulz, на территории России – с HTS, позволило нам рас-

ширить портфолио с точки зрения систем охлаждения», – пояснил К. Дмитриев.

«Зеленое» будущее

Сегодня во всем мире набирает силу тенденция к снижению использования углеводородов при производстве энергии и переходу на возобновляемые источники. Как указал архитектор решений Digital Power Division Huawei в России Алексей Кудрявцев, ведущие страны мира, согласно подписанным международным соглашениям, будут снижать использование углеводородного топлива и к середине века перейдут на «чистую» энергию. По оценкам Международного агентства по возобновляемым источни-

кам энергии, в настоящее время доля «чистой» энергии составляет 25%, но через 30 лет повысится до 86%, а мощность, вырабатываемая солнечными электростанциями, достигнет в 2050 г. 8519 ГВт.

Для улучшения экологического состояния планеты Huawei предлагает свои продукты в области солнечной энергетики. В этом году компания начинает поставлять солнечные инверторы на российский



рынок. «Главная задача – уменьшение стоимости электроэнергии на солнечных станциях. Сегодня для крупных станций мы можем обеспечить стоимость электроэнергии менее 2 руб. за 1 кВт•ч и 3 руб. – для более компактных электростанций», – сообщил А. Кудрявцев.

Энергию надо не только экологично вырабатывать, но и экономно использовать. Разработанная Huawei интеллектуальная система охлаждения ЦОДа, использующая технологию iCooling, позволяет анализировать график энергопотребления на объекте и прогнозировать изменение температуры, что дает возможность снизить PUE на 8–15%.

...Люди соскучились по живому общению и были рады поговорить с коллегами и экспертами напрямую, а не с помощью веб-конференций и других способов удаленных коммуникаций. Но все же главный секрет успеха мероприятия, повышенного внимания к прошедшей конференции – рост интереса к дата-центрам, что является важной и такой приятной тенденцией для игроков этого рынка.

Николай Носов

Беспилотники на МАКС-2021



Регуляторные проблемы мешают сократить отставание нашей страны в области беспилотных летающих аппаратов.

Современный самолет – это, по сути, летающий центр обработки данных, управляющий всеми узлами аппарата, в котором функции пилота сводятся к общему контролю и принятию мер в экстремальных нештатных ситуациях. Логичное дальнейшее развитие – полный отказ от использования пилотов на борту воздушного судна, что позволит существенно снизить расходы на эксплуатацию. В области беспилотных летательных аппаратов (БПЛА) Россия отстает от лидеров, но в последнее время энергично пытается сократить разрыв, о чем свидетельствовали разработки, демонстрировавшиеся на Международном авиационно-космическом салоне.

Больше беспилотников – тяжелых и разных

Одним из первых в небо поднялся небольшой вертолет. Впервые в истории авиасалона в летной программе появился беспилотник – холдинг «Вертолеты России» представил новый летательный аппарат вертолетного типа БАС-200. Максимальная взлетная масса БПЛА составляет 200 кг, он развивает скорость до 160 км/ч, несет коммерческую нагрузку массой до 50 кг, выполняет полеты продолжительностью до 4 ч на высотах до 3900 м. Умещающийся в небольшом автомобильном фургоне наземный комплекс управления обеспечивает связь с беспилотником на расстоянии до 100 км.

В России хорошие предпосылки для использования БПЛА – огромные пространства со слабо развитой системой дорог, до некоторых районов добраться по суше просто невозможно. Да и пилотов сегодня уже не хватает. Дроны же могут в автоматическом режиме выполнять целый комплекс разнообразных работ: вести видеомониторинг в видимом и ИК-диапазоне, выявляя объекты с заданной температурой, и геодезическую аэрофотосъемку или съемку сельхозугодий в различных участках спектра электромагнитного излучения для оценки прироста биомассы; обнаруживать утечки метана на магистральных газопроводах; собирать данные для цифровых двойников наземных объектов методом воздушного лазерного сканирования; распознавать изображения, например, при поисково-спасательных работах.

Все эти работы способны выполнять беспилотные комплексы ZALA, созданные производителем беспилотных систем из Ижевска. У компании есть центр организации полетов, который резервирует воздушное пространство на территории России, центр обработки данных мониторинга

и аэрофотосъемки с подразделениями в Ижевске, Москве, Краснодаре, Сургуте и Новосибирске и сеть летных отрядов, выполняющих полеты в интересах заказчиков.

Цифровые двойники для разработки и испытаний

Беспилотные летательные аппараты – бурно развивающаяся и перспективная отрасль бизнеса. Они имеют разное назначение, широкое разнообразие типов и размеров, могут быть сложными и дорогостоящими изделиями. Однако если в процессе их проектирования будут приняты ошибочные конструкторские решения, это может привести к потерям опытных образцов на испытаниях и снизить инвестиционную привлекательность разработки. Для того чтобы снизить риски, компания Siemens предложила вести разработку БПЛА с использованием цифровых двойников (ЦД). На первом этапе путем моделирования определяются оптимальный тип и архитектура БПЛА, исходя из его назначения. Затем обосновывается оптимальный выбор входящих агрегатов и компонентов, решаются задачи прочности и аэродинамики. ЦД позволяет виртуально выполнить полный комплекс необходимых испытаний, до изготовления опытных образцов получить БПЛА с требуемыми характеристиками, существенно сократив затраты на натурные испытания, доводку и сертификацию изделия.

Виртуальные испытания БПЛА проводятся на цифровом полигоне, в состав которого входят цифровые двойники самого летательного аппарата, местности и системы управления. ЦД летательного аппарата включает в себя полный комплекс его систем (силовая установка, батареи, топливная, электрическая и другие системы), аэродинамические характеристики и модели сенсоров (камер, лидаров, радаров, ультразвуковых датчиков) для распознавания окружающих объектов и позиционирования БПЛА при полете. ЦД местности может быть представлен как картой зоны полетов, так и моделью, скажем, города или квартала.

Помимо экономического эффекта цифровой полигон и виртуальные испытания повышают безопасность, исключая несчастные случаи, возможные, например, при натурных испытаниях БПЛА в городской среде. «Siemens предлагает разработчикам БПЛА платформу, обеспечивающую выполнение полного комплекса виртуальных испытаний изделия, заменяющих традиционные натур-



ные испытания. Платформа позволяет провести разработку и оптимизацию изделия, проверку его характеристик на всех режимах эксплуатации до изготовления и испытаний реального образца и получить на выходе изделие, которое сразу будет соответствовать заданным требованиям», – пояснил нашему изданию руководитель по развитию направления «Системный инжиниринг» компании Siemens Дмитрий Копанев.

Платформа для летающего такси

Мало научить беспилотники летать, для них нужно создать инфраструктуру автоматических аэродромов, на которых дроны смогут приземляться, разгружаться и перезаряжаться. Все как в «большой», пилотируемой авиации. И работы в этом направлении идут.

Ученые Тамбовского государственного университета (ТГУ) представили универсальную автоматизированную платформу для эксплуатации малых БПЛА самолетного гибридного и роторного типов. Директор Центра компетенций в сфере применения беспилотных авиационных систем ТГУ Артем Киреев рассказал, что платформы образуют сеть взаимодействующих между собой станций, расположенных на расстоянии до 150 км друг от друга. Дрон может взлететь с одной станции, пролететь свой маршрут, выполнить задание и сесть на другую. Станция его примет, автоматически заменит литий-ионную батарею на новую и скачает собранные беспилотником данные. Связь со станциями осуществляется через спутник.

Цель проекта – полностью исключить человеческий фактор из процессов эксплуатации и управления малыми БПЛА вертикального взлета и посадки. Систему планируют использовать для регулярного автоматического беспилотного мониторинга объектов и территорий в удаленных и труднодоступных районах. Платформа может стать основой для построения сетей беспилотной логистики, а в отдаленной перспективе – использоваться в работе персонального беспилотного транспорта, или летающего такси.

Воздушный трактор

Представленные на выставке тяжелые беспилотники, как правило, имеют двойное назначение. Следствие этого – высокая цена. Ее вполне могут заплатить военные, но обычному фермеру такие устройства не по карману.

Ситуацию решила исправить «Производственно-конструкторская компания «Технорегион» из Краснодара, позиционирующая свой ТР-101 как единственный в России гражданский беспилотник массой более 30 кг.

Дизайн модели напоминает самолет кружка авиамоделирования советских времен. Только не надо бегать по полю с коробочкой – фермер комфортно сидит в кабине «Газели» и управляет аппаратом, например опрыскивает поля, с пульта управления. Также БПЛА можно использовать для патрулирования леса или грузоперевозок. При установке дополнительного оборудования один оператор может запустить беспилотник с грузом, а другой – перехватить управление и посадить его в точке назначения. Такое решение удобно для доставки посылок при отсутствии дорог.

Российские проблемы

МАКС-2021 продемонстрировал несомненный прогресс отечественной беспилотной авиации. Но это скорее отдельные успехи. В целом рынок беспилотников в России остается незрелым и сильно отстает от европейского и американского. В частности, у нас практически нет стартапов, взаимодействующих, как на Западе, с крупными корпорациями. Российские госкомпании делают только первые шаги. За техническим прогрессом не успевают регуляторы.

«Главная наша проблема состоит в том, что беспилотные летательные аппараты с взлетной массой свыше 30 кг подлежат обязательной сертификации. Регуляторика сертификации рассчитана на пилотируемую авиацию. Приходится сертифицировать БПЛА по тем же требованиям, какие предъявляются к Boeing 737 или Aerobus 350. Например, в требованиях значится: «Кабина пилота должна быть оборудована...». Где взять кабину пилота в беспилотнике?» – обрисовал ситуацию Андрей Михеев, директор дивизиона по обследованию и мониторингу компании AeroMax.

Дальше всех в сертификации тяжелых БПЛА продвинулась компания «Кронштадт», но это удовольствие не из дешевых. Обычные российские коммерческие компании такого себе позволить не могут. Поэтому пока эксплуатация тяжелых беспилотников возможна только в экспериментальном, но не в коммерческом режиме.

Николай Носов

Уроки от АНО КС ЦОД

АНО «Координационный совет по ЦОДам и облачным технологиям» провела первые обучающие тренинги, посвященные вопросам создания и эксплуатации дата-центров.



Рост спроса на услуги дата-центров выявил нехватку квалифицированных специалистов, знающих, как правильно создавать и эксплуатировать ЦОДы. Это общая проблема, и участники рынка стали решать ее вместе. Объединяющая крупнейшие компании отрасли некоммерческая организация «Координационный совет по ЦОДам и облачным технологиям» (АНО КС ЦОД) провела первые, во многом уникальные для России и стран СНГ обучающие курсы, в ходе которых ведущие эксперты-практики делились своими знаниями и опытом. Для слушателей было важно получить систематические знания о жизненном цикле дата-центра, понять, насколько сложны подобные проекты, и взвесить возможные риски их реализации. По отзывам многих участников, тренинги были также полезны тем, кто хочет использовать коммерческие ЦОДы для размещения собственной ИТ-инфраструктуры. Такие слушатели получили всю необходимую информацию для того, чтобы всесторонне оценить технологические аспекты, критичные для принятия решения о выборе площадки.

Первые два тренинга состоялись в апреле и июне этого года. Программа рассчитана на три полных дня. Три дня интенсивной работы – три направления: планирование и проектирование, строительство и эксплуатация, экономика ЦОДов. Важная особенность тренингов, как и заявляли организаторы, – нейтральная подача материала, охватывающего широкий спектр вопросов проектирования, строительства и эксплуатации дата-центров.

В ходе тренингов последовательно рассматривались все фазы создания ЦОДа – от выработки концепции до эксплуатации, включая бюджетирование строительства и операционные расходы.

Первый шаг – выработка концепции ЦОДа. На этом этапе нужно ответить на вопросы: какие задачи дата-центр должен решать? Каковы требования к его надежности и отказоустойчивости? Каким нормам и стандартам он должен соответствовать? Следующий этап, определяющий само создание ЦОДа, – решение вопросов, связанных с недвижимостью (земельным участком и зданием), получение исходно-разрешительной документации, подведение необходимых инженерных коммуникаций. Какой подход оптимален – строить здание с нуля, приобретать или арендовать существующее строение и реконструировать его? Какие сложности возникают при реализации этих сценариев? На какие подводные камни может наткнуться будущий владелец ЦОДа при выборе площадки и получении документации, получении и подведении электрических мощностей? Есть ли скрытые факторы или факторы отложенного действия, которые повлияют на надежность ЦОДа через год, пять, десять лет после постройки? Этим темам эксперты уделили много внимания, и стало понятно, почему выбор площадки – важнейший фактор успеха любого проекта. На рынке много специалистов в области проектирования зданий и сооружений, однако ЦОДы имеют свою специфику. Что необходимо учесть в ходе разработки проекта, сколько времени уходит на проектирование и почему проектные решения зачастую расходятся с реализованным объектом – все эти вопросы были детально разобраны с практической точки зрения.

Организация инженерных подсистем, являющихся «начинкой» ЦОДа, обычно считается наиболее очевидным кругом вопросов при создании дата-центра, но мне, как человеку, часто участвующему в отраслевых конференциях, было полезно узнать множество практических

Одной из приоритетных задач АНО КС ЦОД мы считаем повышение квалификации и профессионального уровня специалистов в отрасли. Количество дата-центров продолжает расти, а подготовкой кадров для реализации этих проектов и последующей эксплуатации, по сути, никто не занимается. Мы потратили более полугода на разработку программы курса, постаравшись включить в нее ответы на все основные вопросы, с которыми к нам обращаются специалисты, заинтересованные в развитии инфраструктуры дата-центров. Это действительно уникальный для России и стран СНГ обучающий курс, учитывающий наши региональные особенности и опирающийся на профессиональные знания ведущих отечественных экспертов. Мы считаем опыт наших первых тренингов более чем успешным и уже получили много положительных отзывов от тех, кто их прошел.

Дмитрий Бедердинов,
генеральный директор АНО КС ЦОД



тонкостей, о которых обычно не говорят в докладах на больших форумах. К примеру, о возможностях снижения затрат при построении систем бесперебойного электропитания с сохранением двойного резервирования.

Хотелось бы также отметить тему развития инженерных технологий и попытку заглянуть в будущее инфраструктурных и программных решений для ЦОДов. Каждому руководителю, полагаю, будет важно понимать, как те или иные применяемые в ЦОДе решения будут влиять на ТСО проекта и как в перспективе 5–10 лет может меняться ландшафт используемых технологий.

Много внимания организаторы уделили вопросам эксплуатации и технического обслуживания. Были представлены требования, критерии для их оценки, подробно изложены нюансы бюджетирования. В процессе эксплуатации дата-центр обычно заполняется поэтапно, и управление ресурсами – исключительно важный аспект. Одна из самых сложных задач эксплуатации – баланс между утилизацией пространства машинных залов, подведенных электрических мощностей и возможностями отведения тепла от ИТ-оборудования – также была подробно рассмотрена в ходе тренингов.

Как уже отмечалось, организаторы преследовали цель представить слушателям целостную картину создания ЦОДа, от разработки концепции до его эксплуатации. «Значительная часть программы посвящена рассмотрению технологий и инженерных решений, специфичных для ЦОДа и определяющих его техническое совершенство, – пояснил Константин Королев, директор по развитию отраслевых инициатив АНО КС ЦОД. – Подчеркну, что в ходе тренингов рассматривался не абстрактный, «идеальный» ЦОД, а параметры работы реальных объектов с учетом климатических зон эксплуатации, смены времен года, особенностей окружающей инфраструктуры, социальных и техногенных факторов». Другим существенным аспектом тренинга стал лекторский состав: организаторы изначально ставили задачу привлечь в качестве лекторов не «теоретиков от-

расли ЦОДов», а авторитетных практиков, которые имеют за плечами многолетний опыт построения и эксплуатации дата-центров и представляют ныне ведущие ЦОДы страны и компании, специализирующиеся на создании таких объектов и управлении ими. Алексей Солодовников, управляющий директор российского отделения Uptime Institute, отметил эту уникальную черту тренингов, где собрались «все звезды российского рынка дата-центров, делающие все своими руками».

По итогам тренингов каждый из участников получил электронное приглашение на онлайн-портал АНО КС ЦОД для прохождения итогового тестирования. Тестирование призвано проверить качество усвоения полученных знаний и побудить слушателей применять эти знания на практике. Каждый слушатель, прошедший итоговый тест, получил сертификат, подтверждающий завершение курса.

Все прочитанные в ходе тренингов лекции были сняты на видео в высоком качестве с профессиональным монтажом. Доступ к этим видеурокам был также предоставлен всем слушателям тренингов. Планируется в скором времени предлагать этот видеоконтент по подписной модели.

Организаторы сознательно ограничили количество слушателей в группе двадцатью пятью участниками, чтобы создать максимально комфортную среду офлайн-тренинга и необходимую атмосферу для общения. Сейчас прошли обучение две группы, и осенью будут предложены два новых тренинга. Первый из них, посвященный построению ЦОДов, пройдет по уже разработанной программе 13–15 октября в Москве. Второй тренинг построен на новой двухдневной программе, посвященной эксплуатации ЦОДа. Этот тренинг состоится 15–16 ноября, также в Москве, и уже сейчас на него ведется регистрация участников. Подробнее с программой и условиями участия в каждом из тренингов можно ознакомиться на сайте АНО КС ЦОД.

Николай Носов



НОВОСТИ АНО КС ЦОД

ИЮНЬ 2021

Конференция «ЦОД» в Санкт-Петербурге



Представители АНО КС ЦОД приняли участие в 4-й международной конференции «ЦОД: модели, сервисы, инфраструктура», прошедшей 16 июня в Северной столице. С докладом «О культуре владения ЦОдами» выступил Константин Королев, директор по развитию отраслевых инициатив организации. В частности, он представил образовательную программу АНО КС ЦОД: серию тренингов, направленных на популяризацию знаний об отрасли и на повышение квалификации отраслевых специалистов. *Подробнее – на с. 4.*

ЦОД в законе «О связи»

17 июня в Госдуму внесен на рассмотрение проект Федерального закона «О внесении изменений в Федеральный закон "О связи"». Законопроектом устанавливается понятие центра обработки данных и определяется, кто является оператором таких объектов. АНО КС ЦОД выступила одним из ключевых разработчиков положений готовящегося закона, которые касаются ЦОДов.

Прошел второй тренинг АНО КС ЦОД

21–23 июня АНО КС ЦОД провела в Москве второй трехдневный тренинг «Построение ЦОДа». Образовательную программу АНО КС ЦОД прошли уже 49 специалистов, 38 из них успешно сдали экзамены и получили сертификаты. Следующий семинар «Построение ЦОДа» организаторы планируют провести 13–15 октября 2021 г. На 15–16 ноября намечен тренинг «Эксплуатация ЦОДа»: двухдневный очный семинар, нацеленный на формирование и углубление профессиональных знаний о технических и организационных процедурах, регламентах и основных бизнес-процессах эксплуатации центров обработки и хранения информации. *Подробнее – на с. 12.*

НОВОСТИ ОТРАСЛИ

В Якутске построят дата-центр для ГИС

Правительство Якутии одобрило проект создания дата-центра в столице республики. Как сообщил председатель правительства Якутии Андрей Тарасенко, новый ЦОД

в Якутске будет полностью соответствовать требованиям федерального законодательства в области ИТ и защиты информации. Более того, он может стать опорным на Дальнем Востоке и в Арктической зоне РФ. На мощностях нового ЦОДа, который планируется разместить в здании «Ростелекома», будут развернуты все государственные информационные системы Якутии.

Новый ЦОД «Миран»



В Санкт-Петербурге состоялось торжественное открытие второй очереди дата-центра «Миран-2». Первый ЦОД компания запустила в 2010 г., в 2014-м появился второй – «Миран-2». Предлагающий услуги по модели colocation коммерческий ЦОД «Миран-2» соответствует стандарту Tier III Uptime Institute. Первыми вводятся в эксплуатацию 34 новые стойки, в течение года-полутора их число будет доведено до 300. Расчетная мощность ИТ-нагрузки новой очереди – 1500 кВт.

Госструктурам могут запретить строить новые ЦОДы

В проекте плана поддержки ИТ-отрасли, который был представлен вице-премьером Дмитрием Чернышенко, предлагается запретить строить новые дата-центры за счет бюджетных средств, а госзаказчиков перевести на услуги коммерческих ЦОДов. В проекте отмечается, что сегодня госзаказчики нацелены на создание собственных мини-ЦОДов. При этом качество и надежность построенных объектов зачастую невысоки, а затраты на дальнейшую эксплуатацию велики, что приводит к дополнительной нагрузке на бюджет.

Новый ЦОД «Ростелекома» в Санкт-Петербурге

Официально открытый недавно ЦОД компании «Ростелеком» расположен в Калининском районе города между улицами Жукова и Чугунной. Объект имеет общую емкость 800 стойко-мест, мощность 7,4 МВт и площадь свыше 4 тыс. кв. м.



Клиентам ЦОДа доступен широкий спектр услуг, включая размещение серверного оборудования, предоставление облачной инфраструктуры и сервисов. Объект станет еще одной площадкой для организации географического резервирования и послеаварийного восстановления с участием дата-центров в Москве и Удомле.

Гознак открыл ЦОД в Санкт-Петербурге

Проект и построенный дата-центр Гознака сертифицированы на соответствие уровню надежности Tier III Uptime Institute. В шести машинных залах ЦОДа разместятся 470 стоек. Общая площадь ЦОДа составляет 3540 кв. м, расчетная мощность – 6 МВт. Дата-центр находится на охраняемой территории, оснащенной системой контроля и управления доступом и круглосуточным видеонаблюдением.

«Росэнергоатом» завершил приобретение дата-центра StoreData

«Атомдата-Центр», интегратор инфраструктуры коммерческих ЦОДов и дочерняя компания концерна «Росэнергоатом», и Научный инновационный центр завершили сделку по купле-продаже контрольного пакета московского ЦОДа StoreData. Дата-центр работает на рынке с 2010 г., его инфраструктура сертифицирована по стандарту PCI DSS. ЦОД построен в соответствии с международным стандартом TIA-942 и имеет прогнозируемый коэффициент доступности не менее 99,98%. Текущая емкость – 160 стоек.

Андрей Аксенов возглавил компанию IXcellerate в России



Ведущий оператор сети коммерческих ЦОДов в России объявил о назначении Андрея Аксенова на должность генерального директора (CEO). Ранее эту должность занимал Гай Вилнер, который совмещал посты CEO и председателя совета директоров. Основные задачи Андрея в качестве руководителя компании – реализация долгосрочной стратегии IXcellerate, которая включает ввод новых мощностей ЦОДов в соответствии с возрастающим спросом заказчиков на услуги colocation как в Москве, так и в регионах. К 2023 г. компания намерена завоевать 25% российского рынка коммерческих ЦОДов. *Подробнее – на с. 18.*

**АЛЕКСАНДР БАРСКОВ****ЦОД БУДЕТ ОПРЕДЕЛЕН!**

Отрасль ЦОДов в России есть и быстро развивается, а определения того, что же такое ЦОД, на законодательном уровне нет. Для исправления ситуации 17 июня в Госдуму внесен на рассмотрение проект Федерального закона «О внесении изменений в Федеральный закон «О связи»». Он, в частности, формулирует понятие центра обработки данных и определяет, кто является оператором такого объекта.

ЦОДы – ключевой элемент цифровой инфраструктуры как отдельных предприятий и организаций, так и страны в целом. Опережающее развитие отрасли ЦОДов – важное условие повышения конкурентоспособности экономики России. Без обеспечения такого развития невозможно «создание к 2024 г. устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств» (из национальной программы «Цифровая экономика РФ»).

Однако до недавнего времени ни сами ЦОДы, ни операторы ЦОДов в законодательстве не были определены. Это не позволяло говорить об отрасли в отношении реализации мер господдержки, а также полномасштабно использовать инфраструктуру коммерческих поставщиков сервисов ЦОДов для оказания услуг государственным ведомствам и организациям.

Новый закон предусматривает закрепление статуса ЦОДа как инфраструктурного объекта. Предложена следующая формулировка: «ЦОД – сооружение связи с комплексом систем инженерно-технического обеспечения, спроектированное и используемое для размещения оборудования, которое обеспечивает обработку и (или) хранение данных и соответствует утвержденной классификации». Важно заметить, что классификация и ее критерии будут утверждаться Правительством РФ.

Согласно закону, в рамках основной деятельности оператор ЦОДа оказывает услуги размещения оборудования, обеспечивающего обработку/хранение данных. Это значит, что его основная деятельность не связана с услугами хостинга (предоставления вычислительной мощности) или услугами обработки и хранения информации (анализа информации и предоставления его результатов). Таким образом, инженерно-технические системы отделены от ИТ-систем и услуг, что важно для определения периметра ответственности поставщиков.

Законопроект вводит перечень информации, которую операторы ЦОДов должны предоставлять в федераль-

ный орган исполнительной власти в области связи. Это информация о местоположении ЦОДа, его технологической мощности и параметрах энергоснабжения, способах и параметрах подключения к сети связи общего пользования, средней стоимости услуг размещения оборудования для обработки/хранения данных, а также о перспективах развития ЦОДа на ближайший год.

При отсутствии такой информации невозможно составить объективное представление о существующей инфраструктуре связи и обработки данных, планировать ее развитие и контролировать установленные показатели. Кроме того, она необходима для управления сетью связи общего пользования в чрезвычайных ситуациях, для понимания потребностей различных регионов в услугах ЦОДов, для определения возможности перевода государственных и муниципальных информационных систем с ведомственных серверов, не обеспечивающих необходимый уровень надежности, в ЦОДы, отвечающие самым высоким техническим требованиям.

В перспективе операторы ЦОДов, которые в настоящее время вынужденно являются операторами связи, смогут отказаться от лицензий на оказание услуг связи и получить собственный код внешнеэкономической деятельности, введение которого планируется после вступления в силу законопроекта.

«На протяжении последних полутора лет отраслевое сообщество совместно с Минцифрой вело кропотливую работу по подготовке положений предлагаемого закона в части, связанной с ЦОДами, – рассказывает Дмитрий Бедердинов, генеральный директор АНО «Координационный совет по ЦОДам и облачным технологиям» (АНО КС ЦОД). – Объединяющая основных участников рынка АНО КС ЦОД провела множество обсуждений этих положений, и мы рады, что государство на каждом этапе согласований прислушивалось к экспертам рынка. При разработке изменений в закон «О связи» важно было не только корректно сформулировать определения, но и гармонизировать их с текстом закона, с уже используемыми в нем определениями и не войти в терминологические противоречия с НПА, которые обслуживают другие отрасли экономики. Надеюсь, введение ЦОДов в правовое поле послужит дополнительным стимулом ускорения развития нашей отрасли и цифровой инфраструктуры России».

Предполагается, что новый федеральный закон вступит в силу с 1 марта 2022 г.



Война Афины

Игорь Бакланов,
генеральный директор, «ПламСпейс»
(фонд «Сколково»)

В войне за технологический суверенитет любой прорыв – победа, любое заимствование – поражение и отступление. Какое место на карте этих военных действий занимает российский телеком?

Все глаза были невольно устремлены
на эту французскую колонну, подвигавшуюся к ним
и извивавшуюся по уступам местности...
– Славно идут, – сказал кто-то в свите Багратиона.
Л.Н. Толстой. Война и мир

Питерский прогностик Сергей Переслегин выделил в своих работах три уровня современной войны, обозначив их тремя греческими именами:

- война Ареса – горячая война по всем правилам, война армий и военных;
- война Афины – война технологий, инженеров, конструкторов и ученых;
- война Аполлона – война смыслов, война философов, писателей и художников.

Современные технологии – это поле боя Афины, здесь страны сражаются за технологический суверенитет, против технологической оккупации. Любой технологический прорыв – победа, любое заимствование – поражение и отступление. И не нужно тешить себя либеральными благоглупостями на тему мирового разделения труда, глобализации и взаимного обмена технологиями.

Недавно промелькнула новость – американская компания Viavi захотела купить канадскую компанию Exfo, но ей пока отказали. Типичная маленькая биржевая новость, нам-то что? И только профессионалы в разных странах вздохнули, потому что это финал процесса, который шел 20 (!) лет.

В начале 2000-х не существовало международного разделения труда, была конкуренция. В мире насчитывалось 150 технологических компаний, выпускающих измерительную технику для телекоммуникаций. Нишевой рынок, но вершина пирамиды hi-tech. Измерительная техника нужна для разработки самого оборудования связи и по отношению к этому оборудованию является более технологичным сегментом. Чтобы создать измерительный прибор, нужно разбираться в технологии даже лучше, чем разработчики оборудования и проектировщики. Измерения – это квинтэссенция инженерной школы, основа ее суверенитета. «Наука начинается там, где начинаются измерения», – эти слова Д.И. Менделеева должны быть написаны над входом в каждый технический вуз, как ленинскую фразу о кино можно было прочесть в каждом кинотеатре СССР.

В 2000-х годах первые места в проводном телекоме занимали немцы (Wandel & Goltermann) и американцы (Hewlett-Packard), в беспроводном телекоме – опять же немцы (Rohde & Schwarz) и американцы (Wavetek, Hewlett-

Packard, Wiltron). Но места хватало всем. Были сильные школы в Великобритании, Франции, Дании, Испании, Канаде, даже в Италии, Швеции, Венгрии, Чехии, Мексике, Австралии и пр.

Затем начался интересный процесс: американские компании стали последовательно покупать европейские, азиатские и латиноамериканские активы. Без какого бы то ни было умысла, в рамках рыночной и довольно хаотической деятельности. Но с совершенно предсказуемым результатом: измерительные технологии перекочевывали за океан. И неважно, тучные были годы или кризисные, – процессы шли, иногда бурно, иногда спорадически.

Прошло 20 лет, и европейских школ не осталось. Совсем. Все измерительные приборы для телекоммуникаций сейчас делаются в США или в Канаде. Европейский hi-tech (Albedo (Испания), Intec (Германия)) – это осколки, выпускающие три-четыре прибора нишевого назначения. Компании держатся на энтузиазме своих возрастных учредителей, они стратегически не опасны и в мире уже не составляют конкуренции. Не помогли ни поддержка правительств, ни поддержка вузов, ни инновации...

Под шумок разговоров о глобализации и мировом сотрудничестве американцы скупил самый технологичный сегмент современных телекоммуникаций. И финальным аккордом в этой истории станет покупка американцами ключевого канадского производителя, хотя это уже история американского континента.

В войне Афины на инженерном поле современных телекоммуникаций американцы победили. Их главный конкурент – Китай – вот уже 15 лет пытается создать свою школу метрологии, но не получается, не хватает опыта.

Ну а Россия... Россия создала множество инновационных долин и технопарков, оснатив их лучшим американским (!) измерительным оборудованием. В Реестре телекоммуникационного оборудования российского происхождения, который ведет Минпромторг, строчки «измерительное оборудование» нет.

Остается только любоваться, читать новости и повторять историческую фразу: «Славно идут....». ИКС

«Время нам благоволит»

Компания IXcellerate, входящая в топ-3 коммерческих ЦОДов в России, в июле 2021 г. объявила о назначении нового генерального директора. Им стал Андрей Аксенов, с которым мы беседуем о ситуации на рынке и планах развития компании.



– Андрей, вы новый человек в индустрии ЦОДов. Каковы первые впечатления от этого рынка? Как оцениваете темпы его роста?

– Первые впечатления положительные. Сегодня сложился явный дисбаланс в пользу поставщиков услуг: спрос существенно превышает предложение. Это шлейф начала пандемийного периода, когда многие бизнесы перешли в онлайн, а операторы ЦОДов не успели подготовить свои мощности. Предполагаем, что в конце текущего года и в следующем году рынок будет расти еще быстрее.

Мы, как и ряд других игроков, сейчас активно строим новые площадки. Через год-полтора спрос и предложение должны уравниваться. Но и тогда, став более сбалансированным, рынок продолжит динамично развиваться.

Важно, что в России на высшем уровне принята национальная программа цифровизации, видны реальные действия. Цифровизация стала мейнстримом развития российской экономики. И мы, предоставляя инфраструктуру, являемся для наших клиентов важным элементом цифровизации.

– Рост спроса на услуги коммерческих ЦОДов очевиден. В чем вы видите основные причины? Какие группы компаний сейчас наиболее активно пользуются коммерческими ЦОдами?

– Как я уже сказал, за последние полтора года многие компании, в том числе крупные и средние, перенесли бизнес в онлайн. У них возросла потребность в облачных сервисах, а у их поставщиков – потребность в инфраструктуре для развертывания своих платформ. Мы являемся инфраструктурным фундаментом этой цепочки.

Отмечу среди наших клиентов ряд гиперскейлеров, в первую очередь зарубежных, которые продолжают активно развивать облачные и прочие услуги. Кроме того, видим растущий спрос со стороны провайдеров игровых сервисов, которые все чаще запрашивают высоконагруженные стойки для своих облачных приложений.

Также мы фиксируем высокий спрос со стороны банков. Здесь выделяю сегмент систем с искусственным интеллектом. Голосовые помощники, которые используются в чат-ботах, ста-

новятся все более интеллектуальными, и для их работы требуется все больше производительных серверов. Все, что связано с искусственным интеллектом, требует высокопроизводительных вычислений – ведь робот должен отвечать так же быстро, как и человек, без задержки. Это требует больших ресурсов.

Потребность в услугах коммерческих ЦОДов велика. Многие наши крупные клиенты не только ждут, когда мы введем в строй новые мощности на юге Москвы, но и хотят расширить свое присутствие в нашем северном кампусе.

– У IXcellerate амбициозная стратегия – в ближайшие годы компания намерена завоевать 25% российского рынка коммерческих ЦОДов. Когда ожидать ввода в строй новых площадок?

– Сегодня идет активное строительство южного кампуса. В ближайшие шесть месяцев введем в строй порядка 1200 стойко-мест, 12 МВт ИТ-мощности. На севере столицы мы начинаем строительство модульного ЦОДа на 500 стоек. Таковы планы на ближайшие полгода.

Если смотреть на следующий год, то мы должны ввести вторую очередь дата-центра MOS5 на юге Москвы. Это 1200–1500 стоек. На территории северного кампуса начнется строительство дата-центра MOS3, в котором до конца 2022 г. будут запущены не менее 1000 стоек.

– Предполагает ли стратегия компании покупку других ЦОДов?

– В верхнеуровневой стратегии IXcellerate направление M&A выделено в отдельный блок. Но в ближайшие месяцы мы будем концентрироваться на органическом росте. Акционеры купили большую площадку на юге столицы – территорию бывшего завода «Эфес» площадью 400 га с возможностью ввода более 20 тыс. стоек (наш южный кампус). Работы хватает.

Приобретение активов у нас имеет более низкий приоритет. Деньги на M&A зарезервированы, однако мы будем обсуждать конкретные сделки, только если поймем, что они действительно нам выгодны, что окупаемость хорошая. Но концентрироваться исключительно на неорганическом росте мы точно не будем.

– **Каковы планы в отношении выхода в регионы, страны СНГ?**

– Мы присматриваемся к региональному рынку, но конкретных шагов можно ожидать в течение одного-двух лет. Сейчас просчитываем разные тактики. Куда идти: сначала в Питер и дальше на восток или сразу начать с восточных регионов страны. Как идти: путем покупки существующих ЦОДов или строить новые площадки самим. Пока определяемся, но не исключаю выхода в несколько крупных городов России.

Большая часть спроса сосредоточена в Москве, которая была, есть и будет огромным цифровым хабом. Мы не ожидаем, что, скажем, через пять лет доля Москвы на рынке коммерческих ЦОДов радикально снизится. Да и в тех случаях, когда на наш рынок выходят зарубежные игроки, они тоже идут в Москву или через Москву.

Иногда нам поступают предложения о сотрудничестве из стран СНГ, и мы изучаем их очень тщательно. Нам не нужна экспансия только для того, чтобы галочку поставить. Сейчас основной рынок для нас – Москва, второй приоритет – регионы РФ и потом, возможно, в будущем – рынки СНГ.

– **С какими внешними трудностями вы сталкиваетесь в развитии вашей сети ЦОДов?**

– Повторюсь, рынок сейчас на стороне ЦОДов. Но когда нужно быстро ввести в строй большое количество стоек, длительные сроки различных согласований при строительстве тормозят процесс. На них уходит по несколько месяцев.

Другое узкое место – доступность электроэнергии. Для своих площадок мы этот вопрос решили. Но если смотреть на рынок в целом, то многое зависит от того, где строится ЦОД, насколько далеко от генерирующих мощностей и распределительных узлов. Это может сильно влиять на экономику проекта.

Но настрой на цифровизацию в России позитивный, решения по цифровизации каскадируются вниз, в коммерческий сегмент. Время нам благоволит.

– **IXcellerate традиционно работает по модели colocation. Есть ли планы по расширению пакета услуг, или вы сохраните приверженность избранной модели?**

– Мы с акционерами это обсуждали. И пришли к выводу, что colocation будет оставаться нашей ключевой услугой. Потому что здесь есть большой нереализованный спрос. Возможно, через год-полтора мы увидим, что стратегию надо модифицировать. Но пока такой вопрос на повестке дня не стоит. Основная задача сегодня – строить, подключать, обеспечивать резервирование, т.е. быть надежной инфраструктурой для наших клиентов, в том числе облачных провайдеров.

У нас есть еще одно направление бизнеса – собственная пиринговая платформа (Eurasia Peering). Ее мы тоже будем активно развивать. На зарубежном рынке ЦОДы часто имеют такие платформы, на российском это не так. Среди крупнейших коммерческих ЦОДов пиринговой платформой подобного размера владеем только мы.

Наличие такой платформы – наше серьезное преимущество, в том числе с точки зрения минимизации задержки и оптимизации маршрутов передачи трафика. Мы не ставим задачу конкурировать с MSK-IX, скорее, придерживаемся стратегии dual peering, обеспечивая хорошую связность с MSK-IX.

При этом мы позиционируем себя как нейтральную площадку: не являемся оператором связи, не связаны ни с каким телеком-провайдером, поэтому наши клиенты могут пользоваться услугами любого из них. И сочетание нейтральности и максимальной связности очень важно.

– **Сейчас в России реализуются несколько проектов Tier IV. Значит, есть спрос на более надежные отказоустойчивые решения? Как вы реагируете на эту тенденцию?**

– В первую очередь мы озабочены реальной доступностью (uptime) наших сервисов. С 2013 г., по сути за восемь лет эксплуатации ЦОДа, не было ни единого сбоя, предоставление сервисов не прерывалось ни на секунду. Сертификат – это скорее признание качества сервиса, инфраструктуры сторонним институтом. Мы работаем и в этом направлении, но основной фокус – не на сертификации, а на качестве услуги.

Мы не стремимся получить сертификат Tier IV, поскольку сегодня в России это больше похоже на маркетинговый ход. наших клиентов вполне удовлетворяет наличие сертификата Tier III, и мы продолжим сертификацию своих объектов по этому уровню Uptime Institute. Хотя, возможно, при реализации следующих очередей наших ЦОДов обратим внимание на Tier IV. Но это не самоцель. Наша задача – 100%-ная фактическая доступность и соблюдение SLA.

С открытием южного кампуса мы обеспечим связность между двумя площадками, и у клиентов появится возможность резервировать свои системы на уровне ЦОДов: установить часть стоек в один кампус, часть – в другой, организовать реплицирование данных. Расстояние между площадками около 30 км, поэтому такая схема обеспечит катастрофоустойчивость.

– **Какой вы видите IXcellerate через пять лет?**

– Как вы сами упомянули, мы намерены в ближайшее время захватить четверть рынка. Но все же концентрируемся не столько на достижении каких-либо количественных показателей, сколько на том, чтобы максимально удовлетворять потребности наших клиентов. С нами работают топовые бренды из ИТ, банковской и других отраслей. И мы ощущаем свою ответственность за их развитие. Наша миссия – быть их спутником и надежной цифровой инфраструктурой.

Более того, мы хотим помогать цифровому развитию России в целом, внедрению искусственного интеллекта, построению «умных» городов. Как бы пафосно это ни звучало, но мы действительно хотим вместе со страной идти в новую цифровую эру.

**Беседовал
Александр Барсков**

Citizen development как движущая сила автоматизации

**Светлана
Анисимова,**
генеральный
директор в
России,
UiPath

Современные технологии позволяют создавать сложные ИТ-продукты и софт пользователям без глубинных знаний программирования. Одно из таких решений – RPA-платформы.

С ростом уровня цифровизации бизнеса нехватка на рынке опытных разработчиков программного обеспечения становится все заметнее. По прогнозам IDC, к 2023 г. будет создано более 500 млн приложений. В отрасли попросту недостаточно людей, чтобы справиться с таким объемом работы. Если еще несколько лет назад компании по всему миру закрывали разрыв в кадрах, привлекая новых талантливых ИТ-специалистов, сейчас все иначе. Организации пытаются вырастить разработчиков из собственных сотрудников, часто не имеющих никакого отношения к программированию. К чему это приводит?

Singtel, одна из ведущих телекоммуникационных компаний Сингапура, с 2016 г. начала обучать команду работе с инструментами автоматизации. Через какое-то время сотрудники самостоятельно создали программных роботов, которые избавили их от выполнения большинства рутинных операций – от обработки данных до ответов на электронные письма.

Результат процесса и сам процесс, в котором пользователи с минимальными навыками программирования или вообще без них создают ИТ-продукты, называется citizen development. Данное явление оказалось крайне полезным при переходе бизнеса на цифровые технологии и масштабировании инициатив в области цифровизации. (Тренд новый, в русском языке для него пока нет устоявшегося термина, поэтому в этой статье используется английский вариант – citizen development, что можно перевести как «любительская разработка».)

Кто такие citizen developers?

Citizen developers – это люди, которые создают корпоративные ИТ-продукты, не имея опыта или формального образования в области программирования, разработчики-любители. В прошлом их поле деятельности обычно ограничивалось написанием макросов или скриптов в приложениях Microsoft Excel и Access. Однако



сегодня, когда на рынке с каждым днем появляется все больше так называемых low code-инструментов разработки, которые не требуют от пользователя особых технических знаний и навыков, они могут без труда создавать корпоративные и даже общедоступные приложения.

Как правило, citizen developers становятся сотрудниками, имеющие дело с документооборотом или другими рутинными операциями: бизнес-аналитики и специалисты отделов продаж, маркетинга, HR, юристы. Ведь тот, кто ежедневно тратит время на выполнение какого-либо монотонного процесса, с большей вероятностью будет стремиться его улучшить и автоматизировать. И поскольку они хорошо знакомы со всеми тонкостями бизнес-процессов, такие разработчики могут создавать и настраивать ПО, исходя из реальных потребностей пользователей и задач бизнеса.

Кроме того, процесс citizen development не зависит от ограниченного штата ИТ-специалистов: Gartner ожидает, что к 2023 г. количество «разработчиков-любителей» на крупных предприятиях минимум в четыре раза превысит число профессиональных разработчиков. Каждый из них может создавать собственные продукты и решения и встраивать их в рабочие процессы. А значит, такой подход позволит быстрее продвигать в компании цифровые инициативы и ускорить автоматизацию.

Какие навыки необходимы для citizen developer

Чтобы стать citizen developer, не нужны обширный опыт или специализированные навыки в области программирования. Достаточно того, чтобы сотрудник был заинтересован в изучении новых видов деятельности. Ведь для производства даже одного собственного ИТ-продукта без RPA-инструментов необходимо овладеть базовыми знаниями в области ИТ, освоить платформы, принципы кодирования и многое другое.

Помимо желания учиться, у будущего разработчика должна быть глубокая экспертиза в конкретной предметной области, будь то финансы, продажи или маркетинг. Он должен отлично понимать рабочие процессы, видеть, как и где можно их улучшить в соответствии с потребностями пользователей и целями организации. Именно этим citizen developers выгодно отличаются от специалистов ИТ-отделов.

Наконец, они должны обладать решимостью привести что-то новое в бизнес-процессы своих отделов и команд. К примеру, финансисты могут автоматизировать сбор месячной или годовой отчетности и консолидацию бюджетных таблиц, а операторы службы поддержки клиентов – составление предложений по контрактам. Любое из этих действий неизбежно повлечет за собой реакцию других членов команды на происходящие изменения. И далеко не всегда позитивную.

Остальные навыки, от умения фильтровать данные в Microsoft Excel до владения специализированными инструментами вроде UiPath, индивидуальны для каждой конкретной организации и позиции сотрудника. Более того, они должны регулярно пересматриваться по мере изменения потребностей компании. Для этого многие руководители проводят переподготовку персонала – это позволяет создать резерв кадров в расчете на специфические задачи бизнеса.

К примеру, в австралийском банке Heritage еще в 2017 г. осознали, что необходимо автоматизировать такие процессы, как управление взаимоотношениями с клиентами и корпоративное взаимодействие, с помощью RPA и ИИ. Для того чтобы сотрудники освоили необходимые навыки, компания разработала программу обучения. Несмотря на все трудности совмещения обучения с основной работой, в компании обнаружили 10–20 человек, которые могли способствовать цифровизации на всех уровнях бизнеса. Теперь у них есть полноценная команда автоматизации, управляющая 12 автономными и 60 интерактивными роботами.

Чем еще полезны citizen developers?

Во-первых, citizen developers – это катализаторы цифровизации. Для того чтобы цифровая трансформация заработала, автоматизация должна затронуть все уровни компании. Но у ИТ-департаментов далеко не всегда хватает на это времени и ресурсов. Citizen developers могут заняться созданием и внедрением ИТ-продуктов для решения повседневных задач на уровне отдельных сотрудников и подразделений. Это позволит ИТ-отделу сосредоточить усилия на разработке средств автоматизации в масштабах всей организации.

Во-вторых, citizen developers – посредники между бизнесом и ИТ-командой, которые раньше не понимали друг друга. К примеру, даже если бизнес-руководители знали, что должна делать программа, им порой было сложно объяснить это разработчикам, не обладающим знаниями в конкретной предметной области. Теперь ПО для решения специфических бизнес-задач могут разрабатывать сами пользователи, и возможные недопонимания сводятся к минимуму.

В-третьих, citizen developers помогают снизить нагрузку на ИТ-отдел, освобождая ресурсы для высокоприоритетной работы, требующей экспертного взгляда и опыта. Если ИТ-департамент перегружен простыми запросами на автоматизацию, в ходе масштабирования это может вылиться в серьезную проблему.

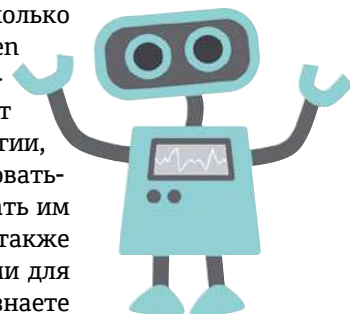
Наконец, citizen developers могут собственными силами спасти себя и своих товарищей по команде от утомительной рутинной работы, до автоматизации которой у ИТ-отдела не доходят руки. В результате сотрудники начинают сами решать свои проблемы, а руководству остается лишь направлять их усилия в правильную сторону.

Инвестиции в людей, а не в средства автоматизации

В 2012 г. аналитики Gartner заявили: «Теперь мы все разработчики». Спустя почти десятилетие мы видим, насколько правы они были. Именно сотрудники, вне зависимости от их позиции в компании, являются основным активом цифровой трансформации.

Один из самых ярких примеров — компания PwC, которая перепрофилировала и повысила квалификацию 55 тыс. сотрудников в США. Компания начала с группы из тысячи добровольцев и научила их использовать передовые инструменты для создания программных роботов. Обучившиеся сотрудники выступили в качестве евангелистов автоматизации по всей компании. Благодаря этому PwC ускорила процесс цифровизации и одновременно повысила уровень вовлеченности сотрудников на 20–30%. Инвестируя в своих сотрудников и дав им шанс экспериментировать и расти, руководство PwC способствовало демократизации процесса автоматизации.

Этот пример наглядно показывает, насколько важно обучать потенциальных citizen developers преимуществам и возможностям low code-платформ и приложений. Нет смысла внедрять инновационные технологии, если сотрудники не знают, как ими пользоваться. Но можно обучить их основам RPA, дать им время и поддержку для экспериментов, а также вооружить инструментами, необходимыми для реализации проектов, – и вскоре вы не узнаете свою компанию. **ИКС**



С3 Solutions и «Новые Технологии»: синергия объединения

Компании С3 Solutions и «Новые Технологии» объявили об объединении и формировании одного из крупнейших игроков на российском рынке инженерной инфраструктуры для ИКТ-объектов. Подробности рассказывают генеральные директора двух компаний: Максим Кыркунов и Алексей Суворов.



Максим Кыркунов,
генеральный директор,
С3 Solutions



Алексей Суворов,
генеральный директор,
«Новые Технологии»

«ИКС»: Каковы причины слияния компаний С3 Solutions и «Новые Технологии»?

Максим Кыркунов: Основные цели – сохранение динамики роста, технологическое развитие и выход в новые для нас ниши рынка, а также усиление экспортной составляющей. Мы работаем на плотном рынке, где быстрый рост возможен в первую очередь за счет подключения партнеров со своей клиентской базой. У компании С3 Solutions среднегодовой прирост выручки последние три года составлял около 80%. Однако понимаем, что дальше развиваться подобными темпами будет непросто. В объединенной компании мы намерены сохранить такую динамику.

Алексей Суворов: Любое объединение преследует цель увеличить объем продаж и общую маржинальность бизнеса: сократить затраты, повысить эффективность за счет увеличения объема выпускаемой продукции. Когда компании работают на одном рынке, возможны два варианта: энергия будет уходить либо на конкуренцию, либо на сотрудничество. Мы за сотрудничество, за синергию объединения, которая позволит существенно увеличить долю занимаемого нами рынка.

Важно, что мы объединяем не только продуктовые линейки, партнеров и команды, мы объединяем нашу экспертизу, возможности R&D, а значит, сможем быстрее разрабатывать новые, востребованные рынком продукты.

М.К.: Также важно и объединение инвестиционных возможностей. В ближайшие два года мы намерены довести площадь наших производственных мощностей до 8 тыс. кв.м, оснастив их более современным оборудованием. Поодиночке такие инвестиции нам осуществить было бы значительно труднее.

Наконец, объединение повысит экспортный потенциал наших разработок. Одна из целей объединения – громко заявить о себе на международном рынке.

«ИКС»: Компания «Новые Технологии» не очень хорошо известна на рынке цодостроения. Расскажите,

пожалуйста, об основных продуктах компании, ее экспертизе.

А.С.: Компания «Новые Технологии» была основана в 2006 г. В 2008 г. мы выпустили первое изделие для телекоммуникационного рынка. Сегодня изготавливаем всевозможные шкафы, открытые и закрытые, настенные и напольные, защищенные, климатические... Последний вариант предполагает задействование систем нагрева и охлаждения. Мы с готовностью комплектуем наши шкафы изделиями других производителей, как зарубежных, так и отечественных. Наши решения установлены почти на всех стадионах, построенных в России к Чемпионату мира по футболу, используются на объектах крупнейших российских компаний, в том числе из нефтегазовой, телекоммуникационной и ИТ-отрасли. Мы присутствуем и в сегменте ЦОДов, но главное внимание до настоящего времени мы уделяли телекому.

М.К.: Хотел бы еще отметить решения компании «Новые Технологии» для систем автоматизации гражданских и производственных объектов, для «умных» городов и зданий. Это очень перспективное направление для нас и наших партнеров. Важно, что в них активно применяются элементы цодовской инфраструктуры. Да и как сегодня «умному» городу или зданию без собственной сети вычислительных и телекоммуникационных узлов?!

«ИКС»: Продуктовые портфели двух компаний пересекаются. Значит ли это, что выпуск части продуктов будет прекращен?

А.С.: Мы работаем для заказчика: если у него есть потребность в продукте, никто не будет снимать его с производства и заставлять заказчика переходить на другое решение. Хотя допускаю, что часть продуктовых линеек будет пересмотрена. Возможно, разработаем новые продукты, которые вберут в себя преимущества существующих изделий обеих компаний. Но без ущемления интересов заказчиков.

М.К.: Полностью согласен с Алексеем. Продуктовые линейки будут жить, пока они востребованы рынком. Никто не лишит заказчиков тех продуктов, которые им нужны. Но,

безусловно, мы тщательно проанализируем все продукты на предмет их дальнейшего развития.

«ИКС»: Что будет с брендами C3 Solutions и «Новые Технологии»?

М.К.: Готовя объединение компаний, мы проанализировали мировой опыт развития брендов в процессах M&A с тем, чтобы сделать интеграцию максимально бесшовной. Понимаем, что в нашей ситуации поддерживать два отдельных бренда нецелесообразно. Рынок достаточно узкий. Поэтому уже в краткосрочной перспективе перейдем к одному сильному бренду. Это будет существующий бренд одной из компаний. Наш анализ показал, что плюсы перехода на единый бренд перевешивают те риски, которые связаны с отказом от одного из брендов.

А.С.: Надо учитывать, что один из наших брендов имеет серьезный маркетинговый потенциал, хорошую узнаваемость. Я говорю про C3 Solutions. Компания «Новые Технологии» развивалась скорее от запросов клиентов, больших бюджетов на маркетинг мы не выделяли. Но каким бы ни был бренд объединенной компании, клиенты только выиграют от возможности получать качественные продукты от более сильной компании с большей экспертизой.

«ИКС»: C3 Solutions хорошо известна на рынке ЦОДов, «Новые Технологии» – на телеком-рынке. Вы будете разделять эти направления?

А.С.: Никаких специальных разграничений внутри объединенной компании делать не будем. Тем более что сейчас идет интеграция рынков телекоммуникаций и ЦОДов. Узлы связи телеком-операторов превращаются в ЦОДы, а дата-центры, в соответствии с концепцией Edge Computing, идут в регионы, размещаются все ближе к местам генерации и потребления данных. Для этого нужны телеком-решения, например, всепогодные шкафы.

М.К.: Все верно. Сегодня среди владельцев крупнейших ЦОДов – телекоммуникационные компании. Мы видим слияние двух отраслей.

«ИКС»: Насколько важно для рынка в целом появление заметно более крупного отечественного производителя, который рождается путем слияния? Откроет ли это вам доступ к новым категориям клиентов?

М.К.: Как уже говорил Алексей, мы рассчитываем на синергию. Наши клиентские базы пересекаются незначительно, поэтому это объединение очень удачно с коммерческой точки зрения. Мы объединяем и партнерские базы, не наступая друг другу на ноги.

Наши компании уже сегодня работают с крупнейшими коммерческими ЦОДами, крупнейшими интеграторами и конечными заказчиками. Но полагаю, что чем крупнее компания-заказчик, тем выше требования к поставщику. Более крупный производитель, конечно, сможет завоевать более высокое доверие, рассчитывать на большее участие в проектах.

«ИКС»: Компания C3 Solutions всегда стремилась к предложению комплексного (полного) решения для

инженерной инфраструктуры ЦОДов. Насколько эта задача сейчас решена?

М.К.: Да, у нас есть комплексные решения, есть проекты строительства ЦОДов под ключ. Пока мы не производим все необходимые компоненты, поэтому заключаем партнерские OEM-соглашения и под нашим брендом предлагаем комплексные решения. При этом тяготеем к работе с российскими производителями, хотя у нас есть опыт сотрудничества и с европейскими вендорами. Здесь нет никаких ограничений, заказчики получают больше возможностей для выбора, а OEM-партнеры – доступ к проектам более высокого уровня и рост своих показателей.

«ИКС»: Как вы оцениваете долю объединенной компании на рынке? Каковы планы ее развития? Возможны ли новые сделки M&A?

М.К.: Мы оцениваем общую долю двух компаний на рынке конструктивов, систем изоляции коридоров и устройств распределения питания для ЦОДов в 23%.

Возможности рынка велики. Решившись на объединение, мы, по сути, первыми из российских производителей делаем такой интеграционный шаг. Поодиночке в ближайшей перспективе на столь конкурентном рынке шансов у нас будет все меньше. Мы общались с руководителями многих российских производителей на предмет возможного объединения, но личные амбиции, желание «сидеть» под своим маленьким брендом не позволяют им осознать новые возможности. И я благодарен руководству компании «Новые Технологии» за проявленную волю принять зрелое предпринимательское решение.

А.С.: Мы с Максимом разделяем идеи о необходимости возрождения и усиления технического и технологического потенциала страны. Поэтому и отдаем приоритет сотрудничеству с российскими компаниями. Мы объехали большую часть страны, посетили почти все компании нашей отрасли. Обменивались опытом, знаниями, практическими навыками. Тех, кто слабее нас, мы готовы делать сильнее. А сами – тянуться за более сильными. В результате такого сотрудничества повышается качество продуктов и услуг, отрасль растет и развивается, привлекает больше инвестиций – выигрывают все. Надеюсь, наше объединение даст рынку еще один мощный импульс развития.

М.К.: Налаженные каналы сбыта и широкая сеть партнеров делают сотрудничество с нами по OEM-схеме выгодным. Но сейчас, проходя процедуру M&A, мы понимаем: объединение ценно тем, что открывает возможность более глубокой интеграции решений. Планируем предложить такой путь и другим игрокам. Мы намерены сформировать зонтичный бренд, собрав под него отечественных производителей систем для ЦОДов и создав производителя мирового уровня и масштаба. И эту концепцию мы скоро представим рынку.

Одной левой: как ИТ-решения меняют работу трактористов

Владлен Валуев,
территори-
альный ме-
неджер по
поддержке
клиентов,
John Deere

Представление о трактористе как о человеке, с ног до головы перепачканном соляжкой, ушло в прошлое. Сегодня такие специалисты выглядят иначе, и даже название профессии изменилось – не «тракторист» или «комбайнер», а «оператор сельскохозяйственной техники».

Человек – слабое звено

Все виды сельскохозяйственной техники претерпели существенные изменения. Электронные устройства, которые есть в машинах, призваны облегчить труд человека и увеличить производительность. Можно сказать, что в связке «человек – машина» именно человек стал в некотором смысле слабым звеном. Поэтому благодаря технологиям оператор постепенно вытесняется из сферы принятия решений. В штатных ситуациях машина это делает сама с помощью инновационных приложений и систем.

Тем не менее последнее слово все равно остается за оператором, который управляет машиной – но уже не за рулем, как прежде, а через дисплей. Для работы с ним необходимы навыки пользования обычным мобильным телефоном. Перелистывание страниц, загрузка приложений, установка нового ПО – все это работает точно так же, как в привычном смартфоне.

Оператор сельскохозяйственной техники должен понимать, что такое сотовые сети, 3G, 4G

и т.д., но сегодня это базовые навыки, которыми владеют даже дети. В машинах даже есть сим-карта – точь-в-точь, как в телефоне. Через нее оператор передает данные о своей работе в офис или получает оттуда предписания, навигационные линии и т.п. Словом, можно сказать, что современная сельскохозяйственная машина – это еще и телекоммуникационное устройство, которое передает данные.

Ничего сложного

Есть распространенное заблуждение, что управлять такой техникой сложно – нужно разбираться в программах, вникать в инструкции и т.п. На самом деле ничего такого не требуется. Как уже было сказано, дисплей, с которого ведется управление, сделан по принципу мобильного телефона, а его интерфейс интуитивно понятен. Точно так же, как мы безо всяких инструкций начинаем пользоваться приложением для доставки пиццы или вызова такси, оператор открывает приложение для





управления машиной и сразу начинает им пользоваться.

Играет роль и геймификация – приложения снабжаются всевозможными иконками, представление данных делается как можно более наглядным, что также упрощает работу с дисплеем. Стоит добавить, что все программы локализованы – в России они представлены на русском языке, а, например, в Казахстане – на казахском. Поэтому вопреки еще одному распространенному стереотипу, который появился в последние годы, оператору сельхозтехники вовсе не требуется знать английский язык.

Чтобы стать хорошим оператором сельскохозяйственной техники, нужны другие навыки, и один из главных – это усидчивость и вдумчивость. Чтобы машина все делала за человека и избавляла его от лишней работы, ее требуется настроить. Поэтому оператору перед выездом на смену надо в течение 10–15 минут провести автоматизацию процессов и ввести нужные данные: границы полей, навигационные линии, указать название клиента, фермы, поля, расстояние до орудия, ширину орудия, при необходимости – температуру почвы, воздуха и т.д. Если этого не сделать, оператору в процессе работы понадобится выполнять гораздо больше действий, он быстрее утомится, а это влияет на производительность.

Конечно, даже при стопроцентно настроенной технике оператор не сидит в кабине сложа руки. Все стало технологичнее, но иногда требуется сделать что-то вручную: заправить химикаты или семена, залить топливо. Это не отменяет ключевого преимущества, которое мы получили благодаря высоким технологиям: машина совершит меньше ошибок, чем человек, и с него по максимуму снимается принятие решений. К тому же повышается прозрачность: машина постоянно подключена к сети, и можно увидеть, чем именно занимается оператор, нет ли нарушений или

ошибок с нормами внесения удобрений или высева, не сливает ли он, к примеру, топливо. Недобросовестные работники считают такой контроль ненужным, но для грамотного специалиста это дополнительная помощь – если он случайно допустит ошибку в настройках, ему тут же придет сигнал, и он сможет оперативно ее исправить.

Не конкуренты, а помощники

Существуют опасения, что машина совсем вытеснит человека, но в обозримом будущем этого не случится. Да, сейчас оператор на одной современной машине делает столько же, сколько выработывают четыре-пять, а то и больше старых тракторов. Но без участия человека все равно не обойтись – именно он принимает окончательные решения и отвечает за безопасность.

К тому же все еще актуальна проблема нехватки кадров, и автоматизированная техника скорее помогает ее решить, чем конкурирует с человеком за рабочие места. Не всем операторам удастся без труда привыкнуть к новым реалиям – как правило, молодые специалисты делают это сразу же, а вот те, кто годами работал по старинке, нередко относятся к современным машинам настороженно. Но опыт показывает, что если таким операторам на практике показать, как техника работает и какой эффект дает, то они понимают, что так проще, что не нужно тратить лишние усилия, а достаточно нажать одну кнопку. Ведь сейчас человек может полностью настроить машину под себя и в буквальном смысле управлять ею одной рукой.

И когда оператор это видит, у него возникает желание постоянно учиться новому и переселиться на такую технику. Не случайно во многих хозяйствах новая техника используется как элемент поощрения – современные машины предоставляют лучшим специалистам, а те, в свою очередь, благодаря им повышают производительность и зарабатывают больше. **ИКС**



Сетевая инфраструктура в ЦОДах

Что изменила пандемия

Сергей Кулаков, аккаунт-менеджер, CommScope
Александр Барсков

Спрос на услуги ЦОДов и облачные сервисы растет, и это повышает требования к масштабированию пропускной способности сети, а также к гибкости инфраструктуры для быстрого подключения новых клиентов/сервисов и переконфигурации в соответствии с меняющимися задачами.

Пандемия не только не затормозила, а наоборот, ускорила развитие рынка коммерческих дата-центров в России. По данным iKS-Consulting, в 2020 г. объем предложения в стойко-местах увеличился на 13%, что превысило темпы роста рынка в предыдущие два года. Экспоненциальный рост объема данных и спроса на услуги ИТ-аутсорсинга станут основными факторами развития рынка коммерческих ЦОДов в ближайшие годы.

При выборе коммерческого ЦОДа заказчики в России сегодня в первую очередь уделяют внимание базовым факторам, связанным с надежностью и отказоустойчивостью (рис. 1).

Растет спрос на ЦОДы с более высокими показателями надежности и отказоустойчивости. В Москве уже построен первый коммерческий ЦОД Tier IV – максимального уровня отказоустойчивости по классификации Uptime Institute. Еще два подобных объекта находятся в стадии строительства.

Пандемия повысила значимость надежной работы ЦОДов, поскольку от развернутых в них ИТ-систем зависят не только бизнес компаний, но и работа органов государственного управления, здоровье и жизнь людей. При этом все более важной становится связность – надежность и производительность сетевой инфраструктуры как внутри ЦОДа, так и вне его, включая соединения между ЦОДами.

Требования к инфраструктуре ЦОДов

Пандемия ускорила общий рост объемов передаваемого по сетям трафика. Так, в период с февраля по середину апреля 2020 г. глобальный интернет-трафик вырос почти на 40% (данные IEA), что обусловлено резким увеличением потребления таких сервисов, как видеостриминг, видеоконференцсвязь, онлайн-игры, социальные сети. Этот рост происходит на фоне общего подъема спроса на цифровые услуги за последнее десятилетие: с 2010 г. число пользователей интернета во всем мире удвоилось, а глобальный интернет-трафик вырос в 12 раз.

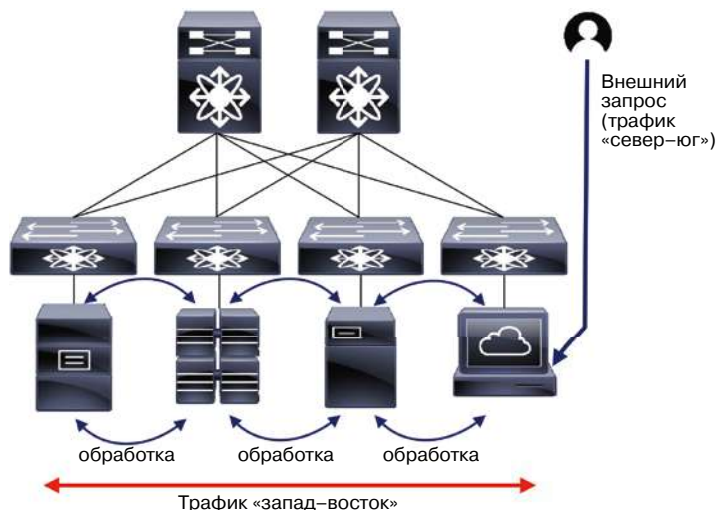
Объем трафика, циркулирующего внутри ЦОДа, т.е. между коммутаторами внутри сети (так называемый трафик «запад – восток»), существенно превосходит объем внешнего трафика – между ЦОДом и потребителями его сервисов (трафик «север – юг») (рис. 2). Главная причина такого доминирования – особенности архитектуры приложений, которые обычно разворачиваются на оборудовании, размещенном в ЦОДе. Например, пользователь, заходя на сайт, хостинг которого обеспечивает ЦОД, порождает всего один внешний запрос к веб-серверу (трафик «север – юг»). Но внутри ЦОДа он создает целый набор подключений: от ба-



лансировщика нагрузки к серверу front-end, от него к серверу back-end, от того к базе данных и обратно (трафик «запад – восток»).

На требования к сети ЦОДа помимо архитектуры приложений сильно влияет их виртуализация. Одиночное приложение, не связанное с хранением данных, редко может генерировать нагрузку на сеть больше 1 Гбит/с, но десятки приложений – запросто. Виртуализованные же приложения могут размещаться на серверах крайне плотно и должны быстро между ними перемещаться, значит, широкая полоса пропускания необходима везде.

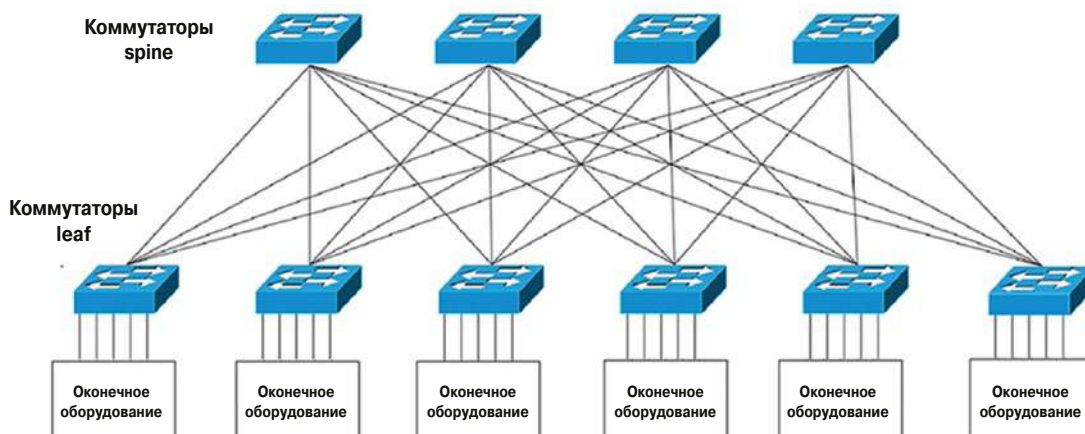
Широкое применение виртуализации и облачных вычислений привело к тому, что для ЦОДов потребовалась новая сетевая архитектура, способная обеспечить меньшее время задержки и большую пропускную способность. Такая архитектура (рис. 3), получившая название сетевой фабрики, основана на соединениях между коммутаторами доступа (leaf) и ядра (spine).



▲ Рис. 1. Оценка важности параметров коммерческих ЦОДов и уровня удовлетворенности их показателями

Рис. 2. Основные направления трафика в сети ЦОДа ▼

Рис. 3. Сетевая фабрика, имеющая архитектуру leaf – spine ►



Сетевая фабрика хорошо подходит для организации универсальных облачных услуг, обеспечивая соединения «каждый с каждым» с прогнозируемой пропускной способностью и с малым временем задержки. Ей присуще внутреннее резервирование благодаря множеству коммутационных ресурсов, распределенных по всему ЦОДу, что повышает доступность приложений. Развертывание и масштабирование такой сети может оказаться намного менее затратным по сравнению с развертыванием и масштабированием сетей на базе традиционных централизованных коммутаторов.

Несмотря на существенные различия, сетевые фабрики схожи с традиционными трехуровневыми иерархическими сетями в том, что они должны быть масштабируемыми, управляемыми и надежными. Использование принципов структурированных кабельных систем позволяет обеспечить необходимое масштабирование и улучшить как показатель среднего вре-

мени ремонта (MTTR), так и общий уровень доступности систем. Организация сетевой фабрики с коммутационным полем кросс-коннекта заметно увеличивает гибкость при подключении оборудования.

На периферии сети, на уровне серверов, сегодня задействуются в основном интерфейсы 1, 10 и 25 Гбит/с. Здесь еще используются медножильные подключения: шнуры СКС или шнуры прямого подключения (DAC) – особенно когда коммутаторы leaf установлены в стойки с серверами (в архитектуре ToR). Если же коммутатор leaf располагается в середине ряда стоек (MoR) или в его конце (EoR), то для подключения серверов чаще применяют оптику (рис. 4). Следует заметить, что архитектуры MoR и EoR становятся все более популярными, поскольку позволяют уменьшить число коммутаторов, что дает возможность снизить сложность сети и задержку при передаче трафика. Переходу на схемы MoR и EoR способствуют и достижения в

Системы управления AIM

Термин AIM (Automated Infrastructure Management), или «автоматизированное управление инфраструктурой», был принят относительно недавно, тогда как описываемые им

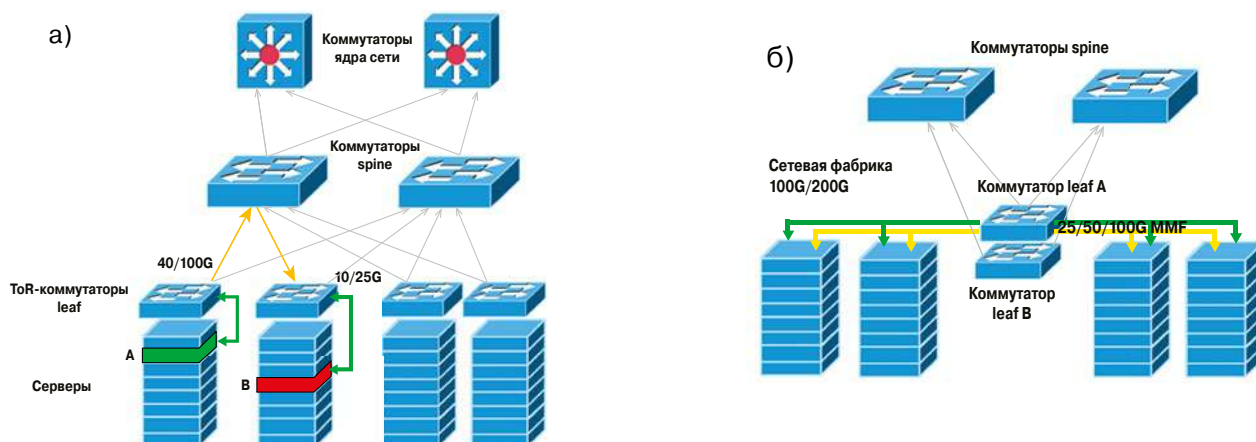


системы управления известны уже почти четверть века. В разные периоды их развития применялись разные термины: «управляемое кроссовое поле», «интеллектуальные СКС» и пр. Но суть всегда была одна – автоматизация управления кабельной инфраструктурой.

Системы AIM состоят из трех базовых компонентов: интеллектуального коммутационного поля, контроллера и ПО управления. «Интеллект» коммутационного поля заключается в его способности регистрировать факты подключения/отключения коммутационных шнуров. Контроллер выступает шлюзом между интеллектуальным коммутационным полем и ПО управле-

ния, предоставляя в реальном времени информацию, которая позволяет точно контролировать происходящие в сети процессы. ПО управления (диспетчер AIM) документирует состояние кабельной инфраструктуры и дает возможность его контролировать через удобный пользовательский интерфейс – как правило, он доступен через веб-браузер.

В 2016 г. стандарт ISO/IEC 18598 утвердил термин AIM, определил базовые функциональные возможности таких систем, а также необходимость открытых интерфейсов для их интеграции с другими системами. Стандарт определяет AIM как «интегрированную программно-аппарат-



области микросхем, повышающие производительность отдельных коммутаторов.

Основная среда для связи между коммутаторами leaf и spine – вне всякого сомнения, оптика, а скорости постепенно приближаются к 200 и 400 Гбит/с (рис. 5). В список оптических решений, поддерживающих 200G и 400G, входят приложения 200GBASE-DR4, 200GBASE-LR4 и 400GBASE-DR4 для одномодовых сред и 400GBASE-SR16 для многомодовых. Для каждого из этих типов волокон есть дуплексные и параллельные варианты. Хотя показатели относительной стоимости меняются, но пока многомодовые системы продолжают требовать меньших капитальных затрат и по большей части остаются проще в поддержке и эксплуатации, чем одномодовые системы.

Помимо высокой производительности сетевой инфраструктуры, для современных ЦОДов важны ее хорошая масштабируемость и управляемость. Они необходимы для оперативного

наращивания мощностей, быстрого подключения новых клиентов и развертывания новых сервисов. Чтобы ускорить выполнение подключений в ЦОДах, все чаще применяют претерминированные кабельные сборки, которые минимизируют объем работ «в полевых условиях» при гарантированном высоком качестве соединений на основе изготовленных на заводе сборок.

Необходимость повышения скорости передачи данных в ЦОДе заставляет увеличивать число оптических волокон. Связано это со все большим распространением параллельной оптики. Если раньше в ядре сети использовались 24-, 72-, 144- или 288-волоконные кабели, то сегодня применяют уже кабели, содержащие 1728, 3456 и даже 6912 волокон (*Подробнее → см. с. 34 «Готовимся к 400G, ждем 800G»*). Инсталляция и обслуживание столь большого числа кабелей требует специальных высокоплотных кабельных систем, которые занима-

▲ Рис. 4. Организация сети ЦОДа по схеме ToR (а) и MoR/EoR (б)

ную систему, которая автоматически детектирует подключение и отключение коммутационных шнуров и документирует состояние кабельной инфраструктуры, включая подключенное к ней оборудование, а также обеспечивает управление инфраструктурой и обмен данными с другими системами».

Согласно ISO/IEC 18598, к числу базовых (обязательных) требований к системам AIM относятся:

- автоматическое определение наличия соединений на кроссовом поле;
- обеспечение в месте установки стойки доступа к электронным нарядам на выполнение работ, трассировочной и другой информации;

- выдача звуковых/визуальных предупреждений о некорректном подключении и отключении коммутационных шнуров.

Стандарт ISO/IEC 18598 требует наличия в системе AIM открытых программных интерфейсов, что критически важно для ее интеграции с другими системами, в том числе:

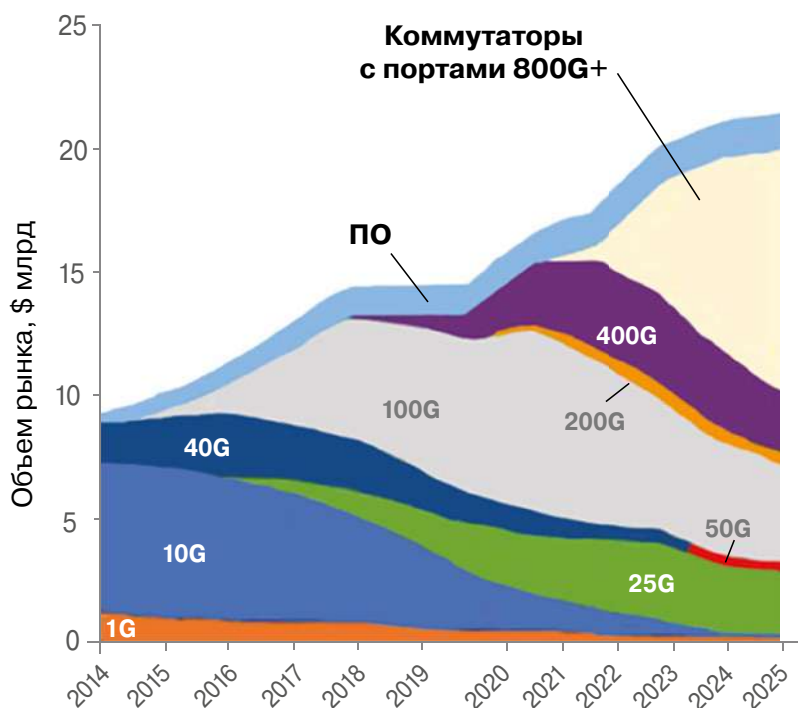
- системами управления зданием (энергообеспечение, освещением, безопасностью, доступом и т.д.);
- системами управления инфраструктурой ЦОДа (Data Center Infrastructure Management, DCIM).

В стандарт ISO/IEC 18598 включен раздел, в котором перечислены преимущества использования систем AIM. Это, в частности, точное и авто-

матическое документирование кабельных трасс – ранее трассировка выполнялась вручную, что часто приводило к ошибкам. Системы AIM позволяют автоматизировать процедуры внесения изменений и эффективно ими управлять, что дает возможность снизить операционные расходы и опять-таки минимизировать вероятность ошибок, связанных с человеческим фактором. Важная функция таких систем – управление инцидентами для уменьшения времени простоя и восстановления ИТ-оборудования и сервисов. Наконец, имеющиеся в AIM возможности управлять емкостью улучшают планирование и повышают процент утилизации портов.

Рис. 5. Объем и структура рынка коммутаторов Ethernet для ЦОДов

Источник: 650 Group, Market Intelligence Report December 2020



ют минимум дорогостоящей полезной площади машинных залов ЦОДов. Например, это могут быть внестоечные ODF-шкафы высокой плотности, которые можно установить в углу серверного помещения.

По мере роста скорости передачи данных максимально допустимые оптические бюджеты сокращаются. Скажем, если для канала 10GBASE-SR при длине 300 м допустимы потери 2,6 дБ, то для канала 100GBASE-SR4 при существенно меньшей длине (70 м) они снижаются до 1,8 дБ (в обоих случаях данные приведены для волокон OM3). Поэтому все более востребованы компоненты с низкими и сверхнизкими задержками: LL (Low-Loss) и ULL (Ultra-Low-Loss). Использование таких модульных претерминированных решений существенно повышает вариативность проектирования кабельной системы, позволяя, скажем, увеличить длину канала и/или число соединителей.

Для повышения вариативности важно и то, что названные решения поддерживают практически все комбинации типов волокон, количества соединений и вариантов топологии для различных архитектур. Это обеспечивает возможность организации высокоскоростных каналов большей дальности, свободу выбора топологии для масштабирования в очень больших и сложных средах и гарантированную производительность приложений как для стандартных, так и для проприетарных систем. В связи с большим числом вариантов подключения серверов, в том числе проприетарных, особую важность приобретают системы управления кабельной инфраструктурой класса AIM.

Инфраструктура ЦОДа должна быть способна к масштабированию, т.е. к переходу на более высокие скорости передачи данных. Поэтому поддержка в будущем 100G, 200G, 400G и даже более высоких скоростей – часть требований к проекту сети, которые влияют на выбор типа волокна (многомодовое или одномодовое), его класса (OM3, OM4 или OM5) и количества пар волокон, установленных на каждом участке.

Для перспективного проектирования сети необходимо рассмотреть целый ряд моментов, в частности:

- фактические (а не средние или типичные) потери, которые вносит каждый элемент проектируемой кабельной системы;
- полосу пропускания конкретной среды передачи (например, OM3 обеспечивает меньшую полосу пропускания, чем OM4, а OM5 – возможность передачи нескольких длин волн);
- возможности параллельных многоволоконных линий и/или сочетания параллельных и дуплексных линий;
- влияние размера ЦОДа – то, как длина каналов ограничит переход к скоростям следующего поколения.

Для помощи в проектировании, развертывании и модернизации (при переходе к более высоким скоростям) оптоволоконной инфраструктуры ЦОДов существует целый ряд инструментов. Они позволяют определить допустимые топологии кабельных каналов для широкого спектра приложений с учетом стандартов, соглашений между производителями и проприетарных спецификаций. Кроме того, предлагаемые производителями СКС калькуляторы выдают требования к затуханию для конкретного канала, одновременно показывая, какие приложения он будет поддерживать.

СКС как сервис в коммерческих ЦОДах

Конкурентоспособность коммерческих ЦОДов зависит, в частности, от скорости развертывания новых сервисов, отказоустойчивости физических линий передачи данных, наличия конкурентных предложений внешних каналов связи. Заранее подготовленная СКС обеспечивает гибкость в планировании и распределении полезной площади как для небольших клиентов, так и якорных арендаторов.

Уровень функциональности и доступности СКС может (и должен) стать одним из важных пунктов SLA, определяющих:

- время, требуемое на подключение нового оборудования;
- отказоустойчивость и резервирование кабельных соединений;
- пропускную способность физических линий (количество волокон, интерфейсы).

Стандарт EN 50600-2-4/ISO 22237-5 описывает четыре класса доступности и топологии СКС для ЦОДов:

Класс 1. Прямое соединение или упрощенная фиксированная инфраструктура.

Класс 2. Фиксированная инфраструктура с резервированием кабельного ввода от оператора связи.

Класс 3. Фиксированная инфраструктура с резервированием операторского кросса и кабельных трасс.

Класс 4. Фиксированная инфраструктура с резервированием кабельных трасс, операторского, центрального и других кроссовых узлов.

Для ЦОДов, к которым предъявляются жесткие требования отказоустойчивости (т.е. для подавляющего большинства таких объектов), рекомендованы СКС класса 3 или 4. Для этих классов обязательна организация коммутационных полей по схеме кросс-коннекта, реко-

мендуется использование претерминированных решений.

Основные требования к СКС в коммерческих ЦОДах:

1. Быстрое и четкое выполнение коммутаций между каналами операторов и зонами размещения оборудования арендаторов, минимизация задержек в линиях связи между облачными провайдерами и их клиентами.

2. Быстрое и четкое выполнение коммутаций между отсеками, рядами и целыми машзалами, занятыми якорными арендаторами.

3. Эффективное перераспределение емкости оптических линий, высвобождаемой в результате ухода (смены) арендатора.

Отношение ряда операторов коммерческих ЦОДов к СКС как к статье расходов (дополнительных затрат) принципиально неверно. Оператор может зарабатывать на СКС, например, взимая плату за выполнение коммутаций к операторам связи (для соответствующего биллинга может использоваться система класса AIM).

Грамотно организованная СКС помогает создавать добавленную стоимость и дополнительные сервисы, которые позволяют оператору ЦОДа оптимизировать использование ресурсов и стать более привлекательным для клиентов. **ИКС**



19 ОКТЯБРЯ 2021

Онлайн-форум о развитии рынка дата-центров и облачных сервисов стран Средней Азии, в первую очередь Казахстана и Узбекистана.

2000 лет назад Шелковый путь представлял собой главную торговую артерию между Европой и Азией. Сегодня, в цифровую эпоху, мы наблюдаем возрождение Шелкового пути как цифровой артерии, включающей высокоскоростные линии связи и дата-центры как основу современных ИТ-сервисов, прежде всего облачных.

ШЕЛКОВЫЙ ПУТЬ

Конференция проходит
в онлайн-формате
Регистрация и подробная
информация на сайте:
dcforum.su

ИКС
МЕДИА



ЦОД «Миран-2»: эстетика и функциональность

В апреле 2021 г. в Санкт-Петербурге введена в эксплуатацию новая очередь коммерческого дата-центра «Миран». Подробности реализации проекта делится региональный представитель компании Rittal по направлению ИТ в СЗФО Антон Морозов.



Антон Морозов,
менеджер по ИТ СЗФО, Rittal

– Оборудование Rittal установлено во многих российских ЦОДах. Чем интересен проект «Миран-2»?

– Этот ЦОД – один из первых проектов, где установлены наши новые серверные стойки Rittal VX IT, которые были анонсированы в 2020 г. Кроме того, ряд технических решений был доработан специально для проекта «Миран-2»: блоки распределения питания (PDU) и система изоляции холодного коридора. Сами стойки Rittal VX IT – очень гибкое решение и были выбраны специально для выполнения требований заказчика. Это такой конструктор, который на основе рамы позволяет собрать то, что нужно конкретному клиенту. Важно, что элементы стойки можно быстро поменять в соответствии с задачей заказчика без «доработки напильником».

– Чем проекты создания коммерческих ЦОДов отличаются от проектов корпоративных дата-центров?

– Владельцы коммерческих ЦОДов чуть меньше внимания уделяют технической составляющей. Экономический аспект для них важнее. Главная проблема в работе с коммерческими ЦОДадами – борьба за стоимость. Не секрет, что такие заказчики часто применяют самые бюджетные решения.

Компания «Миран» не стала экономить на качестве. В проекте используется оборудование ведущих мировых брендов: Rittal, Stulz, ABB и др. При этом мы «прошли по стоимости», выиграв в конкуренции у российских произво-

дителей серверных стоек. Важно, что контракт, заключенный на год, предусматривает поэтапную закупку оборудования. Средства не замораживаются, а рационально и своевременно вкладываются по мере необходимости масштабирования ЦОДа.

– Для коммерческих ЦОДов очень важна и скорость ввода объекта в эксплуатацию. Вы продвигаете свои изделия под слоганом «самый быстрый шкаф», что, видимо, наилучшим образом отвечает таким запросам?

– Этот слоган Rittal подразумевает оперативность и удобство развертывания, обслуживания и эксплуатации. Лично присутствовал при разгрузке и монтаже и подтверждаю, что все быстро и удобно. С момента начала разгрузки до окончания монтажа 34 стоек Rittal с участием директора по строительству ЦОДа «Миран» Виталия Николаева и его команды прошло всего пять часов. И ЦОД – в рабочем состоянии!

Особое внимание уделено возможности обслуживания инфраструктуры одним человеком при минимальных затратах времени и без использования дополнительных инструментов. Например, в течение 10 секунд легко производится навеска и демонтаж двери. Смена левой навески двери на правую может быть выполнена в течение буквально 5–10 минут.

Благодаря улучшенной конструкции рамы ИТ-стойка имеет большую жесткость 19-дюймового вертикального профиля. Стойка VX IT standard выдерживает статическую нагрузку 1500 кг. На такой же вес рассчитан фальшпол в серверном зале. Если заказчик хочет использовать более тяжелое оборудование, можно усилить фальшпол и установить вариант стойки VX IT dynamic, допускающий нагрузку до 1800 кг.

Для разграничения пространства между стойками в проекте применены цельностальные перегородки, позволяющие разделить системы соседних клиентов. Обычно используют шкафы с боковыми стенками. В предложенном нами решении между шкафами вместо двух стенок одна тонкая перегородка. Это экономит место и позволяет улучшить жесткость конструкции ряда стоек. Перегородку можно снять, получится единое пространство – если соседние стойки арендует один клиент.

– А что со скоростью доставки оборудования из Германии?

– Стойки Rittal VX IT – новые. На момент заключения договора на складе их еще не было. Тем не менее, несмотря

◀ Первая очередь нового ЦОДа «Миран-2»



на карантинные меры из-за пандемии и локдаун на территории Германии, задержек в реализации проекта не произошло, оборудование изготовили и привезли даже раньше срока. Производство и доставка шкафов из Германии заняли четыре недели.

Больше всего времени – шесть недель – потребовалось на изготовление и доставку разработанных по специальным требованиям PDU. Но заказ на их производство разместили заранее, так что они даже ждали своей очереди на складе. Учитывая, что «Миран» – коммерческий дата-центр, число розеток в блоке увеличили до 48. Другая особенность – маркировка основных и резервных вводов PDU. Клиенты иногда их путают, поскольку обычные наклейки можно не заметить или они могут отвалиться. Во избежание такой ситуации PDU окрашены в черный и красный цвета.

– В числе уникальных решений вы упомянули систему изоляции холодного коридора. В чем ее особенность?

– Да, компания Rittal специально для клиента разработала систему изоляции холодного коридора. Для корректной работы системы пожаротушения в ней используются откидные панели с электромагнитными замками и децентрализованными шарнирами. При срабатывании системы пожаротушения электромагнитный замок размыкается, панели шириной 600 мм откидываются, благодаря чему гасящий огонь газ хладон из общего зала попадает в коридор.

Компания Rittal всегда стремится обеспечить комфортную и безопасную эксплуатацию своих решений. Учтя высоту стоек 2200 мм и наличие откидных потолочных панелей системы изоляции холодных коридоров, мы приподняли уровень панелей с помощью специальной надстройки, позволяющей безопасно эксплуатировать оборудование находящимся внутри коридора заказчиком и службе эксплуатации ЦОДа.

Первоначально предполагалось, что надстройка будет иметь высоту 300 мм (над стойками). Но когда стойки уже были поставлены, мы увидели, что лотки для кабельной системы находятся ниже. Чтобы надстройка не мешала кабельным лоткам, на производство оперативно отправили изменения и уменьшили ее высоту до 200 мм. Также мы сделали индивидуальное брендинг дверей и специальную окраску элементов коридора.

– Недавно Rittal объявила о стратегическом партнерстве с компанией Stulz. Проект «Миран-2» является одним из примеров такого партнерства?

– Действительно, в ЦОДе «Миран-2» установлены фреоновые кондиционеры Stulz, поставку которых осуществила компания HTS, официальный дистрибьютор Stulz на территории России.

Rittal и Stulz – две давно работающие на рынке семейные немецкие компании, выпускающие надежное, высококачественное и при этом разное оборудование для ЦОДов. Коллаборация позволяет обеим компаниям дополнить

друг друга и предложить полное решение для инженерной инфраструктуры ЦОДа. И проект строительства ЦОДа «Миран-2» продемонстрировал преимущества кооперации наших компаний.

– Для клиентов коммерческих ЦОДов чрезвычайно важна физическая безопасность ИТ-оборудования. Как она обеспечивается в ЦОДе «Миран-2»?

– Начну с того, что реализован индивидуальный подход к системе контроля управления доступом в модуль холодного

коридора. В настоящее время двери снаружи и изнутри открываются по срабатыванию датчика движения, настраиваемого по радиусу и высоте. Инфракрасные датчики не дают закрываться створкам дверей при наличии препятствия между ними, что исключает травмирование человека.

Сейчас в зале установлен один модуль, всего их планируется шесть. В дальнейшем двери в холодный коридор снаружи будут открываться через СКУД здания по персональному коду, чтобы клиент не мог попасть в чужой модуль, а датчики движения будут использоваться только для открывания изнутри.

Помимо этого, как и в других дата-центрах «Миран», на шкафы установлены ручки с кодовыми замками, позволяющими клиенту ЦОДа открывать только свои стойки. Причем использованы уникальные вставки (замочные личинки), которые производятся только для данного ЦОДа. Если клиент забудет код, то представитель «Мирана»

(у которого есть универсальный ключ) может его сбросить, и клиент настроит код заново.

Вроде незначительная деталь – ручки с кодовыми замками. Но они существенно повышают уровень защищенности для клиента. К слову, я не видел других подобных решений на рынке. Конечно, можно установить ручки Rittal на шкафы российского производства, но насколько удачно это получится – большой вопрос. Замечу, что сделать мелкую фурнитуру гораздо сложнее, чем сварить раму стойки. Неудивительно, что есть российские производители, которые петли и ручки покупают у нас тысячами.

Дополнительный плюс – у Rittal и «Мирана» схожие брендовые цвета: оттенки пурпурного, которые используются, например, в оформлении ручки стойки. Мелочей в коммерческом ЦОДе нет.

В целом ЦОД «Миран-2» получился очень красивым и функциональным. Причем эстетика в данном случае работает не только на привлечение клиентов, она позволила повысить удобство эксплуатации и безопасность.



▲ Новая ручка Rittal с кодовым замком для индивидуального доступа в стойку



**ООО «Риттал», 125252, Москва,
ул. Авиаконструктора Микояна, 12,
БЦ «Линкор», 4 этаж
тел. (495) 775-0230
info@rittal.ru, www.rittal.ru**

Готовимся к 400G, ждем 800G

Объем трафика, поступающего в ЦОДы, растет, а новое поколение приложений требует снижения задержки до уровня миллисекунды. Эти тенденции формируют новые вызовы для инфраструктуры дата-центров.

Джеймс Янг, директор по корпоративным ЦОДам, **Джейсон Батиста**, архитектор ЦОДов, **Кен Холл**, архитектор решений для облачных ЦОДов, **Мэтт Бальдассано**, технический директор, CommScope

Главный показатель успеха любой компании – ее способность адаптироваться к изменениям окружающей среды. Назовем это живучестью. Способность ЦОДов адаптироваться и выживать проверяется постоянно – ужесточением требований к пропускной способности, емкости и величине задержки при переходе на более высокие скорости передачи данных в сетевой инфраструктуре. В течение последних нескольких лет мы наблюдали, как скорость соединений в сетях ЦОДов увеличилась с 25G/100G до 100G/400G. За каждым скачком скорости следует короткое плато, которое дает менеджерам ЦОДов возможность подготовиться к следующему прыжку. Сейчас ЦОДы готовятся взять «высоту» 400G.

Удовлетворить растущие требования к снижению задержки и увеличению пропускаемого объема трафика в сети можно четырьмя основными способами:

- снизить уровень потерь сигнала в канале связи;
- уменьшить длину канала;
- увеличить скорость передачи сигнала;
- расширить размер сетевой «трубы».

Дата-центры в какой-то степени применяют все эти подходы, но основное внимание – особенно в гиперЦОДах – уделяется увеличению числа оптических волокон. Исторически магистральные кабели содержали 24, 72, 144 или 288 волокон. Сегодня в таких кабелях используются уже 1728, 3456 или даже 6912 волокон – в 20 с лишним раз больше, чем ранее.

Из выпущенной компанией CommScope электронной книги What's Next for the Data Center: 2021 Trends to Watch.

Когда число волокон растет

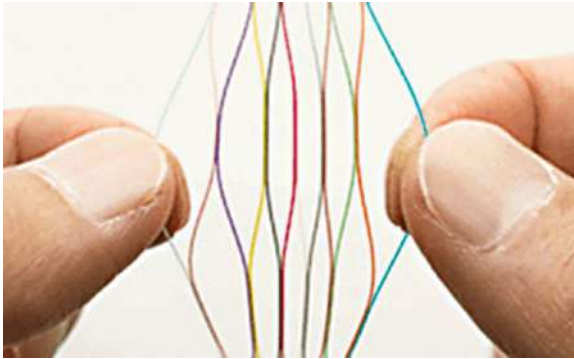
Большое количество волокон в сочетании с компактной конструкцией кабеля особенно важно при организации соединений между ЦОДами (Data Center Interconnect, DCI). Магистральные DCI-кабели с более чем 3000 волокон стали уже типовыми для соединения гиперЦОДов, и операторы планируют удвоить этот показатель в ближайшем будущем. Внутри ЦОДа наиболее высокие требования предъявляются к магистральным кабелям, которые соединяют коммутаторы ядра сети между собой или телекоммуникационные комнаты (meet-me rooms) и коммутаторы spine.

Кабели с большим числом волокон занимают много ценного пространства в кабель-каналах, а их толщина затрудняет обеспечение должной производительности из-за ограничений на минимальный радиус изгиба. Чтобы преодолеть эти проблемы, производители кабелей переходят на рулонные ленточные кабели и волокно диаметром 200 мкм.

Рулонные ленточные волоконно-оптические кабели

Эволюция методов укладки волокон в кабеле позволяет ЦОДам использовать больше волокон, не увеличивая занимаемое кабельной проводкой пространство. Рулонные ленточные волоконно-оптические кабели – одно из последних звеньев в цепочке инноваций.

Конструкция рулонного ленточного кабеля частично основывается на более ранней разработке, ленточном кабеле с центральной трубкой, который был представлен в середине 1990-х гг. и использовался главным образом для внешних сетей. Он содержал ленточные



Источник: журнал ISE

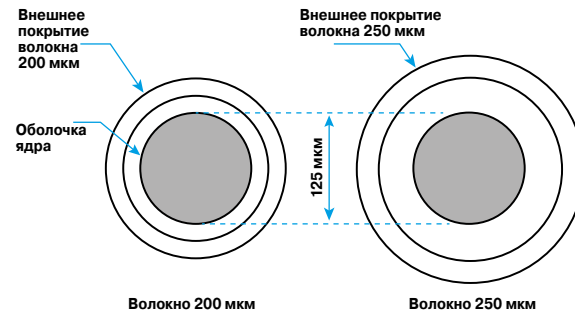
сборки до 864 волокон в одной центральной буферной трубке. В таком кабеле волокна сгруппированы и соединены непрерывно по всей его длине, что увеличивает жесткость конструкции. Это мало влияет на развертывание во внешних сетях, но внутри ЦОДов жесткий кабель нежелателен из-за серьезных ограничений на геометрию прокладки.

В рулонном ленточном кабеле точки скрепления волокон расположены с некоторым промежутком, образуя структуру, напоминающую паутину (рис. 1). Такая структура делает ленту более гибкой, позволяя загружать до 3456 волокон в один двухдюймовый (примерно 5 см) канал, т.е. вдвое плотнее, чем в кабелях с традиционной упаковкой волокон. Это также помогает уменьшить радиус изгиба, что облегчает работу с новыми кабелями в стесненных условиях ЦОДа.

Внутри кабеля прерывисто связанные волокна приобретают физические характеристики свободно уложенных волокон, которые легко изгибаются, что также облегчает прокладку в ограниченном пространстве. Кроме того, в рулонных ленточных кабелях не используется гель, благодаря чему подготовка к сращиванию выполняется быстрее и проще и, следовательно, снижаются трудозатраты. При этом прерывистое скрепление обеспечивает выравнивание волокон, необходимое для сращивания сразу множества волокон в ленте.

Уменьшение диаметра кабеля

В течение десятилетий номинальный диаметр почти всех оптических волокон для систем связи составлял 250 мкм. С ростом спроса на кабели меньшего диаметра ситуация начала меняться. Многие конструкции кабелей практически достигли предела уменьшения диаметра при использовании стандартного волокна. Но волокно меньшего диаметра позволяет дополнительно уменьшить размеры кабеля. В настоящее время в рулонных ленточных кабелях и в кабелях для прокладки в микроканалах применяются волокна диаметром 200 мкм.



Источник: журнал ISE

◀◀ **Рис. 1.**
Точки скрепления волокон в ленточном кабеле расположены с некоторым промежутком

◀ **Рис. 2.** Волокно диаметром 200 мкм имеет ту же сердцевину 125 мкм, что и волокна 250 мкм

Важно подчеркнуть, что единственная часть волокна, которая подверглась изменению, – это буферное покрытие (рис. 2). В волокнах толщиной 200 мкм диаметр сердцевины, как и в обычных волокнах, составляет 125 мкм для сохранения оптических характеристик и совместимости при сращивании. После снятия буферного покрытия процедура сращивания для 200-мкм волокна такая же, как и для его 250-мкм аналога.

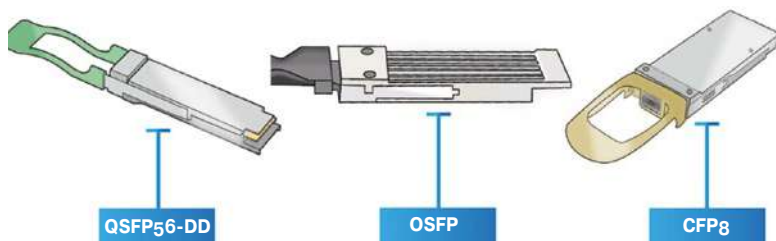
Такие технологические решения, как рулонный ленточный кабель и 200-мкм волокно, активно применяются гиперЦОДа́ми. В ЦОДах, где расстояния между коммутаторами нижнего уровня (leaf) и серверами намного меньше, а плотность соединений – выше, основное внимание уделяется капитальным и эксплуатационным затратам на оптические модули.

Трансиверы и коннекторы для 400G

Многие ЦОДы ориентируются на более дешевые приемопередатчики с лазером VCSEL, которые работают по многомодовым волокнам. Другие выбирают гибридный подход – используют одномодовые волокна на верхних уровнях ячеистой сети, а многомодовые – для подключения серверов к коммутаторам leaf. Сегодня все больше объектов внедряют технологию 400GE, а 50G- и 100G-оптические соединения с серверами становятся нормой, и ЦОДы начинают нуждаться в обоих типах волокна: одномодовом и многомодовом.

Рынок оптических решений для 400G определяется балансом стоимости и производительности. В 2017 г. для модулей 400GE первого поколения, которые предназначались в основном для маршрутизаторов и транспортных клиентских интерфейсов систем спектрального уплотнения DWDM, был выбран форм-фактор CFP8. Размеры модуля CFP8 немного меньше, чем размеры модуля CFP2. В нем используются схемы электрического ввода-вывода CDAUI-16 (16 x 25G NRZ) и CDAUI-8 (8 x 50G PAM4).

Впоследствии модули 400G второго поколения начали изготавливать в форм-факторах QSFP-



Источник: www.prolabs.com

▲ Рис. 3.
Различные варианты трансиверов для 400GE

DD и OSFP (рис. 3). Разработанные для коммутаторов ЦОДов с высокой плотностью портов, эти модули размером с большой палец обеспечивают емкость 12,8 Тбит/с в пространстве 1RU (32 порта 400GE) и поддерживают только схему CDAUI-8.

Модули CFP8, QSFP-DD и OSFP подключаются в «горячем» режиме, но не все модули приемопередатчиков 400GE таковы. Некоторые из них монтируются непосредственно на главной печатной плате, что обеспечивает более высокую плотность портов. Несмотря на это преимущество, индустрия Ethernet продолжает отдавать предпочтение подключаемой оптике для систем 400GE. Такие решения легче обслуживать, и они предоставляют возможность масштабирования по принципу «плати по мере роста».

Для реализации коротких каналов 400G на многомодовом (ММ) волокне имеются различные варианты коннекторов (рис. 4). Стандарт 400GBASE-SR8 позволяет использовать 24-волоконный коннектор MPO (лучше подходит для унаследованных приложений) или однорядный 16-волоконный MPO, который считается наиболее предпочтительным вариантом для подключения серверов, разворачиваемых для облачных платформ. Другой вариант, 400GBASE-SR4.2, предполагает применение однорядного коннектора MPO-12 с двунаправленной сигнализацией, что делает его отличным выбором для соединений между коммутаторами. 400GBASE-SR4.2 – это первый стандарт IEEE, рассчитанный на двунаправленную сигнализацию на ММ-волокнах,

и он предусматривает применение кабелей OM5. Волокно OM5 расширяет многоволновую поддержку для таких приложений, как BiDi, позволяя сетевым архитекторам на 50% увеличивать дальность каналов по сравнению с OM4.

Другие соединители, на которые стоит обратить внимание, – это волоконно-оптические разъемы с очень малым форм-фактором (VSFF) SN и MDC. Они используют технологию 1,25-мм наконечника (ferrule) и могут обеспечивать четыре дуплексных соединения (рис. 5). Однако эти соединители не взаимозаменяемы и конкурируют за то, чтобы стать стандартом VSFF.

Не пропустите 800G

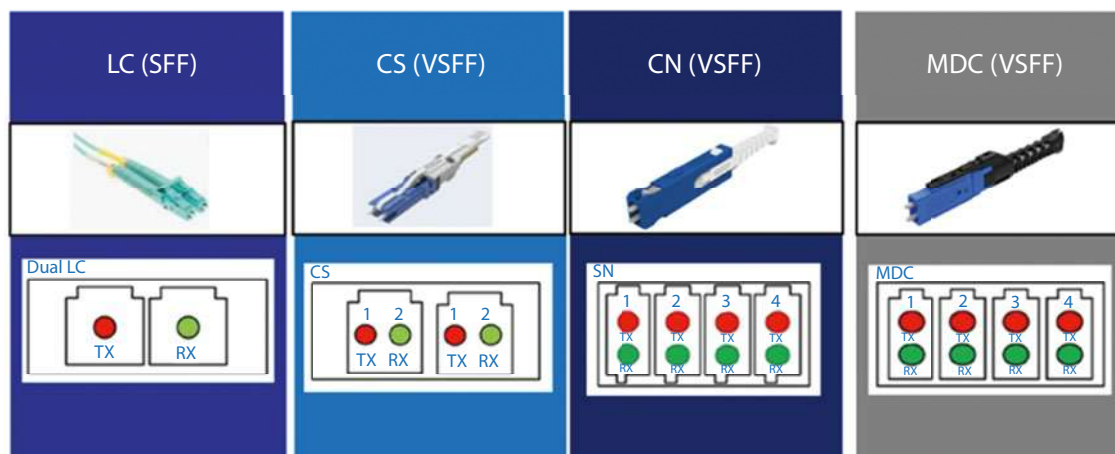
Для любого, кто работает в отрасли ЦОДов более или менее продолжительное время, переход на 400G – еще одна ступень эволюции этих объектов. Эксперты прогнозируют, что оптика 800G станет необходимой уже в течение следующих двух лет. В сентябре 2019 г. была сформирована группа MSA 800G Pluggable для разработки новых решений, в том числе недорогого многомодового модуля 8 x 100G SR8 для пролетов длиной 60–100 м. Цель состоит в том, чтобы вывести на рынок решение 800G SR8, которое обеспечило бы ЦОДы экономически эффективными продуктами для серверных приложений. Подключаемый модуль 800G, помимо прочего, позволит увеличить радиус работы коммутатора.

Тем временем целевая группа IEEE 802.3db работает над недорогими решениями на базе VCSEL-лазеров для передачи 100G на одной длине волны и уже продемонстрировала возможность достичь при такой передаче дальности 100 м на ММ-волокне OM4. В случае успеха эта работа позволит отказаться от подключения серверов в стойке по DAC-кабелям и перейти к архитектуре MoR/EoR с коммутаторами увеличенного радиуса действия. Это обеспечит недорогое оптическое подключение и расширит долгосрочную прикладную поддержку устаревших кабелей с ММ-волокнами.

Рис. 4. Основные оптические коннекторы в сетях ЦОДов

8-волоконные MPO (MPO-8)	12-волоконные MPO (MPO-12)	16-волоконные MPO (MPO-16)	24-волоконные MPO (MPO-24)
Базовая конфигурация QSFP	Большая установочная база	Новый тип	Высокоплотный MPO

Источник: CommScope



◀ **Рис. 5.** Новые типы коннекторов в сетях ЦОДов: с малым и очень малым форм-факторами

Источник: ComptScore

Организации по стандартизации и индустрия тесно взаимодействуют, создавая перспективные решения, которые могут привести ЦОДы к скоростям 400G и 800G. Однако устранение технологических барьеров – это только половина проблемы. Другая – это выбор правильного времени для внедрения. Когда циклы обновления инфраструктурного оборудования составляют два-три года, а новые технологии «поступают» в сеть со все возрастающей скоростью, операторам ЦОДов становится все труднее правильно рассчитать время модернизации. Ошибка же обходится очень дорого.

Хотя детали перехода на все более высокие скорости часто обескураживают, их обсуждение помогает представить процесс в перспективе. Чтобы поддерживать более высокие скорости, требуются подходящие среды передачи. При выборе оптических модулей, которые наилучшим образом отвечают потребностям вашей сети, начните с конца. Чем точнее вы сможете предвидеть необходимые сервисы и сетевую топологию, необходимую для их предоставления, тем лучше сможете подготовить сеть для поддержки будущих приложений.

А что между ЦОДами?

Региональные кластеры ЦОДов создаются все чаще, и высокопроизводительные и недорогие DCI-соединения становятся все более актуальными. Появляются новые стандарты IEEE, которые описывают множество более дешевых вариантов, реализующих принцип plug-and-play для соединений «точка – точка».

Трансиверы, основанные на традиционной четырехуровневой амплитудно-импульсной модуляции (PAM4) для прямого детектирования, способны поддерживать связь до 40 км, обеспечивая непосредственную совместимость с недавно представленными коммутаторами 400G. Но имеются и другие разработки, которые предоставляют аналогичную функциональность при использовании традиционных транспортных DWDM-каналов.

Там, где требуется дальность 40–80 км и более, когерентные системы с расширенной поддержкой «дальнобойной» оптики, скорее всего, захватят большую часть соответствующего рынка высокоскоростной связи.

Когерентная оптика преодолевает ограничения, связанные с хроматической и поляризационной дисперсиями, что делает ее идеальным выбором для более протяженных линий связи. Такие решения традиционно были сильно кастомизированы (и дороги), требуя специальных «модемов» в отличие от оптических модулей plug-and-play.

По мере развития технологий когерентные решения, вероятно, станут более компактными и менее дорогими. В конце концов относительная разница в стоимости может уменьшиться до такой степени, что выгода от применения этой технологии будет ощущаться и для более коротких каналов связи.

Целостный подход к внедрению более высоких скоростей

Переход к более высоким скоростям в ЦОДе происходит поэтапно. По мере развития приложений и сервисов скорость работы систем хранения и серверов также должна увеличиваться. Шаблонный подход к выполнению периодически повторяющихся обновлений поможет сократить время и затраты, необходимые для планирования и реализации изменений. Мы рекомендуем целостный подход, при котором коммутаторы, оптика и волоконные кабели работают как единая скоординированная инфраструктура передачи данных.

В конечном счете то, как все эти компоненты будут работать вместе, определит способность сети надежно и эффективно поддерживать новые приложения. Сегодняшняя задача – внедрение 400G, завтрашняя – 800G или даже 1,6T. Однако фундаментальные требования к высококачественной волоконно-оптической инфраструктуре неизменны, несмотря на изменение сетевых технологий. ИКС

Schneider Electric: перестройка и ускорение

О глобальной индустрии ЦОДов и ее российской специфике, а также о том, как чувствует себя премиальный производитель в условиях усиления конкуренции на рынке, рассказывает Тимур Алтышев, директор по работе со стратегическими заказчиками компании Schneider Electric.



– Тимур, какова структура мировой отрасли ЦОДов? Каковы приоритеты ее развития?

– Объем мировой отрасли дата-центров вышел на головокружительный уровень: это почти 46 млн кв. м совокупной площади (примерно 6,4 тыс. футбольных полей) и энергопотребление около 60 ГВт. Отрасль составляют три основных сегмента: ЦОДы интернет-гигантов (Microsoft, Facebook, Amazon, Alibaba и т.д.), поставщиков услуг colocation (Equinix, Interxion, Digital Realty, Colt и т.д.) и телеком-провайдеров (NTT, Vodafone, China Telecom и т.д.). Все три сегмента растут очень активно. При этом операторы colocation нередко строят дата-центры в соответствии с требованиями конкретных интернет-гигантов по модели build-to-suite, да и в целом около 80% дата-центров colocation закупаются интернет-гигантами.

Консолидация ЦОДов в руках крупных корпораций – около 15 компаний владеют более чем 70% объектов – определяет и основные приоритеты развития, такие как экологичность (масштаб участников рынка побуждает регуляторов предъявлять к ним довольно жесткие требования, и соблюдение этих требований является критичной частью бизнеса уже сегодня), эффективность, скорость вывода объектов на рынок, адаптивность и отказоустойчивость. Кроме того, стандартизация, цифровизация, энергоэффективность – все, что позволяет сделать эксплуатацию ЦОДа максимально простой и эффективной, а строительство – максимально быстрым.

Конечно, структура и приоритеты российского рынка пока значительно отличаются от вышеназванных мировых, но мы видим, что отечественные игроки рынка ЦОДов также ориентируются на эти приоритеты. Schneider Electric на глобальном уровне успешно работает во всех трех сегментах отрасли, и это помогает нам внедрять лучшие мировые практики в отечественных дата-центрах.

– Наблюдаете ли вы снижение интереса корпоративных заказчиков к созданию собственных ЦОДов и их уход в коммерческие дата-центры?

– Да, конечно, как в мире, так и в России эта тенденция очевидна. В большинстве своем профессиональные игроки рынка ЦОДов способны предложить корпоративным заказчикам более быстрое и эффективное решение, чем строительство собственного корпоративного дата-центра. Но и в России, и в мире по-прежнему есть крупные корпоративные заказчики (банки, госструктуры и т.д.), которые предпочитают строить большие ЦОДы собственными силами и умеют это делать достаточно эффективно.

Также мы видим, что корпоративные заказчики, даже переезжая в коммерческий дата-центр, стремятся выбрать инфраструктуру, аналогичную собственной как по составу производителей, так и по топологии и другим особенностям построения. А поскольку Schneider Electric широко представлена и в корпоративных, и в коммерческих ЦОДах, то с помощью наших решений мы предоставляем корпоративным заказчикам возможность использовать унифицированную инфраструктуру в собственных и арендуемых дата-центрах.

– В Москве места в коммерческих ЦОДах раскупаются еще до ввода объектов в эксплуатацию. Поэтому все хотят строить как можно быстрее. Какие организационные и технологические инструменты предлагает Schneider Electric для сокращения сроков реализации проектов?

– Действительно, сегодня скорость выхода на рынок – важнейший фактор успеха. И в этом мы готовы максимально содействовать нашим заказчикам – и при строительстве объекта, и при заполнении существующего дата-центра пользователями. В нашем арсенале есть гибкие условия финансирования, средства раннего планирования производства, европейские и российские складские возможности. На этапе планирования и проектирования ЦОДа наши технические специалисты помогают в поиске оптимального решения, что позволяет сократить сроки внедрения без потерь в эффективности объекта. Цифровые инструменты Schneider Electric, которые приме-

няются при планировании ЦОДа, построены на одной платформе с системой мониторинга и управления инженерной инфраструктурой – это упрощает запуск ЦОДа и выстраивание процессов эксплуатации. Еще один момент, немаловажный для скорости внедрения, – комплексность решения. В наших системах многие вопросы взаимной интеграции элементов проработаны на этапе создания продукта, и нет необходимости тратить на это дополнительное время и силы в процессе создания ЦОДа.

– Не снизит ли столь высокий спрос на услуги ЦОДов требования к уровню технических решений? Скажем, когда площади ЦОДа быстро утилизируются, становятся ненужными системы с модульной архитектурой (для постепенного наращивания ресурсов) и т.д.

– Думаю, большинство участников рынка понимают, что текущий дефицит стойко-мест не обязательно сохранится через два года, а значит, новые объекты надо планировать максимально гибко. Практически во всех проектах, в которых мы сейчас участвуем, присутствует этапность и соответствующая дробность наращивания инженерной инфраструктуры. При этом модульная архитектура, например ИБП, на крупных коммерческих площадках применяется не столько для масштабирования, сколько для более простой и экономически выгодной эксплуатации. В наших новых ИБП Galaxy VL заменить или добавить силовые модули быстро, а главное, безопасно служба эксплуатации может самостоятельно. С другой стороны, дата-центр – это объект критической инфраструктуры, поэтому при любом уровне спроса на его услуги надежность ЦОДа, которая определяется в том числе надежностью применяемых компонентов, – один из основных факторов успешного внедрения. Другими словами, при снижении требований к уровню технических решений слишком высок риск оказаться вне рынка.

– В России растет не только число ЦОДов, но и их размеры. Насколько технические решения для мегаЦОДов отличаются от решений для «обычных» объектов?

– Исходя из того, что заложено в концепции развития, большинство планируемых сегодня в Москве проектов можно отнести к мегаЦОДам, но станут ли они таковыми, будет зависеть от реалий рынка. Ведь строиться они будут этапами. Тем не менее мы наблюдаем как минимум одну особенность мегаЦОДов – им чаще требуются индивидуально адаптированные решения, которые в силу большого масштаба проекта дадут ощутимый эффект. Для нас привычна ситуация, когда мы вместе с заказчиком адаптируем наши продукты, чтобы получить оптимальное решение с учетом особенностей конкретного объекта. У нас уже есть опыт подобного коинжиниринга с российскими заказчиками в системах охлаждения, мониторинга и решениях для размещения серверного оборудования. Отмечу, что благодаря большой и опытной команде технических специалистов Schneider Electric в России подобные изменения практически не отражаются на сроках проектирования и внедрения.

– Мы наблюдаем активизацию строительства ЦОДов в регионах. Какова специфика решений для региональных проектов, особенно с учетом дефицита квалифицированных специалистов?

– Действительно, опытных специалистов в регионах найти достаточно сложно. Мы предлагаем разные варианты решения кадровой проблемы. Первый – максимально упростить эксплуатацию. Этого можно добиться за счет применения модульных архитектур с обслуживанием на уровне модулей, за счет простых цифровых решений для управления инфраструктурой и подключения всех систем к этой единой системе управления. Второй вариант – привлекать к эксплуатации ЦОДа специалистов производителя, т.е. по сути выводить часть службы эксплуатации на аутсорсинг и оставлять на объекте только оперативное управление. Охват территории страны нашей сервисной сетью позволяет это осуществить, и в некоторых региональных корпоративных ЦОДах подобную практику мы уже внедрили.

Вторая особенность развития ЦОДов в регионах – малоизученный спрос. Решением этой проблемы регионально-го развития отрасли мы считаем концепцию модульных и быстровозводимых ЦОДов, что в принципе подтверждают проекты, реализуемые рядом участников рынка. Такой подход позволяет быстрее выходить на рынок, масштабировать или адаптировать инфраструктуру к требованиям региональных заказчиков. У нас есть соответствующие предложения, как собственные, так и разработанные в партнерстве с российскими компаниями.

– Как меняются цели и позиции Schneider Electric на российском рынке инженерной инфраструктуры для ЦОДов?

– Думаю, ни для кого не секрет, что за последние несколько лет конкуренция на рынке инженерных систем, как и на ИТ-рынке, в силу экономических причин существенно ужесточилась. Это не могло не сказаться на доле рынка премиального производителя, и потребовалось определенное время на перестройку продуктового предложения, ценообразования и политики обслуживания, для того чтобы соответствовать реалиям российского рынка.

Так получилось, что именно в 2021 г. практически одновременно произошли прорывные положительные изменения по ряду и технологических, и бизнес-направлений. Schneider Electric представила новые суперинновационные, эффективные и оптимальные по цене ИБП Galaxy VL, расширила портфель решений литий-ионных аккумуляторов. В России и странах СНГ стали доступны экономически эффективные решения для инфраструктуры машзала – линейки Easy Row, Easy Rack и Easy PDU. Сервисная политика стала более гибкой, появились более гибкие схемы финансирования и многое другое. Это позволяет нам ожидать увеличения доли компании на рынке ЦОДов. Сегодня мы можем удовлетворить практически любые требования заказчиков и готовы вместе с ними дальше развивать и двигать вперед отрасль дата-центров в России.



«Инженерка»-2021: это сладкое слово «эффективность»

Александр Барсков,
Николай Носов

В ЦОДе все должно быть эффективно: и концепция, и кабельная инфраструктура, и охлаждение, и система пожаротушения.

Организованная «ИКС-Медиа» конференция Data Center Design & Engineering (DCDE-2021) по традиции стала площадкой для обсуждения всего комплекса вопросов, связанных с проектированием, строительством, оборудованием и эксплуатацией ЦОДа.

Что такое хорошая концепция?

Любой проект ЦОДа начинается с разработки концепции. Этот этап, являющийся частью стадии планирования (рис. 1), очень важен, ошибки на нем могут серьезно увеличить стоимость и сроки реализации проекта или даже сделать его невыполнимым. Несмотря на наличие общепринятых практик и типовых решений, двух одинаковых ЦОДов не найти. «Даже при одинаковых исходных данных 10 компаний предложат вам 10 разных концепций ЦОДа», – обрисовал ситуацию Андрей Воробьев, директор центра разработки приложений ЦОД подразделения Secure Power компании Schneider Electric.

Эксперт Schneider Electric проанализировал некоторые заблуждения, встречающиеся у заказчиков в отношении разработки концепции ЦОДа. «В условиях, когда требования постоянно меняются, заказчики часто просят сделать что-нибудь универсальное. Но чем более универ-

сальна концепция, тем менее эффективным получается конечный результат», – предостерег он.

Нередко заказчики действуют по принципу: чем больше концепций, тем лучше. Они заказывают пять, шесть или даже больше концепций у разных разработчиков, а потом выбирают, как им кажется, оптимальную, используя, в частности, CFD-моделирование (для проверки эффективности системы охлаждения). Но множество концепций не гарантирует получения оптимального результата. Гораздо важнее максимально точно сформулировать начальные данные и конечные цели.

Заблуждаются и те заказчики, которые считают возможным создать хорошую концепцию без поддержки производителей оборудования – «сначала нарисую, а потом пойдем смотреть, что есть на рынке». «Даже если вы построили 10 ЦОДов и строите 11-й, не факт, что оборудование, которое вы использовали год назад, еще есть на рынке. Технологии быстро меняются, и прошлый опыт уже не годится», – отметил А. Воробьев.

Наконец, ошибочно мнение, что использование существующего здания снизит затраты на ЦОД. Если есть возможность, лучше начинать с чистого листа, строить здание специально для ЦОДа. Это будет дешевле и обеспечит более эффективное решение.

При разработке концепции важно грамотно выбрать «квантование» нагрузки – определить оптимальные мощность и число стоек для одного зала, а также топологию систем электро- и холодоснабжения, исходя из конфигурации подведенной мощности, ограничений здания и выбранных моделей основного оборудования. Здесь надо просчитать всю цепочку систем – то, что в Schneider Electric называют power train. Это позволит «не попасть», например, на необходимость обеспечивать работу на высоком токе или устанавливать специальные дорогие системы ИБП сверхвысокой мощности (свыше 5 МВт), что приведет к радикальному увеличению цены.

Также важно еще в концепции учесть, как в дальнейшем ЦОД будет эксплуатироваться.

Рис. 1. Жизненный цикл ЦОДа ►



Источник:
Schneider Electric

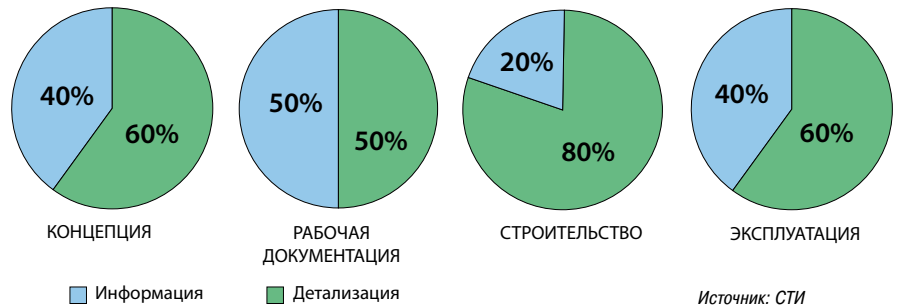
В том числе рассмотреть вопросы автоматизации, актуальность которых повысила пандемия, наглядно показавшая важность «человеческого фактора» в обеспечении доступности ЦОДа. Потребность в повышении уровня автоматизации ЦОДов обусловлена и нехваткой квалифицированных кадров, и стремлением сократить операционные расходы. По мнению А. Воробьева, для всех новых площадок пришло время рассматривать возможность комплексной автоматизации, а для существующих объектов – выборочного внедрения соответствующих технологий. Он считает, что сегодня средства автоматизации наиболее востребованы корпоративными дата-центрами и edge-ЦОДами.

Без BIM'а ЦОДа нет

Индустрию ЦОДов трудно представить без современных цифровых инструментов. Один из ключевых – технология информационного моделирования (BIM), важность которой на конференции DCDE-2021 отмечали многие эксперты. Технический директор компании «Свободные Технологии Инжиниринг» Евгений Колосков был категоричен: «Проектировать и строить ЦОДы сегодня без BIM нельзя!» Он подчеркнул, что ЦОД – это объект, насыщенный дорогостоящими инженерными системами, причем на всех этапах его жизненного цикла, включая проектирование и строительство, решения нужно принимать быстро.

При проектировании необходимо рассматривать различные компоновочные и архитектурные решения, чтобы «выжать максимум из имеющейся площадки». Использование BIM позволяет выбрать оптимальные варианты, а также на ранних стадиях разработки проектной документации выявить и устранить ошибки (рис. 2). Как указал эксперт СТИ, это особенно важно для объектов Tier IV, где надо соблюдать принцип секционирования.

По данным СТИ, крупные госкорпорации применяют BIM уже в 100% проектов, однако коммерческие заказчики – только в каждом пятом. Е. Колосков напомнил о том, что в марте 2021 г. премьер-министр Михаил Мишустин подписал указ, согласно которому с 1 января 2022 г. все объекты капитального строительства, возводимые с привлечением бюджетных средств, обязаны иметь информационные модели. А в июне Президент РФ Владимир Путин поручил до 1 июля текущего года подготовить дорожную карту использования технологий информационного моделирования при проектировании и строительстве объектов капитального строительства.



Понятно, что от BIM не уйти. «Рынок диктует такие условия, что иногда технологическое обеспечение и квалификация компании являются большим конкурентным преимуществом, нежели многолетний опыт и десятки успешных проектов. Внедрение цифровых технологий в процесс проектирования и строительства перестает быть прихотью заказчика и становится обязательным требованием для крупных проектов», – подытожил Е. Колосков.

СКС «на вырост»

Кабельную систему одни эксперты относят к инженерной инфраструктуре, другие – к ИТ. Но вне зависимости от нюансов классификации СКС – это ключевой элемент ЦОДа, значимость которого только растет по мере увеличения объема хранимых данных и повышения требуемой скорости их обработки.

Кабельная система в ЦОДе живет существенно дольше, чем сетевое оборудование. При этом сетевая индустрия активно меняет способы повышения пропускной способности и подходы к построению сетей. И СКС должна «уметь» адаптироваться к изменяющимся требованиям.

Когда в 2002 г. появилась технология 10G Ethernet, сценарий дальнейшего развития высокоскоростных технологий казался понятным. Как напомнил Степан Большаков, ведущий менеджер по работе с клиентами компании CommScore, оборудование 10GE работало по дуплексному протоколу (используется одна пара волокон), при этом предполагалось, что для достижения более высоких скоростей (40G, 100G) будет применяться параллельная передача с увеличением числа волокон. Но затем, когда передовые заказчики начали внедрять 40GE по параллельным протоколам, Cisco предложила дуплексный вариант 40GE, а потом и 100GE. Теперь для одних и тех же скоростей задействуются как дуплексные, так и параллельные протоколы, а клиенты, которые уже реализовали параллельные системы, стали внедрять дуплекс при переходе на более высокие скорости.

Сегодня разработанные институтом IEEE протоколы используют три метода повышения пропускной способности: увеличение скорости по-

▲ Рис. 2. Соотношение значимости уровней детализации геометрии и обработки информации на разных этапах жизненного цикла объекта

тока, числа физических волокон и числа спектральных каналов (рис. 3). В результате за время жизни объекта заказчики вынуждены переходить от параллельных оптических протоколов к дуплексным оптическим протоколам и обратно.

Меняются и подходы к топологии сети. Сейчас часто наблюдается переход от схем EoR/MoR (коммутатор в конце/середине ряда стоек) к более распределенной схеме ToR (коммутатор в каждой стойке). Но в архитектуре ToR объединение большого числа коммутаторов в mesh-сеть часто становится проблемой, считает С. Большаков, поэтому при увеличении производительности отдельных коммутаторов очень вероятен обратный переход к централизованной топологии. Это позволит уменьшить число коммутаторов, энергопотребление и, что самое важное, задержку при передаче трафика. Получается, что за время жизни площадки происходит миграция от схемы с высоким уровнем централизации к распределенной и обратно.

Еще больше запутывает дело наличие сразу нескольких типов многоволоконных MPO-интерфейсов с различным числом волокон – MPO-8, MPO-12, MPO-16, MPO-24, – а также появление новых соединителей класса VSFF с че-

тырьмя (CS) и восьмью волокнами (SN, MDCZ). Вариантов множество, и надо сделать выбор так, чтобы кабельная система поддерживала несколько стадий миграции на более скоростные технологии.

Что здесь можно порекомендовать? «Строить ЦОД на сварной оптике – плохая идея», – заявил С. Большаков. Лучше использовать претерминированные решения, причем со сверхнизким затуханием. «Чем меньше затухание, тем больше вероятность того, что кабельная инфраструктура выдержит следующий этап миграции», – продолжил он. Кроме того, эксперт CommScore советует применять оптические компоненты с полярностью типа В – они универсальны, что упрощает работу службы эксплуатации.

В условиях частых изменений важно, но очень не просто поддерживать в актуальном состоянии документацию, включая кабельный журнал. Для этого С. Большаков рекомендовал использовать системы управления инфраструктурой класса AIM. По его мнению, функционал систем DCIM часто избыточен, а вот AIM решают все основные задачи. В числе особенностей AIM-системы CommScore (imVision) он назвал корректное документирование соединений «один

Рис. 3. Варианты реализации высокоскоростных оптических линий связи ►

Скорость	Уровень PMD	Среда передачи	Дальность	Кол-во волокон	Кол-во длин волн	Скорость одного потока	Стандарт IEEE
25G	SR	1-парный MM	100 м	2	1	25G	802.3by (2016)
40G	SR4	4-парный MM	150 м	8	1	10G	802.3ba (2010)
	FR	1-парный SM	2 км	2	1	40G	802.3bg (2011)
	LR4	1-парный SM	10 км	2	4	10G	802.3ba (2010)
	ER4	1-парный SM	40 км	2	4	10G	802.3bm (2015)
50G	SR	1-парный MM	100 м	2	1	50G	802.3cd (2018)
	FR	1-парный SM	2 км	2	1	50G	802.3cd (2018)
	LR	1-парный SM	10 км	2	1	50G	802.3cd (2018)
100G	SR2	2-парный MM	100 м	4	1	50G	802.3cd (2018)
	SR4	4-парный MM	100 м	8	1	25G	802.3bm (2015)
	SR10	10-парный MM	150 м	20	1	10G	802.3ba (2010)
	DR	1-парный SM	500 м	2	1	100G	802.3cd (2018)
	LR4	1-парный SM	10 км	2	4	25G	802.3ba (2010)
	ER4	1-парный SM	40 км	2	4	25G	802.3ba (2010)
200G	SR1.4	1-парный MM	100 м	2	4	50G	MSA?
	SR4	4-парный MM	100 м	8	1	50G	802.3cd (2018)
	DR4	4-парный SM	500 м	8	1	50G	802.3bs (2017)
	FR4	1-парный SM	2 км	2	4	50G	802.3bs (2017)
	LR4	1-парный SM	10 км	2	4	50G	802.3bs (2017)
400G	SR4.2	4-парный MMF	100 м	8	2	50G	802.3cm (2019)
	SR8	8-парный MMF	100 м	16	1	50G	802.3cm (2019)
	SR16	16-парный MM	100 м	32	1	25G	802.3bs (2017)
	DR4	4-парный SM	500 м	8	1	100G	802.3bs (2017)
	FR8	1-парный SM	2 км	2	8	50G	802.3bs (2017)
	LR8	1-парный SM	10 км	2	8	50G	802.3bs (2017)

Источник:
CommScore

ко многим» (что не позволяют делать традиционные таблицы типа Excel), а также наличие, помимо всех функций автоматизированного управления кабельной инфраструктурой, базовых функций управления емкостью. С их помощью можно оценить доступность ресурсов, наличие места и электрической мощности для подключения нового оборудования.

Безопасное пожаротушение

Широко обсуждаемое событие весны этого года – повлиявший на работу веб-сайтов по всему миру пожар в ЦОДе OVHcloud (Страсбург, Франция). Инцидент еще раз продемонстрировал, что большинство организаций не имеют плана восстановления работоспособности бизнеса в случае пожара, а надеются на надежность ЦОДа, в том числе его средств пожаротушения.

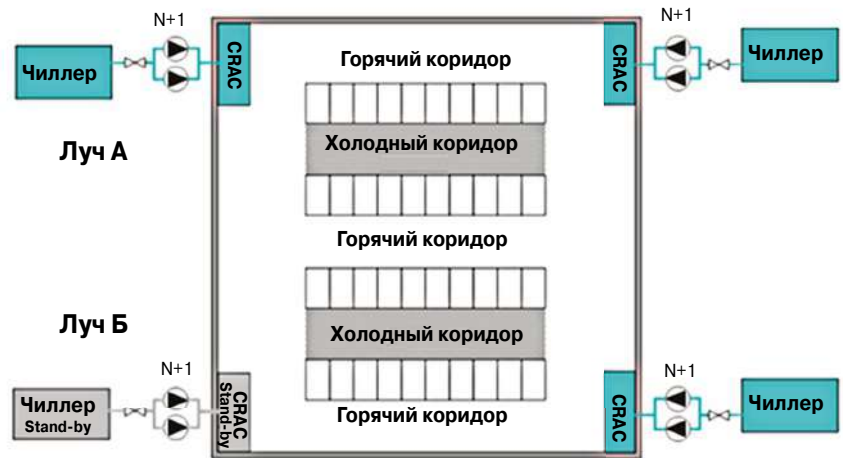
При срабатывании часто применяемых газовых систем пожаротушения дорогой газ заполняет весь машзал. По мнению генерального директора компании Marioff Олега Зуенко, в ЦОДах экономически эффективнее и безопаснее использовать установки пожаротушения тонкораспыленной водой. Когда вода превращается в пар, она поглощает больше тепла, чем любое другое огнетушащее вещество. Эффективность такой системы пожаротушения не зависит от герметичности помещения, а при ее работе функционирование большей части машзала не прерывается. Вода применяется локально, и восстановление работы дата-центра сводится к замене сгоревшего оборудования. Да и по сравнению с хладоном и другими используемыми при пожаротушении газами вода практически бесплатна.

Именно такова разработанная компанией Marioff система пожаротушения HI-FOG. В числе защищенных ею ЦОДов – объекты компании Ericsson в Нидерландах, Комиссариата по ядерной энергии (CEA) во Франции, KIO Networks в Испании, дата-центр IXcellerate в России.

Климатические системы – от сложного к простому

«Последние пару лет мы видим запрос рынка на упрощение климатических систем. Заказчики хотят, чтобы системы были простыми, компактными и, что немаловажно, более понятными в эксплуатации», – констатировал Максим Орехов, технический эксперт Vertiv. Один из вариантов, предлагаемых этой компанией, – связка внутреннего фанкойла и уличного чиллера, по сути, жидкостная сплит-система (рис. 4).

В этом решении применяются небольшие чиллеры со спиральными компрессорами. Такой чиллер в расчете на киловатт холода суще-



Источник: Vertiv

ственно дешевле больших систем, а невысокая мощность (120–150 кВт) подразумевает более простую и дешевую обвязку (трубы, кабели, арматура, баки и т.д.). Небольшие вес и габариты упрощают доставку оборудования и его монтаж. Эксперт Vertiv также указал на малый шаг наращивания мощности, который позволяет легко адаптировать ЦОД к неполной загрузке. Наконец, при использовании подобных решений проще обеспечить отсутствие единой точки отказа, что важно, например, для набирающих популярность ЦОДов Tier IV.

Как сообщил представитель Vertiv, заказчики оценили столь компактные и эффективные системы охлаждения: в России их установлено уже более 100, а это порядка 15 МВт. Решения на сотни мегаватт находятся в стадии проектирования.

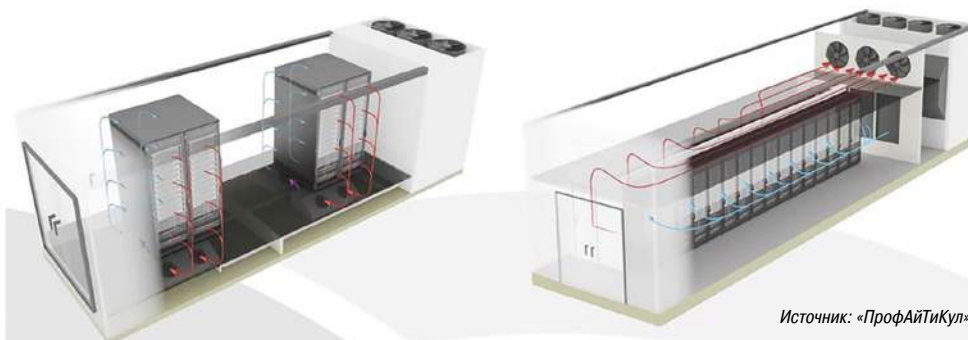
По данным Vertiv, более половины заказчиков рассматривают решения, которым не нужен фальшпол. Это могут быть, например, интегрированные в здания или устанавливаемые в сервисные коридоры решения типа «холодная стена». В качестве альтернативы «стенам» Vertiv предлагает Mega CRAN – периметральный блок на охлажденной воде. Забирает воздух такая система сверху, а раздача может производиться как вперед, так и назад. Соответственно обслуживать ее можно из машзала или из сервисного коридора. Как отметил М. Орехов, машина сочетает преимущества классических кондиционеров и «холодных стен» и по своим характеристикам находится посередине между ними.

Дашь ВОПы!

Несмотря на доминирование в ЦОДах прецизионных кондиционеров, все больше заказчиков интересуются относительно новым (для ЦОДов) классом оборудования: воздухоохлаждающими приборами (ВОПами), которые чаще всего выполняются в виде уже упомянутых «холодных стен».

«До недавнего времени порядка 95% проектов в ЦОДах делались на прецизионных кондицио-

▲ Рис. 4. Система охлаждения на основе связки внутреннего фанкойла (CRAC) и небольшого уличного чиллера



Источник: «ПрофАйТиКул»

▲ Рис. 5.
Использование
ВОПов
в контейнерных
ЦОДах

нерах. И все было бы замечательно, если бы не высоконагруженные стойки, – заметила Александра Эрлих, сеньор-консультант ГК Sabero и генеральный директор компании «ПрофАйТиКул». – В таких проектах на две-три высоконагруженные стойки приходится один межрядный прецизионный кондиционер. Кондиционеры занимают в машзале много места, что дорого и неэффективно. ЦОДам же хочется стоек побольше, расходов поменьше, процедуры эксплуатации попроще. Поэтому они и обратили внимание на ВОПы».

ВОПы сохраняют место в машзале для ИТ-стоек, не требуют ни фальшпола, ни фальшпотолка, зоны их обслуживания располагаются со стороны технических коридоров (по крайней мере в решениях Sabero). ВОП позволяет реализовать принцип низкоскоростного воздухораспределения в сочетании с большой площадью теплообмена. Именно большая площадь обеспечивает низкое сопротивление воздушному потоку в теплообменнике, что дает возможность использовать недорогие вентиляторы с низким энергопотреблением. В результате удастся сэкономить как на стоимости вентиляторов, так и на расходах на электричество. Низкое сопротивление жидкости (максимум 1 бар против 2–2,5 бар в случае прецизионных кондиционеров) означает малые затраты на энергопотребление насосов, а высокий температурный график – увеличение времени работы в режиме фрикулинга. Наконец, низкая скорость движения воздуха обеспечивает его равномерное распределение по машзалу, отсутствие зон турбулентности, формирование единого холодного бассейна, из которого каждая стойка забирает столько холода, сколько ей нужно.

Преимущества ВОПов, по мнению А. Эрлих, настолько очевидны, что приведут к постепенному отказу от традиционных прецизионных кондиционеров в ЦОДах в пользу этого класса систем охлаждения. Причем такие системы охлаждения эффективны в ЦОДах различного типа, включая контейнерные (рис. 5).

Компактный фреон

Но традиционные фреоновые системы не сдаются. Низкие первоначальные затраты делают

их привлекательными для многих заказчиков. Как отметил Александр Ежов, менеджер по продукции «Системы контроля климата» компании Rittal, фреоновые решения обычно используют, когда опасаются протечек систем на основе охлажденной воды, а также когда нужно снизить стоимость решения –

в первую очередь в небольших ЦОДах.

Компания Rittal, выпускающая промышленные кондиционеры с 1988 г., сегодня имеет в своем арсенале весь спектр систем охлаждения (как своей разработки, так и полученных благодаря сотрудничеству с Stulz). Но на DCDE-2021 она акцентировала внимание специалистов именно на своих внутрирядных фреоновых кондиционерах. Модель LCP DX шириной 300 мм может обеспечить холодильную мощность до 25 кВт, что позволяет «снять» со стойки до 23 кВт тепла – очень высокий показатель. Для ряда российских регионов может оказаться важным наличие этого кондиционера в специальном исполнении (разработано совместно с Stulz) для эксплуатации при температурах наружного воздуха до -60°C . Кроме того, производитель может поставлять такие кондиционеры для серверных стоек разной высоты, в том числе 47U и 52U.

Непрерывное охлаждение

Энергоемкие компоненты систем охлаждения обычно не подключают к ИБП, только к системе гарантированного электроснабжения (ДГУ). А после сбоя питания необходимо как можно скорее обеспечить охлаждение. Представленный на конференции продакт-менеджером Mitsubishi Electric Сепреем Новиковым новый высокотемпературный чиллер NR-FC-Z запускается не более чем за 20 с и выходит на 100%-ную холодопроизводительность в пределах 72 с после восстановления подачи электроэнергии.

Для повышения надежности оборудованное автоматическим переключателем (ATS) устройство может быть подключено к двум отдельным линиям электропередачи. В случае отключения электроэнергии в основной линии ATS автоматически переключается на резервную, обеспечивая бесперебойное питание устройства. Благодаря задублированному источнику питания чиллер NR-FC-Z подходит для проектных топологий Uptime Institute Tier IV и может быть использован для критически важных систем.

Российский холод

Отрадно отметить, что на рынке присутствуют системы охлаждения, полностью разработанные

ные российскими компаниями – от «железа» до программного обеспечения. Например, компания BOREY изготавливает работающие на воде рядные кондиционеры ВРК-30 и ВРК-60 для охлаждения средних и крупных ЦОДов. Свои системы она комплектует контроллерами также собственного производства.

На DCDE-2021 компания BOREY презентовала свой мини-ЦОД, оборудованный системой прецизионного кондиционирования с фрикулингом, что позволяет отводить от 3 (модель BMD-3) до 10 кВт (BMD-10) тепла, выделяемого ИТ-оборудованием. Особенность – охлаждение реализовано на воде. Мини-ЦОД представляет собой герметичный шкаф, в котором отсутствуют дополнительные вентиляторы – работают только вентиляторы серверов, которые гонят воздух по замкнутому контуру, передавая тепло теплообменнику. «Аналогов в России и в мире нет. Мы подали патент на безвентиляторный принцип охлаждения в Европе и ждем его одобрения», – сообщил Ратмир Трошин, акционер BOREY.

Когда ЦОДы становятся большими

Увеличение масштабов ЦОДов приводит к увеличению номиналов систем бесперебойного питания. Так, по данным Vertiv, если раньше средняя мощность системы составляла 200–400 кВт, то за последние два года более 60% инсталляций приходится на системы номиналом 500 кВА и более. В числе тенденций в области систем бесперебойного питания М. Орехов назвал повышение плотности мощности систем (как следствие – сокращение занимаемой площади) и возможность работы при более высоких температурах (40°C и выше) без снижения эксплуатационных характеристик.

Ведущие вендоры представили на DCDE-2021 новинки, ориентированные именно на объекты большой мощности. Так, компания ABB впервые в России показала новые ИБП MegaFlex DPA. Это интеллектуальное модульное масштабируемое решение с пеналом на 1500 кВт. Единичный модуль имеет мощность 250 кВт. «На глобальный рынок новинку вывели в конце прошлого года. В прошлом году была одна инсталляция, а за четыре месяца текущего года в Европе этими системами оборудовано 12 площадок с общей установленной мощностью около 20 МВт», – рассказал менеджер по развитию бизнеса ABB Евгений Вецпер.

По утверждению эксперта, решение обеспечивает лучшую на рынке эффективность в режиме двойного преобразования с КПД 97,4%. На 30% снижено выделение тепла. По сравнению с предыдущими решениями компании удалось уменьшить занимаемую площадь на 45%. До 15 лет увеличен проектный срок службы (при соблюдении условий эксплуатации). В течение этого времени через семь лет производится всего одна замена вентиляторов и силовых конденсаторов. Причем для замены вентиляторов достаточно отвинтить два винта, вытащить кассету с вентиляторами и поставить новую. Легко заменяются и конденсаторы.



Vindur CoolWall® – Система «холодная стена» для охлаждения дата-центров



Реклама

- 1 Напольные вентиляторы с большими рабочими колесами и свободным потоком воздуха. Экономия электроэнергии.
- 2 Равномерно охлажденный поток воздуха благодаря конструкции теплообменника. Эффективное охлаждение.
- 3 Снижение энергопотерь за счёт отсутствия турбулентности.
- 4 Поверхность охлаждения от пола до потолка. На 40% выше мощность охлаждения, чем у обычных кондиционеров.

Представительство в России:
ООО «Вайсс Климатехник»
+7 495 787 20 43
weiss.ru@weiss-technik.com

На крупные ЦОДы ориентированы и динамические ИБП, представленные на DCDE-2021 купленной Rolls-Royce компанией MTU. Такие ИБП в отличие от решений на основе аккумуляторных батарей не нуждаются в мощных системах кондиционирования. «Требования к охлаждению минимальные, решения могут работать и при температуре 50–60°C. Для кондиционирования достаточно простой вентиляции», – пояснил Игорь Гегеня, менеджер по продажам дизельного и газового оборудования MTU РУС. По его словам, решения MTU характеризуются низкой стоимостью эксплуатации и сроком службы до 20 лет. Уменьшить занимаемую источниками бесперебойного питания площадь можно, полностью вынеся их из дата-центра. Например, расположив в контейнерах, как это и предлагает делать компания MTU.

Внимание – АКБ!

Очевидна и тенденция к все более активному применению в ЦОДах литий-ионных АКБ. Как сообщил М. Орехов, за последние три года стоимость таких решений снизилась примерно на 10%, а главное – заказчики больше не боятся ЛИ АКБ. «За три года активной эксплуатации литий-ионных батарей не было ни одного инцидента», – подчеркнул он. Все больше производителей предлагают системы с использованием таких батарей. Так, на DCDE-2021 литий-ионные решения – ИБП SmartLi – представила компания Huawei.

Для обеспечения надежной работы систем бесперебойного электропитания важно отслеживать состояние АКБ. Литий-ионные системы имеют встроенные средства мониторинга, а для доминирующих пока на рынке свинцово-кислотных аккумуляторов подобные средства обычно устанавливают дополнительно.

Об опыте эксплуатации системы мониторинга и балансировки батарей в ЦОДе O2хуген рассказал ведущий менеджер отдела проектов компании «Смарт Бэттериз» (бренд ENERGON) Евгений Швецов. В ЦОДе уровня Tier III на 400 стоек с установленной электрической мощностью 12 МВА и фактическим потреблением 1,5 МВт используется 10 ИБП Eaton мощностью от 500 до 600 кВА и 800 батарей.

«Главная проблема в ЦОДе – ограниченное пространство. Мы взяли стеллажи высотой 2,5 м с каркасом повышенной жесткости. На одном стеллаже располагаются 120 батарей – три группы по 40 шт. Однако из-за высокой плотности батарейного массива с дальних батарей оказалось физически невозможно снимать параметры. Поэтому решили поставить на все АКБ системы мониторинга», – пояснил Е. Швецов.

В ЦОДе установили 12 систем мониторинга батарей. Для исключения разбаланса АКБ

установили 480 балансиров S1. В итоге удалось сократить затраты на обслуживание четырех аккумуляторных стеллажей АКБ на 560 тыс. руб. в год, повысить эффективность использования площади ЦОДа, минимизировать негативное влияние человеческого фактора и обеспечить прогнозирование сроков замены батарей.

Мониторинг параметров электропитания

Снижение качества входного электричества – одна из причин растущей заинтересованности ЦОДов в современных системах мониторинга параметров электропитания. Среди других причин – необходимость повышения эффективности использования электроэнергии при повышении надежности и управляемости ее доставки до ИТ-оборудования.

Сергей Дик, директор по развитию бизнеса компании Janitza, рекомендует использовать технические решения, обеспечивающие постоянное измерение необходимых параметров. «Периодические измерения влекут только затраты и не дают никаких преимуществ – прозрачность может быть достигнута только при непрерывном измерении», – отметил он.

По словам представителя Janitza, технические решения компании способны в одной системной среде выполнять сразу три блока функций: энергоменеджмент, мониторинг качества электроэнергии и контроль дифференциальных токов. Данные энергоменеджмента позволяют оптимизировать системы электропитания и снижать расходы на электроэнергию. Основная задача, которую решает мониторинг качества электроэнергии, – обеспечение высокого коэффициента доступности и сокращение времени простоев. Наконец, контроль дифференциальных токов предоставляет возможность раннего распознавания неполадок, что предотвращает перегрузки и повышает пожарную безопасность.

«Чаще всего пожары на объектах случаются по причине нарушения правил устройства и эксплуатации электрооборудования. Измерение дифференциальных токов с высокой точностью позволяет заранее локализовать проблему, которая может привести к пожару», – уверен С. Дик.

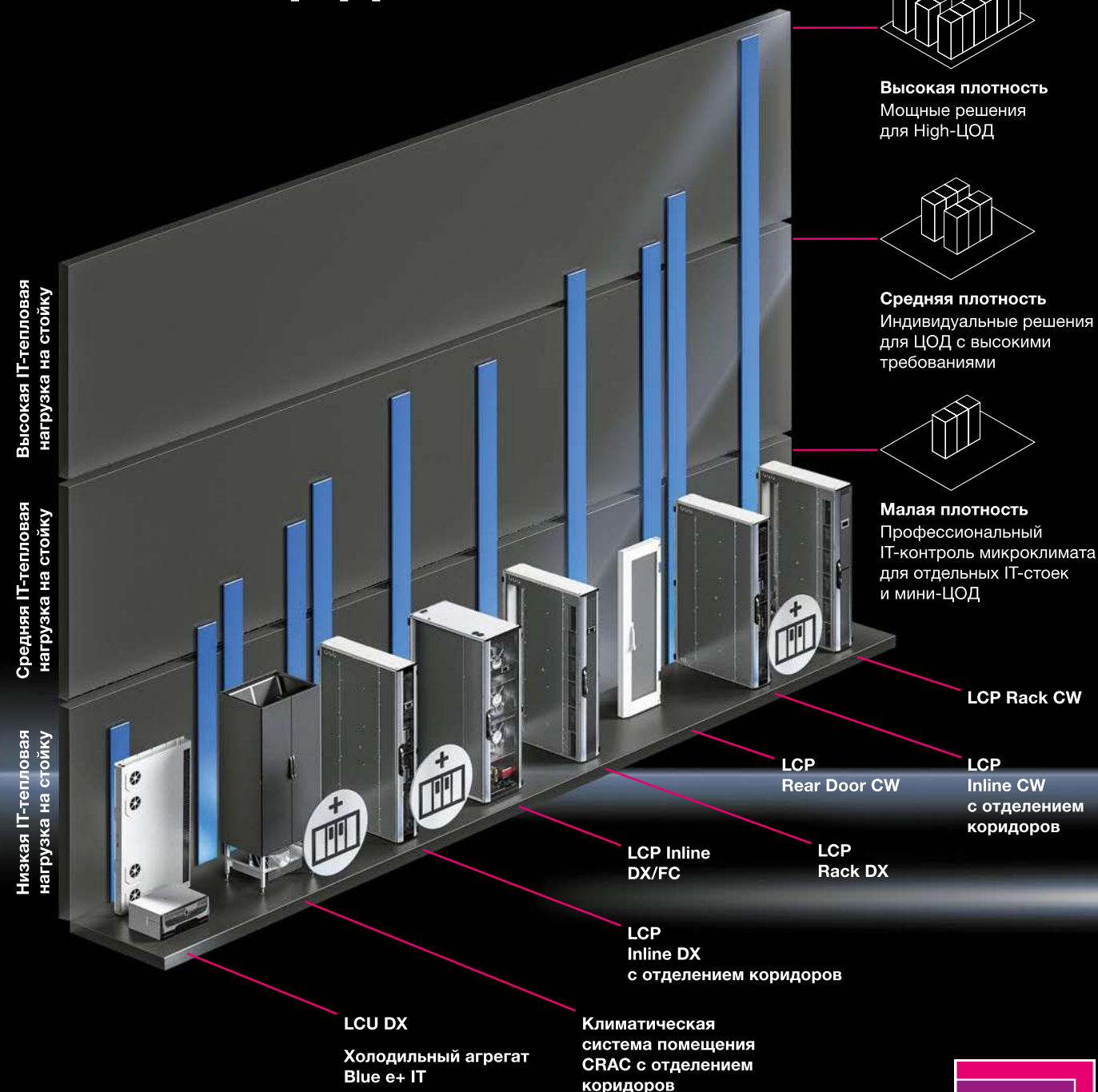
Инженерная инфраструктура ЦОДа – область в целом консервативная ввиду чрезвычайной важности ее надежного функционирования. Инновация имеет шанс быть принятой отраслью только при том условии, что она не увеличит риск остановки работы. А возможность повышения эффективности рассматривается только при неизбежности параметров надежности. **ИКС**

Rittal – The System.

Faster – better – everywhere.



От охлаждения отдельных стоек до всего ЦОД



Реклама

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP

www.rittal.ru



RiMatrix Next Generation: модульное решение горячих проблем

Михаэль Зиденханс

ИТ-директора и операторы ЦОДов должны реагировать на растущие требования к производительности, электропитанию и охлаждению вычислительных мощностей максимально быстро, гибко и энергоэффективно. На помощь им может прийти RiMatrix Next Generation – новая платформа Rittal для создания ИТ-инфраструктуры.

Главная задача Маркуса Шварца, руководителя дата-центра из Arvato Systems в Гютерсло (Германия), – ежедневно обеспечивать надежность процессов в ЦОДе. «Дата-центр должен функционировать круглосуточно и ежедневно. Сбои недопустимы», – заявляет он. Но его тон становится не таким уверенным, когда он говорит о будущем. «Никто не может предсказать, какими будут требования к ЦОДам через три, пять или десять лет», – констатирует Шварц. Многие операторы дата-центров находятся в такой же ситуации, как и он. Им нужно приспосабливаться к неумолимо наступающей цифровизации, но как что-либо планировать, если не знаешь, чего ждать? И можно ли в принципе спроектировать ЦОД, отвечающий не только нынешним требованиям, но и будущим?

«Можно!» – отвечает Михаэль Николаи, руководитель отдела продаж ИТ-решений Rittal в Германии. Один из главных факторов здесь – растущие требования к электропитанию и охлаждению. «Только на охлаждение серверов и стоек с оборудованием приходится до 40% общего энергопотребления дата-центра», – рассказывает Николаи. Это требует масштабируемых и энергоэффективных систем охлаждения.

Весь опыт Rittal в одном решении

Эксперты Rittal взаимодействуют с операторами ЦОДов по всему миру и знают об этих проблемах не понаслышке.

Мы вложили
весь наш опыт
разработки ИТ-систем
в платформу RiMatrix
Next Generation.

Михаэль Николаи,
руководитель отдела
продаж ИТ-решений
в Германии, Rittal



И у них есть ответ: открытая платформа для создания ИТ-инфраструктуры RiMatrix Next Generation – модульное решение, позволяющее операторам ЦОДов планировать будущее уже сейчас. Компоненты платформы можно добавлять или убирать, почти как в детском конструкторе, что делает ее гибко расширяемой и масштабируемой. «Мы вложили весь наш опыт разработки ИТ-систем в платформу RiMatrix Next Generation. Расширив свой портфель решений, мы теперь можем создавать гибкие системы с прицелом на будущее», – подчеркивает Николаи.

Базовыми модулями служат стойки с оборудованием, к которым подключаются дополнительные компоненты для управления микроклиматом, электропитанием, резервным копированием, мониторингом и безопасностью данных. В результате можно сформировать комплексное решение для ИТ-инфраструктуры любого масштаба: от автономных стоек, контейнеров и периферийных вычислительных узлов до колокационных, облачных и гиперЦОДов. Уникальная особенность системы заключается в том, что ее новые компоненты всегда совместимы с уже эксплуатируемыми и даже устаревшими. Это позволяет гибко регулировать каждый аспект ИТ-платформы: ее размер, производительность, безопасность и отказоустойчивость. Независимо от своих планов на будущее, операторы ЦОДов по всему миру всегда смогут получить именно то решение, которое им требуется с учетом местных условий. Поставщики услуг и партнеры, сертифицированные Rittal, работая на объектах, также учитывают локальную специфику. «Благодаря такому подходу мы не внедряем ИТ ради ИТ, – объясняет Николаи, – а предлагаем операторам дата-центров только то, что принесет реальную пользу».

Николаи специализируется на управлении микроклиматом в ЦОДах. В Rittal его называют отцом технологии LCP (Liquid Cooling Package). «Во всем мире мы всегда ищем лучшие местные решения для организации охлаждения на основе фактических потребностей. Ведь то, что хорошо для Швеции, может быть плохо для Германии, а то, что нужно высокопроизводительному ЦОДу, центрам с низкой или средней производительностью совершенно ни к чему», – считает Николаи.

Естественное охлаждение помещений

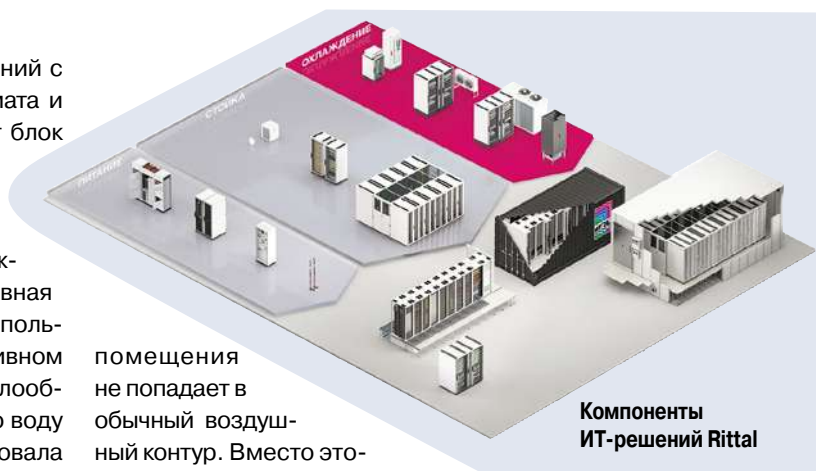
Сегодня широко используется охлаждение помещений с помощью прецизионных систем контроля микроклимата и систем циркуляции воздуха. За охлаждение отвечает блок CRAC (кондиционирование воздуха в серверном помещении), который работает подобно обычному кондиционеру. Охлажденный воздух поступает в ЦОД и подается к стойкам из-под фальшпола. А если наружный воздух холоднее, чем воздух из ИТ-систем, то активная система охлаждения вообще не нужна: вместо нее используется не прямое естественное охлаждение. В противном случае применяются внешние воздухо-водяные теплообменники (наружные чиллеры), охлаждающие нагретую воду из ЦОДа до 20°C и ниже. «Компания Rittal оптимизировала эту традиционную процедуру управления микроклиматом в дата-центрах с мощностями вплоть до мегаваттных», – рассказывает Николай. В идеале при этом способе охлаждения энергия необходима только для питания вентиляторов естественного охладителя и, возможно, насосов холодной воды. «Эффективность этого решения во многом зависит от местных климатических условий», – отмечает эксперт Rittal.

Непрямое охлаждение помещения

Непрямое естественное охлаждение помещений – это альтернативное решение, которое используется в ЦОДе мощностью 1 МВт, принадлежащем медиакомпания Deutsche Welle. Система генерирует охлаждающую мощность только по мере необходимости, что обеспечивает экономию электроэнергии до 60%. Компания Rittal включила этот модуль в свой портфель продуктов, когда начала сотрудничать со Stulz. Эта компания из Гамбурга специализируется на контроле микроклимата в ЦОДах. Благодаря Stulz новая платформа для создания ИТ-инфраструктуры включает в себя высокопроизводительные компоненты охлаждения, такие как системы естественного охлаждения, боковые охладители и чиллеры для помещений. «Это сотрудничество придало заверченный вид нашему портфелю систем охлаждения для дата-центров, дополнив его стандартной системой кондиционирования воздуха замкнутого цикла во всех конструктивных вариантах, а также открыло нам доступ к предлагаемым компанией Stulz услугам прокладки воздуховодов для более крупных проектов», – объясняет Николай.

Охлаждение отдельных стоек

Несомненно, объемы данных и, следовательно, удельная потребляемая мощность ЦОДов будут расти. Это уже происходит в высокопроизводительных дата-центрах, где серверы размещены максимально плотно. В результате на каждом квадратном метре полезной площади потребляется до 30 кВт энергии. При таких условиях традиционные конструкции фальшпола уже не могут быстро отводить образующееся тепло, и здесь на помощь приходит предлагаемое Rittal семейство стоечных охлаждающих решений LCP. «Это наиболее целесообразно как с технической, так и с экономической точки зрения. Стоечные решения – единственный приемлемый вариант в случаях, когда требования к производительности очень высоки», – подчеркивает Николай. Принцип разработанной им концепции состоит в том, что горячий воздух из



помещения не попадает в обычный воздушный контур. Вместо этого он вытягивается блоками

LCP непосредственно сзади серверов, охлаждается с помощью теплообменника и снова подается спереди. LCP реагируют с молниеносной быстротой, что идеально подходит для высокопроизводительных дата-центров.

Эффективное охлаждение чипов

Поскольку воздух плохо проводит тепло, в перспективе ключевую роль будет играть прямое охлаждение процессоров. Обычно такой подход реализуют в виде водяного охлаждения. Одна из альтернатив этому – инновационное прямое охлаждение чипа с помощью современных хладагентов. Такой метод охлаждения ИТ-оборудования помогает достичь максимальной эффективности. Одна из его реализаций – новая безводная двухфазная система жидкостного охлаждения, предлагаемая компаниями Rittal и ZutaCore. «За счет изменения агрегатного состояния вещества эта система поглощает еще больше тепловой энергии от чипов и делает это еще быстрее. При этом охлаждаются непосредственно самые горячие точки и места пикового энергопотребления», – объясняет Николай и подытоживает: «Благодаря RiMatrix Next Generation наш портфель включает в себя решения по кондиционированию для любых целей: от охлаждения отдельных стоек и управления микроклиматом помещений до системы LCP и прямого охлаждения процессоров для сложных высокопроизводительных ЦОДов. Используя холодильные агрегаты Rittal для непосредственного контроля микроклимата стоек, можно добиться 75%-ного снижения энергопотребления и выбросов CO₂».

Таким образом, энергоэффективные и экономичные концепции охлаждения, заложенные в модульную систему RiMatrix Next Generation, позволяют любому оператору ЦОДа сделать сегодня вложения, которые окупятся в будущем, даже если не вполне ясно, каким оно будет. В конце концов, какими бы ни были пропускная способность и плотность мощности дата-центра, он сможет работать прибыльно и безотказно только при наличии эффективного охлаждения.



**ООО «Риттал», 125252, Москва,
ул. Авиаконструктора Микояна, 12,
БЦ "Линкор", 4 этаж
тел. (495) 775-0230
info@rittal.ru, www.rittal.ru**

Стандарт EN 50600: первое знакомство

**Константин
Королев,**
директор
по развитию
отраслевых
инициатив,
АНО КС ЦОД

В российской отрасли ЦОДов немногие специалисты знакомы с европейским стандартом EN 50600, особенностями его применения, возможностью соответствующей сертификации и тем более способны сопоставить его с другими стандартами для дата-центров. Попробуем заполнить этот пробел.

История и состав стандарта

В отрасли центров обработки данных, которая сравнительно молода по общемировым меркам, соответствующие стандарты появились недавно, 15–20 лет назад. Эти стандарты разрабатывались организациями, как входящими в ISO/IEC (например, Ассоциацией телекоммуникационной промышленности США (Telecommunications Industry Association, TIA) и Американским национальным институтом стандартов (American National Standards Institute, ANSI)), так и независимыми от них (скажем, Uptime Institute или BICSI*). В Европе стандартом на создание ЦОДов и управление ими стал разработанный CENELEC стандарт EN 50600 Information Technology – Data Centre Facilities and Infrastructures. Стандарт описывает требования к проектированию, построению и эксплуатации ЦОДов, основанные на предлагаемой классификации этих объектов по четырем уровням готовности и физической безопасности, а также ключевые показатели их эффективности.

Первая версия стандарта появилась в 2012 г. (EN 50600:2012). Фактически стандарт изложен в группе логически связанных документов, которые выходили в целом ряде редакций. Частые изменения текстов, входящих в стандарт, обусловлены как накоплением опыта участниками отрасли, так и совершенствованием применяемых технологий и расширением круга рассматриваемых тем. Если первоначально стандарт фокусировался на принципах и процессе проектирования ЦОДа, то новейшие дополнения затрагивают такие вопросы, как энергоэффективность объекта на протяжении всего жизненного цикла. Последние версии составляющих стандарт документов появились в 2020 г., и работа над ними продолжается. Стандарт существует в трех официальных языковых версиях: на английском, французском и немецком языках.

Стандарт представляет собой свод рекомендаций по построению ЦОДа, отвечающего определенному набору требований с точки зрения надежности и эффективности эксплуатации.

*Стандарт BICSI-002, разработанный BICSI, впоследствии был аккредитован ANSI; его последняя версия обозначается ANSI/BICSI-002:2019.

Международная стандартизация: основные действующие лица и правила

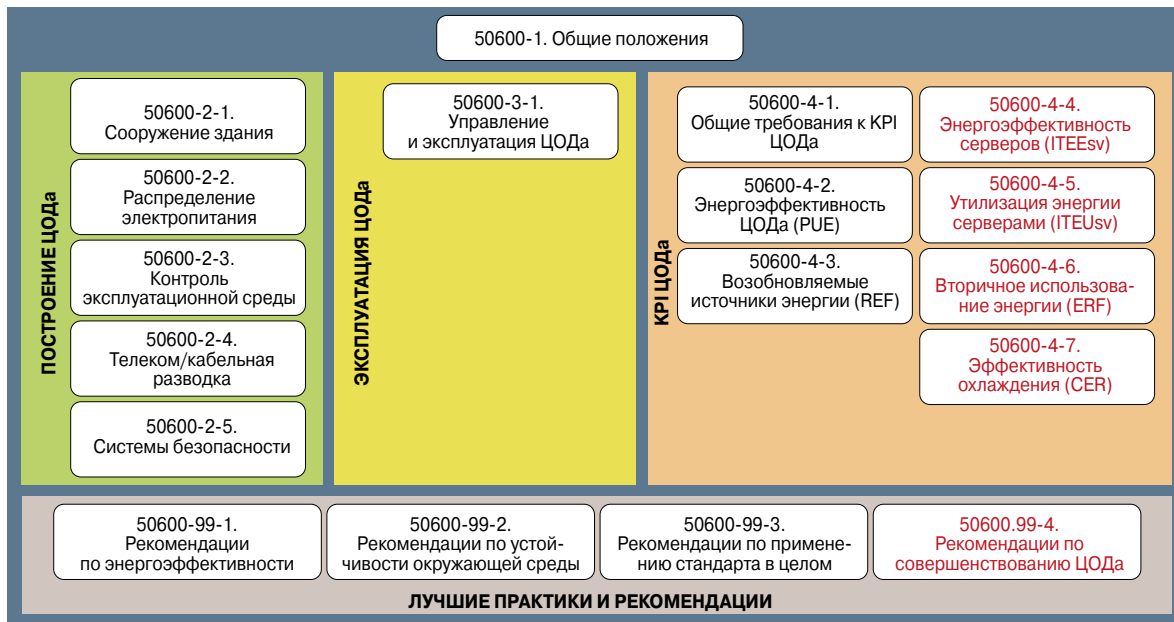
Европейские стандарты, или Европейские нормы (European Norms, EN) – это технические стандарты, которые разрабатываются и поддерживаются тремя некоммерческими организациями: Европейским комитетом по стандартизации (Comité Européen de Normalisation, CEN), Европейским комитетом электротехнической стандартизации (Comité Européen de Normalisation Électrotechnique, CENELEC) и Европейским институтом телекоммуникационных стандартов (European Telecommunications Standards Institute, ETSI). Эти организации формируют систему технического нормирования и

стандартизации в Европе; стандарты многих стран за пределами Европы также согласуются со стандартами EN. Стандарты EN обозначаются EN XXXXX:XXXX, где первые пять разрядов дают номер стандарта, а последние четыре разряда – год его введения в использование.

CEN, CENELEC и ETSI сотрудничают с другими организациями в области международной стандартизации, в том числе с Международной организацией по стандартизации (International Organization for Standardization, ISO) и Международной электротехнической комиссией (International Electrotechnical

Commission, IEC). Это сотрудничество направлено на то, чтобы избежать дублирования стандартов и потенциальных конфликтов между ними. Ряд стандартов ISO и IEC был принят в качестве Европейских стандартов (EN). Такие стандарты имеют обозначения формата ISO EN XXXXX и действуют на всей территории Евросоюза. Отметим, что Россия является членом ISO и IEC.

Важно, что страны-участницы не обязаны использовать стандарты ISO и IEC; каждая страна, в том числе Россия, вправе их применять или не применять. В России Государственная система стандартизации допускает



◀ **Рис. 1.**
Структура стандарта EN 50600

Он рассчитан на совместное использование архитекторами, проектировщиками, строителями и инженерными компаниями (в нашем понимании – системными интеграторами) в процессе создания объекта. Однако стандарт не затрагивает выбор конкретных технологий, решений, типов и марок оборудования, аппаратных и программных продуктов и т.п., оставляя это на усмотрение проектировщиков. Он фокусируется на надежности и эффективности отдельно взятого ЦОДа, не рассматривая геораспределенные модели из нескольких ЦОДов (и, следовательно, степень доступности предоставляемых такой моделью сервисов). Также стандарт не затрагивает требования по электробезопасности и электромагнитной совместимости, поскольку данные вопросы регламентируются другими документами, обязательными к при-

менению и в известной степени аналогичными нашим ПУЭ, техническим регламентам и пр.

Стандарт состоит из пяти частей (рис. 1).

Часть 1 (EN 50600-1). Общие положения и терминология, в том числе классификация ЦОДов по уровням готовности, физической безопасности и энергоэффективности.

Часть 2 (EN 50600-2-X). Рекомендации по проектированию и построению здания ЦОДа и его инфраструктуры в соответствии с классификацией, приведенной в части 1.

Часть 3 (EN 50600-3-X). Требования и рекомендации по эксплуатации, процессам и управлению ЦОДом.

Часть 4 (EN 50600-4-X). Ключевые показатели эффективности (KPI) ЦОДа, рекомендуемые в качестве инструмента анализа и повышения эффективности использования его ресурсов.

разные варианты применения международных и региональных стандартов в качестве национальных (см. ГОСТ Р 1.7-2014 «Стандартизация в Российской Федерации. Стандарты национальные. Правила оформления и обозначения при разработке на основе применения международных стандартов»):

- принятие исходного текста международного (регионального) стандарта в качестве национального (ГОСТ Р) без каких-либо дополнений и изменений. Такой вариант, называемый идентичным стандартом, обозначается так, как это принято для национального стандарта (например, ГОСТ Р ИСО 9001:2000);

- принятие текста международного (регионального) стандарта с дополнениями, отражающими особенности российских требований к объекту стандартизации. Это называют модифицированным стандартом, и в его обозначение к шифру отечественного стандарта добавляется номер соответствующего международного (регионального): например, ГОСТ Р 56106-2015 (ИСО/МЭК 19510:2013).

Европейские стандарты имеют силу на всей территории Евросоюза и превалируют над национальными стандартами, разработанными ранее национальными органами, например, Германским институтом стандартизации

(Deutsches Institut für Normung, DIN) или Австрийским институтом по стандартизации (Österreichisches Normungsinstitut, ÖNORM). Так, в инструкции CEN-CENELEC Internal Regulations, Part 2 говорится, что «Европейский стандарт (EN) несет в себе обязательство применения на национальном уровне, получая статус национального стандарта и отменяя любой конфликтующий с ним национальный стандарт».

Отметим, что данное правило касается государственных стандартов, что не отменяет возможности использования других, независимых стандартов, однако фактически сильно сужает возможности применения последних.

Дополнения (EN 50600-99-X). Дополнительные рекомендации как по применению самого стандарта, так и по обеспечению условий, повышающих эффективность использования ЦОДа.

Классификация ЦОДов

Первая часть стандарта (EN 50600-1:2019, Information technology – Data centre facilities and infrastructures – Part 1: General concepts) излагает основные положения, на которых построен стандарт: понятийный аппарат, общие аспекты, параметры, эталонные модели и функциональные элементы ЦОДа, в том числе требования к внешней по отношению к ЦОДУ инфраструктуре; перечисляет вопросы, нуждающиеся в рассмотрении при анализе бизнес-рисков и операционных затрат; вводит концепцию ключевых показателей эффективности ЦОДа; описывает принципы проектирования, включая маркировки, условные обозначения, требования к документации и т.п.

Наконец, стандарт формулирует, вероятно, наиболее важную для многих концепцию, – систему классификации ЦОДов, основанную на трех критериях: готовности, безопасности и энергоэффективности (рис. 2). Для каждого из критериев выделены несколько уровней. Соответствующий этим уровням объект будет подвержен большим или меньшим рискам и будет по-разному влиять на бизнес компании.

Так, с точки зрения готовности (Availability) инженерной инфраструктуры ЦОДа рассматриваются четыре уровня (класса). Эти классы в принципе подобны (хотя и имеют ряд отличий) уровням Tier, разработанным Uptime Institute, и применяются к системам энергоснабжения, охлаждения и кабельной разводке.

Класс 1. Низкая готовность. Резервирование отсутствует; единичные линии распределения.

Класс 2. Средняя готовность. Резервирование отдельных компонентов; единичные линии распределения.

Класс 3. Высокая готовность. Резервирование на уровне компонентов и дублирование линий распределения. Обеспечивается техобслуживание без остановки сервисов.

Класс 4. Очень высокая готовность. Резервирование на уровне систем и дублирование линий распределения. Обеспечивается отказоустойчивость, за исключением периодов проведения ТО.

При оценке физической безопасности (Physical Security), в которой выделяются четыре уровня (зоны), изучаются возможность несакционированного доступа и устойчивость к внутренним инцидентам, связанным с окружающей средой (пожар, затопление помещений и т.п.), а также к внешним воздействиям природного и техногенного характера. Для критерия энергоэффективности (Energy Efficiency Enablement) вводятся три уровня, зависящие от таких метрик, как коэффициент энергоэффективности (PUE), использование возобновляемых источников энергии (REF) и пр.

Соответствие одному и тому же уровню в рамках трех критериев не является обязательным: ЦОД может одновременно характеризоваться, например, классом 3 по готовности, зоной 4 по безопасности и уровнем 1 по энергоэффективности.

Требования и рекомендации по проектированию и построению ЦОДа

Второй раздел стандарта EN 50600 рассматривает как здание, так и отдельные подсистемы инженерной инфраструктуры ЦОДа применительно к приведенной в части 1 классификации по трем ключевым критериям и их уровням. Раздел включает пять документов.

Часть 2-1. Построение здания ЦОДа (EN 50600-2-1:2015, Information technology – Data centre facilities and infrastructures – Part 2-1: Building construction). Документ перечисляет требования к зданию ЦОДа и вспомогательным сооружениям с точки зрения уровней (зон) физической безопасности. Здесь рассматриваются выбор места расположения ЦОДа, исходя из внешних условий; требования к зданию ЦОДа и его конфигурация; системы противопожарной безопасности; контроль качества строительства. Если проводить параллель с известными у нас стандартами Uptime Institute, то первые два элемента описываются в стандарте на эксплуатационную устойчивость (Tier Standard: Operational Sustainability).

Часть 2-2. Системы электроснабжения и распределения питания (EN 50600-2-2:2019, Information technology – Data centre facilities and infrastructures – Part 2-2: Power supply and distribution). Документ рассматривает источники энергоснабжения для ЦОДа и их организацию; системы распределения электропитания внутри ЦОДа до конечных потребителей; системы заземления и молниезащиты; устройства учета потребления электроэнергии и контроля ее качества во всех ключевых точках системы распределения питания, а также интеграцию таких устройств с системой управления зданием (инфраструктурой).

Часть 2-3. Контроль эксплуатационной среды (EN 50600-2-3:2019, Information technology – Data centre facilities and infrastructures – Part 2-3:

Рис. 2. Система классификации ЦОДов по готовности, безопасности и энергоэффективности ▼

Анализ рисков и влияния на бизнес		
Готовность	Физическая безопасность	Энергоэффективность
Класс 1	Зона 1	Уровень 1
Класс 2	Зона 2	Уровень 2
Класс 3	Зона 3	Уровень 3
Класс 4	Зона 4	

Источник: Euris Technology

Environmental control). Документ определяет требования к контролю температуры, влажности, запыленности, вибраций, а также к физической безопасности систем контроля эксплуатационной среды.

Часть 2-4. Телекоммуникационная кабельная инфраструктура, СКС (EN 50600-2-4:2015, Information technology – Data centre facilities and infrastructures – Part 2-4: Telecommunications cabling infrastructure). Документ излагает принципы организации слаботочной кабельной разводки в ЦОДе, исходя из критерия готовности, сформулированного в части 1. Рассматривается построение СКС различного назначения (поддерживающих системы мониторинга и контроля элементов инфраструктуры ЦОДа и автоматизацию различных компонентов, обеспечивающих связность ЦОДа с внешним миром), а также организация и размещение элементов этих сетей.

Часть 2-5. Системы безопасности (EN 50600-2-5:2016, Information technology – Data centre facilities and infrastructures – Part 2-5: Security systems). Документ описывает системы физической безопасности, контроля и управления доступом на объект (СКУД), меры противопожарной защиты внутри здания и противодействия иным негативным воздействиям как внешней, так и внутренней природы.

Все части второго раздела стандарта многократно корректировались с момента своего появления в 2012 г., и работа над ними продолжается.

Часть 3. Информация об управлении и эксплуатации (EN 50600-3-1:2016, Information technology – Data centre facilities and infrastructures – Part 3-1: Management and operational information). Раздел посвящен организации процессов управления и эксплуатации ЦОДа. Основной фокус документа – эксплуатационные процессы, необходимые для обеспечения требуемого уровня устойчивости и готовности, управление рисками и их минимизация, управление мощностями ЦОДа и энергоэффективность. Особый акцент сделан на соответствии процессов управления ЦОДом текущим и будущим требованиям его пользователей.

Ключевые показатели эффективности

Часть 4 (EN 50600-4-X) состоит из группы документов, в которых рассматриваются ключевые показатели эффективности ЦОДа, служащие для анализа и повышения эффективности использования ресурсов. Изначально этот раздел не входил в стандарт EN 50600 и был разработан не CEN/CENELEC, а IEC. Эти документы были опубликованы в составе международного стандарта ISO/IEC 30134:2016 Information technology – Data centres – Key performance indicators и в рамках взаимодействия между CEN/CENELEC и ISO/IEC были

включены в состав EN 50600 практически без изменений.

В раздел входят следующие документы.

Часть 4-1. Обзор и общие требования к ключевым показателям эффективности (EN 50600-4-1:2016, Information technology – Data centre facilities and infrastructures – Part 4-1: Overview of and general requirements for key performance indicators). Здесь приводятся общая структура раздела, определения и терминология, граничные условия применения KPI, их цели и пр.

Часть 4-2. Коэффициент энергоэффективности (EN 50600-4-2:2016/A1:2019, Information technology – Data centre facilities and infrastructures – Part 4-2: Power Usage Effectiveness). Документ характеризует коэффициент энергоэффективности (PUE) как ключевой показатель эффективности (KPI), позволяющий количественно оценить эффективность потребления электроэнергии; дает определение PUE ЦОДа и категории его измерения; раскрывает взаимосвязь PUE с инфраструктурой ЦОДа и ИТ-оборудованием; описывает измерение, вычисление и корректный учет PUE.

Часть 4-3. Фактор использования возобновляемой энергии (EN 50600-4-3:2016/A1:2019, Information technology – Data centre facilities and infrastructures – Part 4-3: Renewable Energy Factor). В документе рассматривается применение в ЦОДе источников возобновляемой энергии (солнечной, ветряной и т.п.), описывается методология вычисления REF и его корректного учета.

Следующие две части раздела на момент написания статьи находились в разработке и не были опубликованы.

Часть 4-4. Энергоэффективность серверного оборудования (EN 50600-4-4:2019, Information technology – Data centre facilities and infrastructures – Part 4-4: IT Equipment Energy Efficiency for servers (ITEESv));

Часть 4-5. Потребление электроэнергии серверным оборудованием (EN 50600-4-5:2019, Information technology – Data centre facilities and infrastructures – Part 4-5: IT Equipment Energy Utilization for servers (ITEUsv)).

Эти части, описывающие особенности использования размещенного в ЦОДе ИТ-оборудования, с точки зрения данного в части 1 стандарта определения ЦОДа, согласно которому это структура для размещения ИТ-систем, но не сами системы (серверы)*, несколько выбиваются из общей канвы.

*«ЦОД – это структура или группа структур, предназначенных для централизованного размещения, организации взаимодействия и эксплуатации ИТ-систем, сетевого и телекоммуникационного оборудования, которые обеспечивают возможность оказания услуг в области хранения, обработки и передачи данных, а также все объекты и инфраструктуры, используемые для распределения электроэнергии и контроля среды в сочетании со средствами обеспечения требуемой устойчивости и безопасности для достижения желаемого уровня доступности оказываемых услуг». Определение цитируется по ГОСТ Р ИСО/МЭК 30134-1 – 2018.

Часть 4-6. Фактор повторного использования энергии (EN 50600-4-6:2020, Information technology – Data centre facilities and infrastructures – Part 4-6: Energy Reuse Factor). Документ определяет фактор повторного использования энергии (ERF) как KPI, который позволяет исчислять повторное использование энергии, потребленной ЦОДом, описывает методику его измерения, подсчета и учета, а также его применение и взаимосвязь с PUE. Отметим, что ERF не отражает эффективность процесса повторного использования как происходящего вне ЦОДа.

Часть 4-7. Коэффициент эффективности охлаждения (EN 50600-4-7:2020, Information technology – Data centre facilities and infrastructures – Part 4-7: Cooling Efficiency Ratio). Документ рассматривает коэффициент эффективности охлаждения (CER) как KPI, исчисляющий эффективность использования энергии для контроля температуры в машзалах ЦОДа. В документе дается определение CER; описываются взаимосвязи между CER, инфраструктурой ЦОДа и ИТ-оборудованием, а также методика измерения, подсчета и корректного учета CER. В приложениях анализируются соотношения между CER и другими KPI, предлагаются примеры применения CER и даются рекомендации по вторичным (производным от CER) KPI.

Учитывая продолжающееся сотрудничество между ISO/IEC и CEN/CENELEC, можно предположить, что в скором времени четвертый раздел EN 50600 будет дополнен двумя документами, входящими в стандарт ISO/IEC 30134. Это документы, рассматривающие эффективность утилизации углеродных соединений (ISO/IEC CD 30134-8 – Part 8: Carbon Usage Effectiveness (CUE)) и воды (ISO/IEC CD 30134-9 – Part 9: Water Usage Effectiveness (WUE)).

Дополнения

Помимо перечисленных выше документов, составляющих стандарт EN 50600, к нему примыкают несколько дополнений. Это справочные тексты, не являющиеся частью собственно стандарта, технические рекомендации, или «лучшие практики».

Часть 99-1. Рекомендуемые практики для управления потреблением энергии (CLC/TR 50600-99-1:2020, Information technology – Data centre facilities and infrastructures – Part 99-1: Recommended practices for energy management). Рассматриваются практики, направленные на снижение энергопотребления и/или повышение энергоэффективности ЦОДа. Отмечается, что данные практики не являются универсальными и могут быть применены не в любом ЦОДе.

Часть 99-2. Рекомендуемые практики влияния на окружающую среду (CLC/TR 50600-99-

2:2019, Information technology – Data centre facilities and infrastructures – Part 99-2: Recommended practices for environmental sustainability). Сборник лучших практик, направленных на снижение влияния на окружающую среду со стороны как новых, так и существующих ЦОДов. Учитывается воздействие, связанное не только с электричеством, но и с использованием воды и загрязняющих веществ. Эти практики также не являются универсальными и также могут быть применены не в любом ЦОДе.

Часть 99-3. Руководство по применению стандарта EN 50600 (CLC/TR 50600-99-3:2018, Information technology – Data centre facilities and infrastructures – Part 99-3: Guidance to the application of EN 50600 series). Это сборник дополнительной информации по положениям и требованиям стандарта EN 50600, а также руководство по его корректному применению и интерпретации.

Часть 99-4. Модель максимального развития ЦОДа (TR 50600-99-4 – Data Centre Maturity Model). Это один из самых новых документов серии 50600, находившийся на момент написания статьи в разработке, которую ведет ассоциация Green Grid. Сам документ, вероятно, будет рассматривать принципы развития ЦОДа на протяжении жизненного цикла и, судя по последним новостям, впоследствии может открыть собой новый (пятый) раздел стандарта (EN 50600-5-1: Data Center Maturity Model).

Сопоставление с другими стандартами

EN 50600 – вероятно, наиболее всеохватывающий стандарт для ЦОДов и потому весьма популярен. Помимо того, что он является единым для всех стран Европы (исключая СНГ и Украину), он стал основой для создания ряда аналогичных стандартов различного уровня применения. Так, стандарт ISO/IEC TS 22237:2018 Information technology – Data centre facilities and infrastructures представляет собой практически полную копию первых трех разделов EN 50600.

Кроме того, на основе EN 50600 многие организации разрабатывают свои стандарты. Из этих документов наиболее известен, пожалуй, TSI STANDARD (Trusted Site Infrastructure), подготовленный европейской корпорацией TÜViT. Строго говоря, основные принципы и методология анализа инфраструктуры ЦОДа были разработаны TÜViT еще в 2002 г., до появления EN 50600, и основаны на германских национальных стандартах DIN, но сегодня этот стандарт приведен в соответствие с принципами EN 50600. TSI STANDARD рассматривает ЦОД в девяти различных аспектах, включая окружающую среду, здание, пожарную безопасность, физическую безопасность, кабельную разводку, энергоснабжение, холодоснабжение, организационную структуру, документацию



Источник: TÜViT

Класс готовности

- Распределение электропитания
- Контроль эксплуатационной среды (охлаждение)
- Телекоммуникации и СКС
- Симуляция отказа источника внешнего энергоснабжения

Класс безопасности

- Системы контроля доступа
- Политики контроля
- Смежные объекты

Энергетическая эффективность

- Стратегическое управление
- Соблюдение политик энергоэффективности
- Точная фиксация PUE и KPI

Эксплуатационный профессионализм

- Техобслуживание
- Противопожарная защита
- Кадровая политика
- Обучение и развитие персонала

Источник: DCA

на объект и применение геораспределенной модели из нескольких ЦОДов (рис. 3).

EN 50600 также послужил основой для сбора рекомендаций по организации и построению ЦОДа, выпущенного британской компанией Data Center Alliance (DCA). Три ключевых критерия EN 50600 (готовность, безопасность, энергоэффективность) DCA дополнила эксплуатационным профессионализмом (рис. 4). Соответствие этим четырем критериям проверяется в ходе аудита ЦОДа, предлагаемого компанией.

Помимо названных, много производных от EN 50600 разработок, дополняющих стандарт в том или ином ключе, ведется как в Европе, так и в мире.

Сертификация

Учитывая популярность EN 50600 в ряде регионов, многие владельцы ЦОДов хотели бы иметь возможность убедиться, что их объект соответствует стандарту. Подтвердить такое соответствие может сертификация.

Однако для стандарта EN 50600 общепризнанного, официального механизма сертификации нет. Разработчики стандарта не проводят сертификацию сами и не уполномочивают на это третьих лиц (как это недавно стало практиковаться в отношении стандарта ANSI/TIA-942B). Текст документа также не оговаривает каких-либо механизмов удостоверения соответствия ЦОДа стандарту.

Между тем никто не вправе ограничить деятельность компаний, которые заявляют о возможности выполнения независимого аудита ЦОДа на предмет соответствия EN 50600 и подтверждения этого соответствия своим сертификатом. Причем проводить аудит может практически кто угодно: создатель ЦОДа или его компонентов; пользователь или оператор ЦОДа; независимый внешний аудитор. При любом сценарии оборотной стороной такого аудита и сертификации может быть некорректное применение положений стандарта к оцениваемому ЦОДу и, как следствие, искаже-

ние реального положения дел. Тем не менее сегодня многие и европейские компании, и организации из других частей света предлагают аудит ЦОДа для удостоверения соответствия как EN 50600, так и производным от него собственным версиям. Вот далеко не полный список таких организаций:

- TÜViT (Германия), предлагает два вида аудитов, в соответствии с EN 50600 и своим стандартом TSI;
- Certification & Information Security GmbH (CIS), Германия;
- Future-Tech, Великобритания;
- Upsite Technologies, США;
- Capitoline, Великобритания;
- Data Center Group GmbH, Германия;
- BSI Group, Великобритания;
- Data Center Alliance (DCA), Великобритания;
- Enterprise Product Integration (EPI), Сингапур;
- InnovIT AG, Австрия.

Во многих случаях предлагаемая сертификация заставляет вспомнить об Uptime Institute, поскольку состоит из двух этапов: анализа проекта и анализа объекта и DCCC (DC Conformity Certification), при этом сертификат зачастую имеет срок годности. Ряд компаний идет еще дальше и аккредитует другие организации на проведение аудита и сертификации по своей программе (DCA).

Что же касается «настоящей» сертификации, то ее механизм до сих пор не представлен. Первым шагом к упорядочению ситуации с сертификацией ЦОДов сторонними компаниями можно считать выпуск справочных дополнений CLC/TR 50600-99-X, призванных прояснить положения стандарта в отношении всех этапов построения ЦОДа – планирования, проектирования, закупки, инсталляции, интеграции, эксплуатации и обслуживания – для всех участников процесса, включая владельцев, операторов, команду эксплуатации, проектировщиков, строителей, поставщиков, агентов пусконаладочных работ и прочих действующих лиц. ИКС

◀◀ **Рис. 3.**
Элементы
TSI.STANDARD

▲ **Рис. 4.**
Ключевые
критерии оценки
ЦОДа согласно
стандарту DCA

STANDARDS

МегаЦОДы: когда размер имеет значение

Дата-центров в России становится все больше, и сами они постоянно укрупняются. Об особенностях проектирования и построения мегаЦОДов рассказывают эксперты компаний «Свободные Технологии Инжиниринг» и «Ди Си Квадрат».



Экспертов, имеющих практический опыт реализации проектов мегаЦОДов, в России немного. Сотрудничество между Евгением Вирцером и командой, составившей костяк компании «Свободные Технологии Инжиниринг», с одной стороны, и Александром Мартынюком и его компанией «Ди Си Квадрат» – с другой, началось более пяти лет назад в проекте создания крупнейшего корпоративного ЦОДа в Восточной Европе. Синергия опыта и экспертизы двух команд помогает эффективно реализовать новые амбициозные проекты, над которыми сейчас идет совместная работа.

«ИКС»: Существует ли общепринятый критерий того, с какой мощности дата-центр называют уже мегаЦОДом: 1 МВт, 2 МВт или 10 МВт? И где та граница, с которой начинаются гиперЦОДы?

Евгений Вирцер: Общепринятого критерия нет, но, на мой взгляд, приставку «мега» можно применять, когда мощность ЦОДа превышает 10 МВт. ГиперЦОД, полагаю, это объект мощностью от 100 МВт. Хотя, конечно, эти границы условны.

«ИКС»: МегаЦОД – это обязательно проект greenfield, с нуля и в чистом поле? Всегда ли мегаЦОДы реализуются за пределами крупных городов?

Е.В.: Действительно, в 99% случаев мегаЦОД – это про-



Евгений Вирцер, генеральный директор, «Свободные Технологии Инжиниринг»

ект с нуля в чистом поле, поскольку разместить крупный дата-центр в существующем здании крайне проблематично. Но российские коммерческие мегаЦОДы сегодня в основном располагаются в Москве или самом ближайшем Подмосковье. Обусловлено это прежде всего качеством каналов связи и транспортной доступностью для клиентов. А вот корпоративные мегаЦОДы чаще планируются и размещаются за пределами больших городов.

Александр Мартынюк: Не стоит недооценивать, однако, привычку основных игроков рынка коммерческих ЦОДов строить по принципу brownfield. Основное преимущество такого подхода – скорость вывода стоек на рынок. А это сейчас



Александр Мартынюк, исполнительный директор, «Ди Си Квадрат»

самый ценный ресурс! И тогда мультимегаваттные ЦОДы размещают в бывших заводских цехах и складских зданиях.

Хочу также подчеркнуть, что для ЦОДов отлично подходят типовые склады класса «А», которые имеют большую высоту до кровли (около 12 м), большепролетные конструкции с шагом колонн 9 и 12 м и высокую нагрузочную способность плиты – на уровне 5 т/кв. м. В Европе и особенно в США складские здания широко используют подобным образом. Общестроительная часть в этом случае недорога и легкодоступна.

Все большие проекты сотканы из нюансов. И в строительстве мега- и гиперЦОДов таких нюансов мега- и гипермного. Один из них – объем внешнего оборудования инженерных систем, производимый ими шум и выделяемое тепло. В черте города подобные инсталляции вызывают массу сложностей в плане согласований и влияния на окружающую площадку.

«ИКС»: Считается, что чем крупнее ЦОД, тем ниже его удельная стоимость (в пересчете на стойку или на единицу мощности). Ваш опыт это подтверждает? За счет чего получается добиться экономии?

Е.В.: С одной стороны, чем крупнее ЦОД, тем больше возможные скидки у производителей и соответственно ниже удельная стоимость. С другой стороны, любая ошибка на этапе проектирования и строительства вследствие масштаба оборачивается большими лишними тратами. Поэтому крупный ЦОД требует самого пристального внимания на всех подготовительных этапах.

Эффект масштаба начинает работать уже при переходе проекта за условную границу 500–1000 стоек. Если говорить о том, что помогает снижать стоимость строительства, то следует начать со стоимости 1 кВт мощности систем энергоснабжения и охлаждения. Чем крупнее установка, тем ниже удельная стоимость вырабатываемого ею киловатта холода или электричества.

Но, кроме этого, есть еще масса аспектов чисто инженерного свойства – топология систем, определение оптимального в техническом и ценовом плане кванта единичной мощности устройств и т.д.

У эффекта масштаба есть и обратная сторона: слишком большие машины накладывают ограничения на минимальную нагрузку на этапе эксплуатации. Вы ведь понимаете: на малых оборотах спорт-кары себя в полной мере не проявляют.

«ИКС»: Если говорить о сроках реализации проекта: мегаЦОД строить дольше, чем «обычный» дата-центр? Или срок реализации не зависит от размера объекта?

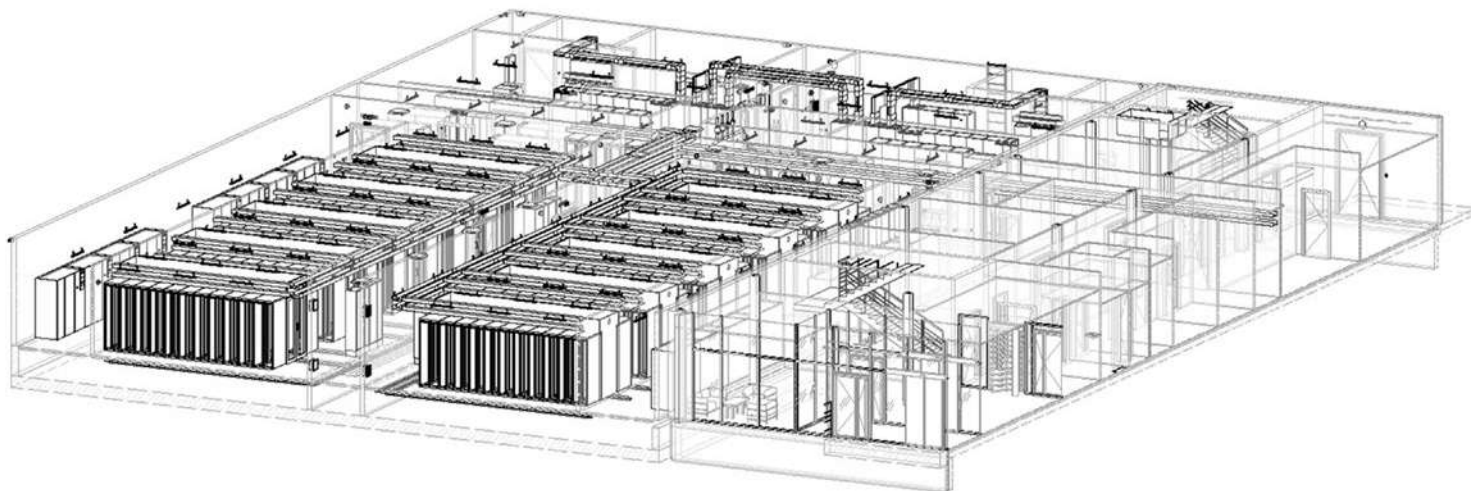
А.М.: Конечно, срок реализации проекта зависит от масштабов объекта, хотя и не линейно. При правильном планировании ЦОД на 3–5 тыс. стоек можно строить ненамного дольше, чем объект на 500 стоек.

Нельзя забывать и про пусковые комплексы, или этапы ввода. Если сначала строится первая очередь, например 1 тыс. стоек из 5 тыс. проектной мощности, то эти первые стойки выйдут на рынок несколько позже, чем при строительстве отдельного ЦОДа на 1 тыс. стоек, зато последующие будут готовы к запуску гораздо быстрее, чем в случае строительства ЦОДов по 1 тыс. стоек, причем с полноценным капстроением очередей.

«ИКС»: Каковы особенности подготовки к реализации проекта мегаЦОДа: подбор площадки, проектирование?..

А.М.: Особенности определяются масштабом проекта, конечно. Но факторов много: площадь земельного участка, ограничения, связанные с возможностью вести масштабное строительство, в том числе круглосуточно (в районе жилой застройки это невозможно), влияние на окружающую среду (выхлопы ДГУ прежде всего), на соседние строения и объекты (шум, тепло)... Нельзя забывать про подъездные дороги и их резервирование. Важно изучить возможность «приземлить» на участке несколько корпусов и строить некоторые из них, параллельно введя в штатную эксплуатацию часть мощностей.

Проект крупного ЦОДа, как правило, предусматривает этапы ввода проектных мощностей. Но часть инфраструктуры должна создаваться сразу, чтобы исключить влияние стройки на эксплуатацию.



Еще на этапе концепции и при последующем проектировании необходимо принимать во внимание множество нюансов. При выработке решений для масштабных проектов важно учитывать опыт эксплуатации и обслуживания подобных ЦОДов.

«ИКС»: Есть ли у мегаЦОДов преимущества по сравнению с небольшими объектами при подключении к электросетям?

А.М.: Несомненно, большой ЦОД – это большое энергохозяйство. Выбор уровня электрического напряжения и технических решений может оказать сильное влияние на стоимость и функционирование ЦОДа на этапе эксплуатации.

Широко известны на рынке проекты ЦОДов, в которых реализуется подключение к сетям высокого напряжения. Это означает дополнительные требования к площади и увеличение расходов на этапе строительства, но дает экономии на тарифах на этапе эксплуатации. Если смотреть на принимаемые решения с точки зрения общей стоимости владения, то переход на более высокое напряжение при подключении к сетям энергоснабжения может быть обоснован. Энергоснабжение больших ЦОДов – вопрос, в котором важны как технические, так и экономические детали.

«ИКС»: В чем особенности основных инженерных систем мегаЦОДа: охлаждения, электропитания? Сужается ли выбор решений на рынке, скажем, из-за того, что моделей ИБП сверхбольшой мощности меньше, чем просто мощных?

Евгений Колосков: По сути, любой мегаЦОД представляет собой несколько одинаковых модулей, каждый из которых является средним по размеру ЦОДом. То есть никаких дополнительных принципиальных ограничений на инженерные системы большие размеры ЦОДа не накладывают. Исключения, конечно, бывают, но они редки. Из особенностей можно выделить применение ДГУ на 10 кВ.

Имеет смысл также сделать акцент на следующей технической стороне инжиниринга крупного ЦОДа: когда мы проектируем мультимегаваттный объект, мы понимаем, что мощности будут вводиться в строй не все сразу, а поэтапно. То есть проектные решения, принятые в начале строительства, должны быть достаточно гибкими, чтобы сохранять актуальность в течение длительного времени. И вот тут проявляется инженерная смекалка и опыт. Мы готовим решения, которые позволяют, не затрагивая компоновку объекта, изменять параметры энергопотребления стоек, повышать надежность и уровень резервирования, локально использовать другие системы охлаждения. Конечно, гибкость имеет определенные границы, но для больших проектов она крайне важна. Это инструмент сбережения вложенных инвестором денег.

«ИКС»: Каков оптимальный размер машинного зала мегаЦОДа? Сейчас на рынке есть успешные проекты

дата-центров с залами на 1 тыс. стоек. Значит ли это, что выгодно строить крупный ЦОД как один машзал – скажем, на 5 тыс. или 10 тыс. стоек?

Е.В.: Нет какого-то одного оптимального варианта, иначе все ЦОДы строились бы под копирку. Очевидно, что наблюдается укрупнение машинных залов, но в нашей практике больше 500 стоек в зале пока не было. Укрупнение машзалов удобно тем, что можно более гибко размещать стойки разного уровня нагруженности. Ну и, конечно, с точки зрения резервирования систем большой машзал более выгоден, чем маленький.

«ИКС»: Крупный ЦОД – это всегда сверхнадежный ЦОД: Tier III или даже Tier IV? Или это не так, ведь ЦОДы гиперскейлеров имеют низкий уровень резервирования?

Е.К.: Надежность ЦОДа никак не привязана к его размеру, а диктуется исключительно потребностями клиентов и рыночным спросом.

Есть разные бизнес-модели и технические стратегии. Кто-то строит одну-две высоконадежные площадки. Кто-то осуществляет резервирование на уровне площадок, и поэтому на выход из строя любой из них смотрит много проще.

Одно можно сказать с уверенностью – миф о том, что Tier IV стоит гораздо дороже, чем Tier III, мы успешно развеяли. Накопленная экспертиза и освоенные уникальные инструменты дают возможность оптимизировать затраты на высоконадежные ЦОДы.

«ИКС»: Как вы считаете, будет ли сегмент мегаЦОДов за счет большей экономической привлекательности расти быстрее, чем сегмент небольших дата-центров?

Е.В.: На рынок выходят новые игроки, которые раньше никогда не строили ЦОДы. Игроки, готовые инвестировать большие деньги. Соответственно, количество крупных проектов растет. В качестве объекта недвижимости крупный ЦОД сегодня – очень привлекательный актив. Опять же есть ряд затрат, которые растут нелинейно с увеличением размеров ЦОДа, и чем крупнее ЦОД, тем меньше их удельный вес, что приводит в итоге к снижению стоимости стойки и возможности заработать больше при сдаче стоек в аренду или продаже объекта.

А.М.: Рынок будет развиваться в первую очередь именно за счет крупных проектов. Тому есть много причин, в числе которых – запросы клиентов на большие кванты ввода в эксплуатацию стоек и потенциал развития в рамках выбранной площадки. Нарастивать проектные мощности на существующей площадке гораздо удобнее и выгоднее.

В мире число гипер- и мегаЦОДов растет очень быстро, а масштабы отдельных объектов уже достигли гигаваттных мощностей.



Евгений Колосков,
технический директор, «Свободные Технологии Инжиниринг»



СВОБОДНЫЕ
ТЕХНОЛОГИИ
ИНЖИНИРИНГ

<http://sv-tech.ru>

ЦОД без наружных систем охлаждения

Фонтаны в качестве элемента климатической системы офисного ЦОДа позволяют избавиться не только от наружных систем охлаждения, но и от пересушенности воздуха в офисе, а заодно снизить уровень стресса сотрудников.

В современном мире сложно предложить просто офис в аренду в просто бизнес-центре. В условиях, когда 30% сотрудников и более то и дело должны работать дистанционно, предприятиям все чаще требуются серверы с удаленным доступом. Причем желательно, чтобы они располагались там же, где находится сам офис. И те бизнес-центры, которые в состоянии предложить пользование локальным мини-ЦОДом в составе комплекса предоставляемых услуг, оказываются у заказчиков в приоритете. Сегодня при выборе офиса наличие мини-ЦОДа «у дома» не менее важно, чем доступность парковочных мест.

Парадоксально, но при высокой востребованности такой услуги предложений на рынке пока немного. Почему?

Основной фактор, тормозящий развитие мини-ЦОДов формата «у дома», – сложность размещения наружных систем охлаждения. Владельцы бизнес-центров ни в коем случае не готовы устанавливать их на красивом, разработанном ведущими архитекторами фасаде. При этом локальный мини-ЦОД стараются расположить на площадях, которые трудно сдать в аренду под офисы. В основном это подвальные/полуподвальные помещения. Вот тут и возникают сложности с размещением наружных блоков. Хорошо, если в здании есть технический этаж и решетки, обеспечивающие воздухообмен, тогда наружные блоки, пусть и сильно переразмеренные, можно установить там. Хуже, если для размещения наружных систем охлаждения отдают крышу. Как правило, в этом случае длина трасс систем фреонового охлаждения мини-ЦОДа становится критичной. А что делать, если даже крышу бизнес-центра использовать под наружные системы нельзя?

Современные небоскребы

Давайте вспомним черно-белые фильмы. Сколько в них было великолепных фонтанов! Многие из них прекрасно дожили до наших

дней. Мы любим рассказывать друг другу о замечательной умиротворяющей атмосфере фонтана Треви в Риме или о величественных фонтанах в Версале, Нимфенбурге, Петергофе. И забываем о том, что раньше фонтаны не только служили украшением, но и прежде всего являлись частью системы охлаждения. Сегодня фонтаны стали новейшим трендом оформления бизнес-центров в Западной Европе.

Цены на офисы в крупнейших мегаполисах Европы стремительно растут, несмотря на пандемию и связанные с ней требования удаленной работы. Увеличивается плотность работников на квадратный метр, а вместе с ней и стресс, которому офисный работник подвергается ежедневно. Одним из способов снижения стресса и в буквальном смысле улучшения микроклимата в офисе стали фонтаны.

Тоска по тишине

Не секрет, что большие команды работают более продуктивно и с меньшим бюрократизмом, занимая одно большое помещение, а не отдельные маленькие комнаты. Кроме того, вызванный пандемией кризис заставил многие компании переехать в офисы меньшей площади и «уплотнить» сотрудников, увеличив количество людей на квадратный метр. Шум, вызываемый разговорами и работой оргтехники, мешает сосредоточиться. В такой обстановке сложно разговаривать по телефону, особенно если приходится говорить на иностранном языке. Эксперты Калифорнийского университета еще в 2018 г. провели исследование, в котором приняли участие порядка 20 тыс. человек, и пришли к неутешительным выводам: работнику, которого отвлекли от решения задачи, в такой обстановке понадобится минимум 23 мин, чтобы снова на ней сконцентрироваться. Представьте, сколько времени ежедневно в подобном офисе должен тратить работник на выполнение своих обязанностей, как часто его будет что-то отвлекать. Неудивительно, что решение рабочих задач иной раз растягива-

Александра Эрлих,
генеральный директор,
Анна Галкина,
руководитель консультационного центра,
«ПрофАйТи-Кул»





ется на значительно более долгое время, чем это позволяют условия конкуренции.

Шум голосов в больших помещениях часто разносится на расстояние до 18 м. В отличие от глаз, мы не можем закрыть уши и отвлечься от посторонних шумов. Биологически мы устроены так, что шум подсознательно воспринимается как сигнал возможной опасности и, как бы мы ни старались, наш мозг постоянно будет отвлекаться на такие сигналы. Даже если использовать беруши или специальные наушники, мы будем продолжать «слышать» шум, воспринимая его через движения, на уровне биополя.

Проблема известна давно, и ее пытались решить по-разному: от установки шумопоглощающих экранов до специальных электронных «ловушек шума», которые, к сожалению, генерируют сильное электромагнитное излучение, негативно влияющее на мозг человека. Пробовали выдавать сотрудникам наушники, заставляя работать в них, пробовали устанавливать изолированные телефонные кабинки. Все меры имели свои негативные последствия.

В 2017 г. одно немецкое предприятие впервые использовало совершенно естественный способ гасить шум в офисе: фонтаны. Толчком для принятия решения стала, как ни странно, старая теория биополей, которой в то время увлекся владелец компании. Напомню: согласно этой теории, каждый человек создает вокруг себя некое биополе, и мы общаемся не только ментально, но и на уровне биополей. Зачастую именно совместимость или, наоборот, несовместимость биополей определяет наше отношение к тому или иному человеку. Так вот, по все той же теории биополей, отношения человека и воды всегда позитивны. Нас успокаивает шелест волн, шум во-

допада, стук дождевых капель по листве, например. Когда мы хотим отвлечься от проблемы и переключиться, мы часто стремимся попасть к воде. Чем больше водоем, тем лучше. Мы словно чистим свое биополе рядом с водой. Скажете, пахивает битвой экстрасенсов? Точно так же скептически была воспринята идея в консервативной Германии. Но небольшое новаторское немецкое предприятие не испугалось скептиков и поместило воду в офисе. В виде фонтанов.

Системы охлаждения ЦОДа фонтанами

Несмотря на то, что развитие систем охлаждения дата-центров постепенно смещается в сторону свободного охлаждения, требования к уровням влажности и запыленности, а также регион размещения дата-центра зачастую не позволяют полностью отказаться от внутренних замкнутых систем охлаждения, таких как фреоновая или водоводяная (она же водогликолевая).

В чем заключается особенность охлаждения именно дата-центров? В основном – в довольно высоком температурном графике холодоносителя, будь то вода, раствор гликоля или фреон. Причем тенденция такова, что с каждым годом температура нормальной работы ИТ-оборудования становится все выше, а это, в свою очередь, означает, что при прочих равных условиях (например, месте размещения) с каждым годом требуется все меньше наружного/уличного оборудования. То есть фактически за счет увеличения температурного напора* между холодоносителем и окружающей средой, в которую мы хотим отвести тепло нашего дата-центра, нам необходимо все меньше условной площади поверхности теплообмена. Почему площадь теплообменной поверхности условная? Все мы так или иначе привыкли к градирням/драйкулерам/выносным конденсаторам, которые имеют определенную площадь теплообменной поверхности, но если эту часть системы заменить на фонтан, то понятие площади становится действительно условным, поскольку площадью поверхности теплообмена будет площадь соприкосновения водяной глади и воздуха.

Как видите, принципиально схема системы охлаждения ЦОДа на основе фонтанов практически не отличается от классической схемы охлаждения. За одним-единственным исключением: вместо наружных градирен используются офисные фонтаны. Эффект охлаждения тот же, что у мокрых градирен. Вода охлаждается в падении. Чем длиннее и извилистее путь воды, тем силь-

* Температурный напор – это разность между средней температурой холодоносителя и температурой охлаждающего его агента. Например, если воздух с температурой 35°C охлаждает воду с графиком 50/46°C, то температурный напор составит: $(50 + 46)/2 - 35 = 13^\circ\text{C}$.



нее эффект охлаждения. Однако, в отличие от мокрых градирен, офисный фонтан находится внутри помещения, где исключены скачки влажности. Наоборот, благодаря большой концентрации оргтехники воздух в офисе всегда сухой, даже слишком. Отчего эффективность применения фонтанов в системе охлаждения становится еще выше. Можно даже предотвратить унос воды в системе, устанавливая фонтаны закрытого типа. Правда, при этом теряются эффект увлажнения и звук падающей воды.

Какие же преимущества с точки зрения именно охлаждения дает это решение? Прежде всего всю систему можно разместить внутри здания, а это означает, что можно обойтись без раствора гликоля. Кроме того, с каким бы потрясающим КПД мы не выбрали теплообменник, все равно всегда присутствует паразитное термическое сопротивление стенки, или, говоря проще, потери по температуре. Сравним температурные режимы традиционных систем и систем с фонтанами, исходя из того, что минимальные допустимые законами физики потери температуры на теплопередачу составляют 3К. Если мы рассматриваем систему с фреоновым кондиционером и выносным конденсатором с температурой конденсации 50°C при температуре воздуха на улице 32°C по сухому и 21°C по мокрому термометру, то температурный напор у нас составит 12°C. В системе же с водоводяным чиллером и мокрой градирней закрытого типа в контуре «градирня/конденсатор» чиллера будет циркулировать раствор гликоля с графиком 47/42°C максимум (температура конденсации фреона – 50°C), т.е. максимальный температурный напор составит 20,5°C.

Эти два варианта системы несколько идеализированы. В аналогичных условиях открытым

фонтаном мы можем охладить воду до 21°C, т.е. до температуры мокрого термометра. Если бы мы, скажем, охлаждали фонтаном жидкость с графиком 47/42°C, то температурный напор составлял бы уже не 20,5°C, как в предыдущем случае, а 23,5°C. С другой стороны, при 21°C по мокрому термометру мы легко можем получить при помощи фонтана график 26/21°C. Жидкостью с таким температурным графиком можно охладить ЦОД до 27°C, а при очень большом желании, и что уж душой кривить, почти неограниченных габаритных размерах оборудования – и до 24°C, причем напрямую, без чиллеров и компрессоров.

Если же посмотреть на систему через призму реальности, вернувшись все-таки к компрессорной технологии, то можно говорить о температурном напоре в 26,5°C (при расчетной температуре конденсации 50°C). Это открывает большие возможности для уменьшения мощности охлаждающего оборудования и, как следствие, CAPEX системы охлаждения. Но самое приятное – неважно, какую систему охлаждения в мини-ЦОДе формата «у дома» вы предпочитаете: фонтаны можно использовать как во фреоновой, так и в водоводяной системе. Вы можете охлаждать помещение машзала прецизионниками, холодными стенами, подфальшпольными ВОПами – все эти элементы прекрасно сочетаются с офисными фонтанами. Систему можно сделать бесконечно надежной: фонтаны резервируются точно так же, как и любые наружные элементы системы охлаждения. При использовании офисных фонтанов закрытого типа даже не нужно резервировать источники воды: как в самой обычной водоводяной системе, вода циркулирует по замкнутому контуру и нигде не исчезает. И никаких наружных систем охлаждения. ИКС



Инновации ABB в ЦОДах 3data

Флагманский дата-центр «Э2» компании 3data стал первым объектом в России, на котором установлены новые ИБП DPA 250 четвертого поколения от компании ABB. О сотрудничестве сети ЦОДов и вендора – Максим Церулев, технический директор 3data, и Виталий Морозов, руководитель направления «ЦОД и телеком» ABB.



Максим Церулев



Виталий Морозов

«ИКС»: Расскажите, пожалуйста, об истории сотрудничества 3data и ABB.

Максим Церулев: С компанией ABB мы работаем с самого первого нашего объекта, на котором было установлено электрощитовое оборудование этого производителя. Оно хорошо себя зарекомендовало, более того, по соотношению «цена – качество» считаю его оптимальным на рынке.

Планируя ЦОД «Э2» на шоссе Энтузиастов, мы решили использовать и другое оборудование ABB, в том числе ИБП. Одна из причин – архитектура устройств. ABB – один из немногих вендоров, который предлагает действительно модульные ИБП: каждый модуль – независимый, а общий корпус – простое механическое изделие, где ломаться нечему.

Привлек и высокий КПД: около 97,5%. Мы бережно относимся к энергетическим ресурсам, поэтому стараемся использовать их максимально эффективно. Кроме того, высокий КПД источников бесперебойного питания означает, что место их установки не потребует оборудовать дорогостоящей системой охлаждения – на этом тоже можно сэкономить.

Виталий Морозов: В ЦОДе «Э2» все основное энергетическое оборудование, за исключением ДГУ, – производства ABB: от ГРЩ и ВРУ до устройств вторичного распределения электропитания в машзалах. Причем все распределительные устройства оснащены самыми современными цифровыми функциями, в том числе функциями измерения и мониторинга. А установка ИБП DPA 250 S4 стала первой в России.

«ИКС»: Не рискованно ли быть пионером?

М.Ц.: Опасения, конечно, были. Но когда мы убедились, что ИБП основаны на надежных, проверенных временем схмотехнических решениях, они рассеялись. Новые устройства построены на архитектуре, которая известна своей надежностью.

В.М.: Децентрализованная параллельная архитектура (DPA) – основа наших ИБП. Устройства, построенные на такой архитектуре, установлены на сотнях объектов в России, включая коммерческие и корпоративные ЦОДы. На ряде объектов такие ИБП успешно функционируют уже более 10 лет.

Архитектура DPA предусматривает, что каждый силовой модуль является законченным ИБП. Он содержит все компоненты классического онлайнowego ИБП. Более того, к каждому модулю можно подключить собственную аккумуляторную батарею. Отсюда максимальная надежность: да-

же маловероятный выход из строя любого из модулей никак не повлияет на обслуживание нагрузки. А заменить модуль может один человек без специнструмента.

«ИКС»: Насколько важна модульность решений современным ЦОДам?

М.Ц.: Модульность позволяет вводить в эксплуатацию системы по мере роста нагрузки, вкладывая средства тогда, когда необходимо. Правда, сегодня, когда площади ЦОДов в Москве раскупаются, как горячие пирожки, возможность плавного наращивания мощностей менее важна. Так, для нашего нового ЦОДа мы сразу заказали все модули ИБП, понимая, что проблем с утилизацией площадей не будет – большая часть стойко-мест находит покупателей еще на стадии строительства.

Но, несмотря на это, модульная архитектура сохраняет свои преимущества с точки зрения гибкости расширения и резервирования. Модульные ИБП обеспечивают более высокую плотность (с учетом резервирования), на их основе проще реализовать более высокий уровень отказоустойчивости. А если на одном объекте что-нибудь случится, можно взять модуль с другого и привезти даже на легковой машине.

В.М.: Хочу заметить, что принцип модульности реализован и в других продуктах ABB, в частности, в установленной в ЦОДе «Э2» системе SMISLINE TP – это первая в мире втычная шинная распределительная система, позволяющая менять устройства и компоненты под напряжением. В ЦОДе «Э2» она установлена в RPP-стойках, обеспечивающих распределение электропитания в машзале, и дает возможность быстро и безопасно менять автоматы и их фазировку без прерывания электропитания.

«ИКС»: На каких уровнях реализованы функции измерения и мониторинга в системе электроснабжения ЦОДа «Э2»?

В.М.: На всех уровнях. Начиная с уровня ГРЩ и ВРУ и заканчивая уровнем распределения электропитания в машзалах, включая АВР и ИБП. В шкафах распределения в машзалах установлены анализаторы сети M4M, а также система мониторинга токов на базе модуля CMS-700.

В системе распределения ЦОДа «Э2» установлено цифровое оборудование ABB, являющееся основой для построения комплексного цифрового решения ABB Ability Energy and Asset Manager на базе облачной платформы ABB Ability, которое было разработано для сбора и анализа

параметров электросети и состояния оборудования. В настоящий момент передача данных осуществляется в локальную систему управления компании 3data, но при необходимости легко можно внедрить облачную систему, путем установки специального шлюза и оформления подписки.

Из всего цифрового комплекса мониторинга хочу особо отметить систему CMS. В коммерческих ЦОДах важно измерять энергопотребление на уровне стойки. Традиционно для этого устанавливают достаточно дорогостоящие PDU с такой функцией. Мы предлагаем осуществлять измерения централизованно – на уровне распределительного шкафа машзала (RPP-стойки). Суть системы CMS проста: на каждом полюсе автоматов в распределительном щите монтируется недорогой датчик тока, который и позволяет производить измерения. Подчеркну универсальность системы: она не привязана к втычным автоматам, может использоваться и с другими решениями, причем не только от ABB.

М.Ц.: Да, система мониторинга мощности на уровне распределительных щитов – одно из важных преимуществ решения ABB. Благодаря ей можно отказаться от покупки «умных» PDU. Даже реализовав резервирование, мы получили примерно четырехкратный выигрыш в стоимости этой системы. Наряду с экономией средств и сокращением числа кабелей решение позволяет меньше лазить в серверные стойки, что повышает операционную устойчивость ЦОДа.

«ИКС»: Какие еще технические решения ABB, установленные в ЦОДе 3data, можно отметить?

В.М.: Как я уже говорил, этот ЦОД вообрал в себя многие инновации ABB. В их числе – новый автомат ввода резерва (ABP) TruONE. Соленоидный принцип переключения, а также интеграция силовой части и контроллера в одном корпусе обеспечивают низкое время переключения – время токовой паузы при обратном переключении менее 50 мс. Конечно, как и другие элементы цифровой системы ABB, это устройство обладает возможностью измерения параметров сети, передачи данных в ABB Ability и интеграции с этой системой.

На уровне ГРЩ/ВРУ установлены воздушные автоматические выключатели Emax2. Их особенность – возможность настройки двойных уставок, такого функционала нет ни у кого из других производителей. Поясню функцию двойных уставок на примере. Одна из задач воздушных автоматических выключателей – как можно дольше «держат» ток короткого замыкания. Но если с оборудованием работают люди, то задача обратная: надо провести отключение как можно быстрее. Поэтому, если дверь шкафа, где расположен щит, открыта (т.е. с ним работают люди), система задействует другие уставки – на максимально быстрое отключение. Это может спасти жизнь людям.

Также отмечу программные продукты ABB, которые сильно облегчают работу проектировщиков. Эти продукты позволяют, в частности, быстро рассчитать тепловые режимы и построить карту селективности по всей электрической цепочке. 3data размещает свои ЦОДы в уже существующих зданиях, при этом в ходе проектирования могут меняться схемы подключения к городской сети и другие параметры. Наши выделенные инженеры по ЦОДам и программы дают возможность максимально быстро провести все необходимые пересчеты, что ускоряет проектирование.



«ИКС»: Каковы дальнейшие планы сотрудничества?

М.Ц.: По состоянию на август 2021 г. подведенная к ЦОДу «Э2» мощность равняется 720 кВт. Но уже к октябрю ее планируется увеличить до 1,1 МВт. Поступление необходимых модулей ИБП мы ожидаем в ближайшее время. Проект оказался успешным, ИБП DPA 250 S4 хорошо себя показали, поэтому для нашего следующего ЦОДа, строящегося на Алтуфьевском шоссе, мы выбрали эти же ИБП. И два из них уже приняли на площадке.

Как известно, одинаковых ЦОДов не бывает. Поэтому и для нового ЦОДа решение было доработано. В частности, если объект на шоссе Энтузиастов рассчитан на установку стоек средней мощностью 5,5 кВт, то в новом дата-центре этот показатель увеличен до 7,5 кВт.

В принципе я сторонник унификации оборудования. Так, для систем кондиционирования придерживаемся продукции Stulz – мы устанавливаем ее на всех объектах, и она ни разу не подвела. Как уже говорилось, электрощитовое оборудование у нас с самого первого объекта тоже одного вендора – ABB. Теперь и ИБП ABB будут на двух объектах, что упростит задачу эксплуатации и поддержания ЗИПа.

В.М.: Видите, у нас общие предпочтения: Stulz является и нашим добрым партнером. В тех странах, где ABB предлагает ЦОДы под ключ, мы используем климатическую технику этого производителя.

На российском рынке цодостроения планы ABB понятны: рынок устойчиво растет, и мы стремимся наращивать нашу долю на нем. Мы усиливаем команду по ЦОДам новыми сотрудниками, выводим на рынок новые продукты: ИБП для крупных ЦОДов DPA Megaflex на 1500 кВт, новые автоматические выключатели Tmax в литом корпусе, которые мы скоро ожидаем, систему InSite для мониторинга модульных автоматов и т.д.

ABB

www.abb.ru

Оцениваем площадь и состав помещений крупного ЦОДа

Андрей Павлов,
генеральный директор,
Максим Матвиенко,
главный инженер проекта,
«ДатаДом»

Какова должна быть площадь ЦОДа, чтобы на ней расположились и машинные залы для ИТ-оборудования заданной мощности, и различные технические и вспомогательные помещения, необходимые для функционирования всего объекта?

На самых ранних этапах проработки проекта ЦОДа, еще на этапах концепции и эскизного проектирования, будущий цодовладелец задается вопросом, какую площадь должно иметь здание для дата-центра и какова должна быть площадь земельного участка для него. Безусловно, эти характеристики индивидуальны для каждого объекта, но существуют некоторые закономерности и обязательные требования.

В каждом ЦОДе, помимо машинных залов, есть множество технических и вспомогательных помещений. И если на небольшом объекте часть из них можно объединить или не создавать, то в крупном ЦОДе их перечень достаточно стабилен и предопределен особенностями функционирования.

Общая оценка площади ЦОДа

В качестве примера будем рассматривать один крупный ЦОД, в проектировании которого мы принимали участие. Его характеристики:

- мощность ИТ-оборудования – 15 МВт;
- общая площадь здания – 28 тыс. кв. м;
- площадь машинных залов с учетом помещений для установки внутренних блоков кондиционеров – 6 тыс. кв. м;
- площадь участка под застройку – 17,5 тыс. кв. м.

Исходя из этих данных, можно вычислить среднюю ИТ-нагрузку на 1 кв. м машинных залов. Она равна $15000 \text{ кВт} / 6000 \text{ кв. м} = 2,5 \text{ кВт/кв. м}$, и это практически типовое тепловыделение для современных коммерческих ЦОДов ($2\text{--}2,5 \text{ кВт/кв. м}$). При этом площадь, приходящаяся на одну стойку, составляет около 5 кв. м (в ЦОДе установлено порядка 1250 стоек со средним потреблением 12 кВт каждая). Такая большая площадь на одну стойку при обычном значении $2\text{--}2,5 \text{ кв. м}$ – это вынужденная мера, обусловленная желанием заказчика раздавать холодный воздух из-под фальшпола в достаточном количестве в любом месте машинного зала, что повлекло за собой организацию холодных коридоров шириной намного больше стандартных 1,2 м.

При использовании межрядных кондиционеров этот параметр можно было бы снизить до менее чем 3–4 кв. м и еще больше повысить плотность тепловыделения залов, но для заказчика первоочередным требованием была максимальная гибкость в установке серверного оборудования с различными габаритами монтажных стоек, что плохо сочетается с применением межрядных кондиционеров.

Если исходить из характеристик наших предшествующих проектов, то для машинных залов площадью 6 тыс. кв. м следовало бы запланировать технические и вспомогательные помещения примерно вдвое большей площади. То есть общая площадь здания составила бы порядка 18 тыс. кв. м. Но в нашем случае здание имело площадь 28 тыс. кв. м, что в более чем в полтора раза превышает расчетную величину. Чем это вызвано?

Дело в том, что площадь прилегающей территории весьма скромная, и поэтому чиллеры наружной установки разместили на кровле, а трансформаторную подстанцию (ТП) 20/0,4 кВ и ДГУ – внутри здания, что повлекло за собой существенное увеличение его площади.

Так, на прилегающей территории могло бы расположиться оборудование ДГУ и ТП, помещения для которых заняли в здании 2,5 тыс. кв. м., а также АКБ (порядка 5 тыс. кв. м.). (Место под чиллеры на кровле площадью 7 тыс. кв. м в расчет не включаем.) Соответственно при вынесении помещений ДГУ, ТП и АКБ на прилегающую территорию площадь здания сократилась бы на 7,5 тыс. кв. м и составила около 20,5 тыс. кв. м, а площадь застройки с учетом путей проезда и прохода между оборудованием увеличилась бы на 14,5–20 тыс. кв. м – до 37 тыс. кв. м. Эти цифры гораздо лучше коррелируют с нашими предшествующими расчетами площади здания ЦОДа и прилегающей территории.

Для первичной оценки необходимой площади здания и земельного участка при строительстве ЦОДа мы используем следующие формулы:



$$\frac{\text{Площадь машинного зала}}{\text{Общая мощность ИТ-систем}} = \frac{2-3 \text{ кВт/кв. м}}{2-3 \text{ кВт/кв. м}}$$

либо

$$\frac{\text{Площадь машинного зала}}{\text{Количество стоек} \times 2-5 \text{ кв. м на одну стойку}^*}$$

$$\frac{\text{Площадь здания}}{\text{Площадь машинного зала} \times (3-4)}$$

$$\frac{\text{Площадь участка для строительства ЦОДа}}{\text{Площадь здания} \times (2-2,5)}$$

Безусловно, формулы можно использовать с рядом оговорок. Мы предполагаем, что здание будет иметь не более трех-четырех этажей. Административно-бытовой комплекс предусматривает размещение разумно достаточного количества персонала для поддержания текущего функционирования объекта, без перевода в него всего департамента разработки предприятия. Площади складских и иных вспомогательных помещений также ограничены разумными рамками. Тем не менее формулы помогут хотя бы в первом приближении понять, какой площади здание и земельный участок нужны для планируемого объекта.

Помещения ЦОДа

Все помещения дата-центра мы делим на два крупных подмножества – основные технические (помимо собственно машинного зала) и вспомогательные.

Основные технические помещения ЦОДа

Помещения механических систем (охлаждения, отопления и вентиляции):

- венткамера, в которой располагается оборудование технологической вентиляции ЦОДа;
- водомерный узел/насосная;
- индивидуальный тепловой пункт;
- помещение водоподготовки;
- помещение охлаждающих установок машинных залов (в рассматриваемом примере внутренние блоки системы кондиционирования были вынесены за пределы машинных залов из соображений безопасности, что потребовало размещения их в отдельном помещении с ограниченным доступом персонала. Эти площади мы включили в площадь машинных залов);
- форкамера – камера смешения воздуха для поддержания нужной его температуры при поступлении к дизель-генераторным установкам;
- холодоцентр – помещения, где располагаются насосные группы и системы управления гидравлическим контуром системы охлаждения.

* Чем крупнее ЦОД, тем площадь в расчете на одну стойку мощностью 5–6 кВт ближе к 2 кв. м, но при увеличении мощности стойки работает обратный тренд – удельная площадь стремится к 5 кв. м и более.



Энергия интеллекта

Ведущее аналитическое агентство России и СНГ в сфере телекоммуникаций, ИТ и медиа

- Аналитика
- Стратегии
- Бизнес-планирование
- Информационно-аналитическая поддержка
- Потребительские опросы в B2C и B2B сегментах



Лондон



Киев



Москва



Алматы

ИТ

Телеком

Медиа

Контент и сервисы

Системная интеграция

Голосовые услуги

Платное ТВ

Навигация и LBS

Дата-центры

ШПД

Мобильное видео

M2M

Облачные сервисы

Мобильный интернет

Игры

NFC

ИТ инфраструктура

VAS

Интернет-порталы

E-commerce

Офисная техника

Межоператорские услуги

Видео-контент

Теле-медицина



В нашем случае помещения механических систем заняли 4,6 тыс. кв. м, т.е. примерно 75% площади машинных залов.

Телекоммуникационные помещения:

- кроссовые помещения для оборудования пассивной коммутации СКС;
- серверные помещения для активного оборудования ЛВС;
- помещение антенно-фидерной связи;
- помещения оптического ввода в здание.

Телекоммуникационные помещения заняли 1 тыс. кв. м (15% площади машзалов).

Помещения систем безопасности:

- станции АУГПТ. В проекте были предусмотрены несколько центральных станций газового пожаротушения, а также несколько локальных – для обслуживания серверных и кроссовых помещений;
- центральный пост безопасности комплексной системы безопасности, в котором размещаются оборудование и операторы систем безопасности здания.

Эти помещения не требуют больших площадей и заняли 500 кв. м, менее 10% площади машзалов.

Помещения энергетических систем:

- помещение ДГУ;
- помещение загрузки трансформаторов;
- помещение РУ 20 кВ;
- трансформаторная;
- электрощитовые (ВРУ, ГРЩ и этажные щитовые);
- помещения ИБП и АКБ.

Наряду с системами холодоснабжения энергетические системы – одни из наиболее объемных, они заняли 4,5 тыс. кв. м – 75% площади машзалов.

Центральный диспетчерский пульт – сердце ЦОДа, где собирается информация о его состоянии и размещается оперативный инженерный персонал. Его площадь составляет 5% площади машзалов (300 кв. м).

Вспомогательные помещения ЦОДа

Административные помещения. К этой категории относятся кабинеты руководителей, переговорная и учебный класс.

В нашем примере эти помещения заняли около 1 тыс. кв. м, т.е. 15% площади машзалов.

Технические помещения. В эту категорию входят помещения, в которых располагаются рабочие места технического персонала:

- администраторов комплексной системы безопасности;
- главного инженера;
- группы немедленного реагирования;
- оператора СКС;
- подрядчиков;
- механиков;

- электриков;
- электромехаников;
- уборщиц.

Сюда же относятся помещения, в которых проводятся оперативно-диспетчерские, ремонтные и организационные мероприятия:

- помещение для проведения оперативных совещаний;
- помещение современных технологий;
- мастерская;
- помещение распаковки оборудования;
- помещение административно-хозяйственных служб.

Все эти помещения заняли около 1,5 тыс. кв. м (25% площади машзалов).

Складские помещения:

- склады ЗИП и прибывшего технологического оборудования;
- склад оргтехники;
- склад контрольно-измерительной аппаратуры;
- помещение уборочного инвентаря;
- склад постовой одежды;
- помещение для сушки и хранения одежды и обуви;
- помещение временного накопления мусора.

На крупных объектах каждой службе целесообразно выделять под разные цели хранения отдельные помещения, и в таком случае соответствующие помещения вносят весомый вклад в общую площадь объекта – 60% площади машзалов (3,5 тыс. кв. м).

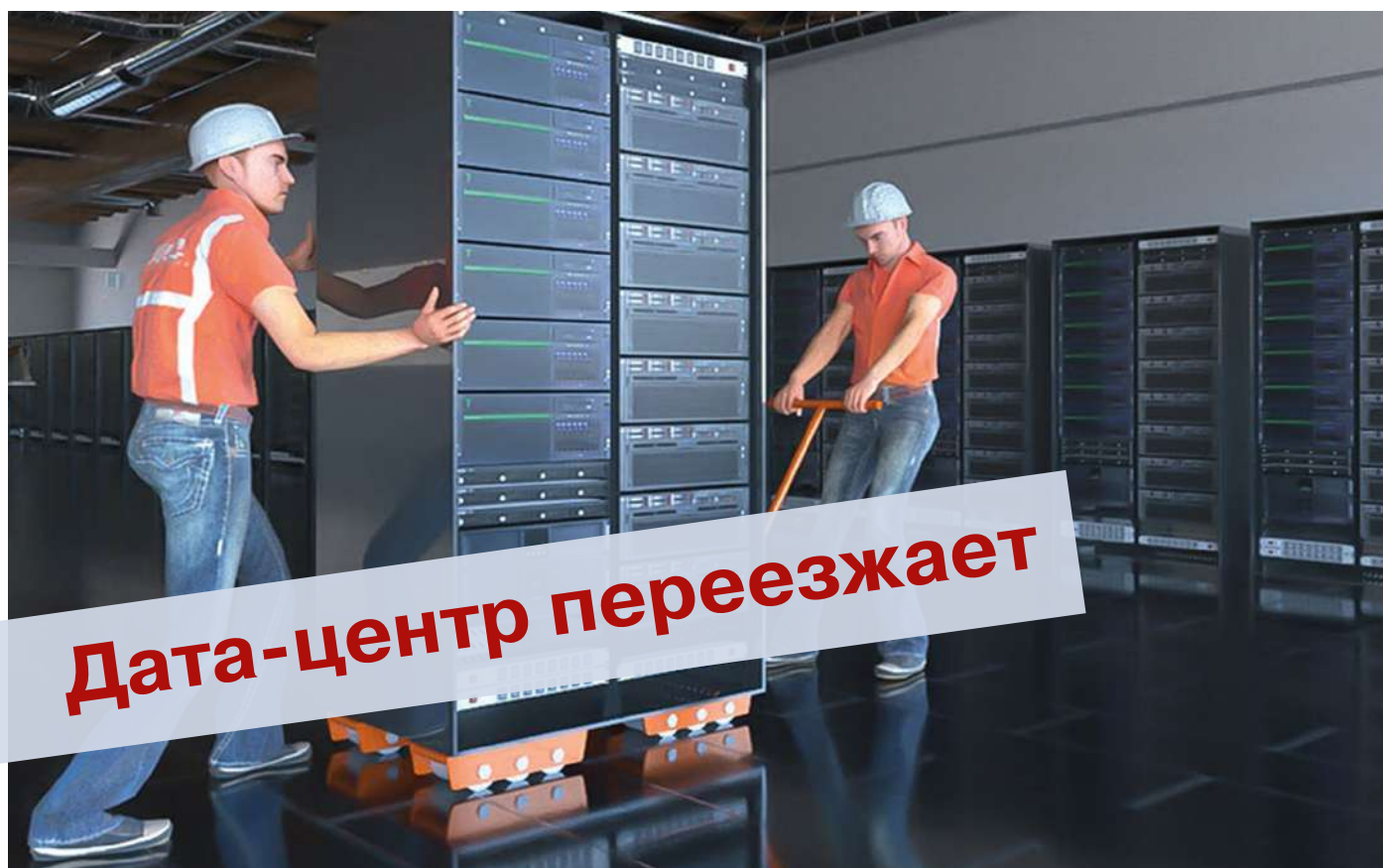
Помещения персонала. Сюда входят раздевалки, душевые, помещение приема пищи, санузел.

Эти помещения вносят незначительный вклад в общую площадь ЦОДа, в нашем случае – порядка 500 кв. м, и то лишь по причине большой этажности объекта и наличия большого количества непрофильного персонала и гостей на территории объекта.

Места общего пользования: тамбур, вестибюль, гардероб, лифтовый холл, лестничная клетка, коридор.

Эти помещения, относящиеся как к технологическим, так и к административно-бытовым, хотя и играют наименее важную роль в функционировании инженерных систем ЦОДа, но занимают существенную долю площади здания, равную примерно 75% площади машзалов (4,5 тыс. кв. м).

Как и предыдущие наши работы, эта статья не претендует на истину в последней инстанции. Но, возможно, рассказ о площади и функционале помещений на примере крупного корпоративного ЦОДа поможет читателю оценить свои потребности при строительстве собственного объекта. **ИКС**



Дата-центр переезжает

Перенос ИТ-ресурсов компании в коммерческий ЦОД – проект, требующий всесторонней проработки: от заключения договора с провайдером, определения порядка размещения оборудования и организации линий связи до настройки регламентов и бизнес-процессов на новой площадке.

Как показывает практика, при переносе ИТ-систем на другую площадку компании наталкиваются на множество подводных камней, и предварительное тщательное планирование столь хлопотного процесса – это 80% его успеха. Что же важно не упустить из виду, готовясь установить свое оборудование в коммерческом дата-центре? Приведенные ниже рекомендации сформировались в ходе консультаций и обсуждений с организациями, планировавшими переезд в ЦОД.

Будем исходить из того, что компания уже выбрала дата-центр, подходящий по местоположению, декларируемому уровню надежности (Tier), присутствию операторов связи, стоимости услуг и множеству других параметров, вплоть до дружелюбного отношения, квалификации и клиентоориентированности персонала ЦОДа.

С чего начать?

Как правило, на период переезда создается рабочая группа, в которую помимо ИТ-специалистов включаются финансисты, представители административного и HR-блоков, коммерсанты и юристы. Это обусловлено немалыми затрата-

ми и потенциальными рисками, которые могут и должны оценить все участники рабочей группы и которые особенно велики при высоком уровне цифровизации деятельности компании. Снизить риски, сопряженные с переездом, поможет привлечение в рабочую группу специалистов выбранного дата-центра.

В период, предшествующий переезду, с провайдером услуг ЦОДа прорабатывается договор на размещение ИТ-оборудования. Для уточнения деталей советуем попросить провайдера организовать для вас экскурсию по дата-центру. Это обычная практика, которая соответствует политике открытости большинства коммерческих ЦОДов.

Хорошие отношения – с хорошим договором

Отношения с провайдером оформляются договором на оказание возмездных услуг ЦОДа, в котором учитываются действующие на объекте регламенты, политики и процедуры.

На этапе запроса технико-коммерческого предложения (ТКП) у провайдера выбранного вами ЦОДа и подписания с ним соглашения о конфи-

Людмила Старикова,
независимый эксперт
Владимир Назаренко,
независимый эксперт

денциальности (до принятия решения о подписании договора) рекомендуем также запросить:

- регламенты информационной безопасности;
- сертификаты соответствия различным рекомендациям и стандартам, применяемым для ЦОДов;
- план обеспечения непрерывности бизнеса и план аварийного восстановления, принятые в ЦОДе;
- проект договора об оказании услуг ЦОДа;
- соглашение об уровне обслуживания (Service Level Agreement, SLA);
- технические условия (ТУ);
- регламенты удаленного, круглосуточного, простого/оперативного техобслуживания оборудования заказчика, а также квалифицированного удаленного администрирования.

Целесообразно выбирать провайдера, у которого в системе договоров с заказчиком имеется SLA. В SLA фиксируются показатели качества услуг colocation, гарантирующие бесперебойное энергоснабжение и поддержание температурно-влажностного режима, который предусмотрен рекомендациями ASHRAE – 2011 TC9.9, и система компенсаций за их нарушение. Как правило, обсуждение этих вопросов – центральный пункт преддоговорной работы.

Договор с провайдером должен регламентировать процедуру обработки запросов. В большинстве современных ЦОДов применяются системы управления запросами заказчиков (тикетные системы), которые документируют деловую переписку по каждому запросу в нумерованный тикет – электронный документ (аналог медицинской карты в поликлинике), позволяющий регистрировать всю информацию: суть запроса, действия персонала ЦОДа, инциденты, результаты проведения работ и оказания дополнительных услуг администрирования, а также следить за соблюдением SLA и текущим статусом исполнения каждого запроса службой поддержки клиентов ЦОДа в процессе параллельной обработки потока поступающих запросов.

Кроме того, полезно ознакомиться:

- с годовым графиком технического обслуживания оборудования инженерных систем ЦОДа, при котором возможны отключение энергоснабжения или остановка систем охлаждения стоек;
- системами технического учета оборудования, принимаемого в ЦОД, и учета соединительных линий и технических параметров стоек. В большинстве ЦОДов для технического учета применяются кабельные журналы и ИТ-системы собственной разработки. Лучшие практики техучета подразумевают использование системы DCIM или базы данных управления конфигурациями и связями, адаптированной к инфраструктуре ЦОДа;

- системами охранного телевидения, СКУД и процедурами обеспечения информационной и физической безопасности;

- правилами посещения ЦОДа и проведения работ с оборудованием во время посещения. Эти правила накладывают ряд ограничений на проведение отдельных видов работ непосредственно в машинном зале. Например, не разрешается снимать крышку с демонтированного из стойки оборудования. Для этого оборудование нужно перенести в специальную клиентскую комнату.

Как размещаться на новой площадке?

Один из основных вопросов при переезде – где именно будет размещено ИКТ-оборудование: в арендованных у провайдера стойках-шкафах или в собственных стойках, которые вы хотите перевезти? От этого решения будут зависеть состав и стоимость заказываемых услуг, а следовательно, и операционные затраты, включаемые в бизнес-план переезда.

Для расчета затрат на услуги ЦОДа целесообразно провести инвентаризацию ИТ-оборудования, которое планируется переместить. В запросе ТКП, направляемом провайдеру, нужно указать потребность в стойко-местах, арендуемых стойках, соединительных линиях и прочих услугах. Многие провайдеры предлагают заполнить специальную форму (анкету), в которой указывается количество стоек, единиц размещаемого оборудования, их типы, размеры и мощности, разъемы, а также другие требуемые вам технические характеристики. Помощь в заполнении такой анкеты всегда могут оказать коммерческие и технические представители провайдера.

В идеальной ситуации провести инвентаризацию перевозимого оборудования и получить ответы на запрос ТКП от разных провайдеров услуг ЦОДа следует до подписания договора с выбранным провайдером, но жизнь зачастую вносит в планы свои коррективы. Инвентаризация – процесс небыстрый и не всегда совпадает со сроками запроса ТКП. Иногда она вообще не проводится до начала переезда, которое может по тем или иным причинам сместиться. Версии коммерческих предложений обсуждаются и уточняются с провайдерами ЦОДов многократно в ходе переговоров и торга о ценах на услуги провайдера. Поэтому окончательный список услуг ЦОДа может быть сформирован как до подписания договора, так и непосредственно во время переезда или даже после него. Это создает дополнительные риски и напряженность для сторон, заключающих достаточно сложный договор возмездного оказания услуг.

Для ускорения ввода в эксплуатацию переносимых со старой площадки ИТ-систем следует за-

ранее тщательно спланировать и документировать установку единиц оборудования в юниты стоек, рассчитать их энергопотребление, продумать организацию внутростоечных и межстоечных соединений, а также соединений между стойками, которые будут расположены в разных машинных залах ЦОДа. В идеале должен быть разработан проект размещения оборудования, учитывающий, с одной стороны, технические условия ЦОДа, а с другой – ваши потребности в инфраструктуре и коммуникациях. Наличие такого проекта облегчит жизнь и вам, и провайдеру, избавив от необходимости множества согласований. Проект может быть подготовлен провайдером либо специализированной организацией.

Проект включает планы размещения и подключения стоек к системам бесперебойного энергоснабжения в машинном зале, распределения оборудования по стойко-местам/холодным коридорам, расчет потребляемой электрической мощности и мощности холодообеспечения. При размещении нестандартного оборудования провайдеру может потребоваться с помощью специального ПО промоделировать воздушные потоки в горячих и холодных коридорах машзала и провести их дополнительную оптимизацию.

После выделения провайдером предполагаемых номеров стойко-мест и/или стоек в серверном зале рекомендуем на месте оценить их расположение, проанализировать перспективы развития своего ИТ-узла и возможность комфортного проведения технических работ как в стойках, так и в клиентской комнате.

Если часть работ по размещению оборудования в арендованные стойки и инсталляции соединительных линий планируется передать персоналу ЦОДа, то необходимо начертить фасады стоек (виды спереди и сзади), нанести номера и типы устанавливаемого в юниты оборудования и сформировать таблицу соединений портов патч-кордами.

При планировании размещения и эксплуатации оборудования в ЦОДе необходимо соблюдать технические условия: предельную допустимую мощность на одну стойку, максимальный ток на каждую из трех фаз в каждом вводе энергоснабжения стойки, ток на одну розетку. Это важно, поскольку у многих провайдеров стоят автоматические выключатели, рассчитанные на 16 А по каждой фазе. Для того чтобы не произошло непредвиденного срабатывания автомата по одной из фаз, может потребоваться установить другие разъемы, автоматические выключатели и кабели питания на 32 А. Это зависит от планируемой максимальной мощности потребления стоек при заполнении их оборудованием. При использовании своих стоек нужно согласовать с провайдером типы

розеток для подключения к системе энергоснабжения ЦОДа.

Обратите внимание на указанные в ТУ ограничения, а именно:

- предельный (пиковый) электрический ток, разрешенный для каждой фазы (при трехфазном питании) в каждом из двух вводов стойки;
- равномерность распределения выделенной мощности по всем фазам и внутренним розеткам стойки при подключении вилок питания оборудования;
- суммарная предельно допустимая мощность на одну стойку.

Если в стойках размещается серверное или иное оборудование, имеющее только один источник питания, то рекомендуем установить автомат ввода резерва (АВР), который, как правило, можно взять у провайдера в аренду. Это с вероятностью 99,982% обеспечит бесперебойную работу серверного оборудования с одним источником питания (для ЦОДа уровня Tier III по классификации Uptime Institute). Провайдер дает подобные гарантии только для серверного оборудования с двумя взаимно резервируемыми источниками питания либо для оборудования с одним источником питания, подключенным через АВР, который обеспечивает энергоснабжение стоечного оборудования от одного из двух взаимно резервируемых независимых энергопроводов стойки.

Принимая решение, использовать ли свои стойки или арендовать их у провайдера, важно выяснить максимальное количество юнитов в стойках выбранного ЦОДа. В некоторых ЦОДах высота стоек ограничена 45U. Следует учитывать планы дальнейшего развития своего ИТ-кластера: предусмотреть возможность увеличения количества стойко-мест для размещения новых стоек (собственных или арендованных) в холодном коридоре.

Если планируется арендовать у провайдера стойки целиком, то необходимо выяснить особенности системы распределения электропитания (PDU) внутри стоек. В некоторых ЦОДах устанавливают интеллектуальные PDU, которые обеспечивают защиту от превышения тока для каждой розетки, предусматривают удаленное управление (отключение и включение розеток в стойках) через интернет и локальную сеть ЦОДа и учитывают мощность, потребляемую подключенным оборудованием. Такие системы позволяют осуществлять удаленный мониторинг всего оборудования, установленного в стойке. Управление происходит по каналу защищенного удаленного доступа через интернет, и его можно делегировать клиентам ЦОДа. Такие сервисы не дешевы и требуют заблаговременного заказа у провайдера, но позволяют дистанционно полностью контролировать си-

туаацию с энергоснабжением размещенного в ЦОДе оборудования.

Система охлаждения оборудования, размещаемого в ваших стойках, может быть нестандартной. Охлаждающий воздух из холодного коридора может подаваться не на передний фасад стойки, а, например, сбоку или снизу. Такая схема требует разработки специального технического решения. Провайдеру нужно будет создавать в холодном коридоре нестандартные конструкции (специальные воздушные короба) или менять организацию существующих холодных коридоров, что повлечет за собой дополнительные расходы.

При размещении высоконагруженных стоек могут понадобиться:

- замена автоматических выключателей;
- установка дополнительных отводных блоков от шин системы распределения электроэнергии ЦОДа для организации нескольких вводов энергоснабжения к нагруженной стойке;
- установка дополнительных PDU;
- дополнительное моделирование воздушных потоков провайдером;
- установка «доводчиков», забирающих поток охлажденного воздуха из-под фальшпола и увеличивающих его скорость, особенно для подачи в верхние юниты стоек.

Также могут потребоваться другие технические мероприятия, обеспечивающие повышенную мощность энергоснабжения и интенсивное охлаждение оборудования, размещенного в нагруженных стойках.

Мониторинг параметров энергоснабжения и климатических условий стойки – вопрос первоочередной важности. Мониторинг стоек в ЦОДе может быть организован по-разному: от наблюдения температуры и влажности в общем серверном зале на сайте ЦОДа до специальной опции, доступной в личном кабинете заказчика. Такая опция позволит контролировать температуру именно в том холодном коридоре, где установлены ваши стойки. Логично запросить у провайдера техническую возможность индивидуального сетевого подключения для мониторинга стоек в режиме реального времени. Конечно, можно установить свою систему дистанционного контроля

температуры, но в случаях превышения температуры провайдеры, как правило, рассматривают жалобы заказчиков, основываясь на показаниях собственной системы мониторинга ЦОДа.

Размещение оборудования в коммерческом ЦОДе зачастую влечет за собой необходимость усиления физической и информационной безопасности. В машинном зале можно по запросу создать safe-зону, т.е. обнести часть машзала защитным ограждением для эксклюзивного размещения ИТ-ресурсов. Такое ограждение из сетки, которая пропускает воздух, имеет дверь с механическими замками или замками СКУД и предотвращает физический доступ любых посторонних лиц. На огороженном пространстве располагаются стойки с холодными и горячими коридорами. Иногда для повышения физической безопасности дополнительное ограждение создается и под стойками, в пространстве фальшпола. В огороженные зоны можно дополнительно установить датчики систем охранной сигнализации, видеокамеры и датчики движения, средства доступа в зону по биометрическим данным.

Планирование и организация коммуникаций в ЦОДе

До переезда необходимо спланировать резервируемую телеком-инфраструктуру, СКС и кросс-коннект, а также выбрать системы связи для подключения размещаемого оборудования. Возможно, вопрос с вводом в ЦОД двух ВОЛС от разных операторов связи уже решен – эту информацию предоставит провайдер. Могут потребоваться волокна, каналы L1 (лямбды), системы DWDM, каналы доступа в интернет и т.п.

Некоторые компании самостоятельно нанимают подрядчиков для прокладки в ЦОД собственной ВОЛС. Для этого необходимо запросить у провайдера технические условия ввода кабеля в ЦОД, его прокладки к стойко-месту, договор на сопровождение и технический надзор при проведении работ.

Далее следует проработать с провайдером техническую возможность заказа соединительных линий между стойками, между машинными залами дата-центра и третьими провайдерами услуг связи, имеющими точки присутствия в ЦОДе и обеспечивающими доступ в интернет и VPN. Нужно предусмотреть установку собственных или арендованных патч-панелей (коммутационных панелей) в стойках. При необходимости можно арендовать специализированные стойки для телеком-оборудования. Эти факторы влияют на инвестиционную составляющую бизнес-плана переезда и требуют оценки целесообразности того или иного варианта. Под эту же категорию работ подпадает создание сети коммутаторов в размещаемом в ЦОДе ИТ-кластере.



Можно заранее предусмотреть механизмы для удаленного управления серверными системами и СХД: KVM или ILO (Integrated Lights-Out – механизм управления серверами в условиях отсутствия физического доступа к ним).

Спланируйте также заполнение кабельных лотков, убедитесь, что в СКС провайдера места достаточно. При этом нужно учитывать, что для проводных соединительных линий и оптических кабелей используются разные системы лотков. Если вам понадобится установить дополнительные индивидуальные лотки, то необходимо это указать в запросе к провайдеру и провести их проектирование.

Вопросы логистики

Предварительный этап позволяет принять окончательное решение о соответствии новой площадки вашим требованиям. Далее начинается проработка процедур, связанных с собственным переездом, а именно:

- технической ревизии;
- инвентаризации товарно-материальных ценностей;
- маркировки;
- демонтажа оборудования;
- временного хранения до вывоза;
- упаковки;
- погрузки, перевозки, разгрузки;
- выравнивания температуры оборудования;
- распаковки;
- временного (до двух суток) безвозмездного хранения в ЦОДе;
- возмездного (более двух суток) хранения на складе ЦОДа;
- монтажа оборудования.

Все эти работы компания выполняет самостоятельно или заказывает у провайдера. Подписание актов приема-передачи оборудования, принятого на ответственное хранение в ЦОД, обычно проводится после его размещения в стойке.

Стойки с установленным в них серверным и СХД-оборудованием имеют очень большой вес (до 1000 кг) и, как правило, не перевозятся без демонтажа. После демонтажа оборудование упаковывается для обеспечения безопасной погрузки-разгрузки и транспортировки на новую площадку. При отсутствии специальной договоренности сотрудники коммерческого ЦОДа обеспечивают только надзор, временное хранение и учет ввезенного оборудования и не занимаются его переносом по территории ЦОДа и монтажом в стойки. Это придется делать своими силами при помощи ручных тележек, предоставляемых провайдером.

Для минимизации перерывов в бизнесе требуется хорошо продумать весь процесс переезда и проводить его с концентрацией усилий, с привлечением дополнительного персонала или

аутсорсинговых и транспортных компаний. Однако следует заметить, что услуги переезда в ЦОД обычно дороги (300–450 тыс. руб. за перенос трех стоек с оборудованием).

Из-за пробок на дорогах завозить оборудование в ЦОД предпочтительнее ночью. Оборудование завозится крупными партиями и временно хранится в ЦОДе до момента его установки в стойки. Во многих ЦОДах имеется возможность безвозмездного хранения в течение одних-двух суток. Услуги более длительного хранения оказываются на возмездной основе, поэтому целесообразно ознакомиться с условиями хранения и обсудить их с провайдером заранее.

При переезде с привлечением аутсорсинговой компании или заказе логистических услуг у провайдера ЦОДа необходимо согласовать ответственность за случайную порчу перевозимого оборудования. Возможно, потребуются дополнительные затраты на проверку технического состояния и функционирования оборудования до и после переезда. В подобных случаях составляются технические акты с целью определения стороны, ответственной за возможный или проявившийся ущерб. Также на период переезда оборудование можно застраховать.



В заключение несколько слов о финальном документе, формализующем процесс переезда в ЦОД. Это согласованный всеми участниками проекта план-график организационно-технических мероприятий и работ с указанием даты и времени их проведения, ответственных лиц, необходимых контактов и, возможно, особыми условиями. На основании плана-графика контролируется процесс переезда на новую площадку.

Предоставление стоек провайдером может проходить поэтапно, каждый этап сопровождается подписанием сторонами актов о дате предоставления стойки и начале оказания услуг. Обычно с этой даты осуществляются платежи за услуги ЦОДа.

Надеемся, что описание рутинных, но жизненно необходимых процедур поможет участникам рабочей группы выработать консолидированную позицию и в минимальные сроки и с минимальными потерями (а лучше вообще без них) переместить ИТ-узел вашей компании в коммерческий ЦОД. **ИКС**

ЦОДы, знакомьтесь: Jenbacher!

Компания INNIO – производитель газопоршневых двигателей и генераторных установок Jenbacher – пока не слишком известна на российском рынке ЦОДов, однако способна предложить для отрасли весьма эффективные решения. Подробнее – Вячеслав Герасиков, старший менеджер по продажам и развитию бизнеса в России и СНГ.



– Вячеслав, расскажите, пожалуйста, о вашей компании.

– История нашей компании уходит корнями в 1487 г., когда австрийский промышленник Якоб Фугер открыл плавильный завод. В XVIII в. компания была одним из мировых лидеров в выплавке чугуна, в XIX в. производила широчайший ассортимент промышленной продукции (режущие и буровые инструменты, валы, мельницы и т.п.), в середине XX в. – локомотивы, которые поставлялись и в СССР. В 1957 г. был начат выпуск газопоршневых двигателей под маркой Jenbacher. В определенный момент компанию приобрел концерн General Electric, что позволило значительно расширить производственные мощности. В начале XXI в. производство газовых двигателей Jenbacher было выкуплено у GE частной финансовой компанией, объединившей производство продукции Jenbacher и Waukesha под торговой маркой INNIO. Сегодня штаб-квартира компании находится в Австрии, в тирольском городке Йенбах, некогда давшем название нашей продукции.

С начала производства газопоршневых установок нашими клиентами стали многие компании по всему миру, относящиеся к самым разным отраслям: от владельцев сельскохозяйственных теплиц и объектов животноводства до крупных предприятий тяжелой промышленности и инфраструктурных объектов, например аэропортов. Немало клиентов у нас и в России. Сегодня в стране эксплуатируются более 800 установок номиналом от 300 кВт до 4,4 МВт и суммарной мощностью около 1,8 ГВт.

Что же касается топлива, используемого в наших установках, то это не обязательно природный газ. Это может быть чистый водород или водородная смесь, а также практически любой газ, получаемый при добыче или переработке нефти и природного газа и имеющий в основе метан.

– Чем обусловлен сегодняшний интерес компании к рынку ЦОДов?

– Мы рассматриваем отрасль ЦОДов как весьма динамичную и перспективную: в 2020 г. каждый пятый киловатт произведенной в мире электроэнергии потреблялся дата-центрами. За рубежом нашими установками пользуются многие дата-центры, в России же мы только начинаем движение в этом направлении, однако уже видим стойкий интерес к своим решениям. Газопоршне-

вые станции являются объектом внимания крупных коммерческих и операторских ЦОДов и так называемых гиперскейлеров. Сегодня мы ведем работу с несколькими компаниями из этого сегмента.

– Дата-центры в России традиционно используют дизельные генераторы. Каковы преимущества предлагаемых вами решений Jenbacher, работающих на водороде или природном газе?

– Преимущества наших решений заключаются в низкой стоимости генерируемой электроэнергии, заметно ниже тарифов электросетевых компаний, а также в экологичности и высоком ресурсе. Существующие тарифы электросетевых компаний колеблются в разных регионах от 6 до 10 руб./кВт·ч. В то же время с учетом цен на газ стоимость электроэнергии, произведенной нашими установками, составляет около 2,5 руб./кВт·ч. Разница очевидна. Если же сравнивать стоимость электроэнергии наших установок со стоимостью электричества от традиционных ДГУ, то разница становится драматической: стоимость 1 кВт·ч, произведенного ДГУ, – 15–18 руб.

Если мы рассматриваем ситуацию с приобретением дата-центром дополнительных мощностей, наши преимущества становятся еще более очевидны, поскольку затраты на техническое присоединение к сетям электроснабжения ощутимо выше, чем стоимость генерации того же объема электроэнергии газовой станцией.

Добавьте сюда экологическую чистоту и заведомо больший ресурс газопоршневых генераторов по сравнению с ДГУ, и вы поймете причины растущей привлекательности наших решений для дата-центров.

Еще одна отличительная черта наших решений – это тригенерация: помимо электроэнергии, установка вырабатывает большое количество тепла, которое может быть утилизировано. Разумеется, для дата-центров тепло не является необходимостью – они сами производят его в значительном объеме. Но тепло может быть использовано для получения холодного воздуха с помощью абсорбционных чиллеров. Это позволяет снизить стоимость владения.

Что же касается водорода, то эта технология, безусловно, передовая, и наша компания предлагает соответствующие решения еще с 2018 г. Однако сегодня стоимость производства водорода высока, а его доставка и

хранение сопряжены с определенными сложностями. Конечно, решение данных вопросов есть лишь вопрос времени, и мы с оптимизмом смотрим в этом направлении и уже ведем пилотные проекты, преимущественно в химической промышленности.

– Основная задача ЦОДа – работать бесперебойно. Как вы подходите к вопросам надежности энергоснабжения?

– Прежде всего нужно отметить, что перебои с подачей газа весьма редки, в отличие от подачи электричества из электросетей. Для обеспечения надежного электропитания нагрузки на объекте мы можем организовывать схемы энергоснабжения, в которых электрические вводы и наши генераторы резервируют друг друга. В таком контексте газовые установки могут выступать основным, более дешевым источником электроэнергии, когда мы лишь при пиковых нагрузках «добираем» электричество из внешней сети. С другой стороны, газовые генераторы могут быть альтернативой ДГУ и служить резервными источниками электричества. Существуют даже объекты, где используются и газопоршневые станции, и электрические вводы, и ДГУ.

Применение для газовых двигателей особых материалов позволяет обеспечить высокий ресурс и продолжительный срок службы, и это сильно отличает нашу продукцию от моделей двигателей, изначально спроектированных как дизельные и адаптированных для работы на газе. У таких двигателей ресурс весьма низок, а вероятность выхода из строя заметно выше.

Наши установки могут работать в различных природных условиях. У нас есть инсталляции в Заполярье, в условиях сверхнизких температур, и наоборот – в жарких регионах. Например, одна из установок, используемых в Узбекистане в добывающей промышленности, работает при внешних температурах 50–60°C, в условиях частых песчаных бурь, на высоте 800 м над уровнем моря.

Еще один аспект надежности – это своевременное proactive техническое обслуживание устройств, которое проще и выполнять которое нужно реже, чем в случае ДГУ. Сравните, скажем, частоту замены топливных фильтров для солярки и для газа.

– В настоящее время многие обращают внимание на экологичность применяемых решений.

– Экологичность – один из козырей нашей продукции. Она соответствует самым строгим требованиям в этой сфере. За счет использования газа мы сокращаем выбросы CO₂ и NO_x в атмосферу на 90%. Это серьезный шаг в уменьшении «углеродного следа».

Кроме того, поскольку не нужно размещать топливохранилища, заметно снижаются риски утечки или возгорания топлива и, как следствие, негативного экологического воздействия.

При переходе к использованию водородных решений воздействие на окружающую среду вообще будет нейтральным – водород не зря называют чистым топливом.

– Для любого дата-центра значимый фактор – стоимость эксплуатации и владения объектом. Как на ней отражается использование решений Jenbacher?

– При оценке стоимости решений важно правильно подходить к расчетам. Безусловно, приобретение газовых установок обходится дороже, нежели ДГУ. Однако, во-первых, уже при первоначальных вложениях нужно учитывать отсутствие ряда затрат, например, на организацию топливохранилища и на техприсоединение к электрическим сетям, стоимость которого порой существенно выше стоимости газовой установки.

Во-вторых, эксплуатация газовых установок намного дешевле. Как я уже отмечал, стоимость 1 кВт·ч для газовой станции в разы ниже, чем даже для электрических сетей, не говоря уже о ДГУ – 2,5 руб. и 16 руб. соответственно! Следовательно, окупается такая система значительно быстрее, хотя это зависит от времени работы. При эксплуатации в постоянном режиме система окупит себя по сравнению с использованием электричества от внешней сети за период от одного до четырех лет, а в резервном режиме – уже спустя 4 тыс. ч наработки.

Также нужно отметить, что стоимость обслуживания подобных систем ниже, а ресурс до капитального ремонта составляет 80 тыс. моточасов (сравните с 8–30 тыс. моточасов для ДГУ). После переборки газовая станция может прослужить еще такой же срок. Ее расчетный срок службы составляет 40 лет.

В свете того, что во многих случаях получать лимиты на электричество затруднительно и многие потребители переходят на энергосервисные контракты, использование газовых станций зачастую предпочтительнее подключения к внешним энергосетям.

– Сегодня компании в отрасли сталкиваются с серьезной проблемой – недостатком квалифицированных инженеров. Как вы подходите к вопросам сервисного обслуживания?

– Безусловно, качественное сервисное обслуживание важно, и для нашей компании – это вопрос репутации. В России обслуживание осуществляется через сеть наших дистрибьюторов, обладающих складами необходимых запчастей и квалифицированным персоналом, который проходит подготовку в нашем учебном центре.

Кроме того, предметом гордости нашей компании стала глобальная система удаленного мониторинга всех установок. Она круглосуточно снимает показатели по всему миру, анализирует эти данные и уведомляет сервисное подразделение компании о необходимости проведения регламентных работ или отклонениях в функционировании той или иной установки, что позволяет проактивно провести нужные работы и предотвратить выход оборудования из строя. Благодаря такому решению оборудование у нас выходит из строя чрезвычайно редко.

JENBACHER

INNIO

www.innio.com/ru/rucis



VSaaS-провайдеры: перспективные клиенты для ЦОДов

Николай Носов

Провайдеры услуг облачного видеонаблюдения – пока небольшой, но активно растущий сегмент пользовательской базы дата-центров.

Ограбление рядом с банком

Лет семь назад, когда я работал в банке, с необычной просьбой к нам обратился руководитель небольшой компании. Придя в понедельник на работу, он обнаружил исчезновение крупной суммы денег из сейфа. Одна из камер наружного наблюдения банка контролировала и площадку перед входной дверью его фирмы, поэтому проситель хотел посмотреть записи с нее за выходные.

Руководитель компании-соседа потратил на просмотр видео больше дня, но смог найти момент ограбления. Двое крепких мужчин с надетыми на головы капроновыми чулками подошли к двери, а через некоторое время вынесли из нее сумку. Маскировка не спасла – по фигурам и манере поведения определили, что это бывшие охранники, уволенные два месяца назад. Система видеонаблюдения помогла их идентифицировать, но одновременно выявила проблемы.

Во-первых, система сбора и хранения видео была не по карману небольшой компании. Ей просто повезло, что рядом находился наш банк. Во-вторых, даже система банка не смогла быстро найти нужные записи. Никакой видеоаналитики не было, все записи пришлось просматривать вручную, и хорошо еще, что похитителей помнили.

Безопасность сегодня

Теперь организовать видеонаблюдение стало проще. На помощь пришли облачные технологии. Больше не нужна локальная система сбора и хранения данных видеонаблюдения – изображение передается в облако с обычной камеры, подключенной к интернету, и просматривается с обычного смартфона. Простейший облачный сервис «videонаблюдение как услуга» (Video Surveillance as a Service, VSaaS), месячная плата за который сопоставима со стоимостью пары поездок на такси, доступен не только небольшим компаниям, но и частным пользователям. Можно удаленно контролировать, не пытаются

ли посторонние залезть в домик на даче, смотреть, кого впустил в квартиру ребенок или престарелый родственник, наблюдать за уборкой или ремонтом квартиры.

При этом не требуется даже ехать в офис облачного провайдера и заключать договор. Достаточно купить и установить Wi-Fi-камеру, скачать приложение на мобильное устройство, создать аккаунт, добавить камеру, указать пароль сети и поднести к ее объективу отображенный на экране QR-код.

Средства аналитики помогут быстро найти нужный момент. Не знаю, смогли бы они распознать человека с надетым на голову чулком, но и это уже не кажется невероятным.

Развитие рынка

Сервис VSaaS появился в США в 2009 г. и быстро стал набирать популярность. Доля мирового рынка систем и сервисов видеонаблюдения на основе IP-камер, по данным Grand View Research, сравнялась с долей аналоговых камер в 2015 г. (рис. 1), а в 2020 г. объем мирового рынка видеонаблюдения в целом приблизился к \$100 млрд. По оценкам Transparency Market Research, в 2027 г. этот рынок достигнет \$132 млрд.

Всего год спустя после появления VSaaS-сервисов в США их начали предлагать и в России, причем российские разработки ни в чем не уступали зарубежным, а в некоторых областях, таких как распознавание лиц, даже опережали американские.

По оценкам МГТС, российский рынок видеонаблюдения растет ежегодно на 20%, причем доля облачных услуг видеонаблюдения увеличится с 6,7% в 2015 г. до 14,1% в 2022 г. (рис. 2).

Бизнес-модели, достоинства и недостатки

При обращении к поставщику VSaaS-сервисов на долю клиента остается покупка и установка камер видеонаблюдения, а системы сбора, обработки и хранения видеоинформации становятся

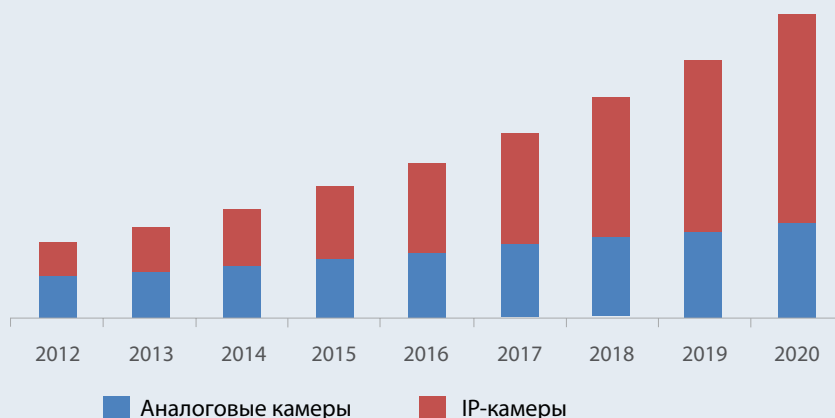
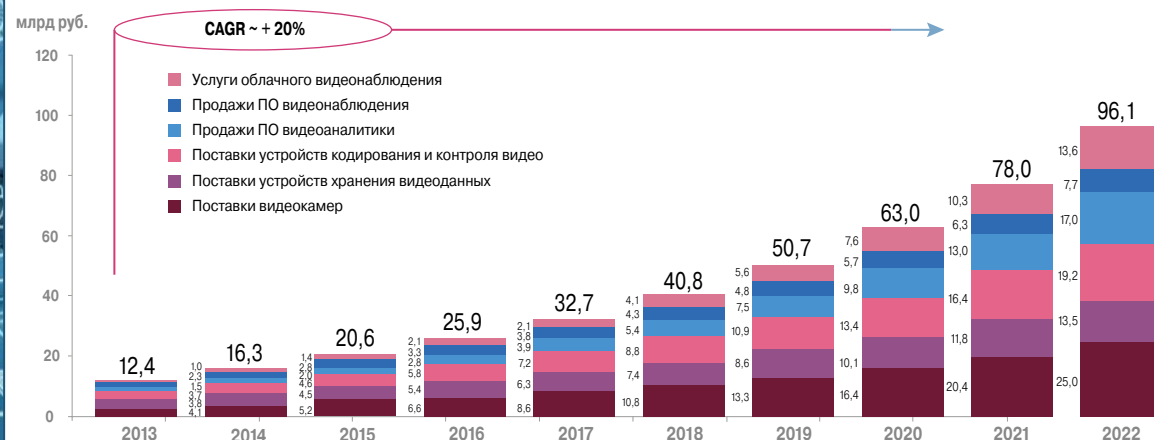


Рис. 1. Мировой рынок видеонаблюдения и VSaaS по продуктам в 2012–2020 гг., в денежном выражении ▼

Источник: по материалам Grand View Research, 2020

Рис. 2.
Рынок видео-
наблюдения
в России,
млрд руб. ▶

Источник:
оценка МГТС



заботой провайдера. При этом возможность подключения к сервису, как правило, от производителя камеры не зависит. Плата за сервис определяется целым рядом параметров: количеством подключенных камер, количеством пользователей, имеющих право доступа к камерам, временем хранения данных в облаке, наличием или отсутствием «умного» поиска в видеозаписях и т.д.

Использование сервисов VSaaS дает клиенту ряд преимуществ.

- Не надо закупать и монтировать системы видеонаблюдения на объекте (за исключением собственно видеокамер). Капитальные расходы заменяются операционными.
- Обеспечивается гибкость и масштабируемость – если камера не используется, за нее не нужно платить, а если требуется подключить дополнительные торговые точки и филиалы, то это можно сделать быстро.
- Появляется независимость от вендора и поставщика услуг. Не важно, какое до этого закупалось оборудование и какие использовались стандарты сбора и хранения данных. Пользователь не зависит даже от облачной платформы – провайдера VSaaS легко можно поменять.
- Увеличивается надежность хранения данных. Пожар в серверной предприятия не уничтожит данные в облаке, а гибель видеорегистратора не помешает расследованию аварии автомобиля.
- Благодаря квалификации специалистов облачного провайдера, своевременному обновлению программного обеспечения, шифрованию передаваемых и архивных данных повышается уровень кибербезопасности. В облаке легче организовать безопасный многопользовательский доступ к видеокамерам и управлять распределением прав.
- Облака дают возможность предлагать новые сервисы, которые трудно реализовать on-premise,

скажем, онлайн-трансляцию с камеры на веб-сайт или в социальные сети. Так, компания «Додо пицца» использует VSaaS для персональной онлайн-трансляции готовящегося для клиента заказа.

Революцию в видеонаблюдении совершило внедрение элементов искусственного интеллекта. Теперь можно, например, распознать лица посетителей магазина, их возраст, пол и даже испытываемые ими эмоции. Сверить вошедших в торговый зал покупателей со списком лиц, уже замеченных в воровстве товара, и обратить внимание охранника на потенциального нарушителя. Проанализировать успешность рекламной кампании, подсчитав повторно пришедших в магазин покупателей. Выявить VIP-клиентов и предложить им улучшенный сервис. Связать по API облачные системы видеонаблюдения с ERP-системами предприятия, подключить облачные системы бизнес-аналитики.

Вместе с тем VSaaS не панацея, и переход на эти сервисы имеет ряд ограничений.

- Использование VSaaS не всегда экономически оправдано – в крупных центрах с большим количеством камер по-прежнему выгоднее оказывается локальная система видеонаблюдения. Хранение данных в VSaaS организовано циклически – по истечении заданного времени старые данные стираются и на их место записываются новые. Тем не менее хранение больших объемов данных в облаке может обойтись в кругленькую сумму.
 - Не всегда удастся обеспечить стабильное широкополосное подключение камер к интернету. Это особенно критично, если надо постоянно передавать видеопоток, а не только реагировать на заранее заданные события.
- В каждом конкретном случае нужно взвешивать плюсы и минусы, но для небольших организаций и компаний, использующих отдельно стоящие камеры, облачные сервисы, как правило, предпочтительнее.



VSaaS и ЦОДы

Операторы сервисов облачного видеонаблюдения – активные пользователи услуг коммерческих дата-центров. Как рассказал нашему изданию Андрей Юдников, CEO и основатель компании Ivideon, одной из первых начавшей предлагать услуги VSaaS в России, компания арендует в ЦОДах стойки с ИТ-оборудованием, на котором разворачивает свою облачную платформу видеонаблюдения. Часть серверов задействуется для обработки информации в режиме реального времени, часть – для хранения архивов. Видеоданные сервиса геораспределены по 15 дата-центрам уровня Tier III, сервисом пользуются свыше 5 млн клиентов из 100 стран мира. Видеоинформация занимает большой объем, при этом по требованиям клиентов или законодательства хранится до 30, в некоторых странах даже до 90 дней.

Часть команды Ivideon перебралась в «Ростелеком», где продолжила развивать сервисы видеонаблюдения и видеоаналитики. Среди операторов связи в сегменте VSaaS заметна также МТС.

Спрос на VSaaS повысится с распространением систем «умного» города. Ряд игроков, в том числе МТС, уже сейчас активно строят частные сети LTE и 5G и на их основе разворачивают облачное видеонаблюдение. Например, в августе 2020 г. во Владивостоке МТС запустила в нескольких скверах систему «умного» видеонаблюдения, которая способна подсчитать количество посетителей, распознать пол, возраст и эмоции человека, найти потерявшегося в сквере ребенка по описанию одежды и зафиксировать появление дыма и огня. Одна камера и обеспечивает безопасность, и собирает статистику, которую администрация может использовать для развития инфраструктуры.

Особенно полезно внедрение видеоаналитики на транспорте. Например, камеры могут оценивать поведение водителя общественного транс-

Можно рассчитывать, что рынок VSaaS займут телеком-операторы, которые будут предоставлять видеокамеры по сервисной модели. Драйвером массового использования видеоаналитики станут сети 5G, распространение которых ожидается в 2024–2025 гг. Технологии 5G обеспечат скорость, минимальные задержки и слайсинг – разделение общего сетевого пространства на сегменты с определенными свойствами. Выделение гарантированной полосы пропускания критично для видеонаблюдения.

порта, такси или каршеринга: берет ли он в руку мобильный телефон, курит или засыпает. Эта информация не только позволит оперативно сделать замечание водителю, но и будет передаваться для дальнейшего «разбора полетов» в центр управления безопасностью движения. Над подобными проектами уже работают такие компании, как «СКАУТ – Корпоративные решения», Skytracking и другие.

Дополнительный толчок развитию рынка дала пандемия, резко увеличившая спрос на измерение температуры тела с помощью тепловизоров. Такой сервис в облачном варианте также относят к VSaaS.

Сервисы VSaaS целесообразно предлагать на базе региональных ЦОДов, ведь качество канала и величина задержки для видеонаблюдения критичны. Провайдеры облачного видеонаблюдения с постоянно растущими запросами на количество стоек, объемы трафика и систем хранения – перспективные клиенты для ЦОДов... ИКС



Антон Салов,
независимый
эксперт RCCPA



ИИ в медицине: тренды и примеры применения

Владимир Крылов,
профессор математики,
научный консультант,
Artezio
(ГК ЛАНИТ)

Попробуем проанализировать, как решения на основе искусственного интеллекта применяются в медицинских учреждениях и как они влияют на качество диагностики и лечения.

ИИ и медицина сегодня

В этой статье мы будем рассматривать медицину как систему научных знаний и практической деятельности, целями которой являются сохранение и укрепление здоровья человека, продление его жизни, лечение и предупреждение болезней. Под содержательной стороной термина «искусственный интеллект» будем понимать технологии, основанные на обучении компьютерных систем и предназначенные для замены действий человека при выполнении каких-либо процессов. Такое определение позволит сосредоточиться на практических аспектах и избежать вопросов философского плана, которые часто сопровождают обсуждение ИИ в непрофессиональных кругах.

Какова же ситуация с применением ИИ в медицине по состоянию на июнь 2021 г.? На наш взгляд, такая фиксация времени необходима ввиду бурного развития рассматриваемой обла-

сти. В 2020 г. журнал Nature опубликовал весьма наглядную диаграмму (см. рисунок) роста количества публикаций в профессиональном медицинском сообществе о применениях технологий машинного обучения.

Экспоненциальный рост числа исследований, как правило, сопровождается постоянным расширением круга решаемых задач. Поэтому мы не будем претендовать на исчерпывающую картину применения ИИ в медицине, а попытаемся очертить наиболее успешные или перспективные с нашей точки зрения направления.

ИИ в хирургии

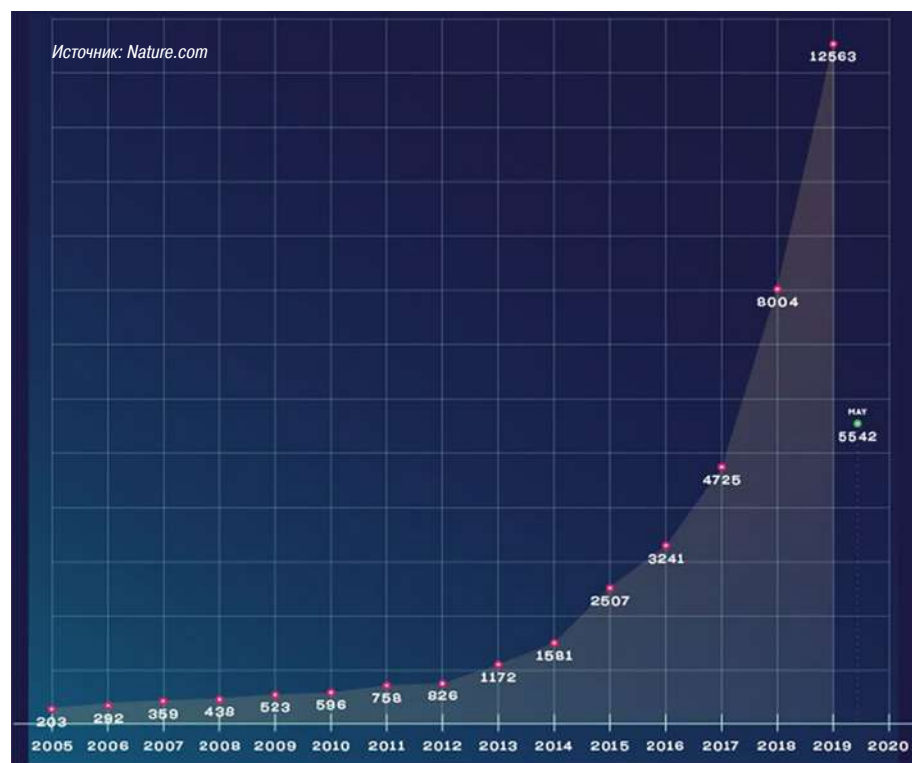
Речь идет о роботах, участвующих в хирургических операциях и сопровождающих хирургические операции и послеоперационных больных. По данным MarketsandMarkets, глобальный рынок хирургических роботов будет расти в среднем на 10,4% и достигнет \$6,5 млрд к 2023 г. против \$3,9 млрд в 2018 г.

В 2018 г. более 5 тыс. хирургических роботов использовались более чем в миллионе медицинских процедур по всему миру. Важно заметить, что термин «робот» часто создает неправильное представление о том, что роботы выполняют хирургические операции. Это не совсем так.

Роботы с искусственным интеллектом применяются все чаще в микрохирургических процедурах. Но не следует считать, что скоро будут оперировать только роботы-хирурги. Зато справедливы ожидания, что роботы с ИИ помогут хирургам работать лучше.

Согласно одному из исследований, проведенному с участием 379 пациентов врачей-ортопедов, хирургические операции с использованием искусственного интеллекта вызвали в 5 раз меньше осложнений, чем операции, где хирурги работали в одиночку. Роботизированная хирургия – это актив-

Динамика количества публикаций о применении технологий машинного и глубокого обучения в медицине в 2010–2020 гг. в электронной библиотеке PubMed ▼



но развивающаяся и эффективная технология, которая приобретает все большее значение при различных медицинских процедурах в неврологии, гинекологии, ортопедии, торакальной и общей хирургии, при установке зубных имплантатов, а также трансплантации волос. Роботизированные технологии позволяют врачам с минимальным опытом или практикующим врачам, плохо знакомым с той или иной операционной процедурой, проводить лечение на уровне, которого они не смогли бы достичь даже в результате многолетней практики. Помощь робота во время операции уменьшает последствия тремора рук оперирующего врача, а также устраняет случайные движения.

Робот Da Vinci, который считается одним из самых передовых в мире хирургических роботов, предоставляет врачу набор хирургических инструментов, которые можно использовать при проведении минимально инвазивной хирургии, и обеспечивает лучший контроль над обычными процедурами.



Приобрел большую популярность и миниатюрный мобильный робот Heartlander. Он минимизирует повреждения, которые необходимо причинить пациенту для доступа к сердцу во время операции. Робот входит в грудную клетку через небольшой разрез ниже грудины. Используя это устройство, хирурги теперь могут выполнять стабильное и локализованное картирование, зондирование и лечение всей поверхности сердца.

ИИ в диагностике

По оценкам IBM, 90% данных в отрасли здравоохранения – это изображения, и их объем увеличивается быстрее объемов всех других медицинских данных. Начавшие свое триумфальное шествие с распознавания изображений собак, автомобилей и рукописных цифр, нейронные сети очень пригодились при обработке разнообразных визуальных данных.

Возможности нейронных сетей помогают трансформировать сферу радиологии, экономя время и деньги медицинских организаций. После того, как медицинское изображение полу-

чено с помощью МРТ, компьютерной томографии, ультразвукового или рентгенологического исследования, врач должен проанализировать его на наличие каких-либо отклонений или признаков заболеваний. Для выявления сколь угодно серьезного состояния требуется интерпретация нескольких визуализационных исследований.

После обучения с использованием больших наборов данных исследований системы на основе ИИ способны анализировать медицинские изображения и сообщать об обнаруженных особенностях, например, небольших опухолях, которые человеческий глаз может упустить. Такие системы выявляют закономерности и предоставляют информацию о характеристиках любых отклонений от нормы, экономя время врача.

В тех случаях, когда у пациента есть несколько снимков, сделанных на протяжении некоторого времени, искусственный интеллект также может анализировать динамику заболевания. Так, для проверки работы своей системы на основе ИИ в корпорации Google провели эксперимент: снимки предложили изучить шестерым сертифицированным радиологам. В тех случаях, когда диагноз ставился по единственному снимку, искусственный интеллект справился так же или даже лучше людей. Системе удалось диагностировать на 5% больше случаев рака и сократить ложноположительные вердикты на 11%.

Виртуальные помощники медсестры

Согласно недавнему отчету Accenture, использование виртуальных помощников медсестер в сфере здравоохранения может сэкономить \$20 млрд в год за счет уменьшения на 20% времени, которое медсестры тратят на обслуживание пациентов. Сегодня рядом с живыми медсестрами в госпиталях США уже работают компьютерные помощники, от которых можно получать советы, подсказки и другую информацию. Например, цифровой ассистент Салли, улыбающаяся женщина в белом халате, или медбрат Уолт. Салли и Уолт – это анимированные аватары, виртуальные личные тренеры по здоровью из платформы iCare Navigator на базе искусственного интеллекта, предназначенной для взаимодействия с пациентами и их обучения.

Компания TeleHealth Services, разработавшая iCare Navigator, утверждает, что использует электронные медицинские записи пациентов и применяет машинное обучение для выстраивания индивидуальных отношений. Приложение определяет, когда пациент будет наиболее восприимчив к информации о состоянии своего здоровья и можно будет лучше всего управлять его лечением.

Толчком для создания платформы iCare Navigator стали исследования Медицинской школы Бостонского университета, в ходе которых были разработаны виртуальные медсестры Луиза и Элизабет, объясняющие пациентам, например, когда принимать лекарства. Оказалось, что 74% пациентов предпочли получить рекомендации при выписке из стационара от виртуальной медсестры, а не от человека.

Молли от компании Sensely – еще один популярный аватар медсестры с искусственным интеллектом, который используют Калифорнийский университет в Сан-Франциско и Национальная служба здравоохранения Великобритании. Молли задает пациентам вопросы, касающиеся их здоровья, оценивает симптомы и на основе симптомов дает рекомендации по наиболее эффективному лечению.

Таким образом, вместо того, чтобы искать обнаруженные у себя симптомы в интернете, сегодня человек может получить помощь от виртуальной медсестры. Виртуальные медсестры не только предоставляют медицинские консультации по поводу распространенных заболеваний или недомоганий, но также позволяют записаться на прием к врачу. Они доступны круглосуточно и без выходных и готовы ответить на вопросы в режиме реального времени. Это одно из основных приложений искусственного интеллекта в здравоохранении, которое все чаще применяется для повышения информированности и улучшения навыков самоуправления у пациентов с хроническими заболеваниями. Благодаря виртуальной медсестре пациент сможет предотвратить ухудшение своего состояния.

Системы мультимодальной диагностики

В развитии ИИ можно выделить несколько трендов, один из которых связан с интеграцией типов (модальностей) данных, на которых выполняется обучение. Например, для аудиовизуального распознавания речи визуальное описание движения губ объединяется с аудиовходом для предсказания произнесенных слов. Информация, поступающая из источников различных модальностей, может иметь различную предсказательную силу и топологию шума, а в некоторых источниках данные могут отсутствовать. Неоднородность мультимодальных данных затрудняет построение моделей.

Важно изучить, как представлять входные данные и обобщать их таким образом, чтобы они отражали несколько модальностей. Например, текст представляется символами, а аудио и визуальные модальности – сигналами. В контексте медицинского применения вся диагностическая информация о пациенте может быть

интегрирована в такие мультимодальные данные и обрабатываться системой ИИ, обученной рассматривать как внешнее изображение человека и фрагментов его тела, так и результаты анализов, МРТ- и КТ-изображения, аудиозаписи ответов на вопросы и т.д.

Все это приближает нас к построению универсального диагноста, использующего холистический подход к диагностике заболеваний, и сокращению количества посещений разных врачей-специалистов для назначения эффективного лечения.

Приложения для здоровья на базе искусственного интеллекта

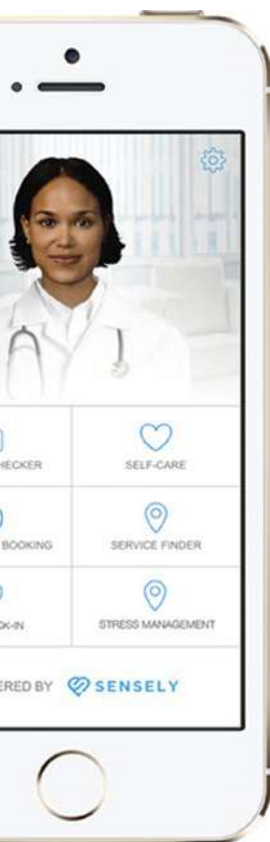
Самое большое потенциальное преимущество искусственного интеллекта – возможность помочь людям оставаться бодрыми, чтобы им не приходилось посещать врача или по крайней мере делать это не слишком часто. Искусственный интеллект и интернет медицинских вещей (IoMT) уже постепенно меняют парадигму с «реактивного» здравоохранения на «проактивное».

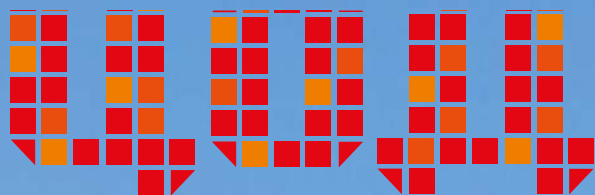
Сочетание искусственного интеллекта и IoMT со временем сделает подключенные устройства для мониторинга состояния здоровья более интеллектуальными. ИИ и огромные объемы данных, генерируемые IoMT, также могут использоваться для постановки диагноза.

Различные приложения для здорового образа жизни на основе искусственного интеллекта, такие как MyFitnessPal и HealthTap, предоставляют людям полный контроль над своим здоровьем и благополучием, обратную связь с медицинскими учреждениями и рекомендации для поддержания здоровья. Например, HealthTap узнает о симптомах пациента и их изменении с течением времени и координирует процесс лечения: отправляет напоминания, предоставляет текстовые ответы, сопоставленные с данными об истории болезни, руководствами, созданными врачами, а также обеспечивает возможность проведения онлайн-консультаций по видеоконференцсвязи.

ИИ в медицине – это прорыв?

Можно ли назвать применение ИИ прорывом в диагностике и лечении? На мой взгляд, сегодня прорыв еще не произошел. Поэтому я бы использовал количественную оценку развития технологий, например, число успешных исследовательских проектов в этой области или число публикаций. Если такой показатель растет экспоненциально, то можно говорить о быстром продвижении вперед. С этой точки зрения мы присутствуем при развитии прорывных технологий диагностики и лечения. ИКС





МОДЕЛИ СЕРВИСЫ ИНФРАСТРУКТУРА



3-я МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ И ВЫСТАВКА

Екатеринбург 25 ноября 2021

Hyatt Regency Ekaterinburg

На конференции традиционно рассматриваются вопросы развития индустрии дата-центров и облачных сервисов на территории УФО и восточных регионов страны, а также основные аспекты создания, эксплуатации и управления ЦОДами.

- Развитие рынка КЦОДов и облачных услуг в РФ: Москва и регионы
- Мировые тренды в области развития сервисных моделей и инфраструктуры ЦОДов
- Современные технологии и решения для инженерной и ИТ-инфраструктуры ЦОДов
- Переход в облако. Опыт и новации
- Edge-ЦОДы для различных сегментов экономики



подробно о программе и участниках
на сайте конференции ekb.dcforum.ru



16+

Реклама

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

ОРГАНИЗАТОРЫ



ПРИ
ПОДДЕРЖКЕ
И УЧАСТИИ



Минцифры
России



КООРДИНАЦИОННЫЙ СОВЕТ
ПО ЦОДАМ И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

UptimeInstitute®

Рынок кибербезопасности стремится в облака

Николай Носов

Массовый переход бизнеса к использованию облачных сервисов способствует более активному развитию еще одного сегмента облачного рынка – обеспечению информационной безопасности по сервисной модели.



Год назад в начале пандемии портал «ИКС-Медиа» опубликовал статью «Облака, ЦОДы и туалетная бумага на фоне пандемии», в которой прогнозировалось, что пандемия подхлестнет спрос на облачные сервисы. Статья вызвала неоднозначные комментарии, эксперты справедливо указывали на негативные тенденции, связанные с экономическим спадом и сокращением спроса со стороны ряда отраслей среднего и малого бизнеса. Тем не менее пандемия стала катализатором перехода к облачным технологиям, о чем свидетельствует и зафиксированный iKS-Consulting рост выручки облачных провайдеров на 19,5% (до 99,7 млрд руб.).

Эпидемия COVID-19 не только ускорила процессы цифровой трансформации и переход к облакам, но и породила новые проблемы. По данным iKS-Consulting, 93% опрошенных компаний в числе главных вызовов, обусловленных пандемией, назвали создание безопасного цифрового рабочего пространства при быстром переходе на удаленную работу.

Согласно исследованию Qrator Labs, если в 2015 г. лишь 27% финансовых организаций планировали увеличить бюджеты на информационную безопасность, а четверть намеревалась их сократить, то в 2021 г. снижать расходы никто не собирается, а увеличить их планирует половина. Однако одними деньгами проблему не решить, нужны специалисты, обладающие экспертизой в области ИБ, а вот их-то на рынке не хватает.

Безопасность облака и из облака

Зато экспертиза есть у облачных провайдеров, и у них открываются новые возможности для бизнеса: как и любое предприятие, провайдер должен обеспечивать свою информацион-

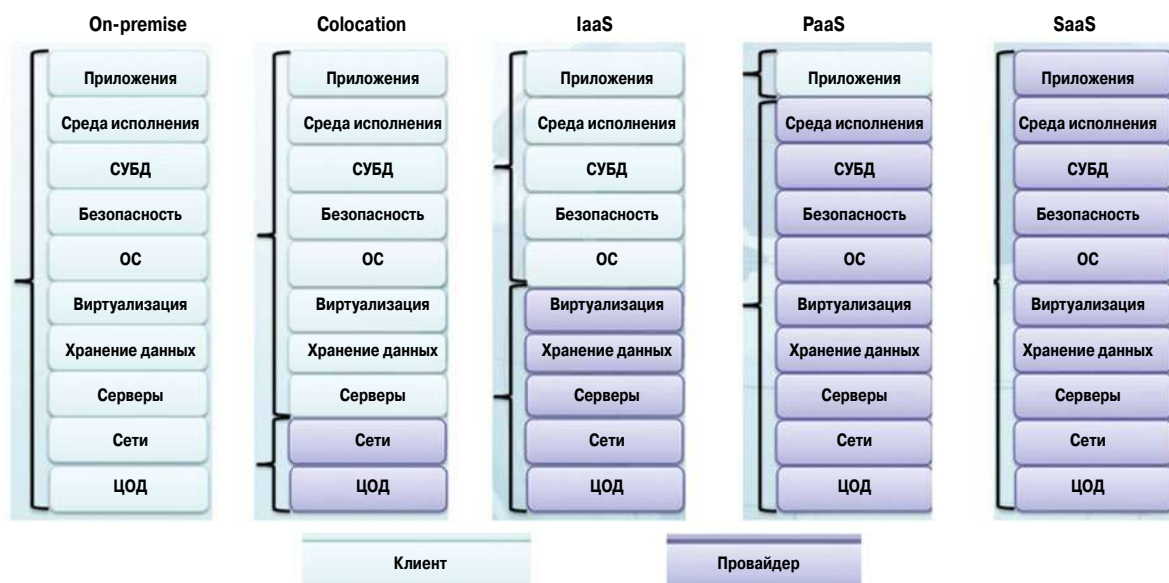
Сегодня на рынке наблюдается дефицит ИБ-специалистов – по данным аналитиков, найти таковых не могут 32% компаний, а 47% недовольны квалификацией имеющихся сотрудников. В этих условиях единственным способом получить качественный сервис по разумной цене будет передача части функций информационной безопасности на аутсорсинг. И мы видим, что все больше ИБ-директоров готовы разговаривать на эту табуированную ранее тему.

ную безопасность, но в то же время он может монетизировать вложения в ИБ, оказывая соответствующие услуги клиентам. Провайдер и так выполняет часть функций ИБ-службы компаний, поскольку атаки на его ресурсы угрожают не только ему, но и его клиентам. Кроме того, провайдеры начинают предлагать продукты ИБ из облака по сервисной модели (SECurity as a Service, SECaaS) и брать на себя часть функций служб ИБ предприятия, предлагая управляемые услуги безопасности (Managed Security Services, MSS). Это удобно для бизнеса, отдающего на аутсорсинг непрофильную деятельность и зачастую не имеющего квалифицированных ИБ-специалистов. Чем выше уровень аутсорсинга, тем больше функций кибербезопасности перекладывается на плечи провайдера (рис. 1).

В рамках модели on-premise за кибербезопасность отвечает клиент, в случае colocation провайдер берет на себя функции физической за-



Александр Иванов, менеджер продуктов SECaaS, SberCloud



◀ **Рис. 1.** Зоны ответственности клиента и облачного провайдера при разных моделях использования ИТ-инфраструктуры

щиты – контроль доступа, температурный режим, пожарную безопасность, отвечает за сеть. При использовании модели IaaS к провайдеру переходит забота о хранении данных и работе платформ виртуализации, а при SaaS – уже практически всех систем.

Можно сравнить облако с отелем или домом. В частном доме за свою безопасность полностью отвечает жилец. Отель, разрешающий туристу поставить на своей территории палатку, соответствует модели colocation. Постояльцу не придется беспокоиться о безопасности территории – отель отвечает за забор и въездные ворота. В модели IaaS турист получает пустую комнату, но с входным замком, защищающим от проникновения соседей. SaaS – это полностью оборудованный согласно потребностям клиента номер с сейфом для хранения денег и документов и круглосуточной возможностью вызова персонала.

Используя подход агентства Moodys, занимающегося исследованиями и анализом рисков, можно выделить семь столпов безопасности SaaS (рис. 2). Их же можно считать семью столпами облачной безопасности в целом.

Семь столпов облачной безопасности

Управление доступом. Риски несанкционированного доступа существенно возрастают при массовом переходе на удаленную работу. Больше удаленных пользователей – больше шансов у злоумышленников провести атаку распылением паролей (найти слабый пароль,

перебирая наиболее популярные комбинации). Упрощает работу хакеров и привычка пользователей устанавливать один пароль для разных систем. Пароли могут перехватываться внедренными на устройство жертвы кейлогерами.

Методы защиты известны – разграничение прав и сегментация: использование Active Directory (AD), четкое расписывание ролей, контроль соответствия прав пользователей их текущим задачам, контроль выбывших пользователей. Облачная специфика – появление в модели угроз новых потенциальных нарушителей в лице персонала облачного провайдера. На разграничение прав доступа у персонала провайдера следует обратить особое внимание. Одна группа должна иметь права на обслуживание систем, другая – исключительно на распределение прав доступа, третья – на расследование инцидентов. Если продолжить аналогию с отелем, горничные могут убирать номер, администратор – выдавать ключи, охранник – работать с системой видеонаблюдения. Но ни одна из этих групп не должна иметь права делать все.

Важную роль играет многофакторная аутентификация (МФА). Нужен еще как минимум один канал проверки подлинности пользователя. Второй фактор аутентификации служит для того, чтобы удостовериться, что доступ запрашивает именно тот человек, которого система идентифицировала по логину и аутентифицировала по первому фактору – паролю. Ведь пароль мог быть украден или просто подобран, в том числе простым перебором с помощью программ, широко представленных в интернете.

Рис. 2. Семь столпов безопасности SaaS ▼



Источник: Moodys

Контроль сети. Защита от сетевых угроз в облаке обеспечивается использованием групп безопасности, сегментацией и разграничением прохождения пакетов по сети, выделением изолированных зон с помощью физических или виртуальных маршрутизаторов, снабженных списком управления доступом к сети (Network Access Control List). Такие зоны провайдер может предоставлять и на физическом уровне, выделяя в машзале стойки с защищаемыми данными, например, для процессинга или бизнес-критичных систем банка.

Защиту сети усиливает единый шлюз для доступа к инфраструктуре клиента, например, специально отведенный компьютер в демилитаризованной зоне (Jump Server), через который происходит обмен пакетами между внутренней и внешней сетями. Использование единой точки входа улучшает контроль трафика и уменьшает поверхность атаки.

Защита периметра. Основной способ защиты периметра – межсетевые экраны (МСЭ), работающие на уровне портов и IP. Также используются «белые» и «черные» списки надежных и ненадежных сайтов. Например, в банках доступ из внутренней сети часто осуществляют только по «белым» спискам проверенных адресов.

Более тщательный анализ трафика проводит система обнаружения вторжений (Intrusion Detection System, IDS) – программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими через интернет. В отличие от межсетевого экрана, контролирующего только параметры сессии (IP, номер порта и состояние связей), IDS «заглядывает» внутрь пакета (до седьмого уровня OSI), анализируя передаваемые данные благодаря технологии глубокого инспектирования пакетов.

Дверь лучше не только запирать на замок, но и дополнительно защищать, выставив возле нее охранника. IDS всего лишь помечает подозрительные действия, а в качестве секьюрити выступают хостовые системы предотвращения вторжений (Intrusion Prevention System, IPS), защищающие локальную систему от вирусов, руткитов и взлома. Они способны самостоятельно перестраивать пакетный фильтр или прерывать сеанс и контролируют гораздо больше системных параметров: процессы, целостность системных файлов и реестра, записи в журналах.

Подозрительные пакеты размещаются в песочницах, которые используются для запуска, или «взрыва» (detonation) подозрительных файлов или URL-адресов. Выявляя подозрительное поведение, песочницы могут обнаруживать

В ближайшие годы облачные провайдеры перейдут на полноценную SECaaS-модель – самостоятельно или в партнерстве с крупными провайдерами кибербезопасности.

вредоносные программы «нулевого дня», на что не способны антивирусные программы. Впрочем, и классические антивирусы не утратили популярности.

Закрыть внутреннюю инфраструктуру от внешних злоумышленников помогает трансляция сетевых адресов (Network Address Translation, NAT), которая «на лету» меняет IP-адрес в пакетах, проходящих через маршрутизатор. Сходные функции защиты выполняет прокси-сервер. Клиент из внутренней сети подключается к прокси-серверу и запрашивает ресурс (например, e-mail), расположенный на другом сервере. Прокси-сервер либо подключается от своего имени к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша.

Наиболее распространенная атака на периметр – отказ в обслуживании (Denial-of-Service, DoS), в том числе распределенная (DDoS). В числе методов защиты – фильтрация трафика через сайт специализирующейся на такого рода сервисе компании.

Управление виртуальными машинами. Защита виртуальных машин (VM) включает в себя управление базовым программным обеспечением, своевременную установку обновлений и постоянную инвентаризацию – для того, чтобы обеспечить отсутствие в системе неиспользуемых VM. Необходимо контролировать образы виртуальных машин, хотя это требование более критично для модели IaaS, когда пользующийся публичным облаком злоумышленник может «залить» специально подготовленный образ VM для атаки через гипервизор.

Хорошо зарекомендовало себя так называемое укрепление системы. Оно состоит в удалении лишних программ, функций, учетных записей, приложений, портов и разрешений, благодаря чему уменьшается поверхность атаки – злоумышленники и вредоносные программы имеют меньше возможностей закрепиться в ИТ-экосистеме. Такое укрепление необходимо проводить на протяжении всего жизненного цикла системы: от начальной установки, настройки, обслуживания и поддержки до вывода из эксплуатации в конце срока службы.

Защита данных. Наибольший интерес для злоумышленника представляют данные жертвы. При размещении их в облаке появляются



Рустэм Хайретдинов,
директор по росту
бизнеса, BI.ZONE



Антон Александров,
руководитель
отдела развития
сервисного и
технологического
партнерства,
Positive
Technologies

О том, что SECaaS – состоявшийся тренд, на наш взгляд, говорить рано. Но и единичным предложением это явление уже не назовешь. Интерес к решениям и продуктам ИБ проявляют как облачные провайдеры, так и пользователи.

дополнительные угрозы утечек, обусловленные уязвимостью бизнес-процессов или архитектуры провайдера, а также действиями его персонала (в том числе халатностью). Например, утечка может произойти из-за недостаточного внимания к безопасности резервных копий. Наиболее простой способ защиты – шифрование, лучше всего ключами клиентов, недоступными для обслуживающего персонала. Если злоумышленник доберется до данных, то не сможет легко их расшифровать, и атака станет экономически невыгодной.

Другие риски связаны с расположением данных в облаке. Зачастую клиент не знает, где они реально находятся. Некоторые типы данных, например персональные, должны храниться в стране происхождения. Иначе возникает риск штрафных санкций за невыполнение требований локальных регуляторов.

Есть риск «расползания» данных по инфраструктуре, копирования и хранения конфиденциальных данных в областях, доступных пользователям, которые, согласно политике безопасности, не должны иметь к ним доступа (например, к данным о заработной плате сотрудников – информации, весьма чувствительной для сотрудников). В качестве защиты используются разнообразные методы анализа – автоматического поиска персональных или конфиденциальных данных.

Управление инцидентами. Мало зафиксировать атаку, надо разобраться, что произошло, и принять меры для ликвидации последствий и предотвращения подобных инцидентов в будущем. С этой целью следует постоянно вести мониторинг систем, анализировать журналы действий пользователей и программ. В облаках особое внимание стоит уделить API (Cloud API) – одному из наиболее распространенных способов взаимодействия микросервисов, контейнеров, систем и приложений. На инциденты ИБ могут указывать слишком частые вызовы API. Усиливают защиту аутентификация, авторизация и шифрование трафика.

Предотвратить инциденты помогут системы расширенной защиты от угроз (Advanced Threat Protection, ATP), имеющие доступ к информации о новых угрозах и методах защиты от глобально-

го сообщества ИБ-профессионалов. А системы расследования мошенничества помогут подготовить документы и доказательную базу для суда.

Надежность и доступность. Кибербезопасность подразумевает комплексное обеспечение безопасности информационных ресурсов, в том числе защиту инженерной инфраструктуры. Важную роль играют резервирование, избыточность и возможность самовосстановления систем.

Доступность ресурсов для пользователя повышает использование сети доставки контента (CDN), но такая сеть также требует защиты. Как, впрочем, и распределенная инфраструктура, которая все чаще помимо главного облака включает в себя системы on-premise, периферийные (edge-) облака и устройства интернета вещей. Про периферию забывать не следует, ведь уровень безопасности системы в целом определяется безопасностью самого слабого звена.

Предотвратить все атаки невозможно, правильнее исходить из минимизации их последствий, разработать регламенты действий в случае их осуществления. Если преступнику удалось зашифровать данные, парализовав деятельность компании, надо иметь возможность восстановить данные из резервной копии. Алгоритмы расследований и планы аварийно-восстановительных работ должны быть сформированы заранее.

Спрос на безопасность из облака

Как уже говорилось, пандемия подхлестнула переход к облачным технологиям, бизнес задумался об обеспечении безопасности в новых реалиях, и облачные провайдеры могут с пользой для себя оказать им поддержку. Причем не только в облачной, но и в гибридной инфраструктуре. Например, они могут анализировать в облаке информацию о безопасности, собираемую в системах on-premise, выполняя анализ данных в облачных системах SIEM или SOC, с помощью своих специалистов по ИБ или специализирующихся на информационной безопасности партнеров.

Большинство облачных провайдеров сегодня предоставляют широкий набор сервисов кибербезопасности, таких как защита от DDoS-атак, межсетевые экраны, включая МСЭ уровня веб-приложений, SOC и др. Однако с технологической точки зрения эти решения чаще всего не являются cloud native, т.е. не используют облачную архитектуру в своей основе и не имеют глубокой интеграции в систему оркестрации облака. «SECaaS на современных технологических рельсах предоставляют единицы провайдеров, преимущественно специализирующиеся на кибербезопасности. Наиболее

качественную защиту может обеспечить комбинация IaaS/PaaS-сервисов облачного провайдера и SECaaS облачного провайдера кибербезопасности», – считает Рустэм Хайретдинов, директор по росту бизнеса компании BI.ZONE. В числе других востребованных облачных сервисов безопасности эксперт назвал: VPN-соединение, которое, скорее всего, будет предоставляться в рамках модели SD-WAN с обязательной поддержкой криптографии по ГОСТу; тестирование на проникновение; сервисы непрерывного поиска и устранения угроз (MDR/CloudEDR) с поддержкой контейнерных сред; безопасный веб-шлюз (Secure Web Gateway), когда вместо прямого подключения к веб-сайту пользователь получает доступ к SWG, который затем осуществляет безопасное подключение пользователя к желаемому ресурсу; системы управления ключами.

В плане монетизации для провайдеров наибольший интерес представляют сервисы, на базе которых можно предлагать пользователям дополнительный набор услуг. Скажем, если антивирусную проверку производит провайдер, клиенту нет нужды покупать дополнительный сервис настройки и мониторинга. Достаточно доступа к антивирусному серверу на стороне провайдера и возможности сканирования ресурса. «Если же мы говорим о сервисе на основе SIEM-системы, то здесь клиенту не обойтись без настройки SIEM для себя, и скорее всего, такой клиент захочет получить дополнительный сервис мониторинга событий ИБ, что принесет дополнительный доход провайдеру», – привел пример Антон Александров, руководитель отдела развития сервисного и технологического партнерства Positive Technologies. У самой Positive Technologies наиболее востребованы сервисы защиты веб-приложений (с помощью

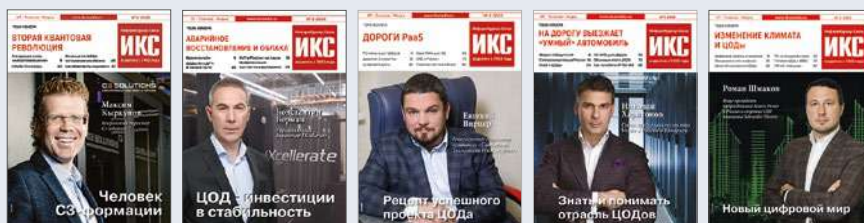
межсетевых экранов уровня приложений) и сервисы анализа информации и мониторинга событий ИБ – на базе SIEM-систем. Тройку замыкают сервисы глубокого анализа сетевого трафика для выявления угроз.

Облачные перспективы

Рынок облачных технологий в России отстает от общемирового на несколько лет, поэтому, глядя на сегодняшние тренды за рубежом, можно предсказать, что ждет нас завтра.

Сейчас там популярны концепция сетевого доступа с нулевым доверием (Zero Trust Networks Access) и периферийный сервис безопасного доступа (Secure Access Service Edge), но, как подчеркнул менеджер продуктов SECaaS SberCloud Александр Иванов, для применения в российских реалиях эти подходы требуют некоторого переосмысления в части криптографии. Также он рекомендует обратить внимание на решения для управления состоянием защиты облачных сред (Cloud Security Posture Management), которые позволяют автоматизировать процесс выявления и устранения рисков, характерных для облачной инфраструктуры. Большинство утечек из облака связаны с человеческим фактором и ошибками конфигурирования, и использование перечисленных инструментов снижает вероятность подобного рода инцидентов. Также будет активно развиваться направление MSS, когда заказчику предоставляются не отдельные инструменты, а комплексная услуга защиты.

Термин SECaaS получил у нас особую популярность после фразы комика Равшана из «Наша Russia»: «Секаса осена не хватает». SECaaS действительно не хватает. Но облачные провайдеры видят запрос рынка, так что можно надеяться, что SECaaS в стране будет больше. **ИКС**



**Специальные условия
при оформлении подписки
для корпоративных клиентов!**

Оформляйте подписку

в редакции — по телефону: + 7 (495) 150-6424

или по e-mail: podpiska@iksmedia.ru

ИнформКурьер-Связь

ИКС

издается с 1992 года

Игры в песочнице

Михаил Кондрашин,
технический
директор в
России и СНГ,
Trend Micro



Противостояние вредоносного ПО и антивирусов привело к тому, что привычный сигнатурный анализ стал недостаточно эффективным. Поэтому все большую популярность завоевывает использование песочниц. Как их реализовать и каковы особенности их работы?

Принцип работы песочницы таков: если не удастся выявить вредоносный характер файла путем проверки его по базе сигнатур, то защитные решения запускают его в специально подготовленной изолированной среде и наблюдают за происходящим. Если файл не выполняет подозрительных или явно опасных действий, его «выпускают» в основную систему. В противном случае защитное решение блокирует файл, перемещая его в карантин и запрещая выполнение.

Почему снизилась эффективность сигнатурного анализа

В распоряжении киберпреступников сегодня имеется инструментарий для создания исполняемых файлов с одной и той же функциональностью, но с совершенно разным кодом, в котором нет характерных последовательностей-сигнатур, позволяющих обнаружить его зловредность.

Еще одна особенность современных угроз – многоступенчатый характер проникновения в систему. Причем начальные стадии обычно реализуются с помощью различных скриптов, в том числе внедренных в офисные документы.

Наконец, нельзя не отметить все более целевой характер кибератак. Стремясь монетизировать преступную деятельность, хакеры занимаются промышленным шпионажем, вымогательством и хищением данных. В качестве жертв они выбирают крупные компании, в сетях которых есть чем поживиться, и не тратят время на незначительные мишени.

Чтобы убедиться в попадании вредоносного кода по назначению, в него встраивают процедуры проверки, которые анализируют характеристики окружения и переходят к выполнению «полезной нагрузки» только в том случае, если окружение соответствует целевому.

И тут на помощь приходят песочницы. Для их реализации могут использоваться следующие подходы:

- изоляция на базе системных политик и списков контроля доступа;

- изоляция на базе частичной виртуализации/контейнеризации;

- полная изоляция в виртуальной машине.

Каждый из подходов имеет свои особенности, благодаря которым находит применение в различных продуктах.

Песочницы на базе политик

В этом случае для защиты основной системы от проверяемого процесса в среде Microsoft Windows может использоваться, например, Software Restriction Policy – встроенный механизм для формирования политик запуска программ. С его помощью можно управлять разрешениями на запись или изменение объектов файловой системы и реестра, создавая соответствующие правила.

Такой подход позволяет удобно обмениваться данными между процессами внутри песочницы и реальной системой, задавая нужный уровень защиты от вредоносных модификаций. Ограничивающие правила не дают процессам атаковать основную систему из песочницы через интерфейсы ОС, и системе защиты не приходится постоянно «откатывать» файловую систему и реестр к начальному состоянию. Благодаря этому песочницы на базе политик лишь незначительно снижают производительность целевой системы, что позволяет их использовать в «лайтовых» версиях антивирусных средств.

Недостатки такого варианта песочниц – это продолжение его достоинств: сложность реализации максимально точного набора ограничивающих правил и невозможность лишь частичного отката изменений внутри песочницы. Кроме того, в песочницах, работающих на базе основной системы, случаются «пробои» защищенной среды с выходом вредоносных программ в основную ОС.

Песочницы на базе частичной виртуализации

Это более сложный в реализации и затратный по системным ресурсам вариант. Тут для проверяемого процесса создаются копии объектов файло-

вой системы и реестра на компьютере пользователя. Если вредонос попытается записать что-либо в файловую систему или в реестр, то для основной системы ничего не изменится – модификации подвергнется лишь дубликат внутри песочницы, реальные данные не пострадают. Дополнительным слоем защиты остается контроль прав процесса. Он блокирует атаки изнутри песочницы через интерфейсы операционной системы.

Из недостатков частичной виртуализации следует отметить более сложный обмен данными между песочницей и основной системой. Кроме того, после каждого проверочного запуска процесса контейнер песочницы требуется очищать, чтобы вернуть в начальное «чистое» состояние. Также остается актуальной проблема «побега из песочницы» – обхода созданных ограничений и выхода вредоносного кода в основную систему.

Песочницы на базе полной виртуализации

Это самый безопасный вариант песочницы, который отличается самым большим потреблением системных ресурсов. Для запуска необходима виртуальная машина с установленной операционной системой, а значит, потребуется больше процессорной мощности и дискового пространства.

Недостаток таких песочниц – еще большая сложность обмена данными, а также увеличение времени на приведение образа виртуальной машины в начальное состояние.

Песочницы с полной виртуализацией серьезно замедляют работу основной системы, поэтому обычно их реализуют в виде сетевых решений на базе выделенного сервера в облаке или внутри сети компании.

Сетевые песочницы

Сетевые облачные песочницы не снижают производительность компьютера пользователя и позволяют проводить проверку на различных операционных системах. Побег из такой песочницы не превратится в угрозу благодаря полной изоляции от рабочего места сотрудника.

Для взаимодействия с сетевыми песочницами на компьютер пользователя устанавливается агент – специальная служба, которая передает подозрительные файлы на проверку. Анализ файлов в облачной песочнице происходит дольше, чем при использовании выделенного сервера в сети компании. Время ожидания результата проверки может достигать нескольких минут, в течение которых запуск файла будет приостановлен.

Важное достоинство сетевых песочниц – возможность создания окружения, максимально точно копирующего типовые рабочие места компании. Дело в том, что вредоносное ПО, ориентированное на проведение целевой атаки, проверя-

ет компьютер, на котором запущено. Если оно обнаружит запуск в виртуальной среде или отсутствие нужных файлов, вредоносные функции могут просто отключиться, и проверка будет пройдена без потерь. Таким образом, чем точнее песочница эмулирует рабочие компьютеры, тем лучшая защита будет обеспечена.

Следует отметить, что облачные песочницы в этом плане проигрывают песочницам на выделенных серверах, поскольку не поддерживают работу с настраиваемыми образами. В случае же с локальным сервером песочниц загрузка на него образа реальной рабочей станции – достаточно простая задача.

Чтобы максимально приблизить конфигурацию виртуальных машин внутри песочницы к реальным условиям, нужно иметь возможность не только загружать образы, но и настраивать их – редактировать перечень языков, устанавливать драйверы и софт, управлять содержимым рабочего стола. Это важный момент, поскольку именно эти элементы окружения часто используются как триггеры для запуска вредоносного содержимого. Продвинутое вредоносное ПО относительно легко определяет стандартные образы песочниц, после чего маскируется под безобидные файлы и обходит защиту.

Максимальную эффективность обнаружения неизвестных угроз на сегодняшний день обеспечивают сетевые песочницы на базе выделенного сервера. Доступные для использования реализации облачных песочниц пока не поддерживают в качестве среды тестирования загрузку собственных образов виртуальных машин, копирующих инфраструктуру рабочих мест заказчика.

Облачные песочницы стоит рассматривать при ограниченном бюджете или территориальной распределенности инфраструктуры. В этом случае затраты на сетевое взаимодействие могут съесть всю выгоду от разницы в стоимости облачного и локального решения.

Взгляд в будущее

Количество вредоносного ПО растет с каждым годом, поэтому технология песочниц неизбежно останется одним из базовых направлений развития защитных комплексов. Следует ожидать повышения производительности, расширения перечня типов анализируемых объектов и добавления новых моделей обнаружения потенциальных угроз, внедрения искусственного интеллекта и машинного обучения.

Помимо этого, мы прогнозируем расширение перечня поддерживаемых операционных систем в качестве сред анализа объектов и развитие функциональности для встраивания песочниц в экосистемы заказчиков с минимальными изменениями ИТ-инфраструктуры. ИКС



Пользователи зарубежных мобильных технологий: заложники или жертвы?

Обеспечение безопасности страны и граждан в киберпространстве невозможно без создания национальной мобильной платформы.



Александр Першин, руководитель рабочей группы по безопасности мобильных технологий, АРСИБ

Мобильная угроза

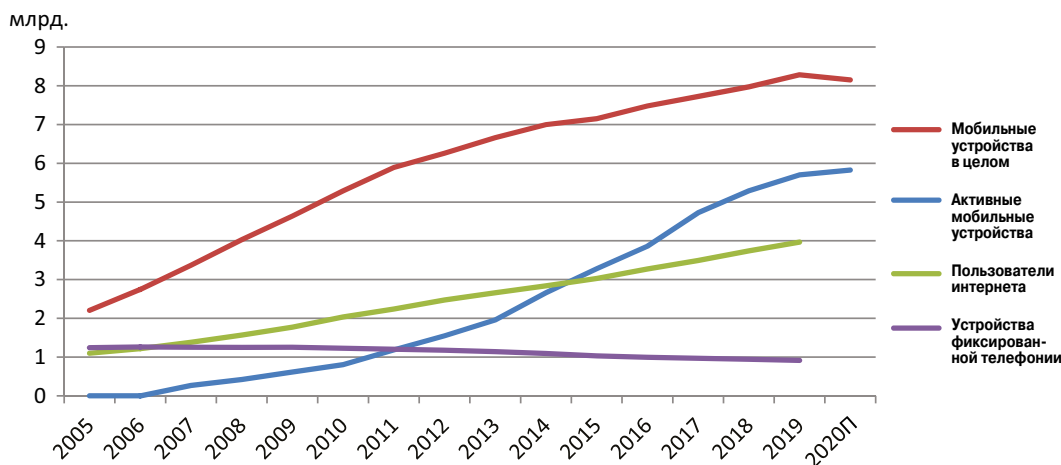
Мобильные устройства давно стали неотъемлемой частью бизнес-процессов компаний и государственных организаций, важным инструментом повышения эффективности их работы. Так, к ноябрю 2020 г. общее количество мобильных устройств в мире, по оценкам Международного союза электросвязи, превысило 8 млрд, причем почти 6 млрд из них были активными (рис. 1).

Стремительно развивающиеся мобильные технологии порождают и новые угрозы, в числе которых – наличие недекларируемых возмож-

ностей (НДВ) в программно-аппаратном обеспечении устройств и приложениях сторонних компаний, трассировка и подмена местонахождения, отслеживание действий пользователей через приложения и др.

Эти вызовы и угрозы обусловлены специфическими особенностями мобильных технологий: с одной стороны, для них отсутствует понятие «периметр контролируемой зоны», а с другой – есть возможность неограниченного во времени и в пространстве несанкционированного доступа к мобильному устройству.

Рис. 1. Рост числа различных коммуникационных устройств и пользователей интернета ▶



Источник: МСЭ

Проблемы микроэлектроники

Большинство современных мобильных устройств построено на базе микропроцессоров архитектуры ARM (Advanced RISC Machine). Современный ARM-процессор – это «система на кристалле» (system on chip), т.е. в одном корпусе содержатся процессор, память, контроллеры внешних устройств для взаимодействия с внешним миром.

Начиная с версий ARM Cortex A5 (мультимедийные процессоры) и R4 (для промышленной электроники и встраиваемых систем), в микропроцессорах появился механизм TrustZone, обеспечивающий аппаратную изоляцию двух параллельных миров: доверенного (безопасного, Secure World) и обычного (нормального, Normal World), в котором работают приложения под управлением привычных ОС (рис. 2).

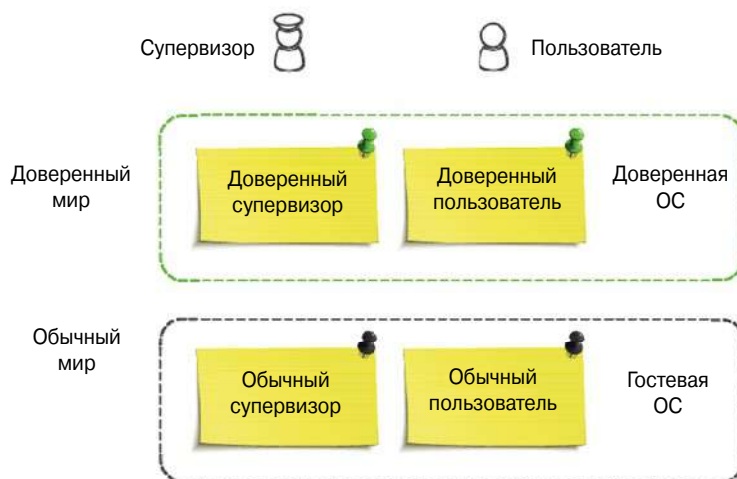
При загрузке процессора сначала загружается специализированная компактная Secure OS, находящаяся в Secure World и контролирующая все коммуникации процессора с внешним миром (контроллеры и периферию). Она же формирует и профиль безопасности (доступные ресурсы, например, объем памяти, внешняя периферия и пр.) для гостевой, т.е. основной ОС (iOS, Android, Sailfish («Аврора»), Linux, Windows и др.) в Normal World.

Несмотря на то что эти два мира изолированы друг от друга, между ними есть тесная связь и возможность общения. Во-первых, Secure OS и загруженные в нее трастлеты (доверенные приложения) имеют неограниченные возможности и могут получить полный доступ ко всем ресурсам – памяти, ключам, устройствам ввода-вывода. Во-вторых, в ядре всех ОС (включая сертифицированные), работающих в Normal World, есть команды передачи управления Secure OS.

Риски использования TrustZone

Декларируется, что TrustZone создана для обеспечения контроля за распространением контента (платное ТВ, музыка, видео), безопасных платежей (Secure PIN) и хранения криптографических ключей (шифрования и подписи), выполнения криптографических операций в изолированной среде (Secure OS) и работы доверенных корпоративных приложений (удаленный безопасный доступ, VPN, аутентификация; защищенная почта; защищенная передача данных и голоса).

Однако при этом приложение из TrustZone может скрытно (и без возможности обнаружения) выполнять шпионские функции (включать микрофон, камеру, вывод на экран, контролировать обмен данными, манипулировать информацией – подменять координаты GPS/



ГЛОНАСС, осуществлять кражу криптографических ключей, отпечатков пальцев с сенсора, ключей для доступа в государственные и корпоративные информационные системы и т.п.). В результате возникают большие риски дистанционного отключения связи, инфраструктуры управления, контроля информационных потоков, перемещения транспорта и людей.

Механизм TrustZone содержат практически все современные ARM-процессоры. «Движки» большинства мобильных, встраиваемых ОС (iOS, Android, Tizen, Sailfish) построены на ядре Linux. При инициализации устройства ядро обращается к механизмам TrustZone (Secure Monitor). Удалить вызовы Secure Monitor из ядра «гостевых» ОС нельзя – они перестанут работать на этих процессорах, так как управлением режимами энергосбережения, загрузкой аппаратных ядер процессора, кэшем и пр. занимается именно Secure OS (подобно BIOS в системах x86).

Удалить или заменить Secure OS в TrustZone практически невозможно (она защищена секретным ключом), обнаружить – крайне сложно. Это можно сделать только по косвенным признакам, например, по наличию команд SMC#0 в ядре гостевой ОС.

Написать свою Secure OS и загрузить ее в импортный ARM-процессор – задача нетривиальная, поскольку документация на аппаратный уровень процессоров, как правило, недоступна (особенно для российских компаний), ключи процессора для загрузки своей Secure OS российским разработчикам также никто не даст.

ARM-процессоры с «открытой» TrustZone или без нее крайне небезопасны. Важно отметить, что все это уязвимости самого нижнего уровня – уровня загрузчика ОС, «вшитого» в процессор, т.е. их практически нельзя устранить, зато их может использовать тот, кто знает о них, и знает, как это сделать.

▲ Рис. 2. Изоляция доверенного и обычного миров в ARM-процессорах

России нужна национальная мобильная платформа

По заявлению бывшего сотрудника АНБ США Эдварда Сноудена, смартфоны скрытно передают в эфир информацию о нас и создают то, что он назвал «личным делом». «Фактически это файл, хранящий полную информацию о личной жизни», – пояснил эксперт, предупредив, что эта информация используется в финансовых и других целях.

Кроме того, мобильные технологии наряду с интернетом могут задействоваться как инструмент для совершения различных противоправных действий: террористической деятельности, работы иностранных спецслужб, несанкционированного доступа к персональным или критичным корпоративным данным, составляющим коммерческую тайну, подмены/блокировки данных критической информационной инфраструктуры и пр.



В совокупности перечисленные уязвимости представляют угрозу национальной безопасности. Более подробно с проблемой можно ознакомиться в подготовленной Ассоциацией руководителей служб информационной безопасности (АРСИБ) брошюре «Безопасность мобильных технологий в корпоративном секторе. Общие рекомендации. Версия 2.0». Таким образом, неизбежно встает сакраментальный для России вопрос: «Что делать?». Ответ: создать независимую от зарубежных поставщиков программно-аппаратную мобильную платформу, в терминах брошюры – Национальную мобильную платформу.

Основные компоненты Национальной мобильной платформы:

- Доверенная аппаратная платформа. Она может быть российской или частично зарубежной сборки. Ее могут составлять микропроцессоры, которые произведены, например, в КНР или странах Юго-Восточной Азии, с использованием российских комплектующих и обязательной приемкой в соответствии с правилами, приня-

тыми в Российской Федерации, и выдачей сертификата установленного образца.

- Доверенная мобильная ОС, включающая встроенные или сторонние средства защиты информации от несанкционированного доступа, а также средства криптографической защиты информации (СКЗИ).

Уже внедряемая в России ОС «Аврора» с приложениями и сертифицированным СКЗИ (также имеет сертификат ФСТЭК России по отсутствию НДВ) – это хорошее решение. Но его следует рассматривать только как промежуточное. Главная проблема – микропроцессоры, заведомо не содержащие НДВ.

Наш «Эльбрус»

Таковыми микропроцессорами могут стать чипы серии «Эльбрус». В 2020 г. на базе процессора «Эльбрус-1С+» Институтом электронных управляющих машин им. И.С. Брука (ИНЭУМ) – частью концерна «Автоматика» госкорпорации «Ростех» – совместно с МЦСТ изготовлен облегченный доверенный планшет (рис. 3).

Созданный полностью по российским технологиям 64-разрядный одноядерный процессор «Эльбрус-1С+» разработан на предприятии МЦСТ с соблюдением норм технологического процесса 40 нм.

По современным меркам характеристики используемого в мобильном устройстве процессора весьма скромные. Однако МЦСТ уже создала 16-нанометровый процессор. Чип, получивший название «Эльбрус-16С», стал первым отечественным CPU, достигшим частоты 2 ГГц. Компания планирует полностью завершить его разработку в 2021 г. Новый процессор, поддерживающий работу ОС «Эльбрус Линукс», будет готов к серийному производству к концу 2021 г., а само производство начнется в первой половине 2022 г.

Непосредственный выпуск будет развернут за пределами нашей страны – в России пока нет заводов, способных выпускать 16-нанометровую продукцию. К целевым потребителям нового чипа относятся производители серверов среднего и высшего классов производительности, систем хранения данных, мощных встраиваемых вычислительных узлов, рабочих станций и суперЭВМ. Возможно ли применение этих процессоров или хотя бы «Эльбрус-8СВ» (28 нм, 1,5 ГГц) в мобильных устройствах – вопрос пока открытый.

Мультиклеточные процессоры

Еще одна возможность – использование решений российской компании «Мультиклет» из

Екатеринбурга, которая занимается разработкой и производством высокопроизводительных отказоустойчивых процессорных ядер и процессоров с низким энергопотреблением, спроектированных на базе мультиклеточной архитектуры (множественный поток команд, множественный поток данных), а также устройств на их основе. Так, 16-клеточный процессор MultiClet В (топология 28 нм) за один такт может выбрать и выполнить до 16 команд.

В настоящее время компания перешла от разработки отдельных процессоров к созданию мультиклеточной платформы, т.е. набора IP-блоков, в состав которого входят мультиклеточные ядра, блоки матричных операций, блоки доступа к памяти с разными алгоритмами кэширования. На основе этой платформы можно проектировать мультиклеточные процессоры различного назначения.

Предлагаемая компанией архитектура принципиально отличается от общепринятой фонеймановской архитектуры. По сравнению с традиционными решениями такой же производительности мультиклеточные процессоры потребляют меньше энергии и используют меньше кремниевых ресурсов, а также характеризуются вирусоустойчивостью на архитектурном уровне. Организация программы и система команд этих процессоров таковы, что незаметное вмешательство в вычислительный процесс практически невозможно. Оно неизбежно приведет либо к остановке процессора, либо к неконтролируемому искажению результатов его работы.

«Стерилизация» импортных решений

Другой путь создания доверенной аппаратной платформы – «стерилизация» импортных решений. Она может осуществляться, в частности, с помощью разработанного компанией «Аладдин Р.Д.» программного модуля Aladdin Trusted Security Module (TSM) и предполагает использование доверенной программно-аппаратной платформы с применением технологии TrustZone для ARM-процессоров серии i.MX6 компании NXP/Freescale. Этот подход позволяет заменить обычный загрузчик ОС на собственный доверенный, загрузить собственную реализацию Secure OS (Trusted Execution Environment) и обеспечить контроль над коммуникациями и процессами, загрузку и взаимодействие с любой гостевой ОС без внесения каких-либо изменений в нее или в используемые приложения.

Aladdin TSM включает в себя:

- Модуль доверенной загрузки, реализующий функции электронного замка и удовлетворяющий требованиям профиля защиты ФСТЭК Рос-



Источник: «Ростех»

сии к средствам доверенной загрузки уровня BIOS второго класса.

- Модуль СКЗИ и электронной подписи, реализующий набор российских криптографических алгоритмов и протоколов и работающий как трастлет в изолированной доверенной среде TrustZone с аппаратным доверенным хранилищем ключей.
- Модуль доверенного ввода-вывода для защищенных приложений, недоступного для перехвата средствами обычной ОС.
- Модуль централизованного управления, позволяющий с использованием системы JaCarta Management System дистанционно управлять ключами и сертификатами, загрузкой трастлетов, безопасно обновлять «прошивку» процессора, загружать и анализировать журналы аудита и т.п.

Области применения: мобильные устройства, терминалы, тонкие клиенты, сетевое оборудование, элементы интернета вещей и др.

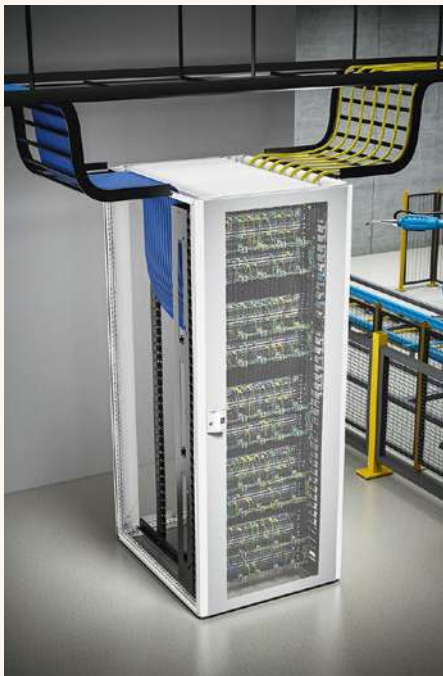
Стандарты безопасности мобильных технологий

Помимо собственных процессора и ОС крайне желательно разработать стандарты, критерии оценки или иные нормативные и регулирующие документы в части безопасности мобильных технологий в корпоративном секторе. За основу можно взять международную систему стандартов Common Criteria (ISO/IEC 15408) в версии 2016 г.

Если не приступить к решению этих задач немедленно, то наблюдаемые сегодня волны кибервойны могут перерасти во всепоглощающее цунами, результатом которого станет киберхаос.

Услышьте нас. Промедление может обойтись дорого... ИКС

▲ Рис. 3.
Прототип планшета на базе микропроцессора «Эльбрус-1С+»



Сетевой шкаф для ЦОДов

Компания Rittal представила TX CableNet – сетевой шкаф, предназначенный для прокладки кабелей с быстрым монтажом.

образом, даже толстые кабельные жгуты быстро соскальзывают с крышки и плавно попадают внутрь шкафа. Это важно для прокладки волоконно-оптических и медных кабелей категории 6 и выше. Конструкция открытой рамы также позволяет использовать всю глубину при подаче кабелей через пол.

Дополнительно можно обеспечить защиту кабельных вводов от пыли и грязи с помощью плотных щеточных буртиков, а также установить вентиляторную панель для контроля микроклимата в шкафу.

Новые корпуса имеют сварную конструкцию каркаса со сплошной системной перфорацией 25 мм, что расширяет список совместимых комплектующих и позволяет закреплять несущие кабельные шины и органайзеры в произвольных местах шкафа.

Продуктовый портфель TX CableNet включает 13 типоразмеров шка-

фов с вентилируемыми дверями или передней обзорной и задней глухой дверью. Доступны корпуса высотой 2200 мм (47 U), 2000 мм (42 U), 1200 мм (24 U), шириной 800 или 600 мм и глубиной 600, 800 или 1000 мм. Кроме того, для нового шкафа разработаны новые вертикальные органайзеры – кабельная трасса, сетчатый кабельный лоток. Вертикальные профильные шины 19” адаптированы для установки блоков распределения питания (PDU) в пространство Zero Unit даже при ширине шкафа 600 мм. Шкафы допускают соединение в линейку без боковых стенок для удобства применения в телекоммуникационных помещениях и ЦОДах. Для достижения максимальной плотности сетевых портов совместно с TX CableNet рекомендуется использовать систему горизонтальных сетевых кабельных органайзеров Rittal NCO.

www.rittal.ru

«Зеленое» решение для энергоснабжения

Компания ДКС начала выпуск гибридных солнечных инверторов-накопителей Energy Omni System (EOS), которые дают возможность использовать солнечную энергию в любое время суток.

В этом решении применяются инвертор на IGBT-транзисторах и ПО с русскоязычным интерфейсом. Накопителями служат литий-железо-фосфатные (LiFePO₄) аккумуляторы с ресурсом до 6 тыс. циклов заряда/разряда.

Инвертор-накопитель EOS управляет источниками электроэнергии (солнечные панели, аккумуляторные батареи, сеть, генератор) в зависимости от нагрузки, тем самым обеспечивая максимальную автономию и качество энергоснабжения. Решение EOS отличается компактностью, длительным сроком беспере-



бойной работы (до 15 лет) и простотой использования.

Линейка EOS представлена однофазными (мощностью 3–6 кВт) и трехфазными (18 кВт) преобразователями и набором аккумуляторов емкостью 4,8–24 кВт·ч. Кроме того, есть возможность использовать EOS для зарядки электромобилей. Для этого потребуется подключить к ним сертифицированные розетки Wallbox.

Удаленный мониторинг системы ведется с помощью мобильного приложения для iOS и Android, разработанного компанией ДКС.

www.dkc.ru

Бюджетные ИТ-шкафы

Компания **Schneider Electric** представляет под брендом **APC by Schneider Electric** линейку ИТ-шкафов **Easy Rack**, которая заменит в портфеле производителя серию бюджетных шкафов **NetShelter SV**.

Разработанные на базе монтажных шкафов **NetShelter SX**, шкафы **Easy Rack** имеют крепкую рамную конструкцию, которая обеспечивает статическую нагрузочную способность до 1200 кг и динамическую нагрузочную способность до 600 кг.

Типоразмеры монтажной высоты 42U и 48U дополнены компактными вариантами 24U для небольших инсталляций. Типоразмеры ширины шкафов остались стандартными – 600 и 800 мм. Шкафы шириной 800 мм кроме стандартных горизонтальных мест для установки 19"-оборудования имеют до 12 дополнительных вертикальных мест 1U в монтажных направляющих для размещения компактного оборудования и аксессуаров. **Easy Rack** имеют четыре типоразмера глубины: 800 мм, 1000 мм, 1100 мм, 1200 мм. Одно из преимуществ перед серией **SV** – увеличенная полезная глубина при тех же габаритах шкафа.

Передние одностворчатые и задние двухстворчатые двери в шка-



фах **Easy Rack** имеют большую по сравнению с **NetShelter SV** площадь перфорации, а также увеличенный до 81% паттерн перфорации. В совокупности это обеспечивает лучшую вентиляцию для беспрепятственного воздухообмена.

Для удобства обращения боковые панели шкафов **Easy Rack** облегчены и разделены горизонтально. Более того, в целях экономии или построения сквозных рядов шкафы **Easy Rack** можно приобрести без боковых панелей.

Крышные панели шкафов **Easy Rack** оснащены отверстиями для ввода кабелей со щеточными уплотнителями и монтажными отверстиями для установки лотков, разделителей и аксессуаров для рядной прокладки и организации кабелей по аналогии с моделями **NetShelter SX**.

В стандартную комплектацию шкафов **Easy Rack** входят встроенные регулируемые ножки и транспортировочные ролики, две пары направляющих с легко читаемой маркировкой юнитов, кронштейны для установки 0U-аксессуаров без применения инструмента, скобы для стягивания шкафов, базовый комплект крепежа и др.

Шкафы **Easy Rack** совместимы с системами контейнеризации **EcoAisle** и **HyperPOD**, системой мониторинга и контроля доступа **NetBotz** и с широким спектром аксессуаров **NetShelter**. В дополнение к этому для **Easy Rack** доступны аксессуары серии **Easy**, а также широкий ассортимент стоечных блоков распределения питания **Easy PDU**.

www.schneider-electric.ru

ИТ-хаб для замены традиционной серверной



Компания **SME** выпустила решение, которое может использоваться в качестве замены традиционных серверных в гражданском и промышленном сегменте, например, для размещения мини-ЦОДа и коммутационного узла одновременно.

ИТ-хаб представляет собой двухсекционный монолитный конструктив с корпусом из листовой оцинкованной стали. Он штатно комплектуется системой кондиционирования воздуха; внутри имеются механические опоры для установки системы газового пожаротушения. Кроме того, в различных исполнениях опционально устанавливаются элементы силового оборудования (**PDU**, **ИБП**).

Шкаф имеет две передние и две задние двери. Каждая из четырех дверей поддерживается тремя петлями, которые скрываются при ее закры-

тии. Снаружи каждая дверь снабжена эргономичным замком с четырьмя точками запираения, а также электрическим замком, работающим от постоянного тока с напряжением 12 В, и соединена с корпусом шкафа заземляющим проводом. Шкаф имеет снаружи кондиционер мощностью 1 кВт.

Доступ к каждой из двух секций шкафа осуществляется независимо. Система контроля доступа может быть интегрирована как на этапе производства, так и непосредственно при установке решения.

www.sme-russia.ru

3DATA Тел.: (800) 505-1800 E-mail: 3data@3data.ru www.3data.ru 4-я обл.	ABB Тел.: (495) 777-2220 www.abb.com с. 62–63	IXCELLERATE РОССИЯ Тел.: (495) 800-0911 E-mail: info@ixcellerate.ru www.ixcellerate.com 1-я обл.
ВАЙСС КЛИМАТЕХНИК Тел.: (495) 787-2043 E-mail: weiss.ru@weiss-technik.com www.weiss-technik.ru с. 45	C3 SOLUTIONS Тел.: (495) 133-1717 E-mail: info@c3solutions.ru www.c3solutions.ru с. 22–23	RITTAL Тел.: (495) 775-0230 Факс: (495) 775-0239 E-mail: info@rittal.ru www.rittal.ru с. 32–33, 47, 48–49
СВОБОДНЫЕ ТЕХНОЛОГИИ ИНЖИНИРИНГ Тел.: (495) 120-2866 E-mail: info@sv-tech.ru www.sv-tech.ru с. 56–58, 3-я обл.	INNIO Тел.: (495) 228-8398 E-mail: contact.ru@innio.com www.innio.com/ru/rucis с. 72–73	SCHNEIDER ELECTRIC Тел.: (495) 777-9990 Факс: (495) 777-9992 www.schneider-electric.ru 2-я обл., с. 38–39

Указатель фирм и организаций

3data 62, 63	HTS 9, 33	Selectel 1, 4, 5	Комиссариат по ядерной энергии (Франция) 43
650 Group 30	Huawei 9, 46	Sensely 80	АНО «Координационный совет по ЦОДам и облачным технологиям» 12, 13, 14, 15, 50
ABB 32, 45, 62, 63	IBM 79	Siemens 10, 11	«Кронштадт» 11
Accenture 79	IDC 20	Singtel 20	ГК ЛАНИТ 78
Aeromax 11	IEA 27	Skytracking 77	МГТС 75, 76
Albedo 17	IEC 50, 53, 54, 93	SME 95	Медицинская школа Бостонского университета 80
Alibaba 38	IEEE 36, 41	StoreData 14	Международное агентство по возобновляемым источникам энергии 9
Amazon 38	iKS-Consulting 1, 4, 5, 6, 8, 9, 26, 83	Stulz 9, 32, 33, 44, 49, 63	Международный союз электросвязи 90
ANSI 50, 55	INNIO 72	TeleHealth Services 79	Минпромторг России 17
Artezio 78	InnovIT 55	TIA 50, 55	Минцифры России 15
Arvato Systems 48	Intec 17	Transparency Market Research 75	«Миран» 4, 5, 6, 14, 32, 33
BICSI 50	Interxion 38	Trend Micro 88	МТУ РУС 46
BI.ZONE 85, 87	ISE 35	TÜViT 54, 55	«Мультиклет» 92
BOREY 45	ISO 50, 53, 54, 93	UiPath 20, 21	МЦСТ 92
BSI Group 55	Ivideon 77	Upsite Technologies 55	Научный инновационный центр. Национальная служба здравоохранения Великобритании 80
C3 Solutions 22, 23	IXcellerate 14, 18, 19, 43	Uptime Institute 1, 5, 8, 13, 14, 19, 27, 44, 50, 52, 55, 69	«Новые Технологии» 22, 23
ГК Cabero 44	Janitza 46	Vertiv 43, 45	«ПламСпейс» 16
Capitoline 55	John Deere 24	Viavi 17	«ПрофАйТиКул» 44, 59
CEN 50, 51, 53, 54	KIO Networks 43	Vodafone 38	«Ростелеком» 14, 77
CENELEC 50, 51, 53, 54	Linxdaticenter 4	Wandel & Goltermann 17	«Ростелеком-ЦОД» 4, 5
Certification & Information Security 55	Marioff 43	Wavetek 17	«Ростех» 92
China Telecom 38	MarketsandMarkets 78	Wiltron 17	«Росэнергоатом» 4, 14
Cisco 41	Microsoft 20, 21, 38, 88	ZALA 10	«Свободные Технологии Инжиниринг» 41, 56, 58
Colt 38	Mitsubishi Electric 44	ZutaCore 49	«СКАУТ – Корпоративные решения» 77
CommScope 26, 34, 41, 42	Moodys 84	«Автоматика» 92	«Сколково» 16
Data Center Alliance 55	MSK-IX 5, 19	«Аладдин Р.Д.» 93	СПб ИАЦ 6
Data Center Group 55	MTU 46	АНБ США 92	Тамбовский государственный университет 11
Deutsche Welle 49	Nature 78	Ассоциация руководителей служб информационной безопасности 90, 92	«Технорегион» 11
Digital Realty 38	NTT 38	«Атомдата-Центр» 14	ФСК 4
DIN 51, 54	NXP/Freescale 93	Балтийский завод 6	ФСТЭК России 92
Enterprise Product Integration 55	ÖNORM 51	«Вертолеты России» 10	«ЭР-Телеком Холдинг» 4
Equinix 38	OVHcloud 43	Гознак 5, 14	
Ericsson 43	Positive Technologies 86, 87	«ДатаДом» 64	
ETSI 50	PubMed 78	«Ди Си Квадрат» 56	
Euris Technology 52	PwC 21	«Додо пицца» 76	
Exfo 17	Qrator Labs 83	«ИКС-Медиа» 4, 8, 40, 83	
Facebook 38	RCCPA 77	Институт электронных управляющих машин им. И.С. Брука 92	
Future-Tech 55	Rittal 6, 9, 32, 33, 44, 48, 49, 94	Калифорнийский университет 59, 80	
Gartner 20, 21	Rohde & Schwarz 17		
General Electric 72	Rolls-Royce 9, 46		
Google 79	SberCloud 83, 87		
Grand View Research 75	Schneider Electric 6, 8, 38, 39, 40, 95		
Heritage 21			
Hewlett-Packard 17			

Учредители журнала «ИнформКурьер-Связь»:

ООО «ИКС-Медиа»:

105066, Москва
ул. Новорязанская, д. 31/7, корп. 14;
тел.: (495) 150-6424

МНТОРЭС им. А.С. Попова:

107031, Москва, ул. Рождественка,
д. 6/9/20, стр. 1;
тел.: (495) 921-1616.



СВОБОДНЫЕ
ТЕХНОЛОГИИ
ИНЖИНИРИНГ

ПРОСТЫЕ РЕШЕНИЯ СЛОЖНЫХ ЗАДАЧ

ПРОЕКТИРОВАНИЕ И СТРОИТЕЛЬСТВО ДАТА-ЦЕНТРОВ

Реклама

Россия, 127055, Москва,
Бутырский вал, д. 68/70, стр. 2
+7 (495) 120-28-66
info@sv-tech.ru
www.sv-tech.ru





Платформа цифрового развития

| Дата-центры | Облачные сервисы | Услуги связи | Хранение данных



+7 (495) 800-1-800
+7 (800) 505-1-800



3data.ru



Реклама