ТЕМА НОМЕРА

СКС-2023: НОВАЯ КОНФИГУРАЦИЯ РЫНКА

ИнформКурьер-Связь
ИКС
издается с 1992 года

Systême electric

Приглашаем на

ИННОВАЦИОННЫЙ САММИТ 2023

Технологическая независимость в новых реалиях

24-25 МАЯ 2023

ТЕХНОПОЛИС

Регистрация

16+

Издается с мая 1992 г.

Издатель
ООО «ИКС-МЕДИА»

участник
АНО КС ЦОД
КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

Генеральный директор
Д.Р. Бедердинов
dmitry@iksmedia.ru

Учредитель:
ООО «ИКС-МЕДИА»

Главный редактор
А.Г. Барсков
a.barskov@iksmedia.ru

РЕДАКЦИЯ
iks@iksmedia.ru

Ответственный редактор
Н.Н. Шталтовная
ns@iksmedia.ru

Обозреватель
Н.В. Носов
nikolay.nosov@iksmedia.ru

Корректор
Е.А. Краснушкина

Дизайн и верстка
Е.В. Денисова

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

СЛУЖБА РАСПРОСТРАНЕНИЯ
Выставки, конференции
expo@iksmedia.ru
Подписка
podpiska@iksmedia.ru

Журнал «ИнформКурьер-Связь» зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, регистрационный номер ПИ № ФС77-82469 от 30 декабря 2021 г.
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.

Адрес редакции и издателя:
105082, Россия, г. Москва,
2-й Ирининский пер, д. 3
Тел./факс: (495) 150-6424
E-mail: iks@iksmedia.ru
Адрес в Интернете: www.iksmedia.ru

Дата подписания в печать: 05.05.23.
Дата выхода в свет: 16.05.23.
Тираж 5 000 экз. Свободная цена.
Формат 64x84/8
Типография: ООО "ПРОПЕЧАТЬ",
адрес типографии 119618, г. Москва,
Боровское ш., дом 2А, корп. 4, кв. 260.

ISSN 0869-7973

Время проверок

Российская индустрия ЦОДов проходит непростой этап кардинальной смены основных поставщиков. И мне все чаще приходится слышать жалобы компаний, что если у ушедших мировых лидеров цифры в спецификациях соответствовали фактическим показателям, то у вендоров «второго эшелона» это далеко не всегда так.

Вот показательный пример. Крупный оператор ЦОДов установил ИБП нового для себя вендора. По характеристикам оборудование один в один соответствовало тем аппаратам именитой американской корпорации, на которые компания ориентировалась прежде. Да и набившая оскомину фраза, что «все делается на одной фабрике в Шэньчжэне»... Короче, новый ИБП установили даже без тщательного тестирования. И реальный КПД оказался существенно ниже заявленного. В результате расходы на электричество выросли, и бизнес-модель перестала «сходиться».

Другой пример. Не менее крупный облачный провайдер в рамках программы развития серверного парка решил закупить отечественное оборудование. Составили список из примерно 30 отечественных производителей (немало!), запросили у них серверы для проверки. Получили продукты от десятка компаний. Тесты не прошел ни один. Конечно, требования облачного провайдера жестче, чем у среднего корпоративного клиента. Но результат все равно печальный.

Или вот совсем простой пример. Про высокоплотные СКС. Да, российские производители (фактически сборщики или перепродавцы китайских продуктов) предлагают решения с той же плотностью оптических разъемов, что и ушедшие Commscope, Panduit, Corning. Формально цифры в презентации соответствуют реальному числу разъемов на панели. Но в таких решениях самое главное – удобство эксплуатации. А оно выяснится только после определенного времени работы с СКС.

Что делать? Быть максимально дотошными. Не покупать по бумажкам. Требовать от поставщика проведения тестов на заводе. Проверять все самим. Понятно, что это может оказаться не по силам небольшим компаниям. Вероятно, они увеличат собой число пользователей сервисной модели – пойдут в коммерческие ЦОДы и/или в облака. Значит, нагрузка на операторов ЦОДов и облачных провайдеров будет расти. А им уж точно нельзя покупать критические системы без тщательного тестирования. Ведь при возникновении проблем в их инфраструктуре клиентам пойти будет некуда.

Успешных тестов,
Александр Барсков

ТЕМА НОМЕРА

СКС-2023: новая конфигурация рынка

с. 22

TravelTech, цифровые кочевники и российский туризм в новой реальности

Н. Носов. Квантовые коммуникации: итоги 2022 года

Э. Лоуренс и др.
Пять прогнозов для ЦОДов на 2023 год

Н. Носов.
Взрывной рост, гособлако и «таблица Менделеева» виртуализации

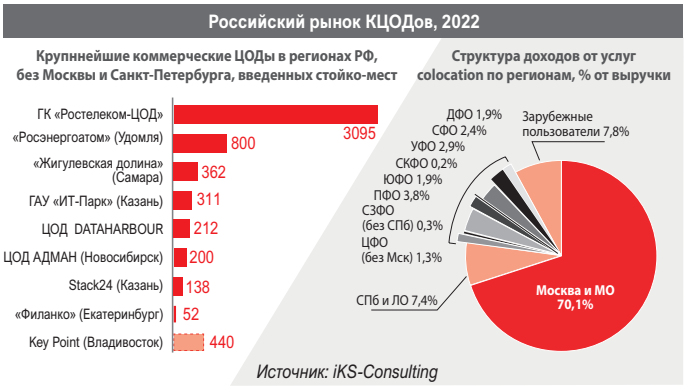
Затянувшийся рассвет

ЦОД модели сервисы инфраструктура

Проведенная «ИКС-Медиа» в Казани ежегодная конференция «ЦОД: модели, сервисы, инфраструктура» показала, что Татарстан, после резкого старта ставший лидером среди регионов по уровню цифровизации, испытывает дефицит ресурсов коммерческих ЦОДов.

Трудности перехода

По данным iKS-Consulting, Приволжский федеральный округ в 2022 г. сохранил третье после двух столиц место по доходам от услуг colocation на российском рынке коммерческих ЦОДов (3,8%), однако к нему подтягиваются УФО (2,9%), СФО (2,4%) и ДФО (1,9%).



Все российские компании работают в сложных условиях санкций, испытывают проблемы с вендорами, логистикой, оплатой и поставками оборудования. Но, например, ГК Key Point, запустившая дата-центр на 440 стоек во Владивостоке, с новыми вызовами справилась и задержала запуск ЦОДа только на три месяца. Построенный ЦОД даже успел пройти сертификацию Uptime Institute и получить сертификат не только на проект (Tier III Design), но и на объект (Tier III Facility) – первый сертификат такого уровня у российского регионального коммерческого ЦОДа.

На этом фоне особенно ярко видны проблемы строительства коммерческих ЦОДов в Татарстане. По суммарному количеству стойко-мест («ИТ-Парк» – 311, Stack 24 – 138) Казань по-прежнему уступает только тверской Удомле, но по динамике ввода новых мощностей – и остальным основным конкурентам. Так, делегаты конференции отмечали, что в регионе очень сложно взять в аренду стойко-место в ЦОДе, свободных просто нет. А новые мощности давно не строятся.

Возводимый в Иннополисе госкорпорацией «Росатом» (в лице «Атомдата-Иннополис» – дочерней компании «Росэнергоатома», входящей в Электроэнергетический дивизион «Росатома») ЦОД должен был быть открыт во II квартале 2022 г., но, по последним данным, срок ввода в эксплуатацию перенесен на декабрь 2023-го. В конце года планируется запустить первую очередь на 1000 стойко-мест. В целом проектное решение ЦОДа в Иннополисе предусматривает до 2000 стойко-мест с надежностью уровня Tier III.

А пока крупнейший ЦОД в Татарстане только строится, делегаты интересовались, не планируют ли дефицитом стойко-мест воспользоваться другие игроки, в том числе участвовавшие в конференции Key Point и Oxygen. Вопросы крайне актуальные: для многих компаний среднего и малого бизнеса использование сервисной модели – единственно возможный путь не только развития ИТ-инфраструктуры, но и выживания в новых условиях.

ЦОД как крепость

Построить ЦОД в Татарстане представители Oxygen не обещали, а вот с облаками готовы помочь. Причем с учетом текущей специфики – резко возросшего числа кибератак. Директор по информационной безопасности Oxygen Кирилл Орлов сравнил ситуацию с идеальным штормом – вал атак на российские компании всех отраслей сопровождается уходом зарубежных вендоров ИБ и прекращением поддержки поставляемых ими решений.

Противопоставить «шторму» можно перенос ИТ-инфраструктуры в облако, находящееся под защитой профессионалов, которые не только отбивают идущие на крепость-ЦОД атаки, но и расследуют инциденты. Компания выступает как MSSP (Managed Security Service Provider), предлагая по подписке сервисы ИБ, в том числе готовые аттестованные отраслевые решения.

Директор по стратегии Oxygen Артур Юсипов назвал предлагаемую компанией модель работы «облачный интегратор для ИТ-департаментов». Такой интегратор предоставляет не только услуги безопасности, но и другие необходимые заказчику сервисы.

Мифы о регионах

Вокруг строительства ЦОДов в регионах сложилось много мифов, которые развеял сооснователь ГК Key Point Евгений Вирцер. Наиболее распространенный миф – ЦОДы в регионах и не нужны, поскольку там все пользуются центральной инфраструктурой и этого достаточно. Эксперт считает, что ЦОД необходим в каждом регионе. При протя-


К. Орлов (Oxygen)


Е. Вирцер (ГК Key Point)


И. Христофоров (ART Engineering)


Интеллектуальные PDU от «МиК»

женности нашей страны задержка в передаче пакета, посланного из Москвы в Омск, достигает 42 мс, а во Владивосток – 114 мс, что делает невозможным использование многих облачных сервисов. Кроме того, иметь рядом ЦОД, пусть небольшой, просто удобнее.

Считается, что строить ЦОД в регионе дорого. На самом деле более сложной будет логистика, дороже обойдутся ошибки в проектировании и рабочая сила с учетом всех командировок, а цены на оборудование окажутся выше из-за низкой региональной конкуренции. Но эти факторы компенсируются низкой стоимостью земли и более дешевой строительной инфраструктурой, поэтому в целом затраты на строительство ЦОДа в регионе будут примерно такими же, как в столице.

Считается, что в регионах остро стоит проблема набора персонала для эксплуатации дата-центра. Действительно, такая проблема есть. Но она есть и в столице, и, как добавил директор по развитию бизнеса в России и СНГ Uptime Institute Константин Королев, во всем мире. Пути решения тоже общие – автоматизация процессов, повышение квалификации на курсах, например, таких, как проводит АНО КС ЦОД. Помогут сотрудничество с вузами, набор и обучение персонала за 6–12 месяцев до ввода ЦОДа в эксплуатацию.

Мифом оказалось утверждение, что в регионах не нужна сертификация ЦОДов в силу малой востребованности у заказчиков. Успешный опыт строительства ГК Key Point ЦОДа в Владивостоке, когда спрос во время строительства за два месяца вырос с 50 до 200 стоек, а в итоге достиг 440, показывает, что запрос на ЦОДы с качеством, подтвержденным сертификацией, в регионах есть. А исполнительный директор компании «Ди Си квадрат» Александр Мартынюк объяснил, что сертификация регионального ЦОДа не такой уж сложный процесс.

ГК Key Point не только развеивает мифы, но и занимается реальным созданием региональной сети ЦОДов. В июне 2022 г. группа анонсировала строительство 35 дата-центров в течение ближайших пяти лет во всех федеральных округах России.

Технические вопросы

Развенчивая миф о непонимании специфики ЦОДов, делегаты активно интересовались техническими новинками, представленными на выставке. Одна из таких новинок – система изоляции коридоров компании ART Engineering, которая позволяет гибко создавать горячие и холодные коридоры в помещениях разнообразной, даже ломаной формы.

С уходом западных вендоров российские ЦОДы столкнулись с дефицитом отдельных позиций оборудования. Но если, скажем, с дизель-роторными системами ситуация действительно сложная, то с СКС особых проблем нет. Российские вендоры активно осваивают освободившуюся нишу. Наглядный пример – новая оптическая СКС Optic X компании C3 Solutions. Помимо кроссового шкафа в поставляемую номенклатуру входят панели в серверных стойках, четыре модификации центрального кросса, оптические магистральные линии и патч-корды.

С интересом делегаты встретили доклад руководителя направления «Энергетика» компании РЭНЕРА Алексея Нешты о российских литий-ионных АКБ для ИБП, которые компания теперь предлагает и дата-центрам. В последнее время мировые цены на литий существенно выросли, что заставило проектировщиков задуматься о целесообразности использования литий-ионных АКБ в ЦОДах, несмотря на все их преимущества. Смягчить ситуацию смогут поставки отечественного сырья. По словам А. Нешты, в России планируется вернуться к добыче лития, прекращенной по экономическим соображениям в 2007 г.

Привлекли внимание представленные компанией «МиК» PDU, которые уже активно используются в ведущих ЦОДах страны. Саратовская компания работает на рынке 15 лет и имеет всю номенклатуру устанавливаемых в дата-центрах PDU, вплоть до моделей с мониторингом каждой розетки.

■■■

В числе решений проблем в развитии дата-центров в Татарстане, которые высветила конференция «ИКС-Медиа», – более активное привлечение на региональный рынок игроков федерального уровня. Это поможет повысить конкуренцию и расширить спектр предлагаемых продуктов и услуг.

В целом у Татарстана есть все, чтобы сохранить лидирующее положение среди регионов. Как отметил директор ДИТ банка «Ак Барс» Константин Черников, к преимуществам республики на рынке дата-центров относятся квалифицированные кадры и энергетика – дело за популяризацией ЦОДов. Рассвет цифровизации наступает небыстро, но он объективно неизбежен.

Николай Носов
Казань – Москва

TravelTech, цифровые кочевники и российский туризм в новой реальности

Несмотря на все сложности последних лет – а может быть, и благодаря им, – информационные технологии прочно вошли в арсенал туристической индустрии.

Такой вывод можно сделать после посещения Международной выставки туризма и индустрии гостеприимства MITT 2023.

Тренды TravelTech

Современную туристическую отрасль невозможно представить без компьютеров. Появилось целое направление TravelTech – применение информационных технологий в индустрии путешествий, туризма и в гостиничном бизнесе. К решениям TravelTech относятся централизованные системы бронирования, системы анализа цен, управления недвижимостью, каналами продаж. Программные комплексы помогают разрабатывать туристические продукты, планировать поездки, заказывать услуги, собирать и анализировать отзывы туристов об отелях, достопримечательностях и путешествиях.

Общемировые тренды развития TravelTech перечислил член правления Российского союза туриндустрии (РСТ) Леонид Мармер. В первую очередь он выделил ориентацию на мобильные устройства, которые стали неотъемлемой частью жизни современного человека. С помощью устанавливаемых на смартфон программ человек находит, бронирует и оплачивает туристические услуги. Мобильные приложения напоминают о времени начала и окончания бронирования номера, а смартфон может даже использоваться вместо ключа (своего рода мобильный консьерж).

Все большее распространение получают цифровые, в том числе бесконтактные платежи. Популярный за рубежом подход к оплате услуг после их получения (Buy Now Pay Later, BNPL) стал шире применяться и в туротрасли, в частности, при оплате отелей.

Не обошло туриндустрию и обострение проблем кибербезопасности. В 2022 г. на 13% увеличилось количество атак злоумышленников, причем число утечек персональных данных выросло на 100%, а мошенничеств при бронировании и оплате услуг – на 150%.

Как и в других отраслях бизнеса, в туриндустрии все чаще используется интернет вещей. Уже не вызовет удивления «умный чемодан», который сам передвигается за владельцем, а в случае потери отправляет ему СМС со своими координатами. Все более «умным» становится номер в отеле, предлагающий постояльцу кастомизированные услуги исходя из его предпочтений, выявленных в цифровом мире. «Умнеют» также автомобили и города в целом.

Искусственный интеллект пробует себя в роли турагента. Обычными становятся чат-боты и виртуальные помощники, способные работать в режиме 24/7. Аватар с ИИ заменяет за стойкой регистрации портье, выдавая ключи и регистрируя постояльца, а нейросеть ChatGPT уже способна писать рекламные буклеты.

Пандемия и карантинные ограничения показали преимущества удаленной работы и привели к появлению так называемых цифровых кочевников. Действительно, если можно удаленно работать из дома, почему бы не делать это из более комфортного места, например, тропического острова, совмещая работу с отдыхом и туризмом. Или, не нарушая разрешенные для пребывания сроки, переезжать из страны в страну, выбирая их по наиболее комфортному сезону и соображениям личной безопасности. Тренд на «удаленку» общемировой – ожидается, что к 2025 г. в США будет 36,1 млн удаленных работников.

Бронируем но-нашему

Участники прошлогодней выставки МИТТ 2022 высказывали много опасений в связи с введением санкций, уходом с рынка западных компаний, в том числе вендоров программного обеспечения.

До событий 2022 г. доминирующее положение на российском рынке онлайн-бронирования гостиниц занимала компания Booking.com. По оценкам президента РСТ Ильи Уманского, ее доля достигала 70%. Теперь ниша освободилась, и в борьбу за нее включились несколько российских компаний, в том числе «Суточно.ру» и «Островок». Обширную базу по местам размещения в Крыму имеет разработанный краснодарцами сайт Tvil.ru. Увеличить долю рынка стремятся тяжеловесы: «Яндекс» с сервисом «Яндекс Путешествия» и купившая сайт Bronevik.com компания МТС (МТС Travel).

Подключилось государство – в марте 2022 г. вице-премьер Дмитрий Чернышенко поручил Ростуризму совместно с Минцифры проработать вопрос создания российского аналога Booking.com. В апреле на туристическом сервисе Russpass, разработанном по инициативе правительства Москвы, появилась возможность бронировать номера в отелях по всей России. Сервис онлайн-бронирования квартир в посуточную аренду запустила занимающаяся продажей недвижимости компания «Циан». Свои сервисы бронирования отелей имеют Ozon, РЖД, 2GIS («Отелло»).

Явного лидера пока нет, российские компании уступают Booking.com по числу предложений, удобству сервиса, техподдержке. И нет уверенности, что бронь сработает, – надежнее дополнительно связаться с отелем и получить подтверждение. Ведь может оказаться, что гостиница разорвала договор с сервисом год назад, а агрегатор забыл убрать ее с сайта.

Появились новые подходы к бронированию. Например, в сервисе бронирования отелей GetHotel клиент сам назначает цену. Система дает выбор отелей, удовлетворяющих требованиям клиента, и возможность торговаться с администрацией. Согласование цены идет в чате сайта.

С прекращением работы в России международных программ бронирования VIP-залов в аэропортах Lounge Key и Priority Pass понадобились аналогичные российские решения. Одним из них стала цифровая платформа бронирования премиальных услуг в аэропортах b2b.vip-zal.ru. Решение автоматизирует процесс заказа таких сервисов, как проход в VIP- и бизнес-залы, сопровождение сотрудником для ускоренного прохождения аэропортовых процедур (fast-track) и встречу по прилету с именной табличкой помощника (meet & assist) в более чем 300 аэропортах мира. Клиент может письменно сформулировать свои пожелания относительно услуг в специальной форме – их прочитает и отправит на обработку используемый в системе искусственный интеллект.

«Умный» номер

Одна из основных проблем, тормозящих развитие внутреннего туризма, – недостаточное количество номеров в отелях. По законам рынка, высокий спрос при ограниченном предложении приводит к повышению цен, что мы и наблюдаем в России, где стоимость номера существенно выше, чем у сравнимого по качеству в большинстве зарубежных стран. Один из выходов – развитие систем апартаментов и сдачи частного жилья. Неудобство для туриста в том, что приходится договариваться о минимум двух встречах с хозяином квартиры: чтобы получить и сдать ключ. Избежать потерь времени поможет приложение RoomSharing. Турист через интернет бронирует номер или квартиру, отправляет на сайт данные своего паспорта. После подтверждения вносит оплату и получает ссылку на мобильное приложение, которое открывает замок, и резервный электронный ключ – код для открытия замка. Если к вам пришли гости, а вы стоите в пробке – можете открыть замок через приложение удаленно, чтобы они попали в ваш номер. При выселении система обновляет пароли. Потом приезжает горничная со своим смартфоном и новым паролем, а владелец номера контролирует время уборки. Как объяснила представитель использующей RoomSharing сети мини- и апарт-отелей Norke Валерия Душевская, приложение интегрировано с системой бронирования и облачной программой управления гостиницей (Property Management System, PMS), разработанной компанией TravelLine.

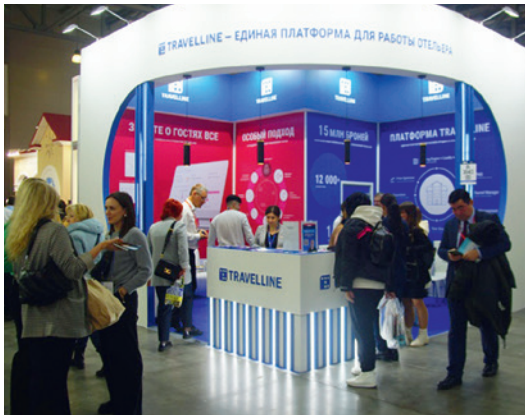
Чтобы использовать приложение RoomSharing, нужно установить специальный «умный» дверной замок. В случае же работы с системой Connect One для управления онлайн-регистрацией гостей в отеле владельцы гостиницы могут приобрести подобный замок самостоятельно. Достаточно, чтобы он позволял установить специальный чип, а таких моделей на рынке много. Благодаря мобильному приложению Connect One гостю не придется стоять в очереди на стойке регистрации: он сканирует смартфоном паспорт, ставит отметку, что соглашается с условиями договора, фотографирует свое лицо (снимает биометрию), регистрирует Wi-Fi и получает на смартфон код доступа, с помощью которого открывает дверь своего номера.

Через смартфон осуществляется все взаимодействие с отелем. Можно вызвать горничную для уборки или поставить значок «не беспокоить». Можно посмотреть, когда будет завтрак и какое меню в ресторане, заказать дополнительные услуги, например, записаться на спа-процедуры. Есть система лояльности, накапливающая бонусы. Негативный отзыв не отправляется на сайт агрегатора, а сразу поступает администрации, которая оперативно решает проблему.

С помощью электронного журнала отслеживаются перемещения персонала и гостей по отелю. Например, на круизном корабле я удивлялся, как точно персонал определял время моего отсутствия в каюте: несмотря на две уборки в день, никого из горничных за время путешествия не видел. Потом вспомнил, что, поднявшись на борт, установил на смартфон местное приложение, и все стало ясно.

Уход с рынка международных решений расчистил дорогу для российских вендоров. Требования франшизы стали неактуальными, и отели начали самостоятельно

Российские сервисы бронирования занимают освободившуюся нишу



Количество российских разработчиков продуктов для туриндустрии растет

Виртуальная реальность – полезный инструмент для продвижения туруслуг

выбирать поставщиков. Из-за санкционного давления отелям стало сложнее получать электронное оборудование для «умных» номеров. Однако SberDevices, дочерняя компания Сбера, предложила интерактивное решение для отелей «Салют Отель», интегрируемое с различными PMS-системами. Это решение использует телевизоры SberTV, мультимедийный смарт-дисплей, оснащенный виртуальным ассистентом с сенсорным, голосовым и жестовым управлением SberPortal и бюджетную приставку к телевизору SberBox. По словам Анастасии Коробковой, менеджера по продукту «Салют Отель» компании SberDevices, решение развернуто в пятизвездочных гостиницах в Москве, Крыму и в сети пятизвездочных природно-оздоровительных отелей Cosmos Group на Алтае.

TravelTech и облака

Туристический бизнес географически распределенный, гибкий, быстро меняющийся. Требуется оперативное онлайн-взаимодействие с широким кругом контрагентов – гостиничными сетями, транспортом, финансовыми организациями, туроператорами, турагентами. Неудивительно, что TravelTech тесно связан с облачными вычислениями, компании широко используют SaaS, а разработчики – облачные платформы.

Новая версия облачной системы увеличения дохода компании Bnovo включает не только модуль бронирования отелей, который можно установить на любой сайт, менеджер каналов (выбор площадок продаж), но и «умную» Bnovo PMS, анализирующую цены конкурентов в городе, сезонность и тренды изменения спроса. По результатам расчетов программа предлагает оптимальную цену продажи номера. По утверждению CEO и основателя компании Валентина Микляева, новая версия будет доступна уже в ближайшее время.

ИТ-компания «Технезис» предложила решение для самостоятельного создания и продвижения цифровых туристических продуктов. В него входят конструктор сайтов, система бронирования, управление взаимоотношениями с клиентами (CRM). Система позволяет создавать каталоги туристической продукции, формировать маркетинговые акции, настраивать каналы продаж, отслеживать отзывы и цены, получать аналитическую отчетность. Цифровая экосистема TOP («Транспортное обслуживание региона») построена на микросервисной архитектуре и функционирует на георазпределенном кластере, который работает в режиме active-active.

Уже упоминавшаяся компания TravelLine занимается интеграцией сервисов – АСУ («1С Отель», Shelter PMS), CRM («Битрикс24», amoCRM), систем аналитики («Яндекс Метрика», Google Analytics), платежных систем (Сбербанк, Тинькофф Банк, «Монета.ру», «Комфорт букинг») и каналов продаж («Яндекс Путешествия», «Островок», Bronevik.com). В предлагаемом модуле онлайн-бронирования появилась функция RoomMix – проживание с переселением, если на нужные даты нет доступных номеров.

С «цифрой» – и в прошлое, и в будущее

Технологии виртуальной реальности, вызывавшие вау-эффект еще лет пять назад, стали в турбизнесе обычным инструментом, который позволяет не только совершить виртуальное путешествие по существующим достопримечательностям, как предлагалось на стенде Новгородской области, но и перенестись в прошлое. Так, на стенде РЖД желающие могли очутиться в старом железнодорожном вокзале в Павловске. Цифровые технологии быстро находят применение в туризме, помогают организовать комфортное и интересное путешествие.

Уход западных компаний, в том числе вендоров ПО, не вызвал коллапса. Конечно, были проблемы, например, при переходе на российское ПО в октябре прошлого года больше суток не работала система бронирования билетов «Аэрофлота». Проблемы остаются – так, по-прежнему при регистрации на обратный рейс в Россию нельзя даже за дополнительную плату выбрать места. Но проблемы решаются – скажем, в ответ на невозможность использования за рубежом российских банковских карт туроператоры начали продавать экскурсии за рубли еще в России. Несмотря на все сложности, туристическая отрасль адаптировалась к новой реальности, все шире использует ИТ-решения и с оптимизмом смотрит в будущее.

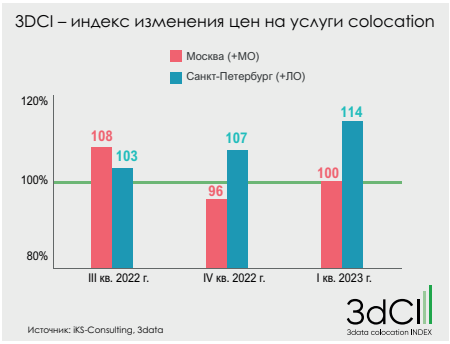
Николай Носов

НОВОСТИ ОТРАСЛИ

«Ростелеком-ЦОД» запускает новый дата-центр «Медведково»

Общая площадь дата-центра составляет 20 тыс. кв. м. ЦОД рассчитан на 16 машинных залов вместимостью 312 стандартных стоек каждый с проектной мощностью 36 МВт. В рамках первой очереди запущено 1248 стойко-мест в четырех машинных залах общей мощностью 9 МВт. В конце мая «Ростелеком-ЦОД» планирует запустить вторую очередь дата-центра «Медведково» также на 1248 стоек, а к концу 2023-го площадка будет полностью введена в эксплуатацию. В этом году намечено открыть еще один крупный объект – ЦОД «Москва-V» уровня Tier IV.

Обновлен индекс 3DCI

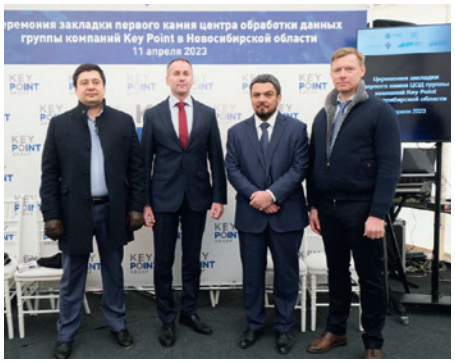


Как показало исследование iKS-Consulting, проведенное в феврале 2023 г., средняя цена на услугу colocation – аренду места для размещения ИТ-оборудования в ЦОДах – в агломерациях «Москва» (включает Москву и ближайшее Подмосковье) и «Санкт-Петербург» (включает Санкт-Петербург и Ленинградскую область) с размещением в марте 2023 г. составила 105,3 и 85 тыс. рублей соответственно. Таким образом, в феврале 2023 г. индекс цен на услугу colocation – 3DCI (3data Colocation Index), полученный при сравнении с ценами в IV квартале (декабрь 2023 г.), в Московском регионе составил 100,5%, в Санкт-Петербурге – 114%. В Москве цена на услугу colocation, хоть и демонстрировала колебания в течение всего 2022 г., но по сравнению с I кварталом 2022 г. выросла незначительно (индекс 3DCI = 103%). В Санкт-Петербурге тенденция к росту тарифов сохраняется, в первую очередь за счет того, что все площадки уже практически заполнены. Индекс 3DCI по агломерации «Санкт-Петербург» в I квартале 2023 г. относительно I квартала 2022 г. составил 125%.

Строительство первого ЦОДа уровня Tier III в Кыргызстане

В начале 2023 г. специалисты компании DataDome присоединились к проекту строительства первого центра обработки данных в Кыргызстане, который будет спроектирован в соответствии с требованиями надежности уровня Tier III по стандарту Uptime Institute. Дата-центр позволит разместить 100 серверных стоек суммарной мощностью не менее 500 кВт. Строительство такого дата-центра позволит цифровым технологиям Кыргызстана выйти на новый уровень. Заказчиком является компания DataTime – вновь созданный оператор центров обработки данных в Бишкеке.

ГК Key Point приступила к строительству дата-центра в Новосибирске



11 апреля состоялась церемония закладки первого камня в фундамент будущего ЦОДа, который строится на площадке Промышленно-логистического парка Новосибирской области. Емкость нового объекта составит 880 ИТ-стоек, общая проектная мощность – 8 МВт. Запуск в эксплуатацию первой очереди запланирован на декабрь 2023 г. Новый ЦОД, как и все дата-центры группы компаний Key Point, будет проходить сертификацию Uptime Institute по уровню надежности Tier III. Генеральный проектировщик и подрядчик объекта – компания «Свободные Технологии Инжиниринг», технический консалтинг осуществляет компания «Ди Си Квадрат».

Еще один ЦОД в Новосибирске – в планах

Как сообщает nsk.bfm.ru, в Новосибирске планируют построить коммерческий ЦОД мощностью 4,8 МВт. Речь об этом шла на совете по инвестициям в региональном правительстве. Возвести ЦОД на 800 стойко-мест в Октябрьском районе мегаполиса краснодарская компания «Проф-Сити» рассчитывает к 2029 г., а реализовать первую очередь – в 2025-м.

К концу года VK достроит в Подмосковье четвертый ЦОД

Источник: gusn.mosreg.ru

Как сообщил в середине апреля Главгосстройнадзор Московской области, организация провела плановую проверку хода строительства ЦОДа «Пахра» в городском округе Домодедово. Этот дата-центр принадлежит компании VK. Площадь высокотехнологичного объекта – более 5 тыс. кв. м. Напомним, соглашение о развитии ИТ-инфраструктуры на территории региона между Правительством Московской области и Mail.ru Group (сейчас – VK) было подписано в рамках ПМЭФ-2021. На данный момент в Подмосковье задействованы три дата-центра и 32 – в столице.

Экономика мировой отрасли ЦОДов

По итогам 2022 г., как сообщает Dell'Oro Group, мировые инвестиции в ЦОДы достигли $241 млрд (учитываются поставки серверов, СХД и гипермасштабируемых платформ). Для сравнения: годом ранее этот показатель составлял приблизительно $209 млрд – рост 15%. Ведущим поставщиком серверов стала компания Dell, за ней следуют HPE и Inspur.

Аналитики также оценили сегмент физической инфраструктуры ЦОДов – Data Center Physical Infrastructure (DCPI). В 2022 г. затраты в данном секторе увеличились на 10% по сравнению с 2021-м. К концу 2022-го крупнейшими поставщиками DCPI-продуктов стали Vertiv, Schneider Electric и Eaton. Аналитики Dell'Oro Group полагают, что рост рынка DCPI в 2023 г. составит также 10%.

В Москве разработали решение для ЦОДов на базе суперконденсаторов

Источник: mos.ru/news

Столичная инжиниринговая компания «Тайтэн Пауэр Солюшн» разработала для ЦОДов решение для бесперебойного питания на базе суперконденсаторных накопителей. Компания в ближайшее время приступит к производству тестового образца и планирует к концу года реализовать проект. Суперконденсатор – это относительно новый тип накопителя энергии, который обладает рядом уникальных свойств. Он отличается от обычных аккумуляторов высокой мощностью, способностью работать при экстремально низких температурах (до −40°С), скоростью накопления энергии, а также степенью отдачи электрического заряда и длительным сроком службы – более 10 лет. Из ограничений – небольшое время автономии (до 30 с).

Казахстан на восходящей траектории цифрового развития

Александр Барсков
Дмитрий Горкавенко, директор по развитию бизнеса, iKS-Consulting

Лежавший некогда на Великом шелковом пути Казахстан сегодня может стать одним из ключевых цифровых хабов Центральной Азии и Евразии в целом. Предпосылками к этому являются высокий уровень цифрового развития республики и планы компаний по организации ИКТ-инфраструктуры.

До недавнего времени основными акторами на рынке услуг коммерческих ЦОДов и облачных сервисов Казахстана выступали провайдеры, которые и развивали этот рынок. Однако в перспективе двух-трех лет для качественного перехода на новый уровень аутсорсинга ИКТ-инфраструктуры потребуется участие ключевых заказчиков, т.е. появление новых «действующих лиц» из среды профессиональных потребителей, которые благодаря своей публичной позиции и сотрудничеству с игроками рынка станут полноценными его участниками. Именно потребители окажут существенное влияние на создание новых продуктов, выработку требований к ним, возникновение новых гибридных моделей и т.п. Следующим этапом органического развития рынка станет формирование профессионального сообщества через обучение, обмен опытом, взаимодействие с органами государственной власти для выработки регуляторных правил и поддержки развития отрасли.

Высокий потенциал рынка коммерческих ЦОДов и облачных сервисов Казахстана подтверждается сегодняшними подходами компаний к организации ИКТ-инфраструктуры и их ближайшими планами, которыми они поделились на конференции Data Center & Cloud Kazakhstan в октябре 2022 г. в Алматы. Эта ежегодная конференция, организуемая «ИКС-Медиа» и проводившаяся уже в шестой раз, стала авторитетной площадкой для обсуждения актуальных вопросов развития цифровой инфраструктуры Казахстана.

В статье использованы результаты опроса, проведенного iKS-Consulting среди делегатов 6-й конференции Data Center & Cloud Kazakhstan. Приведенные ниже воодушевляющие данные объясняются присутствием в выборке крупных компаний, компаний с госучастием, профессиональных потребителей услуг аутсорсинга ИКТ-инфраструктуры и т.п. Данные не репрезентативны для всей экономики Казахстана, но достаточно детально описывают ее «верхний сегмент» и показывают модель, которая станет массовой через три-пять лет.

Рынок ЦОДов и ИТ-аутсорсинг. Текущее состояние

За последние несколько лет ИТ-системы превратились из поддерживающего инструмента в критически важный актив для функционирования бизнеса и государственного управления. Казахстан показывает высокий уровень цифрового развития, который во многом определяется Министерством цифрового развития, инноваций и аэрокосмической промышленности РК. И результаты радуют. Так, в недавно опубликованном рейтинге ООН, отражающем электронное участие граждан во взаимодействии с государством (E-Participation Index), страна заняла высокое 15-е место, тогда как Россия – только 57-е.

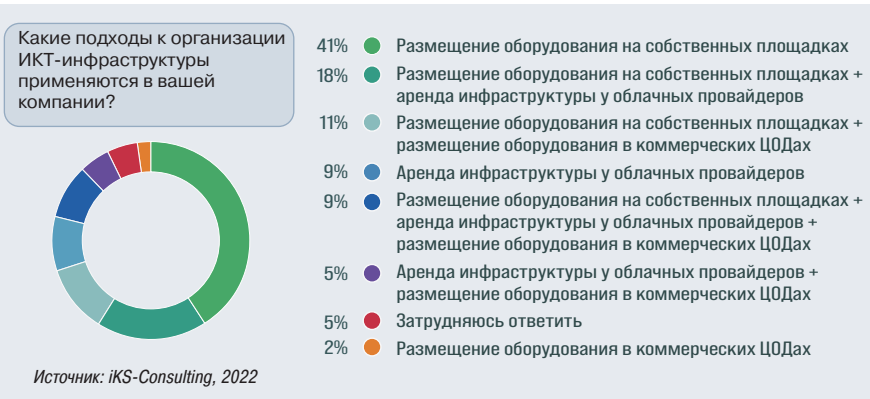
Полномасштабная цифровизация всех отраслей экономики страны осуществляется в рамках Национального проекта «Технологический рывок за счет цифровизации, науки и инноваций». Стремительно растет объем оцифрованных данных, как следствие, повышается спрос на их хранение. Набирают темпы локализация зарубежных (глобальных) и развитие местных облачных сервисов. Владельцы дата-центров и сервис-провайдеры все активнее выстраивают взаимовыгодные партнерские отношения.

Рынок коммерческих дата-центров Казахстана находится в стадии бурного роста. По данным iKS-Consulting, за три года – с 2019-го по 2022-й – количество стойко-мест в коммерческих ЦОДах удвоилось и достигло почти 2,5 тыс. Рост доходов коммерческих ЦОДов также впечатляет: за указанный период – с 9,1 до 17,9 млрд тенге. По прогнозу iKS-Consulting, к 2025 г. этот рынок увеличится до 25,8 млрд тенге.

Более половины компаний крупного бизнеса РК уже отошли от модели использования только собственной инфраструктуры и являются потребителями услуг инфраструктурного аутсорсинга (рис. 1).

Если говорить об использовании для решения ИТ-задач внешних сервисов, то облака пока более популярны, чем размещение оборудования в коммерческих ЦОДах. Так, наряду с собственными площадками инфраструктурные облачные

Рис. 1. Характер использования ИКТ-инфраструктуры компаниями Республики Казахстан ▼



Источник: iKS-Consulting, 2022

Развитие ЦОДов – важное условие для цифровизации Республики Казахстан

Абилкаир Болатбаев, руководитель управления развития новых технологий и инфраструктуры в области связи Комитета телекоммуникаций, Министерство цифрового развития, инноваций и аэрокосмической промышленности РК

Развитие отрасли центров обработки данных – важное условие для полномасштабной цифровизации экономики Республики Казахстан и реализации соответствующих государственных программ. Одним из направлений цифрового развития страны мог бы стать аутсорсинг ИКТ-инфраструктуры для органов государственной власти. Использование инфраструктуры профессиональных ЦОДов для функционирования государственных информационных систем позволит не только повысить надежность и эффективность функционирования таких систем, но и снизить расходы на их поддержку.

Для размещения критически важных для функционирования экономики и государства информационных систем важно обеспечить безусловную надежность и безопасность инфраструктуры ЦОДов. Это требует применения наилучших мировых практик в области проектирования, построения и эксплуатации таких объектов. Не менее важно формирование и совершенствование нормативной правовой базы для регулирования отрасли с учетом государственных интересов Казахстана.

сервисы задействуют около четверти опрошенных, а услуги коммерческих ЦОДов – около 20%.

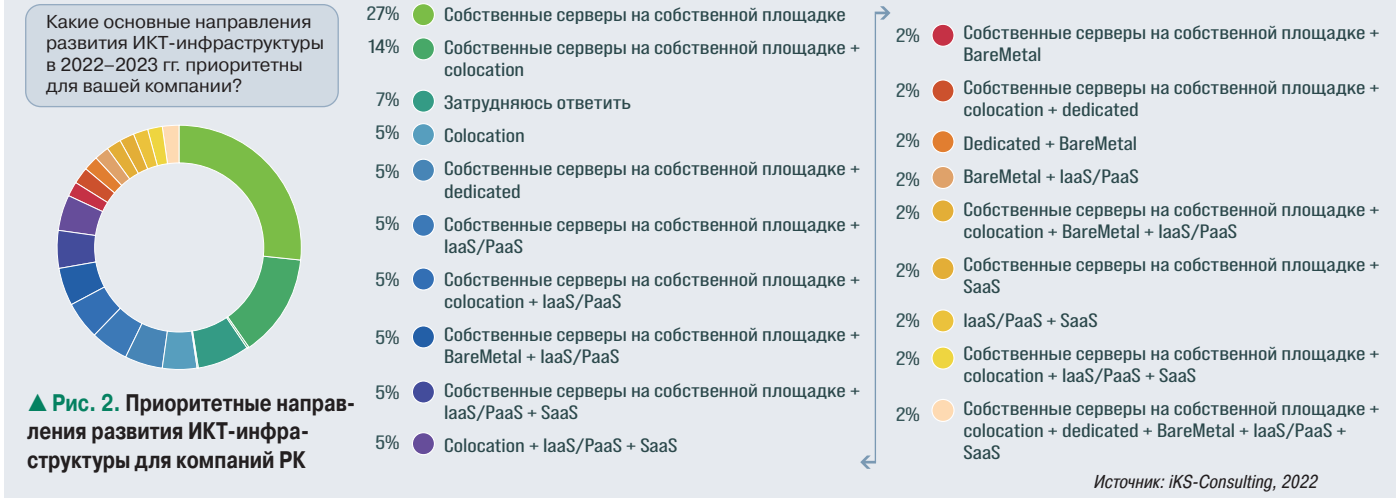
Примерно каждая десятая компания использует все три варианта организации ИТ-инфраструктуры: собственную площадку, коммерческий ЦОД и облачные сервисы. Этот гибридный вариант, по мнению экспертов iKS-Consulting, наиболее перспективен, поскольку позволяет снизить расходы и повысить эффективность функционирования различных систем (приложений), размещая их в оптимальной (с точки зрения нормативных, логистических, экономических и других факторов) для каждой системы среде. Более того, при наличии единой консоли управления такой гибридной инфраструктурой появляется возможность оперативной (в ряде случаев автоматической) миграции нагрузок и приложений из одной среды в другую.

На момент проведения исследования 16% респондентов обходились без использования собственных ИТ-площадок. Более половины из них (9%) решали свои задачи только за счет применения облачных сервисов, а 2% размещали оборудование в коммерческих ЦОДах. Соответственно остальные (5%) задействовали оба этих варианта.

Перспективы развития

Уже в ближайшие год-два доля компаний, прибегающих к услугам коммерческих ЦОДов и облачным сервисам, может существенно увеличиться. По данным iKS-Consulting, развитие собственной инфраструктуры (собственных серверов на собственной площадке) будет приоритетным только для 27% (рис. 2). Все остальные в той или иной степени будут наращивать использование услуг коммерческих ЦОДов и/или облачных сервисов.

Примерно 20% наряду с развитием собственных площадок намерены использовать услуги



▲ **Рис. 2. Приоритетные направления развития ИКТ-инфраструктуры для компаний РК**

Источник: iKS-Consulting, 2022

коммерческих ЦОДов, устанавливая в них собственные серверы (colocation) или арендуя серверы провайдера (dedicated). А еще 11% к перечисленным вариантам будут активно добавлять различные облачные сервисы, причем как IaaS/PaaS и SaaS, так и Bare Metal. Последний вариант представляет собой арендованные (в коммерческом ЦОДе или у облачного провайдера) серверы с установленной средой виртуализации, и его, согласно сложившейся таксономии, аналитики также относят к облачным сервисам.

Интересно отметить, что сделать ставку исключительно на внешние сервисы (приобретаемые у коммерческого ЦОДа и/или облачного провайдера) готовы лишь около 11% респондентов. Это немного меньше доли компаний, которые уже задействуют только такие варианты (16%). Полагаем, это объясняется тем, что заказчики стали более четко определять свои ИТ-задачи и классифицировать (приоритизировать) свои ИТ-ресурсы, осознавая, что при всех преимуществах сервисной модели часть приложений (данных) оптимально оставлять в собственных ЦОДах. Причины могут быть разными, например, необходимость обеспечить минимальное время отклика (при расположении собственного edge-ЦОДа рядом с местом сбора данных), более жесткие требования к безопасности, выполнение нормативных требований и т.д.

При этом в 2022–2023 гг. примерно 60% заказчиков планируют использовать (или наращивать объем использования) сервисов ком-

Госзаказ – отправная точка развития инфобизнеса

Светлана Аблеева,
начальник отдела развития и разработки дивизиона информационных технологий – филиала АО «Казахтелеком»

– Каковы основные препятствия и драйверы развития отрасли коммерческих ЦОДов и облачных сервисов Республики Казахстан?

– Основной драйвер – политика государства, направленная на цифровизацию казахстанского бизнеса и общества в целом. Заказы государства – отправная точка для развития инфобизнеса в РК. Первыми клиентами ЦОДов стали госорганы, холдинги с госучастием и компании, выполнявшие госзаказы.

Другой важный стимул – поворот бизнеса в сторону качественного и массового ИТ-сервиса. Веб-сайт, маркетплейс, диджитал-маркетинг, CRM и т.п. стали обычными инструментами. Пандемия способствовала массовости данной тенденции. Она вынудила заняться цифровизацией многие компании вне зависимости от размера и вида бизнеса. Именно пандемия дала толчок развитию облаков, так как потребовала оперативного управления инфраструктурой, быстрого добавления или сокращения ресурсов.

– Каковы, на ваш взгляд, основные причины перехода корпоративных заказчиков из собственных серверных комнат (ЦОДов) в коммерческие ЦОДы и облака?

– Для наших клиентов одна из основных причин – необходимость расширения бизнеса и/или открытия филиальной сети с централизованным управлением. Для этого требуется наращивание ресурсов и гибкое управление ими. Поэтому многие решаются перейти на облачную инфраструктуру.

Оптимизация затрат тоже зачастую склоняет компании к ИТ-аутсорсингу. Когда требуется обновление серверного оборудования, а бюджет ограничен, бизнес приходит к нам, чтобы арендовать физические или виртуальные ресурсы.

– Каковы ваши планы по развитию своих ЦОДов и услуг, предоставляемых на их основе?

– Сегодня «Казахтелеком» владеет сетью из 27 дата-центров по всему Казахстану суммарной емкостью около 1600 стойко-мест. Среди наиболее интересных объектов – ЦОД в Павлодаре, рассчитанный на 320 стойко-мест. В 2012 г. этот ЦОД получил сертификат Tier III Design от Uptime Institute, а в 2018 г. подтвердил свой уровень, получив сертификат Tier III Facility. Также отметим ЦОД в Акколе, имеющий уникальное конструктивное исполнение. Это, по сути, бункер на 80 стоек, который рассчитан на защиту персонала и оборудования от прямого воздействия различных средств поражения. В 2023 г. мы планируем расширить его на еще одну гермозону вместимостью 44 стойки.

Самый новый ЦОД «Казахтелекома» – модульный дата-центр в Алматы на ул. Диваева. В настоящее время введены в эксплуатацию два модуля суммарной емкостью 84 стойко-места. В 2023 г. планируется завершить организацию еще двух модулей такой же емкости. Одна из особенностей ЦОДа в том, что каждая стойка имеет высоту 50U и поддерживает мощность до 8 кВт.

«Казахтелеком», понимая растущую потребность бизнеса в облачных сервисах (IaaS/PaaS/SaaS), планирует активно развивать и данное направление. Сегодня использование ресурсов ЦОДов в облачных проектах составляет около 25–30%, и мы намерены увеличить эту долю до 50%. Компания сотрудничает с облачным провайдером «ИТ-Град» и другими поставщиками ПО и решений SaaS/PaaS/IaaS, а также разрабатывает программу развития облачных сервисов казахстанского производства.

Политика государства – важный драйвер развития ЦОДов и облаков

Ерлан Минавар, заместитель председателя правления по стратегическому развитию и инновациям, «Транстелеком»

– Каковы основные препятствия и драйверы развития отрасли коммерческих ЦОДов и облачных сервисов Республики Казахстан?

– К числу драйверов развития отрасли коммерческих ЦОДов, безусловно, относятся политика государства, направленная на повышение транзитного потенциала Казахстана, а также проекты создания систем видеонаблюдения, стартовавшие в ряде регионов. Мощным катализатором перехода заказчиков в облака стал рост стоимости оборудования и увеличение сроков его поставки.

Серьезно препятствует развитию отрасли то, что владельцами ЦОДов являются в основном операторы связи. На рынке практически нет компаний, которые специализировались бы именно на услугах ЦОДов. Также стоит отметить неравномерность распределения бизнеса (деловая активность сосредоточена в Алматы, Астане, Караганде, Атырау и Актау), а также отсутствие крупных ИТ-проектов, способных генерировать большой объем трафика (например, социальные сети). Еще один негативный фактор – высокие затраты на строительство и услуги каналов связи и почти полное отсутствие программных продуктов и сервисов, разработанных в Казахстане.

– Каковы, на ваш взгляд, основные причины перехода корпоративных заказчиков из собственных серверных комнат (ЦОДов) в коммерческие ЦОДы и облака?

– В числе таких причин – низкая отказоустойчивость существующих серверных комнат и значительные затраты на модернизацию собственного оборудования. Обращаясь к ИТ-аутсорсингу, заказчики стремятся избавиться от непрофильной для себя деятельности. При этом в облачных услугах их привлекает скорость организации виртуальной инфраструктуры, предлагаемой провайдерами.

– Каковы ваши планы по развитию своих ЦОДов и услуг, предоставляемых на их основе?

– Мы намерены развивать публичные облака и продукты на основе инфраструктурных сервисов (IaaS). Использовать сеть наших ЦОДов в проектах видеонаблюдения (общественная и дорожная безопасность). Кроме того, в наших планах – развитие проектов Smart city, спутниковых проектов, а также модели MSSP (Managed Security Service Provider). Также мы собираемся провести сертификацию дата-центров по стандарту PCI DSS, важному для финансовой отрасли.

Фундамент цифровизации – надежная ИТ-инфраструктура

Сырым Толеулиев, заместитель председателя правления, «Казтелепорт»

– Каковы основные препятствия и драйверы развития отрасли коммерческих ЦОДов и облачных сервисов Республики Казахстан?

– Один из основных драйверов развития рынка услуг ЦОДов и облачных сервисов в Казахстане – цифровизация государственных услуг и банковского сектора. Этот процесс стимулирует цифровизацию других отраслей. Как известно, фундамент цифровизации – это надежная ИТ-инфраструктура: развитие бизнеса всегда требует внедрения новых информационных систем, наращивания вычислительных ресурсов и хранилищ, защиты от киберугроз.

– Каковы, на ваш взгляд, основные причины перехода корпоративных заказчиков из собственных серверных комнат (ЦОДов) в коммерческие ЦОДы и облака?

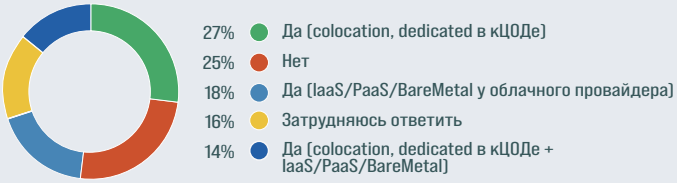
– Если говорить об услугах аренды физической инфраструктуры, то здесь основную роль играет финансовая выгода: содержание собственной серверной требует от компаний больших затрат на инженерную инфраструктуру и штат специалистов. Использование же услуг коммерческих ЦОДов подразумевает, что техническая поддержка инженерной инфраструктуры и профилактические работы ложатся на плечи оператора ЦОДа и компаниям не нужно заниматься непрофильной деятельностью. Это весомые аргументы, с которыми соглашаются даже те ИТ-директора, которые не хотели бы передавать часть функций коммерческим ЦОДам.

А основная причина перехода в коммерческое облако – возможность быстрого запуска продуктов и вывода их на рынок. Такой переход подстегивают и проблемы с логистикой, которые усугубились в 2022 г. Поставка серверного и сетевого оборудования сейчас занимает от полугода.

– Каковы ваши планы по развитию своих ЦОДов и услуг, предоставляемых на их основе?

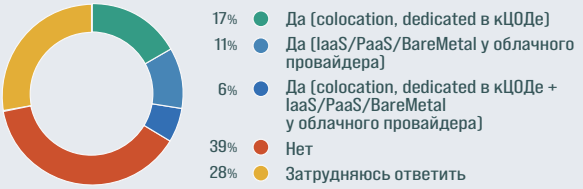
– Мы будем продолжать развивать свою стратегическую позицию сильного провайдера ИКТ-инфраструктуры и повышать ценность своих продуктов для потребителей. Развивать бизнес будем по нескольким направлениям. Во-первых, планируем активно модернизировать и масштабировать собственную технологическую инфраструктуру: в 2022 г. в Алматы ввели в эксплуатацию ЦОД «Сайрам» (Tier III Design & Facility), в 2023 г. собираемся запустить ЦОД Tier III в Астане. Во-вторых, выходим на новые рынки: в 2023 г. наши облачные сервисы станут доступны для клиентов в Узбекистане. В-третьих, мы существенно расширим продуктовую линейку – запустим собственные платформенные сервисы на базе Open Stack, разнообразим консалтинговые услуги в области ИБ и поддержку информационных систем клиентов.

Планируете ли вы размещение собственного оборудования в коммерческом ЦОДе (или увеличение объема уже размещаемого оборудования) либо аренду виртуальной инфраструктуры у IaaS/PaaS (или увеличение объема потребляемых ресурсов провайдера) в 2022–2023 гг.?



▲ Рис. 3. Планы использования компаниями сервисов коммерческих ЦОДов и облачных провайдеров

Планируете ли вы размещение собственного оборудования в коммерческом ЦОДе либо аренду виртуальной инфраструктуры у IaaS/PaaS и в 2022–2023 гг.? (для компаний, которые не используют аутсорсинг ИКТ-инфраструктуры)



▲ Рис. 4. Планы использования сервисов коммерческих ЦОДов и облачных провайдеров для компаний, не использующих аутсорсинг ИКТ-инфраструктуры

Как вы считаете, как изменится бюджет на ИКТ-инфраструктуру в 2023 г. по сравнению с 2022-м?

▲ Рис. 5. Предполагаемое изменение расходов компаний на ИКТ-инфраструктуру в 2023 г.

Оцените, пожалуйста, примерные темпы роста ИТ-инфраструктуры вашей компании в физическом объеме за последние три года

▲ Рис. 6. Увеличение объема ИКТ-инфраструктуры компаний за последние три года

Услугами каких облачных провайдеров пользуется ваша компания?

▲ Рис. 7. Принадлежность используемых в Казахстане облачных сервисов

Источник: iKS-Consulting, 2022

мерческих ЦОДов и облачных провайдеров (рис. 3). Причем среди тех компаний, которые на момент проведения опроса не использовали аутсорсинг ИТ-инфраструктуры, к услугам коммерческих ЦОДов и/или облачных провайдеров обратится 34% (рис. 4). Это неизбежно отразится на развитии соответствующего рынка.

Развитие отрасли ЦОДов и облачных сервисов Казахстана обусловлено не только ростом популярности ИТ-аутсорсинга, но и увеличением расходов компаний на ИТ. Согласно данным iKS-Consulting, в 2023 г. более 60% компаний увеличат бюджет на ИКТ-инфраструктуру (по сравнению с соответствующими расходами в 2022 г.). Причем четверть компаний указали, что этот рост составит 20–25% и более, а 36% оценили запланированный рост в 10–15% (рис. 5).

В целом в последние три года ежегодные темпы роста ИТ-инфраструктуры у половины опрошенных превысили 10%, причем у 16% компаний инфраструктура росла более чем на 30% (рис. 6).

О высоком уровне развития ИКТ в целом свидетельствует средняя мощность, подведенная к стойко-месту (по данным iKS-Consulting, она уже составляет 7,7 кВт), а также формирующийся спрос на еще более высоконагруженные стойки.

На казахстанском рынке коммерческих ЦОДов и облачных провайдеров выделяются четыре компании, образующие группу лидеров. Это «Казахтелеком», «Транстелеком», «Казтелепорт» и QazCloud. Именно проекты, реализованные указанными четырьмя компаниями, внесли наиболее значимый вклад в развитие казахстанского рынка ЦОДов в 2020–2022 гг.

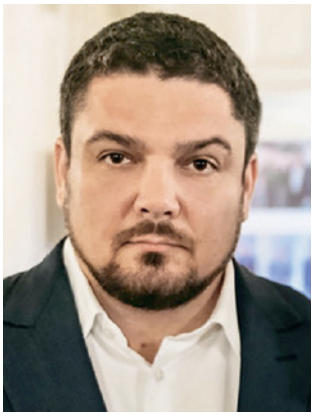
Развитие инфраструктуры ЦОДов позволяет развивать цифровые сервисы, в первую очередь по облачной модели. По данным iKS-Consulting, совокупный объем рынка облачных услуг с учетом прямых государственных закупок в 2021 г. превысил 16,22 млрд тенге. Три четверти объема облачного рынка в стране приходится на инфраструктурные услуги (IaaS). В оставшейся четверти доминирует SaaS. В этом сегменте в основном присутствуют локализованные версии зарубежных продуктов и используются агентские модели продаж.

Развивают облачные сервисы и владельцы крупнейших сетей ЦОДов Казахстана. И эти сервисы все более востребованы местными пользователями (рис. 7). Процесс будет нарастать, поскольку облачные сервисы в стране активно локализуются.

В целом развитие компетенций и формирование профессионального сообщества позволят рынку коммерческих ЦОДов и облачных сервисов Казахстана выйти на новый уровень, что, в свою очередь, даст возможность сформировать и закрепить позиции страны как ключевого цифрового инфраструктурного хаба Центральной Азии и всей Евразии. ИКС

Доверие заказчиков как главный фактор ускорения проектов

О сроках и стоимости проектов, новых игроках и холодных стенах, выборе поставщиков и дефиците кадров – актуальных вопросах отрасли цодостроения – Евгений Вирцер, генеральный директор компании «Свободные Технологии Инжиниринг».



– Какие основные тенденции вы можете отметить на российском рынке цодостроения?

– Выделю две тенденции. Первая – выход на рынок принципиально новых игроков. Речь идет о девелоперах, которые приходят с большими проектами. Особенно это заметно в Москве и Московской области. Сегодня не один, не два и даже не три девелопера уже находятся в стадии реализации проектов. Рынок из-за этого может сильно измениться. Традиционным игрокам такие объемы не под силу. Поэтому либо они будут покупать те объекты, которые построят девелоперы, либо сами девелоперы займут существенную долю рынка ЦОДов.

Вторая тенденция – существенное укрупнение среднего проекта. Если говорить о московском регионе, то в тех проектах, где мы участвуем, объемы измеряются тысячами стоек. В регионах – сотни стоек (не десятки, как было раньше), здесь рынок развивается медленнее, чем столичный. В большинстве регионов отсутствует ярко выраженный спрос по причине отсутствия продукта как такового. Но ситуация меняется, в том числе благодаря проекту Key Point (предусматривает строительство в регионах 35 ЦОДов общей емкостью 10,3 тыс. стойко-мест. – Прим. ред.). Наш опыт показывает: как только начинается строительство дата-центра, так сразу появляется спрос на его услуги.

– Какая экспертиза важна в первую очередь, чтобы успешно строить ЦОДы?

– Нужна совокупность многих компетенций. Ранее ключевой считалась техническая экспертиза в инженерных системах. Это было ядро, вокруг которого все крутилось. Да, такая экспертиза, безусловно, важна, но это не единственное условие успеха. Сегодня недостаточно быть просто хорошим проектировщиком или иметь в штате самых лучших строителей. Необходимо также умение реагировать на любые изменения и быстро принимать правильные решения. Очень хорошо, что у нас в обойме не только цодовские проекты. И опыт, который мы получаем на других проектах – инженерный, управленческий, финансово-экономический, – применяем при создании ЦОДов. Цодостроителям есть чему поучиться в других отраслях, и наоборот.

Кроме того, важна постоянная практика. Если вы сегодня начнете строить объект с представлениями трехлетней давности,то проект будет обречен на неуспех. Все быстро меняется. Надо быть все время «в теме», пропускать через себя новый опыт, чтобы быть готовым к новым вызовам.

Сегодня принципиально поменялось все, что касается выбора оборудования. За последние три-четыре года сильно просело качество исполнителей и подрядчиков монтажных работ. В силу разных причин: одни компании ушли с рынка, другие, наоборот, выросли в ущерб качеству. Этим надо уметь управлять.

– Вы упомянули изменения в выборе оборудования. Российское, китайское или параллельный импорт – в пользу какого варианта вы делаете выбор?

– Точно не параллельный импорт. Он даже не на третьем, а на четвертом месте из трех вариантов. Третье место пока пустое. 80% продукции ушедших производителей мы заместили решениями китайских, турецких и индийских компаний. 20% – российскими. Общаемся с большинством российских производителей, всегда рады использовать отечественное оборудование, но оно не всегда отвечает нашим требованиям.

– С уходом из страны мировых брендов многие заказчики жалуются, что спецификации вендоров «второго эшелона» расходятся с тем, что показывает практика. Сталкивались с таким?

– Сталкиваемся. И на решение этой проблемы тратим массу сил. Много времени уходит, чтобы убедиться – всеми доступными способами – в том, что заявленные характеристики соответствуют фактическим. Это занимает до нескольких месяцев. Например, один завод (не в России) собрал для нас специальную холодильную камеру, в которой тестировали оборудование, измеряли десятки параметров. Наши инженеры несколько раз туда выезжали. Пока не убедились, что заявленные характеристики соответствуют действительности, заказ не разместили. И так со всем новым

оборудованием. Партнеры знают, что нам нельзя просто показать бумажки с характеристиками и ценой. Мы очень дотошны.

– Последние 10 лет удельная стоимость ЦОДов снижалась. Сейчас эта тенденция изменилась?

– Давайте считать так. Примерно половина стоимости привязана жестко к валюте – это цена оборудования. В этой части с учетом смены производителей мы укладываемся в тот же бюджет, что и полтора года назад. Другая половина – рублевая – с начала 2022 г. выросла примерно на 15–20%. Но это без учета падения курса рубля в апреле – мы его еще не ощутили. В целом кардинального подорожания пока нет.

Но замечу, что мы обычно делаем объекты под ключ с зафиксированной стоимостью. И если, скажем, через полгода после начала проекта понимаем, что цена начинает «уезжать», можем оптимизировать проект (даже поменять технические решения) – конечно, без потери качества. Если хотите, это наше ноу-хау.

– В регионах проекты получаются дороже?

– В регионах сложнее строить, но стоимость примерно такая же. В Москве намного дороже земля и техприсоединение. В регионах – логистика, плюс дополнительные затраты на управление проектом. Но «на круг» выходит примерно то же.

– В последнее десятилетие также уменьшались сроки реализации проектов. Изменился ли этот тренд?

– Сокращать не получается, но и не увеличиваем. Сроки по нашим проектам и так вполне «спортивные». Например, во Владивостоке первый экскаватор заехал на площадку в ноябре 2021 г. А 1 февраля 2023 г. объект, причем уже сертифицированный по Tier III, ввели в эксплуатацию. Надо понимать, что это Владивосток, плюс все сложности 2022-го. В апреле 2023 г. заложили первый камень ЦОДа в Новосибирске, а 1 января 2024 г. по плану объект должны ввести в эксплуатацию. И это реально.

Кстати, девелоперы как новые игроки на рынке не могут себе позволить строить ЦОДы так долго, как их строили раньше. Для них время – самый дорогой ресурс. Традиционные игроки живут в другой парадигме: им важно сделать объект с определенным бюджетом и качеством, но срок не самое важное. Сегодня же сроки выходят на первый план, и это добавляет сложности в реализации.

– А что помогает вам выдерживать «спортивные» сроки?

– Секрет – в свободе действий, которую нам предоставляет заказчик. Минимальное число промежуточных итераций и согласований, на которые обычно тратится очень много времени. Поэтому мы и любим работать по принципу «цена под ключ». Потому что все в наших руках. По определенным реперным точкам заказчики нас проверяют, но не надо каждый чих с ними согласовывать. Остается сам срок проектирования и строительства. А он не такой уж жесткий, если все управленческие решения мы принимаем сами. И, пользуясь случаем, хочу сказать заказчикам «спасибо» за высокий уровень доверия.

– Как меняется выбор технологий в условиях нынешней турбулентности? Например, тот же литий сначала подорожал в 10 раз, потом подешевел в пять раз. На что сегодня ориентируетесь?

– Если говорить про аккумуляторы, до февраля 2022 г. последние проекты мы делали на литий-ионных АКБ. Сейчас перешли на свинец. И дело не только и не столько в цене материала. Конкурентное поле сильно сузилось. Литий в основном продвигали ушедшие из России зарубежные производители. Поэтому сегодня литий, на мой взгляд, превратился в очень дорогую игрушку.

Из принципиально нового за последние пару лет – холодные стены. Начали активно их использовать. Это самое большое технологическое изменение в наших проектах.

Еще – на строящихся нами объектах Key Point, начиная с Новосибирска, переходим на префабы – модули бесперебойного питания высокой заводской готовности, которые делаем на своей производственной площадке в Рязани. Для систем охлаждения тоже применяем префабы с узлами обвязки (где много сварки) для холодильных машин и холодных стен. Но их заказываем на других производственных площадках. Использование таких модулей позволяет минимизировать число людей и операций на площадке, повысив при этом качество и сократив сроки реализации. Это особенно важно для региональных проектов.

– Оказывается, у вас есть и собственное производство. А каковы в целом показатели компании «Свободные Технологии Инжиниринг»? Планы развития?

– Производству в Рязани три с лишним года. Выпускаем силовые шкафы, шкафы автоматики, модульные (контейнерные) ЦОДы, а также, как уже говорил, модули с системами электропитания. Осваиваем выпуск систем изоляции коридоров, блоков PDU. Это, конечно, помогает нашему основному направлению – проектированию и построению ЦОДов.

В целом в группе компаний сегодня работают около 300 человек. Выручка по группе в 2022 г. составила примерно 5 млрд руб., а в 2023 г. вырастет еще в 2,5 раза, исходя из проектов, находящихся в реализации. Понятно, что при таком быстром росте остро стоит кадровый вопрос. Наверное, как и всем, не хватает специалистов по управлению большими сложными проектами. Дефицит линейных проектировщиков, хотя штат проектировщиков у нас свой, более 100 человек. Но когда есть много интересной работы, кадровые вопросы решать проще.

В настоящий момент строим ЦОДы общей емкостью 7,5 тыс. стоек. Объекты еще на 6 тыс. стоек находятся в стадии проектирования. То есть всего «в работе» 13,5 тыс. стоек. Приличный объем. Отдельно хотел бы отметить, что у нас в работе находятся четыре проекта Tier IV (два уже строятся, два пока проектируются). По моим данным, такого портфеля проектов нет ни у кого из участников рынка. Еще в 2022 г. были планы начать полноценно работать на международном рынке. Но по понятным причинам эти проекты не реализовались. Международные планы перенесены на текущий год, и все должно получиться.

Квантовые коммуникации: итоги 2022 года

Российский рынок квантовых коммуникаций за год вырос почти на порядок и продолжает развиваться, несмотря на проблемы, стоящие перед отечественными разработчиками.

Николай Носов

Квантовые технологии из кабинетов ученых постепенно переходят в повседневную жизнь. Так, использование технологии квантового распределения ключей (КРК) позволяет защитить сети передачи данных от взлома, в том числе с помощью квантового компьютера. Кроме того, технология обеспечивает генерацию истинно случайного ключа. Снижается риск человеческого фактора – администратор системы не запишет пароль на бумажке, приклеенной к монитору, да и вообще никто не будет знать случайный и автоматически создаваемый пароль. При использовании в корпоративной VPN ключи автоматически вырабатываются и загружаются без участия оператора.

Рынок растет

По данным BCC Research, мировой рынок квантовых коммуникаций в 2022 г. вырос на 22% и составил $378 млн. На 16%, достигнув $240 млн, вырос рынок инфраструктурных решений, в основном за счет более широкого использования квантовых генераторов случайных чисел и устройств квантового распределения ключей для предприятий и магистральных сетей (рис. 1).

Рис. 1. Объем ($ млн) и состав мирового рынка квантовых коммуникаций ▼

Источник: Центр трансфера технологий МГУ
По данным BCC Research Global Market for Quantum Cryptography; анализ фонда НИР «Иннопрактика» без учета рынка образовательных программ

Драйверами роста стали государственные программы поддержки, разработка протоколов и стандартов, лицензирование и сертификация оборудования и общее снижение его стоимости. На 34% увеличился рынок сервисов и услуг, включающий: пилотные проекты КРК и квантовой VPN; защищенные КРК хранилища цифровых активов; защищенные КРК каналы передачи данных.

Среди значимых мировых событий года на прошедшем в январе в Москве первом всероссийском форуме «Доверенные квантовые технологии и коммуникации» Сергей Кулик, директор проектов «Ростелекома» в экосистеме квантовых коммуникаций в РФ, выделил:

- запуск китайского спутника квантовой связи «Цзинань 1»;
- появление коммерческого оборудования с КРК со скоростью генерации ключей 300 кбит/с;
- создание и развитие квантовых сетей связи в Китае, Южной Корее и ЕС.

Развиваются защищенные КРК сети и в России. Основные игроки – «Ростелеком», запустивший защищенный канал связи между Москвой и своим ЦОДом в Удомле, и РЖД. Ведомство планирует создание магистральных защищенных КРК каналов от Москвы до Челябинска и Сочи, на базе которых будет строиться региональная сеть (рис. 2).

Среди других российских достижений 2022 г. эксперт выделил утверждение профессионального стандарта и первую сертификацию оборудования для КРК.

В целом российский рынок за год увеличился почти на порядок – с 270 млн до 2541 млн руб. (рис. 3). В отличие от мирового рынка рост практически полностью (на 2456 млн руб.) достигнут за счет инфраструктурных решений. Основные продукты – доверенные узлы для обмена квантовой информацией, устройства КРК-защиты для предприятий и магистральных линий. Например, в портфеле российской компании «Инфотекс», которая выпускает наиболее полный комплект решений, – квантовая криптографическая

Источник: Центр квантовых технологий МГУ

▲ Рис. 2. Перспективы развития уплотненных каналов связи в рамках дорожной карты РЖД

Источник: Центр трансфера технологий МГУ По данным интервью и анкетирования участников квантовой экосистемы

▲ Рис. 3. Объем (млн руб.) и состав российского рынка квантовых коммуникаций

система выработки и распределения ключей VipNet Qandor, работающий в топологии «звезда» квантовый телефон VipNet QSS и устройства для развертывания доверенных узлов клиентских, распределительных и магистральных сетей КРК VipNet QTN. Производит оборудование для КРК и петербургская компания «СМАРТС-Квантателеком», и другие вендоры.

Проблемы сохраняются

Прежде всего, существуют физические ограничения, обусловленные затуханием луча лазера в оптическом канале. Поэтому как минимум через 400 км нужно устанавливать повторитель, причем он должен находиться в доверенной среде. Над устройствами для работы в недоверенной среде ученые ломают головы, но пока прорывов нет. Но все же благодаря государственной поддержке инфраструктура строится.

Сложнее ситуация с предоставлением квантовых услуг. Оборудование дорогое, а большинство компаний исповедует принцип «пока гром не грянет, мужик не перекрестится». Квантового компьютера, способного взломать используемые средства криптографии (своего рода «черного лебедя»), пока нет, и не очевидно, что в ближайшие годы он появится. Теория взлома сообщений, зашифрованных с помощью алгоритма RSA, известна давно – достаточно применить квантовый алгоритм Шора и иметь компьютер с сотней тысяч кубитов. Но создание такого компьютера – задача крайне сложная. Сегодня самая мощная квантовая система обладает мощностью 433 кубита.

Однако работы продолжаются, и повод для беспокойства есть. В декабре прошлого года группа китайских исследователей опубликовала методику взлома ключа RSA-48. Китайцы взяли за основу методику Клауса-Питера Шнорра и так оптимизировали алгоритм, что для дешифровки ключа RSA длиной 48 бит хватило 10-кубитного компьютера. Ученые утверждают, что при использовании их методики для взлома 2048-битного ключа понадобится всего 372 кубита. Такие квантовые компьютеры уже есть.

Статья вызывает вопросы, прежде всего в плане подготовки классических данных. Непонятна и открытая ее публикация, ведь обладание технологией дешифровки ключей дает стране большие преимущества. Например, ради сохранения тайны о взломе кода «Энигма», применявшегося немцами на протяжении всей Второй мировой войны, англичане даже шли на жертвы среди мирного населения, не принимая мер к защите городов.

Неудивительно, что государство, учитывая сложную геополитическую обстановку, проявляет беспокойство по поводу возможности существования засекреченного «черного лебедя». И готовит ответ в виде использования невзламываемых квантовых технологий и алгоритмов постквантовой криптографии.

«Не все квантовые разработки публичны. Теоретически квантовый компьютер может существовать в формате закрытой разработки и уже использоваться. Однако, скорее всего, мы видели бы признаки его работы. О ней свидетельствовали бы научные открытия, которые предшествовали созданию такой системы. Поскольку задача создания мощного масштабируемого многокубитного квантового компьютера все еще имеет научную составляющую и не все методы его разработки известны, считаю, что такая вероятность мала. Тем не менее важно действовать уже сейчас. Представим, что квантовый компьютер появится через 10 лет. Но есть данные, которые будут важны более длительный срок. Например, генетические данные сохраняют актуальность на протяжении всей вашей жизни и жизни ваших детей. Подобным данным должна быть обеспечена долгосрочная защищенность с учетом возможности атаки “сохрани сейчас – расшифруй потом”», – дал комментарий нашему изданию заведующий лабораторией квантовых технологий НИТУ «МИСиС» Алексей Федоров.

Другие проблемы связаны с оборудованием, которое после введения санкций стало невозможно купить. Нужны аппаратные шифраторы и дешифраторы, лазеры, испускающие последовательности фотонов, и приемники, способные их принять и проанализировать. И это не говоря уже об используемых в устройствах процессорах «Байкал», которые оказались недоступны после того, как Тайвань присоединился к санкциям. Появилось понимание, что в дальнейшем придется полагаться только на свои силы.

Впрочем, эксперты настроены оптимистично – процессы разработки отечественных устройств ускорились, успехи есть, существующие проблемы не остановят развитие квантовых технологий, которые мало-помалу уже входят в нашу жизнь. ИКС

«Темпесто» – дистрибьютор компетенций

Начав как монобрендовый поставщик ИБП Delta, компания «Темпесто» сегодня стала экспертом во всем комплексе вопросов, связанных с бесперебойным и гарантированным электропитанием. О накопленном опыте, старых и новых вендорах – ее генеральный директор Леонид Гаврилов.

– Компания «Темпесто» долгое время была известна на рынке как дистрибьютор ИБП Delta. Что изменилось в вашем позиционировании?

– В этом году нам 15 лет. Почти все это время мы были дистрибьютором Delta, причем монобрендовым. Этакой белой вороной на рынке. Многие не понимали, как мы вообще выживаем. А мы не просто выживали, мы росли.

В 2008 г. мы были единственными, кто подписал дистрибьюторское соглашение с Delta, кто в нее поверил. Это очень интересный производитель, но довольно своеобразный. С одной стороны – мировой лидер в производстве вторичных источников питания, с другой – компания, которая почти всю свою историю (за исключением, может быть, последних 20 лет) работала как OEM/ODM-производитель. Поэтому на момент заключения соглашения маркетинг и поддержка конечных заказчиков отсутствовали в принципе. И нам пришлось самостоятельно организовывать маркетинг, сервисную службу, чтобы поддерживать продажи, осуществлять гарантийный и постгарантийный ремонт оборудования Delta. Получилось это по необходимости. А оказалось нашим преимуществом, которое позволило успешно конкурировать с крупными мультивендорными дистрибьюторами.

Так зародилась концепция «дистрибьютора компетенций», которую мы успешно развивали все эти годы. Мы создали полноценную инженерно-сервисную службу с проектировщиками, с группой ГИПов, а также с теми, кого называем инженерным спецназом, – специалистами, которые проверяют и тестируют оборудование перед каждой отправкой клиенту, а также решают все вопросы, связанные с интеграцией оборудования на объекте.

В прошлом году Delta без громких заявлений, без хлопанья дверями, как ее европейские и американские конкуренты, ограничила прямые поставки оборудования в Россию. Но благодаря многолетнему сотрудничеству с Delta и опыту в организации логистической и транспортной цепочек нам потребовалось всего три месяца, чтобы переориентировать финансовые потоки, каналы поставки. И наши заказчики не заметили перебоев в поставках оборудования и запасных частей. А выстроенная инженерно-сервисная служба позволяет предоставлять также в полном объеме гарантийную поддержку покупаемого оборудования, причем это стандартные два года гарантии с даты ввода в эксплуатацию (что и до 2022 г. практически никто из прямых конкурентов предложить так и не смог). Все наши партнеры и заказчики защищены и в плане ЗИП, и в плане постгарантийной поддержки.

Кроме того, в прошлом году мы расширили перечень вендоров и продуктовую линейку. Начали работать с новым китайским производителем компанией Sinexcel, активно взаимодействуем с российскими предприятиями, такими как «Парус электро».

Но главное, чем «Темпесто» ценна для заказчиков, – это комплексная экспертиза в области систем бесперебойного и гарантированного электропитания (СБЭП и СГЭП). Мы можем не только оценить сложность задачи, но, что часто важнее, – помочь заказчику правильно ее сформулировать. А правильно сформулированная задача – это половина успеха. Далее с учетом технических параметров объекта – места размещения оборудования, особенностей внешнего электропитания, ограничений по мощности, типу подключаемых нагрузок и т.д. – оптимально подобрать оборудование и реализовать на его базе проект.

– Насколько адекватна замена ушедших вендоров? Есть ли риск технологической деградации?

– Технологический разрыв между мировыми лидерами и всеми остальными, конечно, есть. Это факт. Возьмем ту же Delta. Компания производит сотни тысячи единиц продукции в месяц, она имеет большой инженерно-технический штат НИОКР, постоянно работающий над улучшением продукции. У мировых лидеров этот процесс не останавливается. Производители второго эшелона, по сути, используют уже имеющиеся наработки, и передовые решения для них часто недоступны. Кроме того, они часто грешат тем, что заявляют одни характеристики, которые соответствуют лучшим образцам лидеров рынка, а на практике характеристики совсем другие. Такая проблема существует.

Фактически сегодня Delta осталась единственной среди мировых лидеров компанией, продукция которой доступна в России и поддерживается в течение всего жизненного цикла, начиная от подбора и заканчивая ремонтом. Все остальные «обрубили» каналы поддержки.

– Что предлагаете заказчикам, которые лишились техподдержки и ЗИП из-за ухода их традиционных поставщиков?

– Наши инженеры хорошо знают не только оборудование Delta. Более того, сейчас штат сервисной службы активно пополняется специалистами, которые остались не у дел после ухода других производителей. Это инженеры с большим опытом. У нас уже есть экспертиза по продуктам всех ведущих вендоров – Eaton, APC, GE, Tripp Lite, Socomec и др., мы можем проводить сервисные, ремонт-

ные, иногда даже восстановительные работы. Более того, у нас большой опыт по замене оборудования разных вендоров, причем много проектов выполнено еще до 2022 г. Так, на заводах Philip Morris мы меняли требующие планового ремонта ИБП APC на новые Delta. И два варианта – ремонт старых и покупка новых ИБП – по цене оказались примерно одинаковыми.

Накоплен уникальный опыт по модернизации СБЭП и СГЭП в работающих ЦОДах, практически «горячей» замене. Так, для ЦОДа «Трастинфо» в 2021 г. заменили оборудование той же APC общей мощностью 2 МВт на ИБП Delta. Для поддержания работы нагрузки был проведен монтаж резервной системы бесперебойного электропитания на оборудовании Delta из резервного фонда компании «Темпесто», что позволило поддерживать чистое электропитание потребителей (с резервированием) весь период работ по замене. Подобный проект, на 6 МВт, реализовали в Санкт-Петербурге в ЦОДе Linxdatacenter. На объекте «Акадо» старые ИБП Emerson поменяли на Delta еще в 2019 г. Все работы по замене ИБП (суммарной мощностью 3 МВт) предусматривали реконструкцию электрораспределительных систем, питающих и распределительных кабельных линий, монтаж и настройку систем диспетчеризации.

Мы, наверное, единственные в России, у кого такие проекты поставлены на поток. Как понимаете, сейчас актуальность подобных замен только возросла.

– Значит ли это, что «Темпесто» специализируется на ЦОДах?

– В нашем портфеле реализованных проектов, конечно, не только ЦОДы. Есть большой пул заказчиков из разных отраслей промышленности. Это, в частности, «Норникель», «Монди Сыктывкарский лесопромышленный комплекс», «Московская кофейня на паяхъ» и др. Причем защищаем не только ИТ-инфраструктуру, но и производственные линии. Промышленные ИБП есть и у Delta, и у нашего нового китайского вендора Sinexcel.

Большой опыт у нас и в отрасли здравоохранения. Когда МЧС строило ковидные госпитали, примерно 2/3 ИБП по этой программе поставила компания «Темпесто». Все кардиологические центры Москвы оснащены ИБП с нашей помощью. РАН – один из наших ключевых заказчиков, в частности, ИБП устанавливаем в лаборатории для защиты электропитания очень дорогостоящего оборудования.

– На какие новые технологии в области бесперебойного электропитания советуете обратить внимание? Сейчас много говорят о литий-ионных аккумуляторах.

– Пока для подавляющего большинства проектов поставляем свинцово-кислотные АКБ. Более высокая цена литий-ионных АКБ – непреодолимая преграда, они просто не вписываются в бюджет. Сегодня заказчики в основном ориентируются на CAPEX, а не на TCO. Есть заказчики, которые рассматривают TCO на 10 лет, и в этом случае ЛИ АКБ становятся выгодными, но таких заказчиков мало.

Интересное направление – использование б/у аккумуляторов электроавтомобилей. Они недорогие, а их емкость – 70%, а то и 80% номинала. В Китае рынок электромобилей быстро растет, оттуда можно привозить б/у аккумуляторы. Да и в России таких авто тоже будет становиться все больше.

Считаю, что очень недооценены суперконденсаторы. Интересное решение, которое во многих случаях может быть незаменимым, например, для заказчиков, использующих мощные перекачивающие насосы (это водоканалы, нефтегазовые транспортные сети). У них есть серьезная проблема: даже непродолжительные перебои подачи электричества (несколько секунд) «выбивают» автоматику таких насосов. Суперконденсаторы, способные к быстрому заряду и поддержанию нагрузки до 30 с, – оптимальное решение. Этого времени достаточно для запуска резервной ДГУ, находящейся в горячем режиме. К тому же суперконденсаторы по сравнению с АКБ различных типов не требуют обслуживания, имеют более длительный срок эксплуатации и компактны. В мире решения на суперконденсаторах уже широко применяются. Мы просчитываем несколько таких проектов и, уверен, доведем их до реализации.

– Традиционный вопрос о планах развития бизнеса компании.

– Мы продолжаем работу по расширению продуктовой линейки, например, системами питания постоянного тока и электрозарядными станциями для электромобилей. Активно общаемся с представителями Ирана – страны, которая уже 30 лет под санкциями, у них есть очень интересные наработки и решения.

Также продолжаем наращивать региональное присутствие. Сейчас у нас офисы в четырех городах России (Москва, Санкт-Петербург, Краснодар и Красноярск) и в двух за рубежом (Минск и Алматы). Планируем дотянуться до Дальнего Востока, открыть там офис.

Активно прорабатываем наши компетенции по новым технологиям, например, уже упомянутым суперконденсаторам, преобразователям частоты среднего и высокого напряжения. В 2021 г. открыли отдел опытно-конструкторских разработок, который производит кастомизированные продукты, например, PDU с набором функций, которые нужны конкретному заказчику. Покупая такие решения, заказчик получает необходимое оборудование, не переплачивая за лишний функционал (как сейчас часто происходит), но и не ограничивая свои потребности. Еще один пример – совместно с партнерами разработали ИБП для применения на морских судах, прошли всю необходимую сертификацию, уже активно предлагаем это решение рынку.

Сформировали штат специалистов и накапливаем опыт в реализации полного комплекса инженерной инфраструктуры ЦОДов, включая архитектурно-строительную часть, системы холодоснабжения и вентиляции, стойки, изоляцию коридоров, системы распределения и преобразования электроэнергии, мониторинга и диспетчеризации, комплексы безопасности. По тому же холодоснабжению активно привлекаем опытных партнеров. У нас есть хорошие компетенции в верхнеуровневом проектировании и управлении проектом. Мы готовы стать «единым окном» для заказчика, предлагать ему комплексное решение и нести за него ответственность.

СКС-2023: новая конфигурация рынка

А. Барсков

На российском рынке СКС – кардинальная смена основных игроков. Но новые претенденты на ведущие позиции готовы поддержать высокий технологический уровень ушедших мировых лидеров, в том числе в сегменте высокопроизводительных высокоплотных систем для ЦОДов.

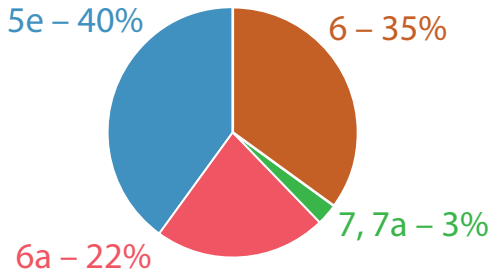
Готовность полноценно заменить технические решения ушедших мировых брендов участники отечественного рынка СКС продемонстрировали на организованной «ИКС-Медиа» конференции и выставке «СКС-2023: ЦОДы, офисы, общественные пространства». Форум, который посетили более 300 делегатов, стал, по сути, смотром «кто есть кто» на изменившемся рынке СКС. Свои продукты представили российские «Гиперлайн», C3 Solutions, ГК НКТ (кабельная система DATALAN), EMILINK (решения NTSS) и LANMASTER. Международный статус форума поддержали белорусская Patchwork и индийская Norden, а продукцию турецкой Canovate показал известный российский ИТ-дистрибьютор компания CompTek.

Основные показатели рынка

По оценке старейшины отечественной отрасли СКС, доктора технических наук, профессора НИУ МГСУ и МТУСИ Андрея Семенова, объем российского рынка СКС (с учетом шкафов и коробов, а также работ по монтажу кабельной системы) составляет примерно $700 млн. Существенный вклад в эту сумму вносит телекомсегмент – операторы связи активно применяют кабели из витых пар в сетях доступа. Количество монтируемых модулей – около 3 млн. За счет малой насыщенности рынка годовые темпы роста практически на треть выше среднеевропейских (4%). Уход из России ведущих западных производителей (которые обеспечивали 50% объема и 35% портов) ведет к значимому переделу рынка.

«Из-за повышения в несколько раз цен на медь и нефть и быстрого падения стоимости электроники приведенные затраты на построение и эксплуатацию СКС уже не могут считаться пренебрежимо малыми по сравнению с остальными статьями расходов на информационную систему, – отмечает А. Семенов. – Восстановить экономическую привлекательность СКС как сложной технической системы с большим количеством степеней свободы можно разными способами». Среди таких способов – использование специализированных продуктов (например, тонких шнуров и кабелей), частичный или даже полный отказ от принципа универсальности (технология PoLAN и др.), а также тесная интеграция с активным оборудованием («длинный Ethernet» и пр.).

Большая часть продаж на рынке (около 70%) приходится на медножильные системы. Однако рост сегмента ЦОДов (на фоне стагнации офисной составляющей) привел к увеличению доли оптических решений до примерно 30%. В области медножильных СКС по-прежнему доминирует категория 5e (рис. 1), но она постепенно теряет свою роль, поскольку в крупных проектах применяются преимущественно кабели категории 6 и выше.



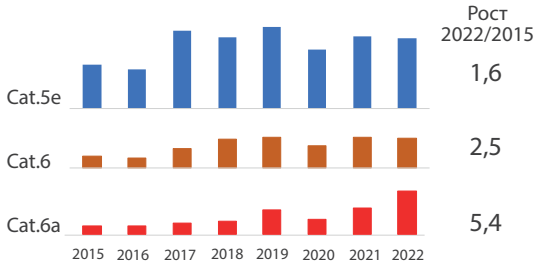
◀ Рис. 1. Распределение продаж медножильных СКС по категориям

Источник: доклад А. Семенова на конференции «СКС-2023» (апрель 2023 г.)

Эти оценки хорошо коррелируют со статистикой продаж, которые привела руководитель направления поддержки дистрибуции компании LANMASTER Татьяна Шмитова (рис. 2). Серьезного спада продаж кабелей категории 5e не наблюдается, но рост продаж категории 6a весьма существенен.

Для большинства офисных задач кабелей категории 5e вполне достаточно, поскольку, по словам А. Семенова, «среднестатистический человек не в состоянии полноценно воспринимать информационный поток со скоростью выше 50 Мбит/с, а доля медицинских и издательских систем, которые работают с объемными файлами, слишком мала». Главная же причина неизбежного повышения категории классических СКС – необходимость поддержки дистанционной подачи электропитания (PoE), причем мощность, подводимая к оконечным устройствам, постоянно растет.

Хотя большинство экспертов связывают развитие офисной кабельной инфраструктуры с медножильными системами, есть и другая точка зрения. Например, известный эксперт по СКС Владимир Стыцько считает, что будущее корпоративных сетей – это оптика. Он указывает, что пандемия существенно повлияла на глобальный рынок СКС, изменив, в частности, модель использования офисных пространств. Сокращение бюджетов на СКС нередко приводит к деградации функционала традиционных медножильных решений. Один из выходов из создавшейся ситуации – переход на пассивные оптические ЛВС (PoLAN, или POL). Они оказы-



◀ Рис. 2. Динамика продаж медножильных СКС различных категорий

Источник: LANMASTER

ваются существенно более выгодными по ряду параметров (см. таблицу), особенно с учетом того, что в 2019–2021 гг. медь сильно подорожала, а оптика выросла в цене не так заметно.

	Passive Optical LAN	UTP Категории 6
Вес кабелей, кг	190	2700
Емкость кабельных трасс, кв. м	0,013	0,11
Монтажные конструктивы	9U/ ~1 шкаф	200U/ ~5 шкафов
Бюджетная оценка	Материалы СКС = 1 Монтажные работы = 1	Материалы СКС × 1–1,5 Монтажные работы × 3–5

▲ POL в сравнении с классической СКС кат. 6 (условный проект на ~2000 Ethernet-портов с PoE)

Эксперт подчеркивает отличия POL от операторского варианта PON. Это, в частности, внутренняя коммутация пакетов (Internal Packet Switching) и другие особенности, включая поддержку PoE, заимствованные из корпоративных Ethernet-сетей. Также благодаря небольшим дальностям возможно использование претерминированных кабельных сборок. Дальнейшее развитие СКС офисного здания и кампуса В. Стыщько связывает с применением гибридных кабелей (с медными жилами для подачи электропитания и оптическими волокнами для подключения ONT), технологии POL для передачи данных и однопарного Ethernet для сервисных сетей out of band.

Основным же «двигателем» технологических улучшений в индустрии СКС, по мнению А. Семенова, являются ЦОДы и оптические решения для них – с выходом в терабитные скорости передачи в среднесрочной перспективе. Причем на расстояниях до 150–200 м (максимум до 400 м) применяется в основном многомодовая оптика, а при увеличенной протяженности (в подсистеме внешних магистралей, при соединении отдельных машинных залов ЦОДов) – одномодовые решения. Согласно статистике продаж LANMASTER, в области оптических систем за последний год наибольший рост показали решения с групповыми соединителями MPO и волокном класса OM4.

Хотя тракты оптической параллельной передачи в ЦОДах сегодня преимущественно реализуются на MPO/MTP, эти групповые соединители, по словам А. Семенова, имеют переделочную конструкцию и ряд недостатков, что вынудило искать им замену. Наилучшие перспективы у суперкомпактных соединителей группы VSFF с вертикальным дизайном, которые поддерживают скорость до 1,6 Тбит/с и эффективно решают целый ряд проблем, связанных с полярностью формируемых трактов, агрегацией каналов и построением отказоустойчивых структур, а также способствуют снижению потерь в тракте за счет уменьшения количества разъемов. Эти свойства воплощены в разъемах MDC (Mini Duplex Connector) американской компании US Conec и SN (Senko Nano) японской Senko. И большинство поставщиков – участников конференции «СКС-2023» уже начинают предлагать решения с использованием таких разъемов.

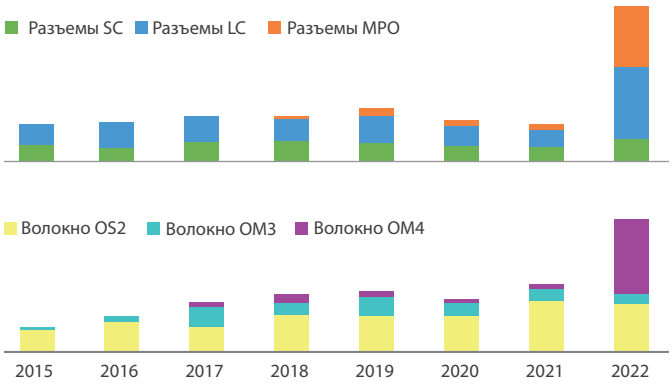
Смотр решений

Конференция «СКС-2023: ЦОДы, офисы, общественные пространства» стала, пожалуй, крупнейшим и наиболее представительным форумом СКС за всю историю существования этой отрасли в России. Поэтому неудивительно, что многие компании приурочили к ней анонсы своих продуктов.

Так, НПП «Гиперлайн» анонсировала новую премиальную СКС Hypercore, нацеленную на применение прежде всего в ЦОДах. Как подчеркнул Александр Брюзгин, директор по развитию бизнеса «Гиперлайн», в основе Hypercore – идеология бренда (а не отдельных продуктов), включающего премиальное решение, канал и сервис. Помимо собственных производственных площадок в России, компания использует контрактное производство по своим ТЗ и ТУ в Беларуси, Китае, Вьетнаме, Таиланде и на Тайване. «Мы работаем по принципу “возьми лучшее и сделай еще лучше”. И обязательно имеем “план Б”», – подчеркнул А. Брюзгин. Для гарантии качества проводится 100%-ное входное тестирование критических компонентов.

Большой интерес у участников форума вызвали сервисные предложения НПП «Гипер-

Рис. 3. Структура продаж различных типов волоконно-оптических систем ▼



Источник: LANMASTER

лайн». По мнению А. Брюзгина, в России никогда не существовало полноценного сервиса для СКС, а предлагаемые западными вендорами системные гарантии он сравнил со страховкой ОСАГО, правила выплат по которой определял сам производитель. «Мы предлагаем не ОСАГО, а полное КАСКО без франшизы», – заявил он. Ставка сделана на минимизацию простоя всей системы, а не просто предоставление компонентов для замены. Сервис предусматривает упреждающий аудит СКС ЦОДа, а также, что очень важно сегодня, – поддержку ЗИП и СКС ушедших брендов.

Если говорить о решениях VSFF, то эксперты «Гиперлайн» сделали свой выбор в пользу SN, а также его многоволоконного варианта SN-MT. «Это самый высокоплотный коннектор в индустрии, – заявил А. Брюзгин. – Можно разместить до 16 волокон в ряду в форм-факторе SN». Также в линейке Hypercore используются соединители Senko AirMT, в которых применяется бесконтактная технология, значительно снижающая воздействие загрязнений на оптические характеристики.

Компания C3 Solutions, известная своими инженерными системами для ЦОДов, также использовала площадку конференции «СКС-2023» для анонса своей новой продуктовой линейки СКС Optic X. Из названия следует, что это оптическое решение и, как большинство продуктов C3 Solutions, оно ориентировано на рынок ЦОДов. Подобно другим российским поставщикам СКС, компания сочетает собственные производственные площадки и контрактное производство. При этом, как рассказал Евгений Марьин, менеджер по работе с ключевыми клиентами C3 Solutions, был проведен «тщательный кастинг» OEM-партнеров, а для гарантии высокого качества применяется входной контроль. Также для повышения качества компания использует коннекторы исключительно американского и японского производителей.

Помимо «джентльменского набора» оптических СКС – претерминированных кабельных сборок, патч-кордов и патч-панелей с оптическими кассетами, – C3 Solutions использовала свои сильные позиции в области конструктивов и предложила специализированные кроссовые шкафы. Другие компании («Гиперлайн», НКТ, EMILINK), также ведут разработку таких шкафов и планируют представить их в ближайшее время.

СКС DATALAN компании «Специализированные кабельные системы» (входит в ГК НКТ) появилась сравнительно недавно – только в прошлом году. Ее создатели 15 лет занимались дистрибуцией швейцарских СКС R&M и Huber + Suhner (по словам Андрея Сахарова, менеджера по развитию бизнеса DATALAN, СКС R&M поставляется в Россию и сейчас), но уже давно задумались над разработкой собственной системы. События 2022 г. реализацию этого намерения ускорили. Как и многие из представленных на конференции систем, DATALAN ориентирована на ЦОДы.

Сравнивая СКС DATALAN с решениями R&M, А. Сахаров заметил, что в первой нет только решений OM5 – в российской системе используется оптика OS2, OM3 и OM4. Но производитель обещает добавить поддержку OM5 – если увидит потребность рынка. Одна из особенностей DATALAN – применение отечественных оптических кабелей. Производство шнуров и кабельных сборок DATALAN создано по стандартам Huber + Suhner и сертифицировано этим производителем. Также представитель компании отметил наличие у системы пожарной сертификации согласно закону № 123-ФЗ по ГОСТ 31565-2012.

Говоря о повышении плотности СКС, Алексей Пахомов, менеджер продуктовой линейки компании Patchwork, выделил новую микросхему для коммутаторов Tomahawk 5 (Broadcom), которая позволяет обслуживать до 64 портов 800GbE, или 128 портов 400GbE, или 256 портов 200GbE. Появление таких решений заставляет пересмотреть представления о высокой плотности СКС. Поэтому поддержка VSFF-соединителей, позволяющих использовать до 432 волокон в 1U, – необходимая характеристика решений поставщика СКС.

Белорусская компания предлагает полный спектр высокоплотных решений для ЦОДов, в

том числе с поддержкой VSFF и 25-летней системной гарантией на кабельные системы, установленные авторизованными партнерами. Среди важных особенностей предложения Patchwork – присвоение каждому изделию серийного номера, который позволяет гарантировать его качество на протяжении всех 25 лет.

ГК EMILINK – игрок с большим опытом и, наверное, наибольшей локализацией производства в России. В вопросе повышения плотности компания, честно говоря, удивила. Казалось бы, в медножильных СКС предел уже достигнут – 48 портов RJ-45 на 1U, больше просто не помещается. Но, как сообщил Дмитрий Голубев, продакт-менеджер СКС, по просьбе одного из заказчиков компания работает над панелью с плотностью 120 портов – это будет изделие высотой 2U, причем порты (всего – 240) будут размещаться не только в вертикальной плоскости.

В оптических системах (в направлении VSFF-решений) компания ориентируется на коннекторы MDC, среди достоинств которых Д. Голубев назвал удобство извлечения и возможность поворота ферул внутри коннектора. Кроме того, компания активно работает над уменьшением диаметра кабельных пучков (MPO/MTP-сборки по 24 волокна) и коммутационных шнуров (используя uniboot-конструкцию для оптики и проводники диаметра 28AWG для «меди»).

Если большинство участников «СКС-2023» уделили больше внимания оптике, то LANMASTER не забыла и про медножильные решения. Компания расширила свой «медный» портфель, предложив в дополнение к традиционной экранированной еще и неэкранированную СКС категории 6а, а также выпустив на рынок систему категории 8, способную обеспечить передачу со скоростью до 40G. Что касается оптических систем, то как и большинство других поставщиков, компания начала предлагать решения со сверхкомпактными соединителями типа SN и CS.

Особенность компании Norden, помимо того, что это производитель из Индии, – очень широкий портфель продуктов СКС, как для ЦОДов, так и для офисов. Помимо претерминированных решений высокой плотности, большой номенклатуры оптических и медных кабелей компания предлагает интеллектуальные кабельные системы. Если говорить о решениях для ЦОДов в целом, то, подобно российским С3 Solutions и EMILINK, Norden тоже предлагает шкафы и ИБП. Кроме того, в ее портфеле есть системы физической безопасности (видеонаблюдение, СКУД), системы оповещения и решения для цифровой обработки и передачи звуковых и видеосигналов. Этот новый игрок, безусловно, заслуживает внимания российских заказчиков.

Что мы потеряли

С уходом западных брендов разнообразие технических решений на российском рынке, конечно, уменьшилось – представленные сегодня продуктовые линейки достаточно однотипны. Кроме того, заказчики более не могут расширять и развивать инфраструктуры, построенные на зарубежных СКС (а таких проектов большинство), или же такое расширение существенно усложнилось.

Ряд экспертов сетует на то, что на российском рынке не осталось «интеллектуальных» СКС с системами управления подключениями. Как отмечает Григорий Вечхайзер, руководитель направления систем безопасности компании «ЛАНИТ-Интеграция», для крупных проектов, где используется 10 тыс. и более портов, отсутствие подобных систем автоматизации существенно затрудняет обслуживание СКС. А на ряде объектов с большой площадью и высокими потолками, например в крупном аэропорту, попасть в точку консолидации СКС – большая проблема. Поэтому системы управления крайне необходимы. Российские производители, конечно, знают это, и большинство из них заявили на конференции, что рассматривают возможность дополнить свои СКС системами управления.

А еще, как метко заметил А. Семенов, мы потеряли «возможность лениться». Да, трудности есть, но они преодолимы. И участники конференции СКС-2023 это убедительно доказали. ИКС

СВОБОДНЫЕ
ТЕХНОЛОГИИ
ИНЖИНИРИНГ

ПРОСТЫЕ РЕШЕНИЯ СЛОЖНЫХ ЗАДАЧ

ПРОЕКТИРОВАНИЕ И СТРОИТЕЛЬСТВО ДАТА-ЦЕНТРОВ

Россия, 127055, Москва,
Бутырский вал, д. 68/70, стр. 1

+7 (495) 120-28-66

info@sv-tech.ru
www.sv-tech.ru

C3 Solutions выходит на рынок СКС

В рамках стратегии, нацеленной на предоставление комплексных решений для ЦОДов, компания C3 Solutions дополнила свой продуктовый портфель линейкой СКС. Продукты соответствуют всем требованиям ЦОДов в плане надежности, масштабируемости и гибкости инфраструктуры, а также удобства эксплуатации.

«ИКС»: Почему компания C3 Solutions обратила внимание на СКС?

Андрей Штонда, руководитель департамента развития продуктовых направлений C3 Solutions: Это абсолютно закономерный шаг, который базируется на позиционировании нашей компании как поставщика комплексных решений для инфраструктуры ЦОДов. Расширение нашей продуктовой линейки – процесс эволюционный. Выбор СКС в качестве следующей ступени развития основан на результатах анализа как уже имеющихся в портфеле решений (серверные, телекоммуникационные и коммутационные шкафы, системы прокладки и организации кабелей), так и событий, происходящих на рынке СКС (в первую очередь это уход с него западных производителей).

«ИКС»: Проводили ли вы исследование требований заказчиков к этой категории продукции?

А.Ш.: Конечно. При создании новых продуктов мы всегда проводим анализ рынка, поскольку стремимся предложить партнерам и заказчикам решения, максимально соответствующие их потребностям. Для более глубокого понимания проблематики данного направления мы усилили экспертизу внутри компании, в том числе за счет привлечения специалистов из поставщиков, покинувших рынок в прошлом году.

За годы работы с зарубежными вендорами, которые выступали в качестве законодателей мод в области СКС, наши заказчики определили для себя архитектурные и технологические предпочтения в сфере построения СКС, привыкли к удобству эксплуатации, высокому качеству продукции. С их уходом нам важно не только органично встроиться в этот ландшафт, в уже имеющуюся у заказчиков инфраструктуру, но и дать им более интересное предложение с точки зрения и технологичности, и сервиса. Для этого мы стремимся обеспечить максимальную взаимозаменяемость компонентов, чтобы работа с новым вендором не вызывала проблем и необходимости делать все заново. Еще один важный аспект, выявленный в результате наших исследований, – это желание иметь многолетнюю системную гарантию, которую вендор дает на смонтированное решение при условии соблюдения всех правил инсталляции и эксплуатации.

«ИКС»: Что входит в линейку СКС от C3 Solutions?

Евгений Марьин, менеджер по работе с ключевыми клиентами C3 Solutions: В линейку оптических решений Optic X входят претерминированные кабельные сборки, патч-корды, наборные патч-панели с оптическими кассетами для установки в серверные шкафы (где подключается конечное ИТ-оборудование) и для организации центрального кросса. Конечно, мы не могли не использовать сильные позиции C3 Solutions в области конструктивов и предложили также специализированные кроссовые шкафы – как для организации коммутационного поля, так и для сварных соединений.

«ИКС»: Есть ли в вашей линейке решения на базе медножильных кабелей?

Леонид Юль, директор по развитию компетенций ЦОД, C3 Solutions: Основа высокоскоростных сетей для ЦОДов – оптика. Но мы понимаем, что для комплексности и завершенности предложения нужна и «медь». На нее приходится 5–10% общего объема СКС в ЦОДах, но если мы как вендор не можем ее предоставить, значит, наше предложение неполноценно. Поэтому мы разрабатываем и медножильные решения.

«ИКС»: ЦОД – это высокие скорости передачи данных. Какие скорости поддерживает ваше решение?

Е.М.: Да, все верно, скорости растут, заказчики уже внедряют решения на 40G и 100G, в проектах – переход на 200G и 400G, ведутся разговоры о 800G. Мы готовы поддерживать все указанные скорости. Понятно, что для перехода на максимальные скорости применяется распараллеливание передачи данных, используются многоволоконные магистральные сборки.

Для достижения высоких скоростей нужно сочетание высококачественных волокна и коннекторов. Причем важно не только качество самих компонентов, но и культура производства при их полировке и других технологических процессах, связанных с терминированием кабельных сборок.

Мы предлагаем в нашей линейке продукцию, в которой используются коннекторы лидеров рынка – Senko и US Conec.

Л.Ю.: Само по себе пассивное оборудование не решает вопрос скорости. Всегда нужна связка пассивного и активного оборудования. Вот недавний пример из практики: один крупный ЦОД планировал строить сеть на многоволоконных (MTP) сборках, считая этот вариант оптимальным по соотношению производительности и стоимости связки пассивного и активного оборудования. Но ситуация изменилась: существенно упали в цене двухволоконные трансиверы на аналогичную скорость, и это изменило выбор кабельной системы. Мы как производитель поддерживаем своих заказчиков в любых начинаниях и готовы предложить то, что им необходимо.

«ИКС»: Еще одно требование ЦОДов – высокая плотность соединений. Каковы характеристики вашей продукции?

Л.Ю.: В результате опроса наших партнеров и заказчиков мы выяснили, что им удобно работать с продуктами, которые обеспечивают поддержку 96 или 144 волокон в 1U. Они считают эти характеристики оптимальными. На это мы и ориентируемся в своих продуктах, хотя у нас есть решения плотностью 192 волокна на 1U.

Мы активно работаем над удобством использования нашего оборудования. В частности, используем патч-корды uniboot, в которых все волокна находятся в одной трубке. Благодаря этому патч-корд становится тоньше, занимает меньше места. Конечно, переход с портов LS на групповые разъемы MTP позволяет повысить плотность почти на порядок, но далеко не все используют для коммутации патч-корды с MTP-разъемами.

Е.М.: Могу добавить, что соблюдать баланс между высокой плотностью, удобством обслуживания и гибкостью системы особенно важно в центральном кроссе. Можно увеличить плотность и выше 192 волокон на 1U. Но пучок патч-кордов, который при этом образуется, будет сложно поместить в типовые органайзеры и сложно обслуживать. В центральном кроссе доступности патч-кордов надо уделять столько же внимания, сколько и плотности.

Л.Ю.: К вопросу о рекордной плотности. В рамках одного проекта мы разработали для заказчика шкаф ODF с возможностью разместить до 17 тыс. сварных соединений. Там используется интересная технология, которая изначально была предложена одним европейским вендором. Мы ее доработали и, надеюсь, улучшили. Но подчеркну, выбор плотности – это всегда баланс технологической возможности и реальной потребности в рамках конкретного проекта.

«ИКС»: Вы уже коснулись удобства эксплуатации. Что для этого сделано в ваших СКС?

Л.Ю.: Для обеспечения удобства обслуживания мы используем патч-корды с коннекторами push-pull: специальный хвостовик позволяет подключать/отключать шнуры без необходимости прикасаться к оптическому порту. Также мы обращаем большое внимание на удобство маркировки оптических полок высокой плотности. Если полка не имеет маркерной площадки, то неважно, сколько в ней волокон, – ее невозможно использовать. Наш богатый опыт в области

шкафов позволяет сделать действительно удобные кабельные органайзеры и прочие элементы размещения кабелей.

«ИКС»: Как вы в целом оцениваете текущую ситуацию на российском рынке СКС?

Л.Ю.: Сейчас делать какие-либо конкретные выводы было бы опрометчиво в силу того, что рынок бурлит, после ухода западных производителей он активно заполняется новыми игроками, и процесс его формирования еще не завершен. Кто-то уйдет, кто-то останется, кто-то сможет поддерживать качество своих решений, кто-то нет. Российские заказчики привыкли к качеству и удобству продукции зарубежных брендов, и вперед вырвется тот, кто сможет предложить им достойное альтернативное решение. Для того, чтобы занять весомую долю на этом рынке, нужно наращивать технологическую экспертизу и развивать комплексный подход. Следуя этой стратегии, мы сможем предложить отечественному потребителю продукты, которые позволят нам стать поставщиком №1.

Е.М.: Замечу, что C3 Solutions успешно работала и в условиях присутствия на рынке западных брендов. Да, сейчас ситуация сложилась в нашу пользу, и часть рынка, которую занимали зарубежные производители СКС, достанется нам. Но уверен, что нас бы ждал успех на рынке СКС, даже если бы западные игроки остались.

«ИКС»: Каковы планы дальнейшего развития линейки СКС?

А.Ш.: Мы видим потребность рынка в качественных решениях и стремимся подстроиться под каждый запрос. В ближайшее время мы планируем собрать обратную связь от заказчиков по уже имеющейся линейке продукции и продолжить развитие с учетом новых запросов со стороны рынка. Думаю, что одним из новых направлений в разработке будет интеллектуальная СКС, оснащенная системой управления.

Пять прогнозов для ЦОДов на 2023 год

Окончание. Начало см. «ИКС» № 1'2023, с. 10.

Энди Лоуренс, исполнительный директор по исследованиям;
Ронда Асьерто, вице-президент по исследованиям;
Дэниел Бизо, директор по исследованиям;
Оуэн Роджерс, директор по исследованиям в области облаков;
Жаклин Дэвис, аналитик-исследователь;
Макс Смолакс, аналитик-исследователь;
Ленни Саймон, старший научный сотрудник;
Дуглас Доннеллан, старший научный сотрудник,
Uptime Institute Intelligence

Продолжающаяся цифровизация будет подталкивать развитие отрасли ЦОДов, но расти им станет труднее: нет определенности, какие требования будет предъявлять новое ИТ-оборудование, усиливается регуляторное давление, повышаются капитальные и операционные затраты.

ПРОГНОЗ 3. ЦОДам предстоит подстроиться под новые чипы

Стандартизация ИТ-оборудования стала для ЦОДов благом: в течение почти двух десятилетий типовые серверы предъявляли более или менее неизменные требования к питанию и охлаждению. Эта техническая стабильность упростила планирование и проектирование объектов и помогла привлечь инвестиции в индустрию ЦОДов. Многие организации смогли провести несколько обновлений ИТ-оборудования без серьезной модернизации инженерной инфраструктуры, благодаря чему продолжительность жизни дата-центров увеличилась.

Стабильность требований помогла и проектировщикам ЦОДов. Они могли с уверенностью закладывать проектную мощность в среднем 4–6 кВт на стойку, а при определении критериев управления температурой следовать рекомендациям ASHRAE. Такая согласованность в вопросах плотности мощности и охлаждения, конечно, зависела от стабильного, предсказуемого энергопотребления процессоров и других серверных компонентов.

Однако наблюдаемый сегодня быстрый рост плотности ИТ-мощности означает, что проектные предположения относительно будущей плотности мощности и рабочей среды начинают меняться. Это увеличивает технические и бизнес-риски. Будете слишком консервативны (т.е. сохраните подход с низкой плотностью), и ЦОД может быстро стать неподходящим для установки нового оборудования. Будете слишком прогрессивны (т.е. предположите высокую плотность мощности и повторное использование тепла) – рискуете значительно перерасходовать средства из-за недоиспользуемых мощностей.

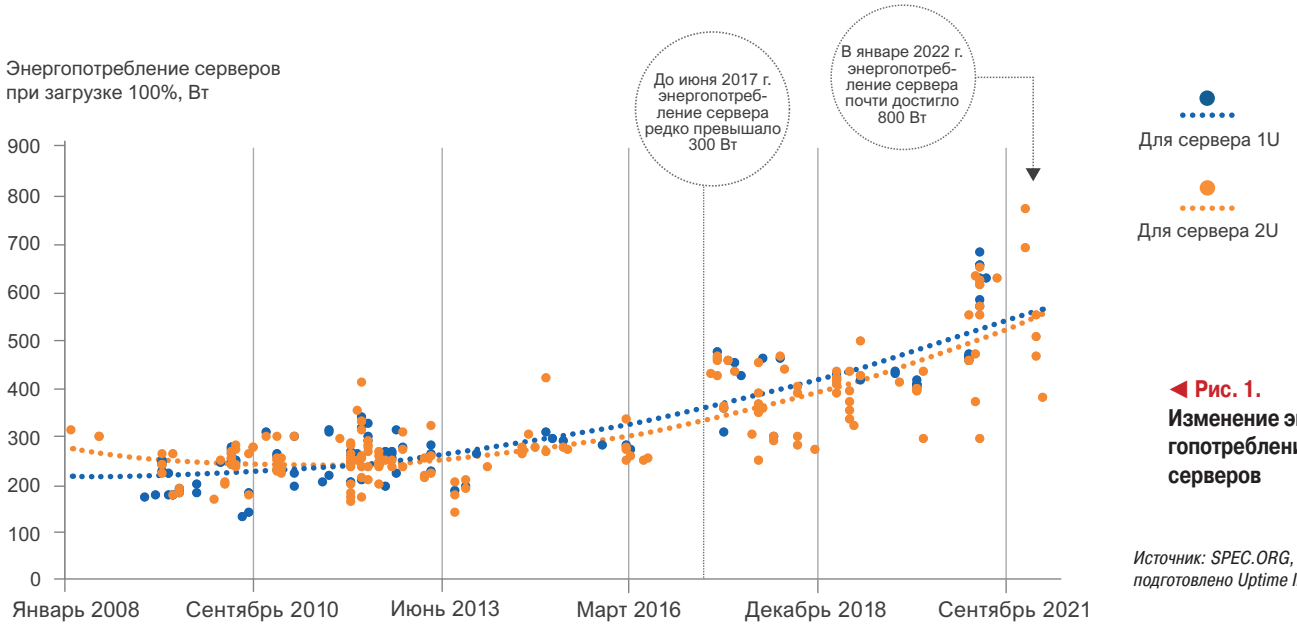
Объекты, построенные сегодня, должны оставаться экономически конкурентоспособными и технически работоспособными в течение 10–15 лет. Но проектировщикам ЦОДов неизвестны будущие спецификации ИТ-стоек, и технические требования к ЦОДам второй половины 20-х годов и далее пока не сформировались. Поэтому инженерам и лицам, принимающим решения, придется исходить из гипотез.

Температура серверов повышается

Мощность серверов и соответственно мощность заполненной серверами стойки становятся все выше. Стойки с экстремальной плотностью мощности все чаще используются, например, в системах высокопроизводительной аналитики и искусственного интеллекта.

Пока тепловая мощность сервера оставалась относительно скромной, удалось установить отраслевые стандарты в области воздушного охлаждения. Первоначальные рекомендации ASHRAE по диапазонам температуры и влажности (предложены в 2004 г., почти 20 лет назад)

Печатается с разрешения Uptime Institute.



◀ Рис. 1. Изменение энергопотребления серверов

Источник: SPEC.ORG, подготовлено Uptime Institute

отвечали потребностям большинства операторов. Впоследствии ASHRAE поощряла постепенное повышение допустимой температуры, помогая отрасли добиться большей энергоэффективности объектов.

Исследования Uptime Institute показывают, что за последнее десятилетие удельная мощность стойки умеренно, но постоянно растет. (Вопреки некоторым ожиданиям, типичное энергопотребление стойки остается ниже 10 кВт.) Эксперты Uptime ожидают, что этот рост в ближайшее время ускорится. Увеличение удельной мощности стоек связано не только с более плотной упаковкой серверов, но и с ростом энергопотребления каждого сервера, что обусловлено появлением на массовом рынке более мощных серверных процессоров, которые более производительны и энергоэффективны – при правильном использовании (рис. 1).

Эта тенденция скоро начнет влиять на нынешние подходы к проектированию ЦОДов. Более «горячие» процессоры уже появились. Новая серия серверных процессоров Intel имеет расчетную тепловую мощность (TDP) 350 Вт и возможность дополнительной настройки до более чем 400 Вт (по сравнению с 120–150 Вт всего 10 лет назад). Через несколько лет предполагается выпустить процессоры с TDP 500–600 Вт. В результате энергопотребление базовых серверов приблизится к 1 кВт или более, что повысит требования как к электропитанию, так и к управлению температурой.

Серверы для высокопроизводительных вычислений (HPC) могут служить ранним предупреждением о проблемах с охлаждением, с которыми столкнутся пользователи обычных серверов по мере увеличения их энергопотребления. ASHRAE в обновлении 2021 г. определила новый тепловой стандарт (класс H1) для серверов высокой плотности, требующий снижения температуры подаваемого воздуха до 22°C, что означает ухудшение энергоэффективности и дополнительные расходы на охлаждение. Во многом это обусловлено большим количеством тесно интегрированных компонентов высокой мощности. Ускорители HPC, такие как графические процессоры, могут потреблять сотни ватт каждый при максимальной мощности – в дополнение к серверным процессорам, модулям памяти и другой электронике.

В ближайшие годы появится больше базовых серверов с аналогичными требованиями к охлаждению – даже без ускорителей. Помимо повышения тепловой мощности процессора следует учитывать и ужесточение требований к допустимой температуре корпуса процессора – например, 55°C, по сравнению с 80–82°C сегодня. А удаление больших объемов низкотемпературного тепла – непростая термодинамическая задача.

Как соблюсти баланс

Многим существующим ЦОДам увеличить плотность энергопотребления будет трудно. Повышение мощности и/или холодопроизводительности может потребовать модернизации действующих электрических систем – ИБП, батарей, распределительных устройств и генераторов. Это дорого и сопряжено с операционными рисками. Но без этого для установки более мощного ИТ-оборудования понадобится больше пространства. По прогнозам, через несколько лет четверть стойки с такими серверами будет потреблять 10 кВт.

Новые ЦОДы проектировщики могут оптимизировать для значительно более высокой плотности мощности. Однако покупка дорогостоя-

щего электрооборудования сопряжена с экономическим риском, если только не предусмотреть гибкое управление ресурсами (например, за счет использования модульных систем высокой заводской готовности).

Потребности в плотности энергопотребления на ближайшие 10–15 лет пока сложно точно спрогнозировать. Достигнет ли средняя мощность ИТ-стойки к концу десятилетия 10, 20 или даже 30 кВт? Даже самые информированные эксперты могут лишь строить догадки.

Управление температурным режимом тоже усложняется. Многие «традиционные» установки неспособны подавать поток воздуха, необходимый для охлаждения ИТ-систем высокой плотности. Более того, для обеспечения относительно низких температур, которые обычно требуются для стоек с высокой плотностью и серверов следующего поколения, нужны более мощные системы охлаждения. А повышение температуры чревато минимум потерей производительности (современные микросхемы снижают производительность при повышении температуры). Поэтому ASHRAE рекомендует выделять зоны с низкой температурой, чтобы свести к минимуму воздействие на энергоэффективность объектов.

Все больше ЦОДов рассматривают возможность использования прямого жидкостного охлаждения (DLC). Несмотря на то что методы разработки и эксплуатации DLC «повзрослели» и на рынке имеется множество вариантов (холодные пластины или погружение), внедрение таких систем сопряжено с рядом проблем. Отсутствие стандартов повышает риски зависимости от одного вендора и перебоев в поставках ключевых компонентов, а также ограничивает выбор конфигураций серверов. Кроме того, большая часть корпоративной ИТ-инфраструктуры (главным образом системы хранения данных и сетевое оборудование) сегодня не могут охлаждаться жидкостями.

Хотя количество моделей серверов с интегрированными системами DLC увеличилось, переход на DLC требует массовой закупки такого ИТ-оборудования. При работе с несколькими поставщиками DLC, у каждого из которых свой набор требований, команды эксплуатации могут столкнуться с технической фрагментацией объектов. А проектировщикам ЦОДов придется планировать не только поддержку рабочих нагрузок со смешанной плотностью, но и более разнородную техническую среду. Сегодня вряд ли многие сотрудники ЦОДов знакомы с деталями процедур обслуживания DLC-систем, особенно систем погружного типа, что подчеркивает важность обучения и отработки процедур эксплуатации. В такой среде вероятность ошибок, связанных с человеческим фактором, только возрастет.

Предстоящие изменения в ИТ-системах ЦОДов будут очень серьезными. В основе этих перемен лежит физика полупроводников, но их движущей силой является экономика инфраструктуры: более мощные чипы, как правило, помогают повысить эффективность инфраструктуры и благодаря приложениям, которые на них выполняются, создают большую ценность для бизнеса. Для операторов ЦОДов откроется множество возможностей получить преимущества над конкурентами, но не без определенного риска. В дальнейшем ключевым фактором станет адаптивность.

- **При планировании ЦОДов необходимо учитывать быстро меняющийся баланс между требованиями к мощности, охлаждению и техническому пространству.**
- **Операторы столкнутся с новыми требованиями со стороны ИТ-систем нового поколения; потребуется общее снижение температуры воздуха в машзалах (с сопутствующим снижением эффективности), создание специализированных низкотемпературных зон или внедрение DLC.**
- **Наличие у ИТ-производителей лишь краткосрочных планов означает, что проектировщикам ЦОДов придется оперировать недостаточно определенными требованиями.**

ПРОГНОЗ 4: Фокус борьбы за энергоэффективность сместится на ИТ

В какой-то степени ЦОДы стали жертвами собственного успеха. Их быстрый рост означает столь же быстрый рост энергопотребления и увеличение нагрузки на энергосети. Большая часть ЦОДов сосредоточена в мегаполисах и вокруг них, что обостряет проблему роста энергопотребления.

В 2010-х гг. в области энергоэффективности были достигнуты значительные успехи, о чем свидетельствует снижение среднего по отрасли значения PUE, но сегодня этот процесс затормозился. Создавать надежную и энергоэффективную инфраструктуру по конкурентоспособной цене становится все сложнее, даже без учета необходимости взаимодействовать с местными органами власти, регулирующими органами и общественностью по вопросам использования энергии и воздействия на окружающую среду.

Однако до сих пор работа по повышению энергоэффективности практически не затрагивала ИТ-системы. На серверную инфраструктуру и СХД приходится наибольшая доля энергопотребления ЦОДов и их физической площади. Они же обладают и наибольшим потенциалом для повышения энергоэффективности и сокращения занимаемой площади. Часто проблема заключается в недоиспользовании ресурсов: просчеты в

Местоположение	Ограничение	Следствие
Сингапур	Трехлетний мораторий на строительство новых ЦОДов с 2019 г. по июль 2022 г.	Новые объекты должны обеспечивать значение PUE не более 1,3
Дублин (Ирландия)	Фактический запрет на строительство новых ЦОДов из-за отказа в подключении к электросети EirGrid с января 2022 г. (возможно, продлится до 2028 г.)	Ожидаются ужесточение процедуры подачи заявки и более строгие требования к ЭиЭ
Нидерланды	Годичный мораторий на новое строительство в муниципалитетах Амстердама и Харлеммермера с 2019 г. Девятимесячный национальный запрет на строительство сверхмасштабных объектов (>70 МВт) с февраля 2022 г. (за исключением муниципалитетов Гронинген и Норд-Холланд)	Введены более строгие правила в сфере ЭиЭ, устанавливающие PUE не выше 1,2 После отмены ожидаются более строгие требования к отчетности в области ЭиЭ и лицензированию для новых гипермасштабных построек
Гротон (шт. Коннектикут, США)	Годичный мораторий на строительство новых ЦОДов (>465 кв. м) с июня 2022 г.	После отмены ожидается ужесточение экологических норм и правил относительно шума для новых объектов
Франкфурт (Германия)	Ограничения на строительство ЦОДов (для облачных сервисов и colocation) в определенных зонах с июня 2022 г.	Ожидаются новые требования к повторному использованию тепла, многоэтажному строительству и соблюдению строгих стандартов эффективности (в стадии разработки)
Округ Лаудон (шт. Вирджиния, США)	Новые объекты могут строиться только в определенных зонах и должны соответствовать более высоким стандартам ЭиЭ (с сентября 2022 г.) Ограничения на подключение от компании Dominion Energy с июля 2022 г.	Для новых проектов – более строгая процедура выдачи разрешений и утверждения проекта, а также необходимость специальных мер по снижению шума. Многие новые проекты будут отложены до тех пор, пока коммунальное предприятие не обновит инфраструктуру передачи энергии (ожидается в 2026 г.)

▲ Табл. 1. Примеры ограничений на строительство ЦОДов, наложенных с 2019 г.

планировании приводят к тому, что спрос на расширение ЦОДов сохраняется даже тогда, когда подготовленные вычислительные мощности еще доступны.

Несмотря на растущие затраты и ужесточение требований к экологичности и энергоэффективности (ЭиЭ), ИТ-вендоры по-прежнему проявляют мало интереса к этой теме. Но в условиях ограниченной доступности электроэнергии на ключевых рынках ЦОДов, а также высоких цен на электроэнергию и растущего давления, обусловленного законодательством в области ЭиЭ, необходимо более серьезно подходить к энергопотреблению ИТ-систем. В частности, нужно стремиться использовать меньшие количества серверов и систем хранения при той же рабочей нагрузке.

Эксперты Uptime определили четыре ключевых фактора, которые будут влиять на повышение энергоэффективности ИТ-систем:

- сопротивление строительству новых ЦОДов со стороны местных органов власти;
- ограниченная доступность мощностей электросетей для поддержки развития ЦОДов;
- ужесточение регулирования в области ЭиЭ и более строгие требования к отчетности;
- высокие затраты на электроэнергию.

Муниципалитетам и поставщикам коммунальных услуг необходимо снизить требования

Опасения по поводу дефицита электроэнергии и земельных участков привели к тому, что с 2019 г. расширились ограничения на строительство новых ЦОДов (табл. 1). Вмешательство местных органов власти и поставщиков коммунальных услуг обычно проявляется в ужесточении процедур подачи заявок, требований к энергоэффективности, а в некоторых случаях в прямом отказе в новых подключениях к электросетям для крупных проектов. Эти ограничения привели к дорогостоящим задержкам реализации цодовских проектов и к отмене некоторых из них.

Новый генеральный план развития Франкфурта (объявлен в 2022 г.) – ключевого финансового центра и центра обмена трафиком – предусматривает переход к высокоплотному и многоэтажному строительству только энергоэффективных ЦОДов. Дублин (Ирландия) и округ Лаудон (Северная Вирджиния, США) являются двумя знаковыми примерами регионов, где энергетические компании временно приостановили или ограничили новые подключения из-за дефицита генерирующих или передающих мощностей. Устранение этих ограничений, вероятно, займет несколько лет. Ряд операторов ЦОДов как в Дублине, так и в Лаудоне отреагировали на эти проблемы, подыскав места для своих объектов за пределами мегаполисов.

Новые правила ЭиЭ

После многолетних обсуждений с основными заинтересованными сторонами власти начали требовать улучшения эффективности и отчетности в вопросах ЭиЭ для ЦОДов. Ключевой

пример – пересмотренная директива ЕС по энергоэффективности (EED), которая направлена на снижение как потребления энергии, так и выбросов углерода.

Этот регламент (вступил в силу в начале 2023 г.) устанавливает новые, подробные требования к отчетности и заставит операторов ЦОДов повышать их энергоэффективность и публиковать соответствующие показатели. В ЕС также приняли законы, которые обязывают регулируемые организации начиная с 2025 г. ежегодно сообщать о рисках, связанных с изменением климата, их потенциальных финансовых последствиях и воздействии на окружающую среду. Это затронет и ряд ЦОДов.

Аналогичные инициативы появляются в США, например, в опубликованном в сентябре 2022 г. отчете Управления по политике в области технологий и науки Белого дома о климатических и энергетических последствиях развития криптоактивов в США. Разрабатывается дополнительное законодательство, которое касается обычных ЦОДов и подготавливает почву для введения в следующие три-пять лет регулирования, аналогичного EED.

Действующее и разрабатываемое регулирование в основном сосредоточено на ограничении выбросов ЦОДами (системами электропитания и охлаждения) парниковых газов. Хотя определения и показатели остаются расплывчатыми, очевидно, что регулирующие органы ЕС намерены расширить сферу такого контроля, включив в него и эффективность ИТ.

Дорогая энергия – навсегда

Текущие энергетические кризисы в Великобритании, Европе, других странах и регионах маскируют некоторые фундаментальные энергетические тенденции. Цены на энергоносители и, следовательно, на электроэнергию находились на восходящей траектории еще до начала конфликта на Украине. Оптовые форвардные цены на электроэнергию резко выросли – как на европейском, так и на американском рынках – еще в 2021 г.

Рост цен на электроэнергию определяется рядом тенденций:

- сохраняющаяся зависимость мировой экономики от нефти и газа (и продолжающееся увеличение потребления);
- недостаточные инвестиции в мощности по производству ископаемого топлива, в то время как альтернативные низкоуглеродные инфраструктуры по производству и хранению энергии пока только разрабатываются;
- гигантское наращивание мощностей нестабильной альтернативной энергетики (в основном ветровой и солнечной), чего нельзя сказать про устойчивую низкоуглеродную генерацию;
- рост спроса на электроэнергию, обусловленный экономическим ростом и электрификацией транспорта и промышленности.

Базовая энергия становится дороже, в том числе из-за развития нестабильной альтернативной энергетики. Независимо от того, сколько источников энергии ветра и солнца (или даже гидроэлектростанций) подключено к энергосети, для гарантированной надежности и доступности ее работа должна полностью поддерживаться устойчивыми источниками генерации: атомными, угольными и все чаще газовыми электростанциями.

Однако популярность возобновляемой энергии (и низкие эксплуатационные расходы) означают, что парк традиционных электростанций работает на пониженной мощности, а все большее их число выводится в режим резерва. Электросетевым операторам – и в конечном

счете потребителям – приходится оплачивать содержание этой избыточной мощности, чтобы гарантировать надежную работу энергосистем.

Энергопотребление ИТ-систем необходимо ограничить

Вопросы высоких цен на электроэнергию, отчетности по выбросам углерода и эффективности долгое время относились в основном к инженерной инфраструктуре ЦОДов. Однако в этой области сделан практически максимум, и дальнейшие усилия приносят все меньше выгод.

В то же время поставщики ИТ-оборудования и ИТ-специалисты имеют немалые возможности повысить энергоэффективность. Оптимизация конфигурации ИТ-оборудования, динамическая консолидация рабочей нагрузки и управление энергопотреблением (включая переход в энергосберегающие режимы, регулирование/ограничение мощности и т.п.) – все это обеспечит существенное повышение энергоэффективности. Тому же будут способствовать большая утилизация ресурсов серверов и использование присущих серверному оборудованию функций эффективности.

Это не просто теоретические рекомендации: операторы веб-систем и облачные провайдеры активно их используют. Нет никаких причин, по которым другие организации не могли бы перенять некоторые из таких практик. В эпоху все более дорогих и дефицитных энергоресурсов, а также растущего давления со стороны регулирующих органов ИТ-руководителям будет все труднее отклонять призывы участвовать в битве за повышение энергоэффективности.

- **Как новые, так и реконструируемые ЦОДы сталкиваются с более жесткими требованиями со стороны местных органов власти, а также с ограничениями доступа к энергоресурсам, особенно в традиционных агломерациях дата-центров.**
- **Более строгие правила ЭиЭ заставят ИТ обеспечивать более высокую энергоэффективность. Еще один важный фактор – ценовое давление, которое вряд ли ослабеет даже в долгосрочной перспективе.**
- **Недоиспользуемые и неэффективно используемые серверы остаются одной из ключевых причин низкой энергоэффективности. Решение проблемы значительно повысит этот показатель.**

ПРОГНОЗ 5: Затраты на ЦОДы будут только расти

Еще два года назад стоимость строительства и эксплуатации ЦОДов стабильно снижалась. Этому способствовало многое: совершенствование технологий, увеличение объемов производства, крупномасштабное строительство, технологии модульного строительства, стабильные цены на энергоносители и низкие капитальные затраты.

Страна	Годовая инфляция, %
Нидерланды	14,5
Швеция	10,8
Германия	10,4
Великобритания	10,1
Дания	10,0
США	8,2
Ирландия	8,2
Сингапур	7,5

◀ **Табл. 2. Инфляция в сентябре 2022 г.**

Однако за последние два года эта тенденция исчерпала себя. Текущие проблемы с цепочками поставки и растущие затраты на рабочую силу, энергию и оборудование – все это приведет к удорожанию строительства и эксплуатации ЦОДов в 2023-м и последующих годах.

Негативное влияние увеличившихся затрат на инициацию и реализацию новых проектов будет ослаблено устойчивым ростом индустрии ЦОДов, подпитываемым глобальной цифровизацией и ростом спроса на ИТ. Поэтому большинство крупных операторов ЦОДов продолжат двигаться вперед. Однако операторы ЦОДов меньшего и среднего размера, которым не хватает ресурсов, чтобы выдержать более высокие затраты, вероятно, столкнутся с серьезными проблемами. Дополнительные расходы на выполнение новых нормативных требований и растущие процентные ставки по кредитам еще больше усложнят их выживание.

Капитальные затраты

Капитальные расходы – важный компонент стоимости жизненного цикла ЦОДа. Деньги были легкодоступными для строителей ЦОДов более десяти лет, но в 2022 г. ситуация изменилась. В странах, где расположены основные агломерации ЦОДов или крупные компании, строящие дата-центры, сегодня высока инфляция (табл. 2), что затрудняет привлечение капитала. Рост спроса на мощности ЦОДов, в том числе отложенного из-за пандемии COVID-19 и из-за проблем с выдачей разрешений и подключением к энергоресурсам, побуждает наиболее активных и занимающих наилучшие позиции на рынке операторов финансировать расширение своих площадок.

Исследование расходов на ЦОДы и ИТ, проведенное Uptime Institute в 2022 г., показывает, что более двух третей корпоративных дата-центров и операторов colocation ожидают увеличения расходов на ЦОДы в 2023 г. Большинство корпоративных дата-центров (90%) заявляют,

что в ближайшие два-три года они будут наращивать свои мощности, причем половина планирует строительство новых объектов.

Недавний рост затрат на строительство, возможно, стал для некоторых шоком. Стоимость строительства ЦОДов и сроки выполнения проектов сократились в 2010-х гг., но сейчас мы наблюдаем разворот этой тенденции. Средний корпоративный ЦОД уровня Tier III в 2010 г., по оценкам Uptime, стоил примерно $12 млн за 1 МВт (без учета стоимости земельных и общестроительных работ), и на его строительство ушло бы до двух лет. Изменения в проектировании и строительстве привели к снижению этих затрат: непосредственно перед пандемией COVID-19 они в лучших случаях составляли $6–8 млн за 1 МВт. При этом выполнение заказа занимало менее 12 месяцев. А для некоторых проектов бюджет не превышал $4 млн за 1 МВт, и на их реализацию потребовалось всего шесть месяцев.

Сегодня ситуация иная. Длительное время ожидания некоторых важных компонентов (таких как ДГУ и мощные ИБП) увеличивает затраты на проекты. По оценкам Uptime, к 2022 г. затраты на проекты уровня Tier III выросли на $1–2 млн за 1 МВт. А сроки выполнения проекта теперь могут превышать 12 месяцев.

Хотя цены на некоторые строительные материалы начали стабилизироваться на повысившемся после пандемии COVID-19 уровне, ожидается, что в 2023 г. они продолжат расти. Дефицит продукции, повышение цен на рабочую силу, полупроводники и электроэнергию – все это оказывает негативное инфляционное воздействие на всю отрасль. В то же время приобретение площадок в крупных агломерациях ЦОДов, предоставляющих сетевые подключения с низкой задержкой, теперь обходится дороже, поскольку в таких местах не хватает подходящих площадей и электроэнергии.

Исследование цепочек поставки, проведенное Uptime Institute в 2022 г., показало, что системы охлаждения машзалов, ИБП и компоненты распределения электроэнергии оказались в наибольшем дефиците. Из 678 респондентов, принявших участие в этом опросе, 80% заявили, что за последние 18 месяцев поставщики повысили цены. В частности, цены на литий-ионные аккумуляторы, которые до 2021 г. ежегодно снижались, в 2022 г. выросли из-за нехватки сырья и высокого спроса.

Более строгие требования к экологичности также повышают капзатраты. Требования в некоторых крупных хабах ЦОДов (например, Амстердаме и Сингапуре) таковы, что реализованы могут быть только проекты с высокой энергоэффективностью. Но выполнение этих требований увеличивает затраты (на проектирование, структурные изменения, системы охлаждения), что поднимает барьеры для реализации новых проектов. Новые стандарты энергоэффективности (в частности, изложенные в пересмотренной директиве EED) еще больше увеличат нагрузку на бюджеты строительства ЦОДов.

Расходы на эксплуатацию и ИТ

Эксплуатационные расходы, связанные с инженерной и ИТ-инфраструктурой ЦОДов, в 2023 г. также увеличатся из-за резкого роста основных затрат. Исследование расходов, проведенное Uptime Institute в 2022 г., показало, что самый существенный рост удельных затрат у большинства операторов ЦОДов обусловлен стоимостью электроэнергии (рис. 2) – в результате высоких цен на газ, перехода на возобновляемые источники энергии и дисбаланса в электроснабжении. Больше всего пострадали от этого повышения Великобритания и ЕС. Хотя ожидается, что цены на энергоносители снизятся (по крайней мере по сравнению с рекордно высокими показателями 2022 г.), они, вероятно, останутся значительно выше, чем были в последние 20 лет.

Второй по величине рост удельных затрат владельцев корпоративных ЦОДов продемонстрировало ИТ-оборудование – из-за сбоев в це-

Какие статьи расходов вашей организации на услуги colocation или корпоративные ЦОДы сильнее всего выросли за последние 12 месяцев? Выберите не более двух.

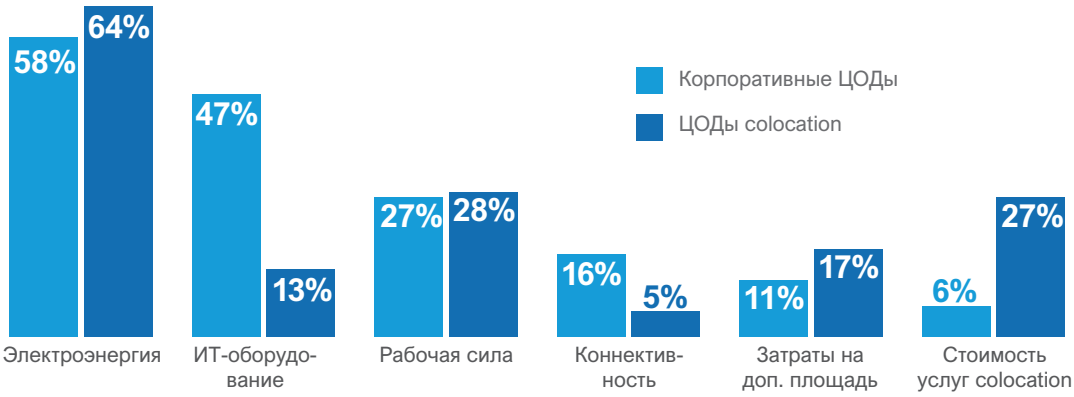
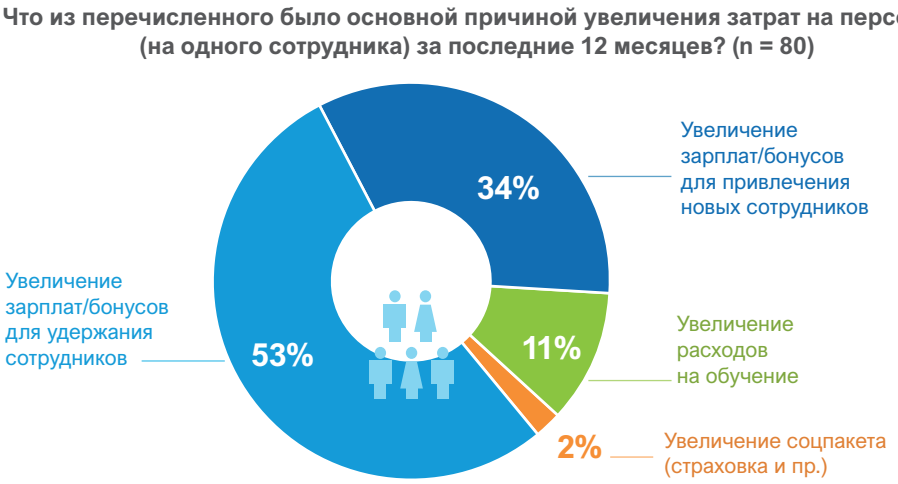


Рис. 2. Рост расходов на ЦОДы ▶

Источник: Uptime Institute, исследование затрат дата-центров и ИТ-служб, 2022



◀ Рис. 3. Причины повышения затрат на персонал

Источник: Uptime Institute, исследование затрат дата-центров и ИТ-служб, 2022

почках поставки, нехватки некоторых процессоров и микросхем для коммутаторов, а также общей инфляции. Спрос на ИТ-оборудование продолжает опережать предложение, а отставание в производстве, вызванное пандемией COVID-19, еще предстоит наверстать.

Эксперты Uptime видят признаки улучшения в области поставок оборудования для ЦОДов, в основном из-за недавнего падения глобального спроса (вызванного экономическими трудностями и циклами инвестиций в ИТ). В результате цены и сроки поставки универсального ИТ-оборудования (за некоторыми исключениями) в первой половине 2023 г., скорее всего, уменьшатся. Но позже в текущем году спрос на ИТ-оборудование для ЦОДов снова возрастет, как только некоторые крупные покупатели ИТ-инфраструктуры ускорят расширение своих площадок, что приведет к ограничению поставок определенного оборудования.

Кадровый вопрос также будет играть важную роль в увеличении затрат на эксплуатацию ЦОДов. Многие операторы утверждают, что они тратят все больше на оплату труда в попытке удержать квалифицированный персонал (рис. 3). Это еще одна проблема для тех компаний, которые не в состоянии соответствовать зарплатным предложениям быстрорастущих технологических гигантов.

Общая картина ясна: в течение следующих нескольких лет затраты на строительство и эксплуатацию ЦОДов в целом значительно возрастут. Хотя компании могут снижать операционные расходы, внедряя средства автоматизации, повышая энергоэффективность и мигрируя в облако, это, вероятно, повлечет за собой новые капиталовложения, новые требования к персоналу и большую техническую сложность.

Будут ли дорожающие ЦОДы подталкивать заказчиков к услугам colocation или к облачным сервисам? Опрос, проведенный Uptime Institute в 2022 г., показал, что, несмотря на растущие затраты, многие компании считают, что эксплуатация локальной инфраструктуры по-прежнему дешевле, чем размещение в коммерческом ЦОДе (54%, n=96) или миграция в облако (64%, n=84).

Однако на быстро меняющемся рынке, где некоторые затраты непрозрачны, оценить стоимость каждого из этих вариантов сложно. Учитывая высокие затраты, связанные с переходом в облако, компаниям, вероятно, будет выгоднее выдержать более высокие затраты на строительство и реконструкцию в ближайшей перспективе и извлечь выгоду из более низких эксплуатационных расходов в долгосрочной перспективе. Однако не всем компаниям это подходит.

У крупных организаций, которые имеют финансовые ресурсы, позволяющие извлечь выгоду из эффекта масштаба, с возможностью более простого привлечения капитала и достаточной покупательной способностью для привлечения поставщиков, удельные затраты, вероятно, будут ниже, чем у небольших компаний (и большинства корпоративных ЦОДов). Но они, скорее всего, столкнутся с более высокими расходами на экологическую отчетность и выполнение требований по отказоустойчивости и безопасности их инфраструктуры.

- **Расходы на критически важную цифровую инфраструктуру (включая ИТ- и инженерное оборудование ЦОДов) в последние годы неуклонно снижались. Сейчас эта тенденция закончилась, и цены будут расти.**
- **К росту расходов ведут проблемы в цепочках поставки и более высокая стоимость денег, энергии и рабочей силы.**
- **Спрос на цифровые услуги продолжает подпитывать спрос на ЦОДы. И нет никаких признаков того, что более высокие цены приведут к снижению спроса, хотя они, вероятно, стимулируют борьбу за повышение эффективности.** ИКС

От дома до ЦОДа: обновленное продуктовое предложение Systeme Electric

Перестроив и адаптировав к новым условиям бизнес, «Систэм Электрик» (ранее Schneider Electric в России) вывела на рынок как комплексные решения, так и отдельные продукты в привычных для рынка и традиционных для себя направлениях, сохранив при этом свою экосистему.

Алексей Соловьев,
технический директор управления по рынку «Информационные технологии», «Систэм Электрик»

С момента продажи бизнеса Schneider Electric локальному менеджменту прошло уже больше полугода, и за это время мы многое перестроили и адаптировали как с точки зрения продуктового предложения, так и с точки зрения внутренних процессов. Но нам удалось сохранить те преимущества, которые ценились нашими партнерами и заказчиками. В первую очередь, экосистему, в которую входят техническая и проектная поддержка, сервис, работа с каналом и проектными институтами и многие другие элементы, позволяющие говорить о выстраивании долгосрочных отношений с нашими заказчиками. Под новым брендом «Систэм Электрик» мы развиваем те же продуктовые направления, которые продвигали в Schneider Electric.

Обеспечиваем бесперебойное питание

Как и раньше, мы предлагаем системы бесперебойного питания: однофазные для защиты рабочих станций и распределенных сетей, и трехфазные – для критически важной инфраструктуры везде, где требуется чистое электропитание.

Наверное, более всего рынок ожидал запуска линеек однофазных ИБП Systeme Electric. Это надежные решения, специально сконструированные для различных условий эксплуатации: от дома и офиса до дата-центров, и в любом месте эти ИБП предотвратят потерю ценных данных и остановку производства.

ИБП малой мощности серии Back-Save обеспечивают высококачественное электропитание и защиту от скачков напряжения для компьютеров и бытовых устройств. Линейно-интерактивные ИБП Smart-Save предназначены для установки в шкафы и стойки для защиты ИТ-оборудования малого и среднего офиса.

В корпоративном сегменте вопрос надежного бесперебойного электропитания также не теряет актуальности. Для защиты чувствительного оборудования серверов, систем хранения данных, узлов связи и автоматизации используются ИБП Smart-Save Online с технологией двойного преобразования, которые характеризуются нулевым временем переключения питания от сети на батарею и наоборот. ИБП этой серии имеют единичный выходной коэффициент мощности, возможность подключения внешних аккумуляторов, встроенный ECOрежим для снижения потерь при относительно стабильном входном электропитании, а модели мощностью от 5 кВт – возможность создания параллельных конфигураций. Это позволяет выстраивать систему бесперебойного электроснабжения с необходимыми уровнем надежности, энергоэффективности и временем автономной работы даже для небольших вычислительных объектов.

ИБП Smart-Save Online SRT

При формировании портфеля трехфазных ИБП мы также старались предложить потребителям устройства с различными характеристиками.

Серия Uniprom рассчитана на применение в промышленном и гражданском строительстве, на тех объектах, где важно минимизировать вложения в создание инфраструктуры. Три линейки ИБП серии Uniprom охватывают диапазон мощностей от 10 до 600 кВА. Наиболее популярные конфигурации, 10–80 кВт, предлагаются в конструктиве «всё-в-одном»: батарейный массив в виде быстрозаменяемых модулей размещается непосредственно в корпусе ИБП. Это дает возможность получить компактное готовое и простое в эксплуатации решение по «классической» схеме «ИБП с 5–10 минутами автономии», не требующее углубленного проектирования.

В ближайшее время мы запускаем еще одну линейку трехфазных ИБП – серию Excelente. ИБП Excelente предназначены для защиты нагрузок разного типа, там, где требуется встроенное резервирование, быстрое и простое обслуживание пользователем. Модульная архитектура ИБП позволяет наращивать мощность и заменять модули силами службы эксплуатации заказчика в «горячем» режиме без выключения ИБП и нагрузки. Помимо резервируемых силовых модулей эти ИБП оснащаются резервируемыми модулями управления, что повышает отказоустойчивость ИБП и всей системы бесперебойного электроснабжения объекта в целом.

Эти решения обычно применяются в серверных и вычислительных центрах, где нагрузка может расти в течение всего срока эксплуатации и при этом нет времени на остановку объекта для изменения конфигурации ИБП или его обслуживания. ИБП сохраняет свои характеристики при температуре окружающей среды до 40°C : даже в случае аварийного отключения системы кондиционирования воздуха источник бесперебойного питания продолжит работу в течение длительного времени. Это также косвенно подтверждает высокий запас прочности компонентов ИБП.

Создаем «витрины» ЦОДа

Второе большое продуктовое направление подразделения IT Business, в которое трансформировалось APC by Schneider Electric, – это критически важные элементы инженерной инфраструктуры ИТ-объектов: не только крупных дата-центров, но и серверных комнат и вычислительных узлов.

Машинный зал – это своеобразная «витрина» ЦОДа. Эстетичность, продуманность технических решений положительно влияют на коммерческую привлекательность ЦОДа, если мы говорим о коммерческих площадках, и позволяют подчеркнуть важность ИТ-направления в случае корпоративных дата-центров.

Серверный шкаф Uniprom Rack

Для создания именно такой «витрины» мы разработали и выпустили новую линейку серверных шкафов Uniprom Rack, стоечных блоков распределения питания Uniprom Rack PDU, а также обширную линейку стоечных аксессуаров и средств изоляции воздушных потоков Uniprom Tools. При разработке мы хотели создать изделия с передовыми характеристиками и, что очень важно, учли пожелания сотрудников служб эксплуатации действующих ЦОДов. Огромное количество улучшений, не всегда даже заметных с первого взгляда, делает удобной и безопасной работу с ИТ-оборудованием в шкафах Uniprom Rack, оснащенных Uniprom Rack PDU, а использование самого дорогого места в ЦОДе – машинного зала – эффективным и технологичным.

Снабжаем холодом

Помимо систем электроснабжения и бесперебойного электропитания ЦОДа, мы развиваем и уже представили рынку наши новые линейки прецизионных кондиционеров– решения для поддержания точных температурно-влажностных параметров воздуха в помещениях машинных залов дата-центров различной мощности и назначения.

Для охлаждения высокоплотной нагрузки можно применять внутрирядные кондиционеры CoolRow холодопроизводительностью до 70 кВт. В зависимости от выбранного типа охлаждения в ЦОДе это могут быть как кондиционеры прямого расширения CoolRow DX, так и кондиционеры CoolRow CW, работающие на охлажденной воде. Кондиционеры выполнены в формате ИТ-стойки, если требуется большая холодопроизводительность, или в формате ½ стойки, если необходимо распределить их по длине ряда.

Для организации фальшпольной схемы кондиционирования воздуха в машинном зале мы запустили линейку периметральных кондиционеров CoolRoom. Линейки кондиционеров DX и CW традиционно можно конфигурировать в соответствии с конкретным проектным решением. Для моделей с прямым расширением в линейке есть различные варианты выносных конденсаторов, как классических, так и с V-образными теплообменниками. Можно выбрать между стандартными компрессорами с фиксированной частотой вращения и компрессорами с инверторным приводом.

В линейках с прямым расширением CoolRoom DX и CoolRow DX мы вывели на рынок модели с функцией фрикулинга. Возможность экономии электроэнергии, которая раньше была присуща в основном системам «чиллер – фанкойл», теперь доступна и в DX-кондиционерах.

При запуске линеек кондиционеров мы постарались учесть большую часть пожеланий заказчиков: машины оснащаются большим русифицированным сенсорным дисплеем и имеют рабочий диапазон внешних температур от −40 до +45°C . Предусмотрены различные варианты воздухораспределения (нижний, верхний или фронтальный выдув охлажденного воздуха) и подвода трасс с теплоносителем (сверху или снизу).

Также в конце 2022 г. мы представили рынку новую линейку чиллеров CoolFlow производительностью от 30 до 2500 кВт. Их можно задействовать как для ИТ-нужд, так и для любых иных потребностей заказчика: получать коммерческий холод или использовать как специализированные установки для охлаждения медицинского диагностического оборудования.

В чиллерах применяется компонентная база последнего поколения: винтовые и спиральные компрессоры с частотной регулировкой производительности и EC-вентиляторы с высочайшей энергоэффективностью. В сочетании с кондиционерами они могут быть использованы для реализации на базе моновендорного решения схемы кондиционирования воздуха в ЦОДе с учетом потребностей конкретной площадки.

Сами холодильные машины доступны в трех различных вариантах: моноблоки воздушного охлаждения с фрикулингом и без него, чиллеры водяного охлаждения с сухими градирнями и бесконденсаторные чиллеры внутренней установки с выносными конденсаторами.

В сжатые сроки нам удалось перестроиться и предложить как комплексные решения, так и отдельные продукты в привычных для рынка и традиционных для нас направлениях. Впереди у «Систэм Электрик» огромная работа по развитию каждого из наших продуктовых направлений, в том числе с более глубокой локализацией производства. Но уже сейчас мы можем сказать: нам удалось сохранить и эффективно адаптировать то, что определяло нас как лидеров рынка, – нашу экосистему – и с точки зрения развития бизнеса, и с точки зрения технических решений.

Пожары в ЦОДах и литий-ионные АКБ

Дэниел Бизо, директор по исследованиям, Uptime Institute Intelligence

Частота пожаров не увеличивается по мере роста ИТ-нагрузки или количества ЦОДов, но они потенциально губительны для объектов, а последующие отключения крайне негативно сказываются на бизнесе их владельцев и арендаторов.

Цена пожара

База данных об отказах (Abnormal Incident Reports Database), которую ведет Uptime Institute, свидетельствует, что пожары в ЦОДах происходят нечасто и редко оказывают существенное влияние на их работу. Всего с 2020 г. публично сообщалось о 14 случаях отключений ЦОДов, вызванных непосредственно пожарами или срабатыванием систем пожаротушения.

Серьезный пожар произошел 1 октября 2022 г. в многоэтажном дата-центре в Панге, к югу от Сеула. В нем пострадал второй по величине многопрофильный холдинг Южной Кореи SK Group. Оператором ЦОДа являлась «дочка» SK Group компания SK Inc. C&C. Согласно полицейским отчетам, пожар начался в аккумуляторном помещении, а затем быстро распространился на остальную часть здания. Пожарным потребовалось около восьми часов, чтобы взять пламя под контроль.

Хотя сообщений о пострадавших не поступало, этот инцидент может оказаться крупнейшим на сегодняшний день отключением ЦОДа, которое было вызвано пожаром. Авария вывела из строя десятки тысяч серверов, включая не только собственные системы SK Group, но и ИТ-инфраструктуру, на которой работает самый популярный южнокорейский мессенджер KakaoTalk. Авария также привела к сбоям в работе интегрированной мобильной платежной системы, транспортного приложения, игровой платформы и музыкального сервиса. У всех этих служб миллионы пользователей. Отключения затронули и облачного гиганта Naver («южнокорейский Google»), который сообщил о сбоях в работе своих сервисов онлайн-поиска, покупок, ведения блогов и медиаплатформ.

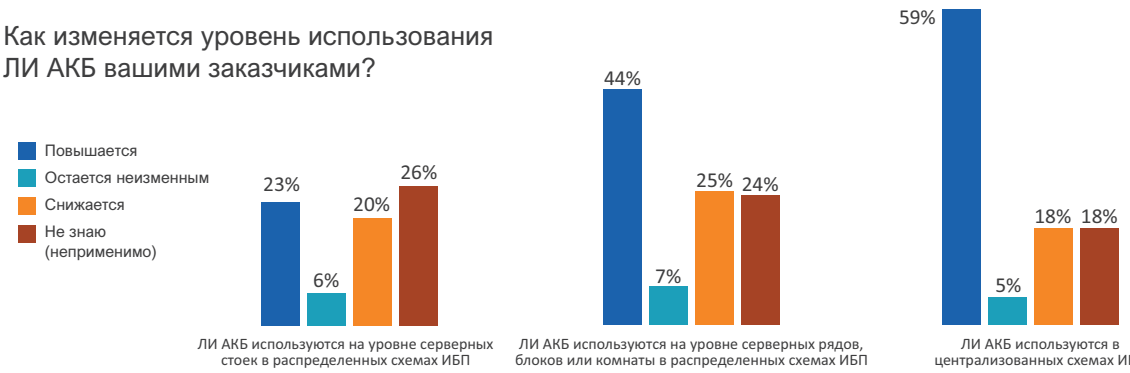
SK Group еще не раскрыла основную причину пожара, но представители Kakao, компании – владельца KakaoTalk, винят во всем установленные на объекте литий-ионные аккумуляторы производства SK on, еще одной дочерней компании SK Group. В ответ SK Group опубликовала записи из системы управления аккумуляторами (BMS), свидетельствующие об отсутствии нештатных отклонений их параметров до инцидента. Однако некоторые местные СМИ утверждают, что на самом деле BMS сгенерировала многочисленные предупреждения.

Последствия отключения ЦОДа не ограничились перебоями в работе ИТ-сервисов и соответствующей потерей доходов их провайдеров. Полицейский рейд в штаб-квартиру SK Inc. C&C; отставка совладельца Kakao Вона Намкунга; создание национальной целевой группы по предотвращению аварий и катастроф с участием военных чиновников и национального разведывательного управления – тоже следствия этого пожара. Наконец, с заявлением выступил президент страны Юн Сок Ель, который пообещал провести тщательное расследование причин пожара и размера причиненного ущерба.

Правительство Южной Кореи объявило о ряде мер, направленных на предотвращение крупномасштабных сбоев в работе цифровых сервисов. Все крупные ЦОДы теперь будут обязаны выполнять разработанные правительством процедуры предотвращения аварий, включая проведение регулярных проверок и учений по технике безопасности. Кроме того, Министерство науки и ИКТ страны будет поддерживать разработку аккумуляторных технологий, снижающих риск возникновения пожара, что представляет национальный интерес для Южной Кореи – страны, где находятся крупные производители литий-ионных элементов, включая Samsung SDI, LG Chem и саму SK on.

Пожар в Панге вызывает в памяти пожар в ЦОДе OVHcloud в Страсбурге в 2021 г. В том инциденте пострадали около 65 тыс. клиентов, многие из которых потеряли свои данные. Предполагалось, что причиной пожара, как и в Панге, были системы бесперебойного питания. По данным Французского бюро расследований и анализа промышленных рисков, распространению пожара способствовали отсутствие автоматической системы огнетушения, несвоевременное

Печатается с разрешения Uptime Institute.



◀ Рост популярности литий-ионных АКБ

Источник: Uptime Institute Intelligence

отключение электричества и особенности конструкции здания.

Вопрос финансовых потерь SK Group, Kakao и Naver еще предстоит решить. Пожар в ЦОДе OVHcloud, по оценкам, обошелся оператору более чем в 105 млн евро, причем страховкой было покрыто менее половины этой суммы. Цена пожара в Панге, вероятно, составит десятки (если не сотни) миллионов долларов.

ЛИ АКБ — повышенный риск?

С литий-ионными аккумуляторами сопряжен больший риск возгорания, чем со свинцово-кислотными АКБ с регулируемым клапаном (VRLA), независимо от особенностей их химического состава и конструкции. Это утверждение поддержано Национальной ассоциацией противопожарной защиты США и другими уважаемыми организациями. При разрушении элементов в литий-ионных батареях образуются горючие газы (включая кислород), поэтому огонь может бесконтрольно распространяться между элементами, по батарейным блокам и, возможно, даже по шкафам, если они не удалены на необходимое расстояние. Такие пожары очень сложно тушить.

Многие операторы ЦОДов до сих пор считали соотношение риска и выгоды от использования литий-ионных аккумуляторов, которые занимают меньшую площадь, имеют более длительный срок службы и пр., вполне приемлемым. Опросы ведущих поставщиков ИБП свидетельствуют о росте числа внедрений ЛИ АКБ в ЦОДах и промышленных системах: некоторые производители сообщают, что более половины своих основных трехфазных ИБП они уже поставляют с литий-ионными батареями. Согласно исследованию Uptime Institute за 2021 г., почти половина операторов ЦОДов используют такие АКБ в централизованных схемах ИБП – три года назад их было всего четверть. И проникновение литий-ионных аккумуляторов продолжает расти (см. рисунок).

Инцидент на объекте SK Inc. C&C подчеркивает важность выбора системы пожаротушения и локализации пожара как ключевых процедур обеспечения отказоустойчивости. Большинство нормативных актов, регулирующих предотвращение пожаров и смягчение их последствий, справедливо концентрируются на безопасности людей, а не на защите активов. Однако операторам ЦОДов необходимо учитывать другие критически важные вопросы, включая защиту оборудования, обеспечение непрерывности работы, а в случае аварии – минимизацию среднего времени восстановления.

Для замедления распространения пожара на ранних стадиях выхода из строя литий-ионных элементов эффективно газовое тушение (в сочетании с системами раннего обнаружения), но для ликвидации последствий крупного теплового выброса оно, возможно, подходит меньше. Вода и пена, вероятно, будут работать лучше. Размещение батарейных шкафов на большем расстоянии друг от друга может помочь предотвратить или ограничить распространение пожара. Разделение аккумуляторных помещений на огнестойкие отсеки (предусмотренное требованиями к отказоустойчивости уровня Tier IV) еще больше снизит риск отключения всего объекта.

Однако такие масштабные меры по предотвращению возгорания могут свести на нет преимущества ЛИ АКБ с точки зрения их более высокой объемной плотности энергии, меньшей потребности в охлаждении и меньшей стоимости владения на протяжении всего срока службы (особенно на тех объектах, где пространство имеет первостепенное значение).

Достижения в области литий-ионной химии и компоновки элементов аккумуляторов позволят решить проблемы эксплуатационной безопасности. Хороший пример – литий-железо-фосфатные (LFP) аккумуляторы, которые не выделяют кислорода при разложении. Более безопасные инновационные химические соединения, такие как натрий-ионные и никель-цинковые, вероятно, предложат более надежное решение проблемы безопасности (и экологичности) аккумуляторов. Но до их широкого распространения увеличение числа литий-ионных аккумуляторов в ЦОДах означает, что вероятность сильных пожаров – с потенциально тяжелыми финансовыми последствиями – может только расти. ИКС

ЦОДы: от модели до эксплуатации

Несмотря на санкции, российские компании проектируют и строят ЦОДы любого уровня сложности. На вопросы нашего издания отвечает директор по развитию компании «Хайтед-Энергетика» Михаил Саликов.

– Михаил, когда клиент говорит, что хочет построить ЦОД, с чего начинаете?

– Прежде всего уточняем, зачем клиенту дата-центр и что он планирует в нем делать. Будет это корпоративный ЦОД или коммерческий? Если коммерческий, то будет он ориентирован на модель colocation или на облака? Могут использоваться обе модели. Определяем с заказчиком концепцию построения ЦОДа, примерную требуемую мощность. Выясняем, есть ли на примете подходящая площадка: будет ли строительство в уже существующем здании (brownfield) или на свободном месте (greenfield). Изучаем возможности подведения электрических мощностей и каналов связи.

Иногда клиенты просят подобрать площадку. В любом случае объясняем возможные риски, рассматриваем варианты решения проблем и примерную их стоимость. Исходя из пожеланий клиента по срокам возведения, мощности, его финансовых возможностей определяем базовые требования, на которые будем ориентироваться на предварительном этапе.

– Каковы основные этапы проектирования ЦОДа?

– Возьмем для примера ЦОД PNK group, проект которого мы закончили. Первая его очередь уже запущена в эксплуатацию, а вторая находится на этапе пусконаладки. Сначала, еще до подписания договора, мы выполнили несколько вариантов эскизного проекта, включающих 3D-модели объекта, чтобы посмотреть, как он будет размещаться на площадке.

Следующий этап – детальное проектирование и подготовка документации для сертификации в Uptime Institute. Причем после событий февраля 2022 г. пришлось сделать перепроектирование. Изначально планировался один ЦОД на 4 тыс. стоек, состоящий из четырех одинаковых модулей, а получилось четыре различающихся ЦОДа, так как часть оборудования заказчик купить не успел. Пришлось искать замену, но российские производители не справлялись с возросшими объемами заказов, поэтому в этих четырех ЦОДах оборудование, например чиллеры и кондиционеры, разное.

На этапе детального проектирования проводилось CFD-моделирование для оценки температур и движения воздушных потоков в проектируемом дата-центре. CFD-модели привязаны уже к конкретному оборудованию, размещенному на площадке.

К сожалению, далеко не у всех российских вендоров есть модели (BIM-объекты) поставляемых устройств, и часто приходится обрисовывать их самим. Конечно, без высокой детализации, которую раньше предоставляли мировые лидеры рынка. Но все же так, чтобы стало понятно, как оборудование размещается и крепится, чтобы избежать коллизий – противоречий в смежных разделах проекта и наложения друг на друга границ объектов.

Кроме того, после автоматического анализа наши специалисты вручную проверяют проект на наличие коллизий. Практика показала, что не все проблемы выявляются автоматически. Например, пересечения лотков и шинопроводов могут идти впритирку друг к другу. С точки зрения Autodesk Revit это вполне допустимо, но неудобно в обслуживании. Хорошо, когда у заказчика уже есть служба эксплуатации ЦОДа, которая на этом этапе может высказать замечания по проекту. Если ее нет, привлекаем своих сервисных инженеров, которые оценят удобство доступа и обслуживания инфраструктуры, чтобы будущая служба эксплуатации объекта вспоминала нашу компанию добрым словом.

В результате проделанных компанией работ заказчик получил BIM-модель объекта, которую использовал на этапе строительства и эксплуатации.

– Как сказался на бизнесе компании уход с рынка зарубежных игроков?

– Проектирование стало сложнее, поскольку рынок покинули многие знакомые заказчикам вендоры. Но это не глобальная проблема. У заказчика могут быть свои предпочтения в отношении вендоров, и мы обязательно их учитыва-

ем на этапе проработки концепции. Но сначала предлагаем оборудование, которое знаем и которое доступно в России.

Компания «Хайтед-Энергетика» давно и плотно работает с Китаем, понимает китайский рынок, но в первую очередь рекомендует российских вендоров, так как они находятся в нашей стране, доступны и не прекратят сервисное обслуживание и гарантийную поддержку, подобно ушедшим поставщикам. Если подходящих решений нет, тогда обращаемся к китайскому рынку – у нас большой опыт работы с имеющими хорошую репутацию крупными китайскими поставщиками.

Кроме того, есть параллельный импорт, хотя мы стараемся его использовать в минимальном объеме.

– Как в условиях санкций выбирать дизель-генераторы и ИБП? На что следует обращать внимание?

– Еще за несколько лет до февральских событий компания провела большую работу по налаживанию взаимодействия с китайскими компаниями. Нашли много качественных поставщиков, работающих, если говорить о дизель-генераторах, с теми же брендовыми двигателями типа Cummins или Perkins, но использующих непривычный для российского потребителя бренд. Так что фактически это то же самое оборудование: собрано на той же хорошей китайской фабрике, протестировано и полностью соответствует заявленным параметрам.

С российскими компаниями знакомимся, изучаем качество оборудования, тестируем. Если есть история эксплуатации, собираем у эксплуатирующих оборудование отзывы о качестве и удобстве обслуживания, доступности комплектующих, скорости реакции производителя. И только после этого начинаем с ними работать.

Иногда с тестовыми образцами все нормально, а качество оборудования в партии падает из-за недостаточного технологического контроля. Поэтому еще на этапе производства стараемся привлекать специальный технический надзор, который периодически присутствует на площадке производителей и контролирует все этапы производства.

– Как выбираете схемы электроснабжения?

– Компания делает комплексное проектирование под ключ, включая системы электроснабжения. Еще на этапе предпроектного обследования мы рекомендуем заказчику предпочтительные схемы резервирования, делаем экономическое обоснование. Часто убеждали, что схема 2N не нужна и вполне достаточно 4/3N – дешевле, энергоэффективнее и удобнее в обслуживании. Но окончательный выбор за заказчиком.

– Как организуется мониторинг систем гарантийного электроснабжения? Как в ЦОДах помогает использование автоматизированной системы диспетчерского управления RedPine?

– Комплекс RedPine, разработку которого компания «Хайтед-Энергетика» начала еще в 2007 г., включает оборудование для сбора данных, программное обеспечение и облачную платформу. Есть три вида решений. Первое – мониторинг качества электроэнергии. Его применяют и ЦОДы, и операторы связи, особенно имеющие много удаленных площадок. Второе – мониторинг генераторных установок и управление ими, когда с помощью нашей системы можно не только осуществлять контроль, но и управлять дизелем, включая сброс некритичных аварий. Его могут использовать не только ЦОДы, но и заказчики с большим территориально распределенным парком оборудования. Третье – мониторинг окружающей среды для серверных и дата-центров. В помещении устанавливается оборудование головного устройства, а к нему по интерфейсу RJ-45 подключаются датчики. С помощью этой системы контролируется состояние оборудования, климатические параметры, наличие напряжения, протечки, срабатывание пожарной сигнализации. В планах развития АСДУ – использование предиктивной аналитики.

При желании заказчик может осуществлять мониторинг через интерфейс устройства (контроллера PedPine), использовать собственную систему SCADA или нашу облачную платформу. У «Хайтед-Энергетика» есть диспетчерский центр, где уже обслуживаются около 500 дизель-генераторных установок и серверных. Если заключен договор, на проблемный объект выезжает сервисная служба. Можем предложить обслуживание ЦОДов по всей России.

– Какие еще публичные проекты есть у компании?

– За последние два с половиной года компания «Хайтед-Энергетика» реализовала несколько проектов в области дата-центров, суммарная мощность которых составила около 100 МВт. В 2022 г. закончили строительство дата-центра в Тверской области для федерального оператора связи, который с нуля строили на лесной площадке.

– В чем особенности сдачи дата-центра в эксплуатацию?

– Компания помогает сдавать ЦОДы в промышленную эксплуатацию. Пакеты узаконивающих документов для ЦОДов и промышленных объектов примерно одинаковые. Различия – в проведении испытаний: для ЦОДов программы испытаний прописаны более глубоко, включая имитацию замен оборудования и отказов.

– Какие у компании конкурентные преимущества на рынке проектирования и строительства ЦОДов?

– В основном «Хайтед-Энергетика» проводит проектирование своими силами – в штате большая команда проектировщиков. К имеющим огромный опыт проектировщикам, инженерам по пусконаладке и сервисному обслуживанию присоединились лучшие специалисты ушедших с российского рынка зарубежных компаний. Отдельное подразделение выполняет строительно-монтажные работы. Компания готова подключиться к проекту создания и эксплуатации ЦОДа на любом этапе. У нас собралась прекрасная команда, которой по плечу реализация проектов любой сложности, вплоть до ЦОДов гиперскейлеров.

Полярность многоволоконных оптических трактов

Андрей Семенов, профессор, МТУСИ

Использование физической параллельной передачи по линиям волоконно-оптической связи в ЦОДах сопряжено с проблемой полярности, более выраженной по сравнению с дуплексными линиями. Способ полного решения этой проблемы – применение групповых разъемов следующего поколения из группы VSFF, а именно MDC и SN.

При построении линий волоконно-оптической связи машинного зала ЦОДа широко применяется физическая параллельная передача. Суть этого технического приема в том, что исходный информационный поток разбивается на несколько одинаковых в известной аппаратуре составляющих, каждая из которых (или их ограниченная группа) передается по отдельному волокну. На приемном конце из сообщений, поступающих по отдельным субканалам, восстанавливается первоначальный сигнал. Параллельная передача технически выгодна тем, что позволяет снизить тактовую частоту линейного сигнала в каждом волокне и тем самым снять схемотехнические ограничения по быстродействию элементной базы, которая используется для построения электронной части оптических приемопередатчиков.

Физический уровень информационной инфраструктуры машинного зала ЦОДа в соответствии с требованиями профильных стандартов (ANSI/TIA-942D и ISO/IEC 11801-5:2017) реализуется как структурированная кабельная система. Кабельные тракты, формируемые на ее основе, предполагают применение разъемных соединителей, с помощью которых отдельные стационарные линии соединяются между собой и подключаются к активному сетевому оборудованию. В случае физической параллельной передачи их функции выполняет MPO/MTP.

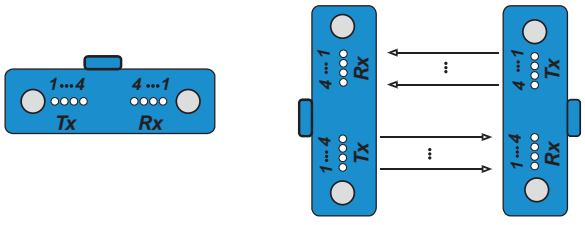


Рис. 1. Особенности нумерации волокон в вилках разъемов MPO/MTP на примере схемы Base8 ►

Истоки проблемы полярности стандартных трактов СКС

При формировании тракта передачи должны быть выполнены требования по обеспечению полярности, т.е. к разным концам конкретного световода следует подключить передатчик и приемник сетевого интерфейса. Волоконно-оптическая аппаратура, в отличие от электропроводных линий, в силу разных причин не поддерживает опцию автоматической перекоммутации цепей передачи (волокон) в случае ошибки. Как следствие задача поддержания полярности решается на физическом уровне применением соответствующих правил, которые касаются выбора конфигурации коммутационного шнура и раскладки волокон линейных кабелей по отдельным розеткам оптического кросса.

В случае типичных для кабельной системы машинного зала ЦОДа многоволоконных трактов проблема порождается самой конструкцией группового оптического соединителя MPO/MTP. В дуплексных трактах она легко решается обращением к правилу трех скрещиваний. В разъеме MPO/MTP этот прием не работает из-за того, что при соединении их вилок в розетке нумерация волокон меняется на противоположную (рис. 1).

Результатом конструктивных особенностей вилок становится принципиально несимметричная структура параллельного оптического тракта, что заметно затрудняет его эксплуатацию. В рамках частичной компенсации этого неудобства в стандартах предусмотрена возможность применения розеток, транковых предоконцованных кабелей и коммутационных шнуров двух основных разновидностей: A и B, которые отличаются друг от друга ориентацией ключевых (направляющих) элементов на противоположных сторонах (рис. 2). Функции таковых у MPO/MTP выполняют выступы на корпусе вилки и вырезы в гнезде розетки. Наличие этих элементов удобно с эксплуатационной

точки зрения, так как они за счет механической блокировки жестко задают ориентацию элементов разъема при соединении.

Типовые конфигурации параллельных трактов

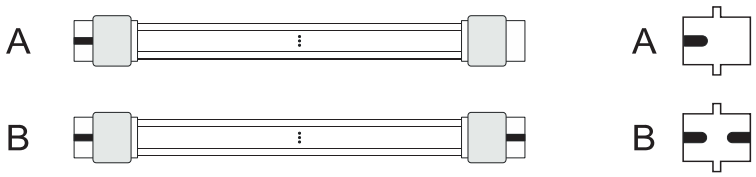
Наличие элементов разновидностей A и B по механической конфигурации позволяет ввести формальные правила построения параллельных кабельных трактов, соблюдение которых гарантирует и соблюдение полярности. Пример такой конфигурации применительно к параллельной передаче показан на рис. 3. Сами тракты, аналогично входящим в них компонентам, делятся на разновидности A и B, а перечень компонентов по полярности, используемых для их формирования, представлен в таблице.

Разновидности элементов, применяемых при формировании трактов различных разновидностей

Метод	Тип тракта	Шнур 1	Розетка 1	Транковый кабель	Розетка 2	Шнур 2
A	Параллельный	A	A	A	A	B
	Дуплексный	A	A	A	A	A
B	Параллельный	B	B	B	B	B
	Дуплексный	A	B	B	B	A

Особенность параллельной передачи – необходимость поддерживать не только функционирование многоволоконной схемы организации связи, но и нормальное функционирование дуплексных сетевых интерфейсов. Соответственно система обозначений A и B из соображений единообразия распространяется на дуплексные кабели, шнуры и розетки, как отмечено в таблице.

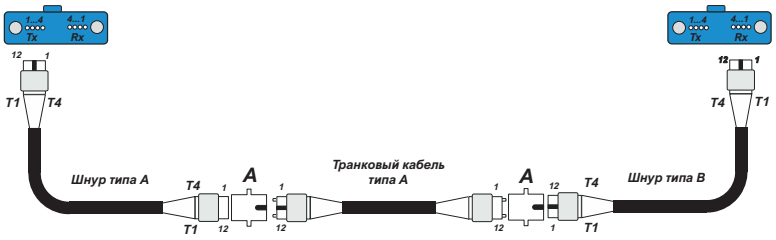
Из данных таблицы непосредственно вытекает, что стандартные параллельные тракты несимметричны по своему топологическому исполнению и за счет этого довольно сложны в текущей эксплуатации. Ситуацию не спасает даже относительная стабильность физического уровня информационной инфраструктуры по



▲ **Рис. 2.** **Разновидности трактовых кабелей/шнуров (слева) и розеток (справа) по полярности**

конфигурации из-за отсутствия физических потребителей ее ресурсов.

Из соображений удобства текущей эксплуатации кабельной системы целесообразно, в дополнение к мероприятиям по достижению правильной полярности, обеспечить одинаковое направление нумерации портов на коммутационных панелях с разных сторон линии, а также однотипную ориентацию вилок коммутационных шнуров при их подключении к розеткам коммутационного оборудования.

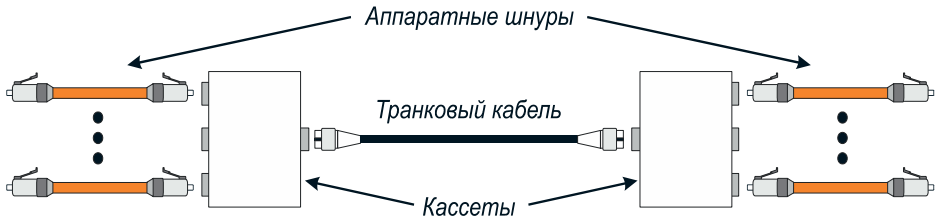


▲ **Рис. 3.** **Построение многоволоконного тракта физической параллельной передачи по схеме Base8 на транковом кабеле типа A**

Применение адаптеров и их особенности

В технике СКС широко применяются адаптеры, с помощью которых с большей или меньшей степенью эффективности расширяются функциональные возможности стационарных линий. В результате кабельная система позволяет решать те задачи или даже классы задач, которые не предусматривались исходной конфигурацией.

Применительно к оптической подсистеме СКС для ЦОДа функции такого адаптера берет на себя кассета. Возможность ее применения, которая не предусматривается в явном виде в базовых нормативных документах, изначально закладывается производителем в элементную базу. Практически это значит, что стационарные линии информационной проводки машинного зала ЦОДа строятся преимущественно по модульно-кассетной схеме (рис. 4). Появление в цепи передачи дополнительных разъемов учитывается ужесточением допусков на те потери,



◀ **Рис. 4.** **Схема простого модульно-кассетного тракта с дуплексным пользовательским интерфейсом**

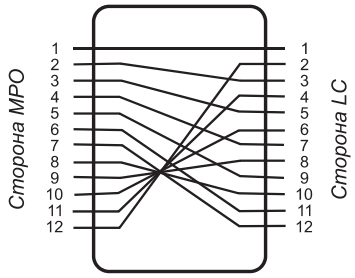


Рис. 5. Внутренняя структура кассеты-адаптера СКС Corning Cable Systems ▶

которые вносятся отдельным соединителем. Выполнение этой процедуры не приводит к серьезным проблемам из-за относительно демократичных норм на потери, отводимых стандартами на отдельный разъем.

Практическая популярность модульно-кассетной схемы обусловлена простотой модернизации структуры линии. Она не требует прокладки нового транкового кабеля и осуществляется без нарушения герметизации путей подачи охлажденного воздуха к активному сетевому оборудованию. Собственно процедура модернизации сводится к простой замене кассет на одной или обеих сторонах линии.

Одна из функций, которые можно без проблем возложить на кассету, – обеспечение полной симметрии линии по пользовательским разъемам. Из анализа данных таблицы непосредственно вытекает, что для этого достаточно изменить раскладку волокон по отдельным розеткам пользовательской стороны, причем в кассете только на одной стороне линии.

Пример подобного решения показан на рис. 5. Удобство эксплуатации в данном случае покупается переходом на несимметричную по кассетам структуру стационарной линии, что несколько усложняет процесс реализации кабельной системы. Для проектной реализации требуется повышенное внимание к конфигурированию отдельных линий, а производитель СКС вынужден расширять номенклатуру выпускаемой элементной базы.

Отдельно укажем, что кроме корпусного исполнения в виде кассеты адаптер может быть реализован по шнуровой схеме, что дополнительно устраняет по меньшей мере один разъем из цепи передачи сигнала с соответствующим уменьшением вносимых потерь. Такой элемент известен под названием разветвительного шнура или шнура-гидры. Из-за некоторого неудобства в процессе эксплуатации он не получил на практике широкого применения и значимо уступает по распространенности кассетам.

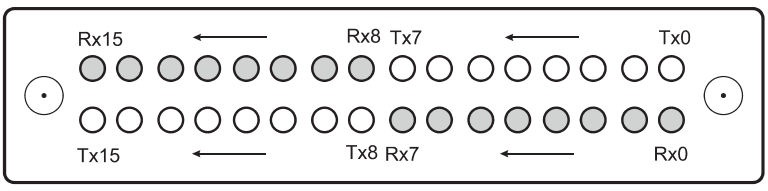


Рис. 6. Схема раскладки приемников и передатчиков в вилке разъема MXC ▼

Изменение конструкции разъема

Как видно из рис. 1, первопричина появления проблемы полярности в физических параллельных трактах на основе соединителя MPO/MTP – это линейный характер раскладки отдельных волокон в армирующем наконечнике. Для устранения этого недостатка достаточно выполнить следующие несложные процедуры:

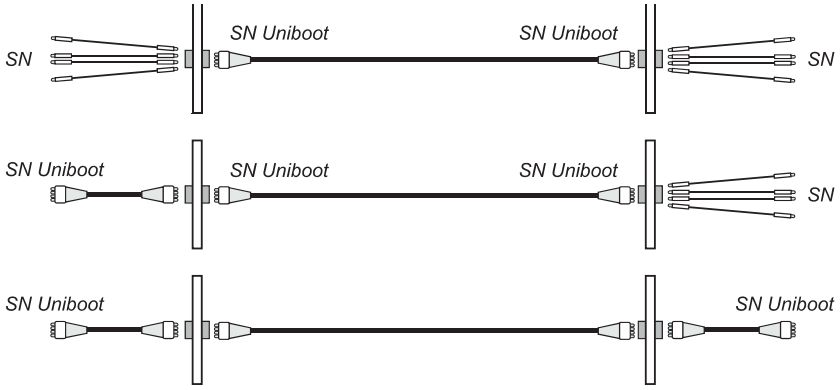
- перейти на обязательную двухрядную схему раскладки отдельных световодов в вилке группового разъема;
- включать вилки в розетку с разворотом на 180°, т.е. применять в коммутационном оборудовании исключительно розетки типа A в том смысле, который задается рис. 2;
- реализовать специальную процедуру раскладки приемников и передатчиков по отдельным посадочным местам армирующего наконечника или его функционального аналога.

Использовать комплекс этих мероприятий возможно даже в разъеме MPO/MTP, однако его результирующая эффективность будет довольно мала. Сказывается то, что при двухрядной схеме расположения волокон для надежного физического контакта оптически активных поверхностей приходится увеличивать усилие нажимной пружины плавающего наконечника практически вдвое, доводя его примерно до 20 Н, что вызывает быстрый механический износ этих поверхностей.

Рассмотренные выше обстоятельства форсированно приводят к необходимости новых разработок. Впервые в серийной технике описанный комплекс мероприятий был полностью реализован в соединителе типа MXC компании Corning. Он в основном повторяет идею MPO/MTP, с тем отличием, что в нем изначально применяется двухрядная схема раскладки волокон с делением передающих и приемных световодов на две группы. На рис. 6 показана иллюстрирующая подобное деление схема соответствия приемников и передатчиков по отдельным волокнам в вилке этого разъема.

Групповые разъемы следующего поколения

Групповые разъемы следующего поколения MDC (Mini Duplex Connector), разработанные американской компанией US Conec, и SN (Senko Nano), созданные известным японским производителем оптической коммутационной техники компанией Senko, в части полярности де-факто используют описанные выше принципы. Эти разъемы относятся к группе VSFF-изделий и ориентированы на реализацию кабельных



◀ Рис. 7.
Основные варианты построения кабельных трактов с использованием соединителя SN

трактов по схеме Base8. Их можно рассматривать как развитие соединителя URM, созданного еще в начале века немецкой компанией Euromicron и нормированного на международном уровне стандартом IEC 61754-34. Изделия конструктивно очень похожи друг на друга, хотя и несовместимы по посадочным местам.

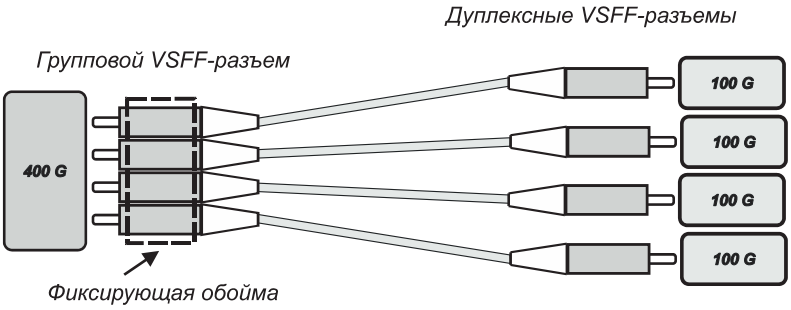
MDC и SN реализованы на индивидуальных наконечниках LC-стиля с внешним диаметром 1,25 мм, которые установлены в корпусе по плавающей схеме. За счет такого подхода достигаются существенно меньшие гарантированные потери и стабильность по обеспечиваемым обратным отражениям.

Существенным шагом вперед по сравнению с MXC является возможность формирования спаренной и счетверенной вилки из дуплексных. Она обеспечивается за счет применения боковой защелки по образцу телефонных разъемов английского стиля. Вилки вставляются в пластиковую крепежную оправку-держатель, которая оборудована собственной групповой защелкой.

Двухрядное расположение отдельных волокон в соединителе, что важно с точки зрения полярности, достигается за счет вертикальной установки отдельных дуплексных вилок в оправку-держатель.

Вилки для установки на транковый кабель без проблем могут выполнены в механически более жестком моноблочном варианте. При сборке стационарной линии такие вилки просто вставляются в обычную проходную розетку с внутренней стороны корпуса оптической полки, что позволяет обойтись без дополнительного разъема и уменьшает потери сигнала в тракте передачи. При этом за счет фактически модульного характера разъема можно построить различные варианты трактов, которые схематично показаны на рис. 7. Сильная сторона техники состоит в том, что адаптация конфигурации линии выполняется непосредственно на объекте установки кабельной системы.

При необходимости адаптации шнура под конкретную конфигурацию транкового кабеля или сетевое оборудование, в том числе в процессе изменения полярности, используется перестановка вилки на другое гнездо групповой пластиковой обоймы либо изменение полярности отдельно взятой вилки. В последнем случае защелка просто переворачивается на 180°, для чего достаточно утопить пластиковый фиксатор в гнездо корпуса и снять ее движением назад.



▲ Рис. 8.
Реализация агрегации высокоскоростных каналов на примере 400G = 4 x 100G

Возможность индивидуального применения вилки широко востребована при построении структур на основе агрегации каналов (пример показан на рис. 8) и построения отказоустойчивых конфигураций.

■■■

Известная проблема полярности при переходе на физические параллельные оптические тракты объективно существенно усложняется по сравнению с дуплексными линиями. Методы решения этой проблемы, описанные в стандартах, не отличаются высокой эффективностью, могут рассматриваться не более как удовлетворительные и создают обслуживающему персоналу существенные неудобства в процессе эксплуатации информационной проводки.

Частичное решение проблемы полярности в случае применения разъемов MPO/MTP достигается за счет использования корпусных адаптеров, что, однако, расширяет номенклатуру элементной базы, усложняет проектирование и затрудняет комплектацию проекта.

Полное решение проблемы полярности возможно только при использовании в качестве разъемного соединителя изделий из группы VSFF, в которую в настоящее время входят MDC и SN. ИКС

Envicool впишется в ваш ЦОД. Прецизионно

Большой опыт и портфель решений, готовность развивать бизнес в России – важные преимущества Envicool, стремящейся на лидирующие позиции в сегменте ЦОДов. Знакомит с компанией Владимир Шепелев, управляющий директор ее российского офиса.

– Давайте начнем с краткого представления компании Envicool.

– Основанная в 2005 г. в Китае, Envicool сегодня работает в более чем 120 странах и является ведущим мировым поставщиком решений прецизионного управления климатом. Более 60% продаж приходится на оборудование для центров обработки данных и ИТ-комплексов. Остальное – системы для телекома, рефрижераторов, зарядных станций электромобилей и пр. В России около 85% продаж – оборудование для ЦОДов и ИТ-комплексов, оставшиеся 15% – телеком.

Envicool располагает шестью заводами в Китае, три из которых занимаются производством прецизионных кондиционеров. В компании работают около 3 тыс. человек, причем более 800 из них – в НИОКР. В прошлом году Envicool преодолела важный рубеж – выпуск трехмиллионной единицы оборудования.

Компания имеет сертификаты ISO9001, ISO14001 и ISO45001, а ее решения сертифицированы по стандартам CCC, CE, UL, TUV, China Evergy Saving и др. Она применяет процесс интегрированной разработки продуктов, а также методы Total Quality Control для управления цепочками поставок с целью максимально эффективного удовлетворения потребностей клиентов. Как член China Communications Standards Association и других организаций, Envicool принимает активное участие в формировании отраслевых стандартов.

– Какие решения Envicool предлагает для ЦОДов? В чем их конкурентные преимущества?

– Основные линейки продукции для ЦОДов – это шкафные прецизионные системы охлаждения воздуха различных типов и конфигураций, как «классические», фреоновые, так и водяные – с подключением к холодильным машинам (чиллерам). Межрядные кондиционеры изготавливаются для различных архитектур построения серверных залов и изоляции коридоров. Кроме того, Envicool предлагает системы для контейнерных и модульных ЦОДов, микросерверных стоек, телекоммуникационных площадок и контейнеров с АКБ. Продуктовый портфель включает также индивидуальные решения для охлаждения различного оборудования.

Вся выпускаемая продукция конфигурируется индивидуально в зависимости от требований заказчиков, обладает высокими показателями энергетической эффективности (EER), имеет компактные размеры и использует компоненты ведущих брендов. Последнее обстоятельство сегодня может оказаться особенно важным для российских заказчиков: например, компрессоры и вентиляторы ведущих западных производителей, к которым привыкли заказчики, напрямую в Россию поставляться не могут, а в составе кондиционеров Envicool – вполне. Со своими производственными мощностями, удобно расположенными относительно заводов поставщиков компонентов, Envicool может изготовить оборудование в кратчайшие сроки (сборка возможна сразу на нескольких производственных линиях, а это десятки блоков в неделю).

– Насколько важны для Envicool «зеленые» технологии? Какие инновации вы применяете?

– Envicool уделяет пристальное внимание эффективности решений, поскольку на охлаждение, в первую очередь классическое, приходится значительная доля общего энергопотребления ЦОДа. Работаем над повышением эффективности как на уровне компонентов, так и систем в целом. В качестве примера приведу:

- фреоновый фрикулинг;
- прямой воздушный фрикулинг, в том числе с применением адиабатического охлаждения;
- системы типа «холодная стена» с низкими скоростями движения воздуха (LSV);
- испарительное охлаждение с теплообменниками «воздух – воздух»;
- решения для непосредственного жидкостного охлаждения микросхем серверов.

Некоторые из этих решений в России пока не слишком актуальны. Это прямое жидкостное охлаждение и прямой воздушный фрикулинг (заказчики стремятся не допускать, чтобы внешний воздух напрямую заходил в ЦОД). Испарительное охлаждение с теплообменниками «воздух – воздух» требует еще на этапе проектирования здания предусмотреть огромные воздуховоды и отверстия в стенах (или в потолке). Этот вариант тоже пока не получил в России должного распространения, но имеет хорошие перспективы. Системы LSV также набирают популярность. Однако наибольшее число запросов мы получаем на фреоновый фрикулинг (в наших решениях эта технология называется iFreecooling). Ее суть заключается в установке дополнительного модуля (насоса хладагента), который позволяет охлаждать фреон уличным воздухом.

– Есть ли примеры использования оборудования Envicool в крупных ЦОДах?

Кондиционеры XRow и CyberMate

В линейку межрядных кондиционеров XRow входят компактные (шириной 300 и 600 мм) модели холодопроизводительностью до 60 кВт, работающие на фреоне (DX) или на захоложенной воде. Шкафные кондиционеры CyberMate – также во фреоновом исполнении (холодопроизводительность 30–120 кВт) и на воде (40–200 кВт).

Система управления собственного производства EVO обеспечивает групповую работу контроллеров кондиционеров, резервирование их вентиляторов, а также управление расходом воздуха в зависимости от нагрузки. Интеллектуальная функция групповой работы помогает избежать несбалансированной нагрузки и координировать распределение холода.

Использование во фреоновых моделях кондиционеров инверторного компрессора с плавной регулировкой холодопроизводительности (10–100%) обеспечивает высокую эффективность при частичной загрузке. Кроме того, фреоновые модели как в шкафном, так и в рядном исполнении поддерживают технологию естественного охлаждения iFreecooling.

▲ XRow DX & iFreecooling

◀ CyberMate DX-V & iFreecooling

– Безусловно. В настоящий момент продукция Envicool уже работает на объектах таких компаний, как «Ростелеком», «Вымпелком», МТС, PNK group, «Росатом», «Транснефть» и т.д. Стоит отметить, что это преимущественно не небольшие серверные, а средне- и крупноразмерные ЦОДы, которые проектировались в соответствии с требованиями Uptime Institute.

Также компания уделяет большое внимание телекоммуникационному рынку: на территории РФ уже установлены более 10 тыс. единиц оборудования на базовых станциях и в термобоксах.

– Как компания работает в России? Кто ее основные партнеры?

– Мы учитывали специфику всех партнеров, включая системных интеграторов в плане проектных продаж, поэтому используем классическую двухуровневую систему продаж. Работаем с крупными дистрибьюторами – OCS, RRC, Marvel.

– Какова логистика поставок в Россию? Есть ли на территории РФ склады оборудования?

– Используем преимущественно железнодорожное сообщение, которое уже прошло «испытание боем» (всплеск COVID-19 на территории Китая в декабре 2022 г.) и хорошо себя зарекомендовало. В случаях срочных поставок задействуем прямые перевозки автотранспортом. К водному транспорту пока не прибегаем.

Хотя исторически складские программы по прецизионному оборудованию не пользовались большим спросом, сегодня по понятным причинам они стали очень востребованными. Мы поддерживаем на складе оборудование всех основных линеек, суммарной холодопроизводительностью несколько мегаватт. Имеется и склад запчастей для всех моделей: любой вентилятор, любой компрессор для любого кондиционера, причем комплектующие в основном европейских брендов.

– Сейчас заказчики вынуждены существенно менять список основных поставщиков. Оборудование каких прекративших поставки производителей может заменить продукция Envicool?

– Мы оказались в нужное время в нужном месте. Да и многолетний опыт работы в одной очень известной и прекратившей поставки компании-производителе помог. Уже наработана база типовых решений по замене оборудования таких вендоров, как Stulz, Vertiv, Schneider Electric (Uniflair), Huawei и т.д.

Один пример. Популярный 20-кВт кондиционер Vertiv имеет габариты 750 x 750 мм, а у Envicool такой же кондиционер – 750 x 755 мм. Разница всего 5 мм. А ведь часто заказчик просит вписаться в определенные габариты. И размеры, и технические характеристики решений Envicool позволяют с легкостью вписаться в проект, в который изначально было заложено оборудование ушедших компаний.

– Каковы ваши планы?

– Учитывая свой опыт и передовое портфолио, стремление усиливать присутствие на российском рынке и готовность инвестировать в него, понятные и прозрачные партнерские и складские программы, мы ставим задачу-минимум – войти в топ-3 производителей. Мы планируем расширять штат сотрудников и развивать сервисную сеть, проводить обучение и оказывать необходимую оперативную поддержку нашим партнерам и заказчикам.

Мониторинг инженерных систем ЦОДа: что, зачем и как

Центр мониторинга ЦОДа

Александр Коняев, главный инженер Южного кампуса;
Николай Лукин, руководитель направления слаботочных систем, IXcellerate

Цель мониторинга – оперативно выявлять неполадки в работе инженерной инфраструктуры, обеспечивая бесперебойную работу всего дата-центра. Без мониторинга невозможно предоставить требуемый современному бизнесу уровень доступности оборудования и надежности сервисов.

Центр обработки данных – это сложный технологический организм, который состоит из множества элементов и инженерных систем. Все его узлы функционируют и взаимодействуют между собой, чтобы обеспечивать бесперебойную работу серверного и телекоммуникационного оборудования. Размещая на своих площадях ИТ-инфраструктуру клиента, оператор дата-центра должен сделать максимум для того, чтобы все системы жизнеобеспечения машинного зала – кондиционирования, вентиляции, пожаротушения и т.д. – работали безупречно. Поэтому, построив высокотехнологичный объект, он должен поддерживать его в идеальном состоянии и избегать сбоев и аварий.

Чтобы иметь уверенность в том, что все системы ЦОДа работают в штатном режиме, нужен постоянный контроль, мониторинг его инженерных систем. С помощью системы мониторинга ведется наблюдение за всеми технологическими процессами и компонентами, которые входят в состав ЦОДа, оценивается их состояние и прогнозируются нештатные ситуации. Система фиксирует любое, даже самое незначительное отклонение от нормы (например, повышение температуры в машинном зале) и сигнализирует об этом. Своевременно полученный сигнал позволяет принять меры и не допустить изменения показателей до критичных – аварийных – значений.

Когда надо задумываться о мониторинге?

Было бы ошибкой считать, что целесообразность внедрения системы мониторинга зависит от каких-либо параметров ЦОДа, например, его мощности или количества стоек. Мониторинг инженерных систем необходим любому дата-центру, и позаботиться о нем нужно еще на этапе проектирования. После запуска объекта внедрить систему будет очень сложно, по меньшей мере понадобится приостанавливать работу ЦОДа, что в принципе недопустимо.

В систему мониторинга поступает информация от сотен объектов дата-центра: трансформаторов, счетчиков электроэнергии, ИБП и других компонентов инженерной инфраструктуры. Это большая, сложная система, и все ее элементы – датчики, контроллеры, анализаторы тока и т.п. – следует подобрать на этапе проектирования ЦОДа, спланировать их расположение, решить, по каким протоколам обмена данными они будут работать, оценить совмести-

мость и т.д. Таким образом, один из этапов проектирования дата-центра – проектирование его системы мониторинга.

Проектная документация

Документация по проектированию системы мониторинга должна содержать следующие разделы:

- список оборудования;
- архитектура системы (схема расстановки оборудования и расположения датчиков, схема подключения контроллеров к сети и т.п.);
- список всех отслеживаемых параметров с заданными (нормальными) значениями;
- пороговые значения отслеживаемых параметров (для определения предаварийных и аварийных ситуаций).

Пороговые значения определяются в первую очередь ГОСТами, опытом эксплуатации тех или иных систем, а также параметрами SLA. Например, согласно отраслевым нормативам, уровень напряжения не должен превышать 220 В ± 10%. Однако в соответствии с предоставляемыми ЦОДами IXcellerate SLA такой разброс значений недопустим: мы должны обеспечивать клиентам «чистое» напряжение в 220 В, ни на один вольт больше и ни на один вольт меньше.

Обычно предусматриваются два вида аварийных оповещений – предупреждения об отклонении от нормы и сообщения о критическом уровне отклонения. Первая ситуация расценивается как предаварийная, вторая – как чрезвычайная. Так, снижение температуры в машинном зале на два градуса, с 23 до 21°, будет идентифицировано как предупреждение (предаварийная ситуация), а если температура опустится ниже 20° – сработает сигнал аварии, которая требует немедленной ликвидации.

Исполнительная документация

Помимо технологического проекта следует разработать также регламенты и инструкции для персонала. В этих документах фиксируется план действий на случай отклонения показателей от нормы. Дежурный инженер должен четко знать, что делать в случае предаварийной или аварийной ситуации, чтобы локализовать неполадки и не допустить коллапса.

Обязательная составляющая системы мониторинга ЦОДа – это аварийные карты, которые готовятся профильными инженерами. Каждую карту заполняет отдельный специалист, поскольку план действий в случае пожара отличается от плана действий в случае протечки кондиционера.

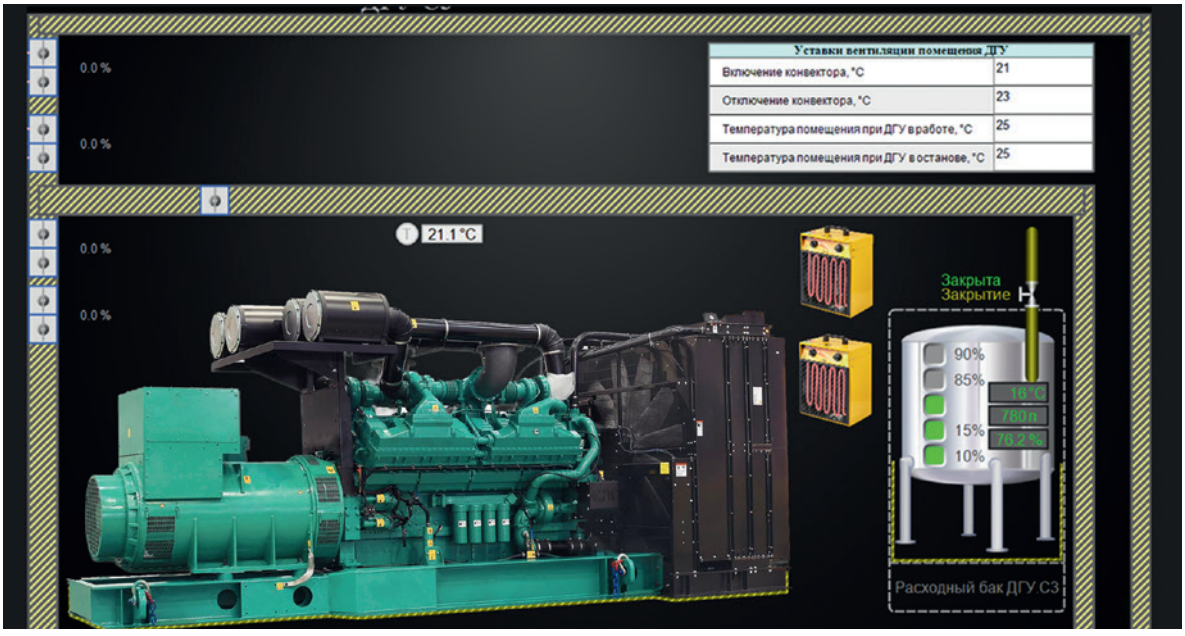
Объединяя технологии и регламенты, мы получаем высокоэффективный механизм управления инженерной инфраструктурой ЦОДа.

Что отслеживает система мониторинга

Мониторинг в ЦОДе охватывает важнейшие инженерные системы:

- электроснабжение (контролируются напряжение в ИБП, сила и частота тока, уровень топлива в баке ДГУ);
- холодоснабжение (температура в помещениях, давление хладагента, отсутствие протечек);
- вентиляция и кондиционирование воздуха (температура на входе и выходе из кондиционера, скорость вращения вентиляторов);
- пожарная сигнализация (возгорание, уровень задымления).

Аварии в дата-центре могут происходить не только из-за сбоев оборудования, но и по вине людей, поэтому отдельная функция системы мониторинга – обеспечение безопасности. Основ-



◀ Мониторинг работы ДГУ

ная задача системы – не допустить несанкционированного доступа в помещения ЦОДа. Для этого внутри объекта устанавливаются охранные извещатели (датчики). Система показывает, через какую дверь вошел человек, фиксирует номер его идентификационной карты, отслеживает маршрут. В случае несанкционированного открытия двери или окна, разбития стекла или движения внутри помещения срабатывает тревожная сигнализация. На пульт охраны передается оповещение, дежурный по видеокамерам производит осмотр и при необходимости следует к источнику тревоги, возможно, предварительно заблокировав двери.

Принципы работы системы мониторинга

Система отслеживает, как функционирует подконтрольное оборудование, и фиксирует возникающие ошибки. Количество наблюдаемых параметров может исчисляться десятками и даже сотнями. Например, в первой очереди ЦОДа MOS5 в Южном кампусе IXcellerate установлено 16 ИБП, и для каждого из них контролируется несколько десятков параметров.

Оборудование. Для снятия первичной информации используются датчики, которые передают полученные данные на контроллеры. Далее вся информация аккумулируется в системе и через единый интерфейс выводится на экраны в центре мониторинга ЦОДа. Дежурные инженеры отслеживают показатели круглосуточно.

Детализация данных. На мониторах отражаются все важные параметры. Специалист видит картину целиком и при необходимости открывает отдельные вкладки – углубляется в детали. Например, отслеживая уровень напряжения в системе, он может просмотреть параметры по каждому вводу в отдельности.

Частота обновления. Частоту «опросов» контролируемого оборудования можно настроить. Будет ли система снимать показания раз в секунду или раз в минуту, зависит от уровня критичности того или иного параметра. Например, в дата-центрах IXcellerate показатели температуры и напряжения отслеживаются не реже одного раза в секунду. Чем чаще поступают данные, тем лучше, поскольку скачок напряжения или температуры может произойти внезапно и пропустить его ни в коем случае нельзя.

Визуализация. Для удобства отслеживания и наглядности все контролируемые системы и их параметры визуализируются в виде схем и карт. Как будут выглядеть показатели на экране, определяется заранее. Каждый дата-центр может настроить визуализацию в соответствии

Датчик температуры

со своими потребностями и предпочтениями. В процессе разработки вида экранов специалисты анализируют, насколько та или иная визуальная подача информации приятна для глаз, и подбирают подходящие и интуитивно понятные варианты. Так, система автоматической пожарной сигнализации не только оповещает о задымлении, но и показывает место срабатывания датчика, чтобы дежурный сразу увидел на плане, где появилось возгорание.

Оповещения. В случае аварийных ситуаций система мониторинга выводит данные на экран (в заданном визуальном формате) и рассылает всем ответственным лицам оповещения с расшифровкой аварии (в формате SMS и e-mail).

Сбор статистики. Все данные, поступающие в систему, агрегируются, архивируются и хранятся на отдельном сервере не менее одного года. Это дает возможность анализировать, как вела себя каждая система в определенный промежуток времени – как держался заряд на батареях, какую температуру поддерживал кондиционер, как часто происходили сбои и т.д. На основе этих данных можно скорректировать работу того или иного прибора.

Резервирование. Для сбора и хранения данных, поступающих в систему мониторинга, используется отдельное серверное и сетевое оборудование. Для организации резервирования потребуются как минимум два сервера, чтобы при выходе из строя одного из них мониторинг продолжил работать на втором. Сами мониторы в центре мониторинга также должны быть подключены к бесперебойному питанию с резервом.

■■■

Центр обработки данных, не оснащенный системой мониторинга, не может обеспечивать уровень доступности оборудования и надежности сервисов, который требуется современному бизнесу. Помимо этого, постоянный контроль работы инфраструктуры помогает увеличить ее сохранность и срок службы за счет достижения оптимальных параметров эксплуатации и своевременной реакции на любые сбои. ИКС

PDU RakTek – решения для ЦОДов

Уникальные технологии и более чем 15-летний опыт работы команды RakTek позволяют предлагать оптимальные решения, нацеленные на задачи клиентов и отвечающие всем требованиям по производительности, безопасности, управляемости и надежности.

Блоки распределения питания (PDU) – «интерфейс» между системой бесперебойного электропитания и обслуживаемым ею ИТ-оборудованием. От них во многом зависят надежность и эффективность работы ИТ-систем. Но с уходом западных вендоров на рынке PDU, особенно интеллектуальных, возник вакуум. Решения RakTek обеспечат тот уровень качества, к которому привыкли заказчики, работавшие с мировыми брендами. А набор уникальных функций ставит их во многих проектах вне конкуренции.

Со сменой вендоров для заказчиков на первое место выходит контроль качества. Каждый PDU RakTek проходит всеобъемлющее тестирование на производстве и снабжается специальным шильдом с его результатами. Кроме того, прежде чем начать продажи этих решений в России, команда RakTek предоставила образцы продукции всем ключевым заказчикам, которые проверяли их как в своих лабораториях, так и в «боевых» условиях – в серверных и ЦОДах. Только после этого принималось решение о покупке.

RakTek предлагает 170 моделей вертикальных (0U) и горизонтальных (высотой 1U или 2U) PDU.

Базовые модели **RakTek Basic** предназначены для надежного распределения электропитания по доступной цене.

Блоки **RakTek Local Metered** оснащаются цифровыми дисплеями, на которые выводятся показатели напряжения, силы тока, активной и полной мощности, коэффициента мощности и потребляемой энергии. В дополнение к локальному контролю модели **RakTek Metered Lite** обеспечивают удаленный мониторинг по сети Ethernet. Эти и все более старшие модели поддерживают возможность подключения различных датчиков.

Модели **RakTek Metered** оснащаются уже двумя Ethernet-портами 1 Гбит/с, а также, как и все старшие модели, имеют съемный контроллер/дисплей с функцией «горячей» замены и поддерживают возможность каскадирования до 16 PDU. **RakTek Metered Plus** дополнительно обеспечивают удаленный мониторинг подключенной нагрузки по каждой розетке. **RakTek Switched** наряду со всеми функциями **RakTek Metered** позволяют удаленно управлять отдельными выходными розетками для перезагрузки подключенного оборудования. Наконец, **RakTek Managed** обладают всеми возможностями RakTek Metered Plus и RakTek Switched.

Модели **PDU RakTek с функцией ATS** обеспечивают резервное электропитание оборудования с одним блоком питания.

PDU RakTek оснащаются универсальными розетками C13/C19 (16A), в которые можно подключить любую вилку – C14 или C20. При покупке PDU многие заказчики заранее не знают, сколько каких розеток им потребуется. PDU RakTek решают этот вопрос окончательно и бесповоротно. Розетки совместимы со штекерами P-Lock и V-Lock, которые обеспечивают защиту от случайного выдергивания шнура. Кроме того, в комплект входит запатентованная система фиксации кабеля RT Lock для вилок C14.

Блоки PDU поддерживают большое число вариантов крепления, в том числе систему скользящих закладных гаек. Монтировать PDU можно как на кабельную трассу, так и на каркас шкафа.

Заказчики часто предпочитают цветовую кодировку PDU. RakTek наряду с базовым (черным) предлагает еще семь цветовых вариантов, причем при заказе партии от 10 штук покраска в альтернативные цвета бесплатна.

PDU RakTek готовы к эксплуатации при температуре до +60°C . Это во многом достигается за счет того, что для защиты цепей используются магнитно-гидравлические низкопрофильные расцепители с высокой скоростью срабатывания. (Многие конкуренты используют обычные автоматы – тепловые расцепители, которые не могут обеспечить надежную работу при температуре выше +45°C.)

PDU RakTek позволяют осуществлять удаленный мониторинг: к одному PDU можно подключить до 16 различных датчиков с возможностью считывания их показаний через веб-интерфейс или выгрузки в вышестоящую DCIM-систему.

Компания RakTek готова кастомизировать PDU по требованиям конкретного заказчика. В России имеется склад запчастей, а модульная конструкция PDU позволяет оперативно ремонтировать их на месте. Но пока таких прецедентов не было. Контроль качества на всех этапах эффективен!

RakTek
raktek.ru

Комплексные решения NTSS для ЦОДов: от шкафов до ИБП и кондиционеров

ГК EMILINK под маркой NTSS предлагает инновационные и надежные решения, позволяющие повысить эффективность и бесперебойность работы дата-центров, снизить риски сбоев и потери данных, что, в свою очередь, поможет эффективному функционированию бизнеса.

Центры обработки данных – основа современной информационной инфраструктуры: именно в них размещаются серверы, СХД и другое оборудование, необходимое для хранения, обработки и передачи данных. Главный принцип работы дата-центров состоит в обеспечении непрерывности работы ИТ-систем, что достигается за счет использования специальных технических решений.

Один из важнейших компонентов ЦОДов – 19-дюймовые шкафы, в которые устанавливаются серверы и телекоммуникационное оборудование, блоки распределения питания (PDU) и источники бесперебойного питания (ИБП), обеспечивающие подачу электроэнергии в случае отключения основного источника питания. Не менее важны устройства охлаждения, которые поддерживают оптимальную температуру в ЦОДе и предотвращают перегрев оборудования, что снижает вероятность отказов и увеличивает надежность системы.

На рынке не так много производителей, способных предложить все основные системы инженерной инфраструктуры ЦОДов. Один из них – группа компаний EMILINK, в портфеле которой – широкий ассортимент оборудования под маркой NTSS.

Шкафы

EMILINK предлагает широкий выбор серверных шкафов, они выпускаются различных размеров и модификаций. Серверные шкафы NTSS могут иметь высоту до 54U и оснащены дверями с высокой степенью перфорации (примерно 85%), что позволяет поддерживать оптимальную температуру для работы серверов. Кроме того, шкафы могут быть окрашены в корпоративные цвета – это помогает подчеркнуть индивидуальность бизнеса заказчика.

Система изоляции коридоров

Разработанная EMILINK система изоляции холодных/горячих коридоров NTSS предназначена для максимально эффективного использования энергии и минимизации затрат на охлаждение. Система обеспечивает правильное направление воздушных потоков в разных зонах ЦОДа, не допуская их перемешивания.

Источники бесперебойного питания

EMILINK предлагает широкий модельный ряд ИБП под маркой NTSS. Это однофазные и трехфазные ИБП 19-дюймового формфактора и напольного типа. Также выпускаются модульные ИБП. Независимо от модели и серии все ИБП NTSS отличаются высокой надежностью. Наиболее мощные ИБП NTSS могут обеспечивать бесперебойное питание до 600 кВт с возможностью масштабирования.

ИБП NTSS работают в режиме двойного преобразования электроэнергии, что гарантирует «чистое» напряжение на выходе и отсутствие задержки при переключении на батареи. Аппараты обладают высокой энергоэффективностью: КПД до 96%, а в ECOрежиме – до 98%. Функция Smart Sleep повышает КПД в режиме двойного преобразования при частичных нагрузках.

ИБП NTSS обладают рядом других преимуществ. Например, «горячая» замена силовых модулей позволяет обслуживать ИБП без отключения нагрузки, а интеллектуальная система заряда батарей с трехступенчатым методом заряда и функцией температурной компенсации – продлить срок их службы. Возможность тестирования ИБП на полной мощности без подключения нагрузки, а также различные интерфейсы сетевого мониторинга и совместной работы делают ИБП NTSS привлекательным выбором.

Блоки распределения питания

Блоки распределения питания (PDU) – это незаменимые компоненты для эффективной работы ИТ-инфраструктуры, которые обеспечивают подключение серверов и сетевого оборудования к источнику электроэнергии. PDU NTSS подразделяются на пять типов: базовые (basic), metered, metered plus, switched и managed.

Базовые PDU – это качественное распределение питания без дополнительных функций. Они имеют компактные размеры по ширине и глубине. В отличие от базовых, интеллектуальные PDU NTSS оснащены контроллером удаленного доступа и гидромагнитными автоматическими выключателями, которые обеспечивают безопасную работу оборудования и эффективное управление энергопотреблением. К интеллектуальным PDU NTSS можно подключить до 10 датчиков мониторинга окружающей среды, в том числе датчик температуры/влажности, вандализма, утечки, открытия двери, задымления и инфракрасный датчик доступа. При подключении более чем одного датчика необходим модуль расширения портов.

Интеллектуальные PDU NTSS обеспечивают возможность дистанционного (по протоколу SNMP) мониторинга

▲Система изоляции холодных/горячих коридоров NTSS

◀ Блоки распределения питания (PDU) NTSS

Прецизионные внутрирядные кондиционеры NTSS ▶

параметров энергопотребления на входе PDU по фазам или даже по каждой выходной розетке. В управляемых версиях PDU (switched и managed) имеется возможность удаленного включения/выключения каждой выходной розетки через сетевой интерфейс, а также в зависимости от показаний датчиков.

Кондиционеры

Прецизионные внутрирядные кондиционеры NTSS выпускаются в двух стандартных размерах по ширине – 300 и 600 мм, имеют высоту 2000 мм и устанавливаются в холодном или горячем коридоре в рядах серверных шкафов. Холодный воздух подается непосредственно на переднюю панель охлаждаемого оборудования, проходит сквозь него, нагреваясь, и снова забирается кондиционером. Такой дизайн позволяет снизить требуемую мощность вентиляторов и повысить энергоэффективность.

Системы внутрирядного холодоснабжения NTSS доступны в двух вариантах – фреоновом DXA с выносным конденсаторным блоком и CW с водяным охлаждением от чиллера. Модели DXA полностью исключают риск протечки воды, в то время как модели CW работают эффективнее, используя водно-гликолевую смесь в качестве хладагента. Выбор системы холодоснабжения зависит от потребностей конкретного проекта.

Кондиционеры NTSS удобны в обслуживании и установке. Устройства снабжены роликами для повышения маневренности и регулируемыми по высоте ножками, обеспечивающими устойчивость конструкции. Монтаж трубопроводов может выполняться как в верхней, так и в нижней части устройства в зависимости от требований к установке.

Кондиционеры NTSS оснащены цифровым контроллером, позволяющим легко настраивать и контролировать параметры работы: температуру, влажность, скорость вращения вентилятора и т.д. Кроме того, контроллер может быть подключен к системе управления ИТ-инфраструктурой ЦОДа (DCIM) для дистанционного мониторинга и управления.

В кондиционерах используются только высококачественные компоненты и материалы, обеспечивающие длительный срок службы и безопасную эксплуатацию. Встроенные системы безопасности – защита от перегрева, перегрузки и короткого замыкания – гарантируют надежную работу устройства. Важно отметить, что кондиционеры NTSS совместимы с множеством дополнительных устройств, в частности с увлажнителями и осушителями воздуха. Это позволяет создать в помещении комплексную систему климатического контроля.

Кондиционеры NTSS обладают высокой энергоэффективностью благодаря использованию передовых технологий, таких как инверторные компрессоры, вентиляторы с частотным преобразователем и т.д. Это дает возможность сэкономить на счетах за электроэнергию.

ГК EMILINK предоставляет широкий спектр сервисных услуг, включая техническое обслуживание, ремонт и замену компонентов, а также обучение пользователей и инженеров.

■■■

Современные требования к ЦОДам ставят перед компаниями, которые занимаются разработкой и производством оборудования, сложные задачи. EMILINK успешно справляется с этими задачами, предлагая своим клиентам инновационные и надежные решения для дата-центров. Использование такого оборудования позволяет повысить эффективность и надежность работы, снизить риски сбоев и потери данных, что, в свою очередь, способствует эффективному функционированию бизнеса.

Взрывной рост, гособлако и «таблица Менделеева» виртуализации

Николай Носов

Облачный рынок адаптировался к радикальным изменениям прошлого года и показал рекордный рост. Облачные провайдеры помогают бизнесу отвечать на новые вызовы. Решения ушедших вендоров вполне могут заменить отечественные средства виртуализации.

Подтверждения этих высказываний были во множестве представлены в выступлениях на 12-й ежегодной выставке и конференции Cloud & Connectivity, организованной «ИКС-Медиа». Самая авторитетная облачная конференция страны, ранее называвшаяся Cloud & Digital Transformation, собрала более 300 делегатов, и еще около 500 участвовали в работе удаленно.

Рост на фоне кризиса

Введенные против России санкции сильно ударили по экономике страны, но в целом положительно повлияли на развитие облачного рынка.

По предварительным данным iKS-Consulting, рынок инфраструктурных облачных сервисов в 2022 г. вырос на рекордные 48,7% (IaaS – 44%, PaaS – 98%), опередив самые оптимистичные прогнозы аналитиков (рис. 1). Сказались и повышение доверия к облачным сервисам, и геополитическая неопределенность. При проблемах с поставками зарубежного оборудования и сложностями планирования компании отдавали предпочтение сервисным моделям, увеличивая OPEX за счет CAPEX. Другие факторы роста облаков – миграция значительной доли пользователей зарубежных сервисов на российские площадки и комплекс государственных мер по защите национального рынка. Уходящие зарубежные игроки передавали активы своим российским подразделениям, которым надо было срочно разворачивать ИТ-инфраструктуру, что в текущих условиях невозможно без использования ресурсов российских облачных провайдеров.

Крупные провайдеры серьезно занялись рынком облачных услуг. Объем рынка увеличился на 28,1 млрд руб., и более половины этой суммы обеспечили три компании: Cloud (ранее SberCloud) – 26%, Yandex.Cloud – 18,2%, «Ростелеком-ЦОД» – 14,3% (рис. 2). Почти трехкратный рост продемонстрировала Yandex. Cloud, на 130% выросла выручка у Oxygen, удвоилась у Beeline и VK.

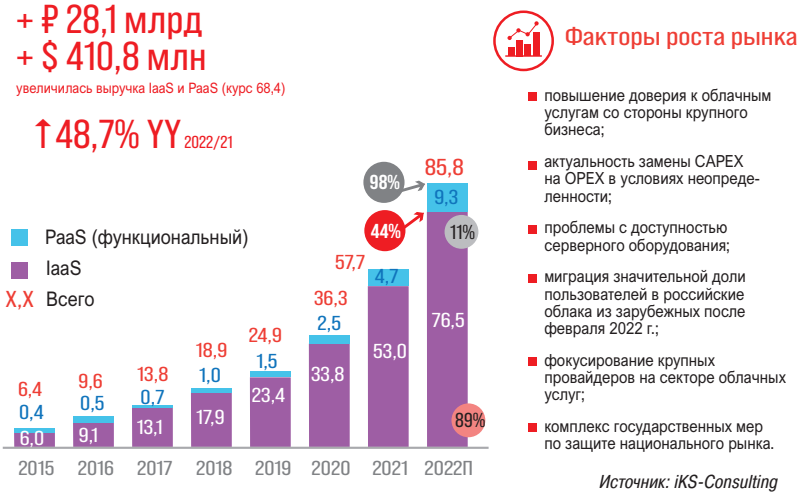
Облако для государства

Стабильный рост потребностей государственных органов в вычислительных ресурсах при низкой фактической их утилизации, дефицит квалифицированных ИТ-кадров, невозможность одновременного использования ресурсов ведомствами стали предпосылками эксперимента Минцифры по созданию гособлака – экосистемы предоставления облачных услуг по сервисной модели государственным заказчикам. Ситуацию усугубили необходимость защиты от санкций и массовое устаревание оборудования.

Эксперимент начался в 2019 г. «Принципы, заложенные в тот момент, были достаточно революционными, раньше никто такого не делал», – дал оценку проекту технический директор «Ростелеком-ЦОД» Алексей Забродин. Первый принцип гособлака – фиксация SLA на конечные сервисы инфраструктуры, а не на время бесперебойной работы оборудования. Второй – переиспользование ресурсов. До этого купленное для одного ведомства оборудование могло храниться в коробке, в то время как было совершенно необходимо не имеющему достаточного административного ресурса другому.

На первом этапе гособлако было набором частных облаков с низким уровнем переиспользования ресурсов. В 2020 г. «Ростелеком-ЦОД» стал делать коммунальное (community) мультитенантное облако с единым контуром управления для быстрого перераспределения ресурсов и подключения новых мощностей – процесса, который раньше с учетом конкурсных процедур растягивался на годы. Сегодня в гособлаке разместились свыше 100 информационных систем более 30 ведомств.

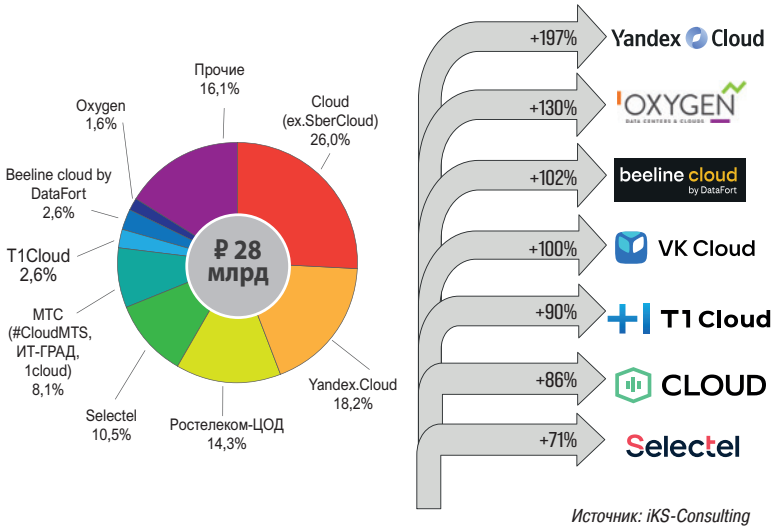
Для обеспечения информационной безопасности гособлако разделено на сегменты: потребите-



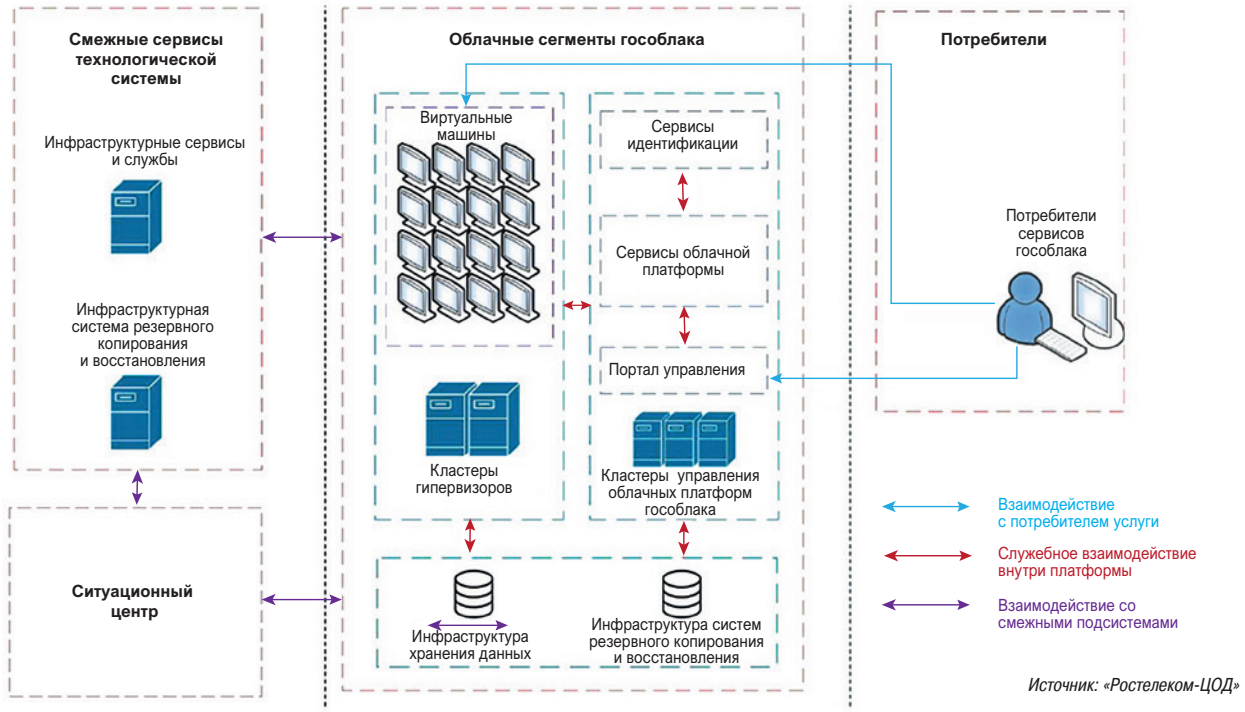
Источник: iKS-Consulting

▲ Рис. 1. Динамика рынка инфраструктурных облачных сервисов

Рис. 2. Игроки рынка IaaS/PaaS ▼



Источник: iKS-Consulting



▲ Рис. 3. Высокоуровневая архитектура облачной платформы

лей, облачные сегменты, смежных сервисов и ситуационный центр со специально подобранными аттестованными средствами защиты (рис. 3). При создании гособлака используется подход строгого импортозамещения – по словам А. Забродина, объем виртуальных машин в гособлаке, работающих на облачной платформе VMware, снизился до 30% и продолжает уменьшаться.

Все под контролем

«Я верю, что промышленность – основа экономического здоровья России – продолжит инвестировать в ИТ и будет все шире потреблять облачные ресурсы», – заявил Михаил Соловьев, директор по облачным технологиям МТС. Один из таких ресурсов, который послужит для мониторинга оборудования, зданий и другой инфраструктуры, – интернет вещей. Для этого МТС в облако #CloudMTS включила свою платформу IoT HUB, открыв ее сторонним разработчикам. Платформу можно использовать вместе с другими облачными сервисами и создавать комплексные решения.

Как рассказал Антон Салов, руководитель стратегии IoT и промышленной автоматизации МТС, разработанная компанией платформа позволяет осуществлять мониторинг и удаленное управление, сбор, обработку и хранение данных, подключение IoT-устройств по различным каналам связи (2G – 4G, NB-IoT, фиксированная связь и др.), информирование по каналам SMS/e-mail/Telegram, аналитику и визуализацию. Платформа – полностью отечественная разработка – реализована на микросервисной архитектуре с использованием открытых технологий. На основе IoT HUB построены, например, система мониторинга инфраструктуры ЦОДа, которая осуществляет контроль электрооборудования, температурного режима и датчиков пожарной сигнализации, и решение «Цифровой водоканал», внедренное в нескольких городах, в том числе в Московской области.

Значительный рост числа проектов создания частных (изолированных) облаков отметил Михаил Нестеров, технический директор компании Oxygen. Строятся частные облака как на зарубежных, так и на отечественных решениях, но при этом доля российских продуктов, по оценкам Oxygen, за год выросла на 300%. Все большей популярностью пользуются и услуги «оборудование как сервис» – HaaS. «Из-за санкционных рисков клиенты могут очень долго ждать оборудования или вообще его не дождаться. Возникают проблемы с запчастями и с техническим обслуживанием. Поэтому HaaS становится все более востребованным», – пояснил М. Нестеров.

Рост сложности ИТ-инфраструктуры, переход на гибридные архитектуры подразумевает повышение требований к связности. «Нужно обеспечить связность между всеми элементами инфраструктуры, зачастую расположенными в разных средах, работающих на разных системах виртуализации», – подчеркнул эксперт Oxygen.

Ниша для маленьких

Небольшим облачным провайдерам все труднее конкурировать с крупными игроками, консолидирующими мощности и ресурсы. Трудно, но не невозможно, главное – выбрать правиль-

ную тактику. Не все же компании пользуются Сбербанком – небольшие банки тоже выживают на рынке, причем в основном из-за отличного знания своего клиента и персонализированных предложений для него. По этому же пути идут небольшие облачные провайдеры, реальная точка роста для которых, по мнению генерального директора 3data Ильи Халы, – предоставление продуктов класса «частное облако» на грани с интеграторской моделью работы с клиентами. То есть они могут выполнять работу облачного провайдера, знающего потребности клиента интегратора и даже предлагать managed services – аутсорсинг части функций ИТ-отдела заказчика. Так делает компания 3data, которая вывела на рынок агрегатор облачных сервисов RCloud by 3data.

Компания 3data обладает необходимым ресурсом для выполнения этой задачи – сетью небольших собственных дата-центров шаговой доступности. Агрегатор облачных сервисов RCloud by 3data поможет создать кастомизированное решение для клиента, экспертиза компании обеспечит правильное построение и поддержку необходимой инфраструктуры. Управление всеми сервисами, которых в настоящее время уже больше сотни, облегчает единое окно.

Среди новых, редко встречающихся на российском рынке сервисов – архивное и резервное копирование на некогда очень популярные, а ныне незаслуженно забытые ленты. Облачный сервис ArcTape обеспечивает хранение в ленточных библиотеках дата-центров 3data. По словам И. Халы, к преимуществам ленточного хранения относятся надежность, долговечность (до 30 лет хранения) и экономическая эффективность. Кроме того, такое хранение можно рассматривать как последний рубеж защиты при хакерских атаках.

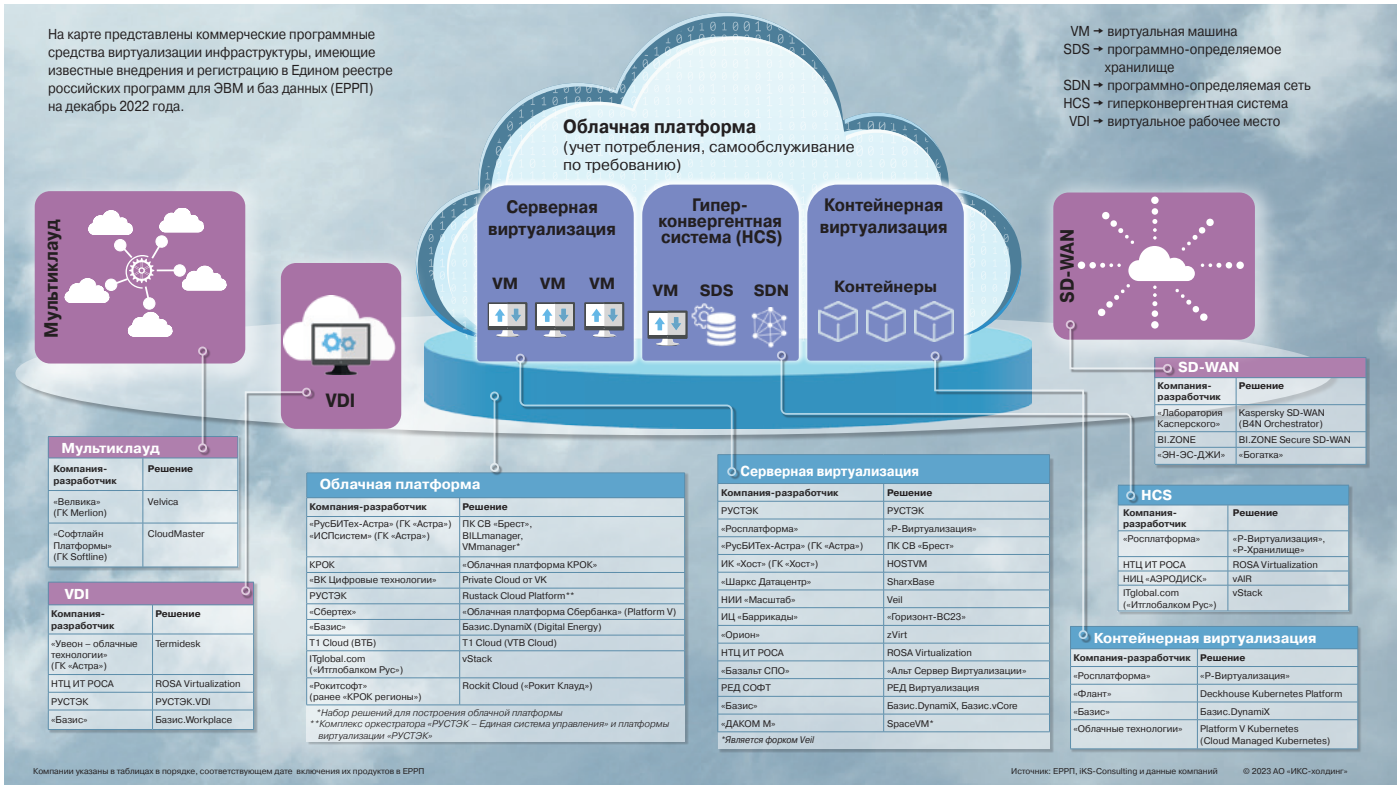
Заграница нам поможет

Тактика с опорой на кастомизированный подход к клиенту и свой дата-центр помогает российским провайдерам бороться с мировыми гиперскейлерами, такими как AWS, Google и Microsoft, на зарубежных рынках. Ряд иностранных компаний покинули Россию, но не запрещают оказывать облачные услуги на базе их решений из-за рубежа. Поэтому компания Softline, например, развернула облако в открытом в 2022 г. ЦОДе в Израиле.

«Мы проработали список вендоров, с которыми можно сотрудничать, и вполне легально построили облако на их решениях», – пояснил руководитель облачных решений Softline Дмитрий Исаев. Таким образом, используя облако в израильском ЦОДе, отечественные компании могут на законных основаниях работать с продуктами многих ушедших с российского рынка вендоров.

Экосистема сервисов Softline включает в себя поддержку миграции в облако, интеграцию с локальной инфраструктурой, консультации, обучение, анализ эффективности использования облаков и предложения по повышению эффективности бизнеса. И конечно, меры защиты от киберугроз, в том числе мониторинг не только

Рис. 4. Карта «Российское ПО виртуализации 2023» ▼



облачных, но и локальных ресурсов. Клиент может арендовать и установить на своей площадке типовое серверное оборудование, использовать частное облако по модели IaaS или новое решение – экосистему SL Universe, вертикальную интегрированную систему, объединяющую инфраструктуру в ЦОДе заказчика, облако Softline Cloud, инфраструктурное и прикладное ПО и конечные устройства пользователей.

Карта российских решений виртуализации

Делегаты конференции получили карту «Российское ПО виртуализации 2023» – новый уникальный продукт, разработанный iKS-Consulting (рис. 4). На карте не только перечислены, но и систематизированы российские решения для виртуализации и облачных платформ. Создана своего рода «таблица Менделеева» российских компаний, позволяющих заменить системы иностранных вендоров, в частности, той же VMware. Аналитики выбирали из не слишком хорошо структурированного и имеющего два классификатора Единого реестра российского программного обеспечения подходящие продукты, связывались с компаниями, выявляя, что и под каким брендом сейчас предлагается рынку, по возможности проверяли заявленный функционал и искали реальные внедрения.

В опубликованных в журнале «ИКС» и на портале IKSMEDIA статьях анализировались стратегии действий компаний-пользователей, технические характеристики решений, компании-разработчики сравнивались по якорным клиентам, внедрениям, популярности и квалификации команд.

Рынок российских программных средств виртуализации бурно развивается, появляются новые продукты и игроки, происходят слияния и поглощения. В этом калейдоскопе нелегко разобраться заказчикам, подбирающим замену зарубежным продуктам. Помощь в выборе пути окажет новая карта, выпуски которой планируется обновлять ежегодно.

Станет ли «Базис» основой?

Наиболее перспективной для использования в гособлаке российской облачной платформой выглядит «Базис.DynamiX», созданная на базе платформы, которая разработана компанией Digital Energy, вместе с Tionix вошедшей в новую компанию «Базис» – дочку «Ростелекома», YADRO и Rubytech. Решения «Базиса» уже используют Минцифры, Федеральная кадастровая палата, «Росатом», Росреестр, Роспотребнадзор и ряд крупнейших российских компаний.

Судя по данным, которые представил директор по развитию бизнеса «Базиса» Андрей Толокнов, разработанный компанией на основе KVM гипервизор «Базис.vCore» по техническим характеристикам ничуть не уступает используемому VMware гипервизору iESX, а по некоторым параметрам превосходит его.

Важное преимущество – наличие интегрируемых между собой продуктов: помимо «Базис.DynamiX» и «Базис.vCore» в экосистему входят виртуальные рабочие места – «Базис.WorkPlace» и система обеспечения информационной безопасности «Базис.Virtual Security».

Не как у всех

Заинтриговало название доклада технического директора Beeline cloud by Datafort Ивана Фрунзе: «Найти альтернативу: как российская платформа BeeCloud Stack меняет курс на отечественную виртуализацию». Прежде всего – появление на рынке новой облачной платформы, не представленной на карте российского ПО виртуализации, да еще и у такого крупного игрока, как «Вымпелком» (бренд билайн).

На деле все прозаичнее – новой платформой оказалась уже имеющая регистрацию в ЕРРП и отмеченная на карте платформа vStack. А вот технический стек действительно альтернативный. Это единственная российская платформа, не построенная на стандартном или переработанном гипервизоре KVM. По утверждению И. Фрунзе, большая часть архитектуры создана внутри решения, а не заимствована из готовых open source-проектов. Платформа базируется на гиперконвергентной архитектуре, включающей решения SDS и SDN компании ITglobal.com (см. рис. 4).

За счет использования гипервизора, разработанного на базе open source-гипервизора bhyve, повышается производительность облачной платформы. Все модули настраиваются и администрируются из единой панели. Платформа рассчитана на использование commodity hardware, что выгодно отличает ее от имеющих ограничения по аппаратным средствам зарубежных аналогов.

■■■

Текущий прогноз Минэкономразвития предполагает, что в 2023 г. российский ВВП снизится на 0,8%. Но это явно не про облака. К санкциям компании адаптировались, спрос на облачные услуги растет. По оценкам вице-президента по развитию инфраструктуры МТС Юрия Самойлова, высокие темпы роста облачного рынка сохранятся, и до 2025 г. рынок будет прирастать на величину до 50% в год. Основными драйверами останутся непрекращающиеся процессы цифровизации, импортозамещение и сложности в поставках оборудования. Поэтому облака будут востребованы. ИКС

Российские облака: уроки 2022 года

Геополитические и экономические изменения привели к нарушениям цепочек поставки и, как следствие, к удорожанию облачных услуг. Импортозамещение стало реальностью, а не просто маркетинговым ходом.

Антон Салов, руководитель стратегии IoT, МТС; эксперт, RCCPA

Мировые и российские тенденции

В 2021 г. глобальные технологические слияния и поглощения по объему превысили $1,24 трлн, а общая капитализация рынка публичных облачных сервисов, по данным Bessemer Venture Partners, в ноябре достигла пика в $2,7 трлн. Этому способствовали сохранение «удаленки» и благоприятное состояние фондового рынка – весь год индексы крупнейших технологических компаний шли вверх.

Однако к концу 2021 г. ситуация изменилась: биржевые индексы S&P500 и Dow Jones пошли вниз. В том же направлении двинулись и индексы высокотехнологичных компаний – NASDAQ и EMCLOUD (BVP Nasdaq Emerging Cloud). Последний был создан для отслеживания эффективности развивающихся публичных компаний, которые в основном занимаются предоставлением облачного ПО и SaaS-сервисов. По нему можно видеть, сколь высоки были ожидания от облаков в условиях пандемии и как менялась ситуация в дальнейшем. Все эти тренды сигнализировали о переходе от VUCA-мира (Volatility, Uncertainly, Complexity, Ambiguity – нестабильность, неопределенность, сложность и неоднозначность) к эпохе BANI (Brittle, Anxious, Nonlinear, Incomprehensible – хрупкость, тревожность, нелинейность, непостижимость).

С такими вводными мы подошли к началу 2022 г. Очень скоро наступил технологический кризис, который перераспределил силы не только на отечественном, но и на глобальном облачном рынке. По данным консалтинговой компании Onside, российский сегмент cloud-рынка прибавил 27,5% и в 2022 г. достиг примерно 150 млрд руб. Во многом на эту оценку повлияло повышение цен на облачные сервисы весной, когда большинство провайдеров подняли цены, некоторые на 50%. Поэтому в действительности рост российского cloud-рынка не столь существенен, а сама динамика неравномерна. В первой половине года мощности покупались «про запас», что обеспечило скачок спроса. Но уже летом стал заметен спад активности, а у некоторых провайдеров заказанные мощности и вовсе начали высвобождаться из-за пересмотра инвестпрограмм и сокращения ИТ-бюджетов. Кстати, спад интереса со стороны бизнеса заметили в основном те небольшие независимые игроки, которые занимаются исключительно предоставлением инфраструктуры.

На рынок в 2022 г. влиял и кризис доверия, наблюдающийся в экономике разных стран последние годы и проявляющийся в настороженности бизнеса к подписной и облачной моделям. На примере российских компаний зарубежные игроки вдруг осознали уязвимость бизнеса, зависящего от сторонних поставщиков сервисов. Причем на кону оказываются не только отключение от инфраструктуры, но и невозможность получить данные назад. В результате копии всех облачных данных стали хранить на территории своей страны, а лучше – в собственном облаке. В свою очередь, это повысило спрос на частные облака, которые развертываются как в ЦОДах облачных провайдеров, так и на площадке бизнес-заказчика. По данным iKS-Consulting, процессы мигра-

ции на отечественную инфраструктуру вызвали рост рынка IaaS на 41%. Этот процесс «деклаудизации» изменил стратегию поведения глобальных облачных игроков на рынке и привел к корректировке моделей угроз.

Отметим ключевые факторы, оказавшие существенное влияние на состояние облачного рынка в России:

- кризис цепочек поставок оборудования и, как следствие, рост себестоимости облачных услуг;
- приостановка деятельности или полный уход иностранных провайдеров и вендоров ПО, отказ в техподдержке;
- рост спроса на отечественное ПО (включая системное и ПО виртуализации) и на программно-аппаратные комплексы, миграция на отечественную инфраструктуру.

Оборудование

Во II квартале 2022 г. часть облачных провайдеров столкнулась с дефицитом оборудования. Справляться с ним приходилось разными способами. Ряду компаний помогла государственная поддержка отрасли в виде субсидий. Другие сами собирали серверы из комплектующих, чтобы удовлетворить галопирующий спрос на облачную инфраструктуру. Третьи (преимущественно А-бренды) и вовсе не испытывали проблем с оборудованием, так как у них были ресурсы на покупку серверов для своих и провайдерских нужд. Остальные смогли наладить поставки лишь к концу III квартала.

До конца II квартала бизнес выкупал или бронировал вычислительные мощности у провайдеров разных уровней. Катализатором стала необходимость миграции с облаков зарубежных провайдеров и переноса данных от глобальных гиперскейлеров, а также резервирование мощностей под будущие проекты или для расширения инфраструктуры.

К середине лета, когда были налажены каналы поставок, наступила «новая реальность», в которой можно работать, – с поправкой на особые правила. К примеру, стало необходимым разносить закупки по времени и каналам: 100 серверов одновременно закупить можно, а 1000 – уже проблематично.

Из-за потенциальных рисков отключения в будущем компании вряд ли решатся использовать облака альтернативных зарубежных провайдеров; как правило, вместо этого обращаются к отечественным cloud-лидерам либо развертывают поверх IaaS собственные серверы для коммуникаций и совместной работы.

Также перед провайдерами встал выбор: закупать noname-оборудование (и при этом не рассчитывать на гарантию или послепродажный сервис) или делать закупки, как раньше, когда гарантию и сервис обеспечивал дистрибьютор или реселлер. Появилась целая прослойка игроков, которые держат склады с запасными частями вместо вендоров, чтобы поддержать принципы RMA (Return Merchandise Authorization – возврат некачественных или неисправных изделий производителю для ремонта, обмена или зачета в баланс) в условиях параллельного импорта.

ЦОДы за рубежом остались, правда, вектор изменился: теперь он направлен не на запад, а чаще всего на юг – в Казахстан, Израиль и Арабские Эмираты. Обеспечить оборудованием или ПО эти ЦОДы проблем не составит, а значит, можно предоставлять услуги, в том числе в России.

В итоге к концу года рынок смог выйти из кризиса благодаря адаптации к возможной работе с любым возможным производителем оборудования с любой моделью предоставления вычислительных ресурсов.

Зарубежные провайдеры

По оценкам экспертов RCCPA, до 2022 г. на долю зарубежных провайдеров приходилось до 30% прироста объема облачного рынка РФ. Наибольший вклад вносили Microsoft и AWS, а также VMware в части ПО для корпоративного стандарта частных и публичных облаков. Сегодня они также продолжают оказывать влияние на рынок: хотя мощности расширить нельзя, можно продолжать работать в рамках действующих контрактов – правда, без перспективы продления и технической поддержки вендора.

Из-за потенциальных рисков отключения в будущем компании вряд ли решатся использовать облака альтернативных зарубежных провайдеров. Как правило, вместо этого обращаются к отечественным cloud-лидерам либо развертывают поверх IaaS собственные серверы для коммуникаций и совместной работы.

В этом году на рынке начали появляться анонсы отечественных решений от сторонних провайдеров, например на базе CommunigatePro, но они не могут в полной мере заменить ни Google Workspace, ни Microsoft 365, а достойного импортозамещения, открытого для клиентов любого уровня, пока ни «МойОфис», ни «Р7» предложить не смогли.

Что касается малого бизнеса, на рынке не хватает оптимизации софта со стороны вендора

В 2022 г. были выучены два урока, которые будут определять ИТ-стратегии.

Первый: эпоха vendor lock закончилась. Привязываться к одному поставщику – стратегия непродуманная и неоправданная.

Второй: цифровой суверенитет перестал быть только маркетинговым ходом.

для работы по облачной модели – должно существовать отдельное направление по работе с провайдерами и их клиентами.

За счет ухода иностранных игроков и недоступности привычных форм оплаты зарубежных сервисов SaaS-сегмент в России, по оценке экспертов RCCPA, впервые за последние 15 лет покажет рост лишь на несколько процентов: потребуется время, чтобы заменить E2E-решения, особенно отраслевые, а также перенести данные из системы Salesforce в ELMA. На этом фоне активизировалась борьба cloud-провайдеров за отечественных поставщиков SaaS-решений. Разработчиков пытаются привлечь на свою виртуальную инфраструктуру ценами, грантами, скидками и поддержкой.

В сегменте SaaS есть и ряд сложностей. Хотя российские гиперскейлеры готовы принять на свои платформы клиентов зарубежных конкурентов, ушедших с рынка, их функциональность не всегда на 100% соответствует иностранным платформам. У большинства фактически отсутствуют IoT- и edge-возможности, которые есть у западных Azure и AWS.

В целом рынок SaaS остался свободным для российских игроков после ухода крупнейших зарубежных конкурентов Oracle, SAP, Cisco, Autodesk, Gurtam, Siemens и Trimble. Поэтому при наличии готового решения в любой из освободившихся ниш можно вырасти в разы: спрос высокий, а предложения практически нет.

В инфраструктурных сервисах дела обстоят гораздо лучше. Отечественные провайдеры готовы принять любого клиента, если он использует только облачную инфраструктуру. У клиентов есть возможность мигрировать даже в привычное окружение VMware – многие провайдеры продолжают оказывать услуги на базе данного стека решений, даже при отсутствии поддержки от вендора. А ряд гиперскейлеров, в свою очередь, готовы оказать услуги по миграции на KVM – иногда бесплатно.

Отечественное ПО и стек для провайдеров

Из-за сложившейся на рынке ситуации отечественные провайдеры стали выбирать различные стратегии импортозамещения. Небольшие провайдеры, не имеющие возможности собственной разработки, предпочли поддерживать стек VMware/Microsoft, который они применяли ранее для оказания услуг, из-за отсутствия средств и ресурсов для миграции на альтернативные варианты (писать свою платформу поверх KVM, «допиливать OpenStack» либо положиться на существующие отечественные или зарубежные платформы из Китая). Путь, по которому идет большинство, – попробовать найти отечественный стек виртуализации и управления облаком. Одной виртуализации мало. Переписывать гипервизор никто не заставляет, но нужно заменить функциональность систем управления облаком. В настоящее время в реестре отечественного ПО находится более дюжины систем виртуализации. Этот аспект эксперты RCCPA обсуждали на дискуссионном клубе «Импортозамещение систем виртуализации для облачных провайдеров» и сошлись во мнении, что альтернативы на рынке присутствуют, и они хороши.

В целом ситуация на провайдерском рынке не видится критичной. Вопрос ЦОДов (дефицита площадей, оборудования и вычислительных мощностей) будет решен или включен в себестоимость. С оборудованием работать научились, с ПО тоже можно побороться.

В 2022 г. были выучены два урока, которые будут определять ИТ-стратегии. Первый: эпоха vendor lock закончилась. Привязываться к одному поставщику – стратегия непродуманная и неоправданная. Второй: цифровой суверенитет перестал быть только маркетинговым ходом. Для бизнеса, работающего на территории России, теперь действительно важно, чтобы облако находилось здесь же, было построено на отечественных технологиях и обслуживалось российской командой. ИКС

Нет облачных услуг без связности

Николай Носов

Строительство ЦОДов в регионах и за рубежом, новые технологии, развитие конкурирующих сетей и увеличение числа точек обмена трафиком повышают связность облачной экосистемы и улучшают доступ к облачным услугам.

Переименование проводимой «ИКС-Медиа» конференции Cloud & Digital Transformation в Cloud & Connectivity отражает возрастающую роль связности в надежном и быстром доступе к облачным ресурсам.

ИТ-инфраструктура предприятия может включать в себя:

- собственные мощности, распределенные по офисам и филиалам;
- оборудование на площадках заказчиков, например, устройства IoT;
- оборудование, предоставляемое провайдером по сервисной модели (HaaS);
- вычислительные мощности, размещенные во внешних ЦОДах по модели colocation;
- ИТ-ресурсы в частных облаках на стороне облачного провайдера;
- сервисы IaaS, PaaS и SaaS в коммунальных (community) и публичных облаках.

Все эти элементы должны быть связаны между собой, иметь возможность обмениваться данными по различным каналам. При этом в разных средах используются разные протоколы, операционные системы, системы виртуализации. Работоспособность такой инфраструктуры во многом определяется связностью узлов – устойчивостью к повреждениям отдельных участков сети, достигаемой за счет перенаправления трафика в обход вышедших из строя участков (кабелей, сетевого оборудования).

Сегодня ситуацию усложняют уход зарубежных вендоров, во многом задающих отраслевые стандарты, проблемы поставки оборудования, массовый переход на импортозамещающие российские продукты, интеграция которых – задача нетривиальная. Отдельная проблема – обеспечение безопасности этой ИТ-инфраструктуры в условиях резко возросшего числа кибератак.

Связанные одной сетью

Не каждая компания может самостоятельно справиться с развертыванием и поддержкой работы всех участков сети. Неудивительно, что многие ищут возможность передать часть функций на аутсорсинг, в том числе облачному провайдеру. «Сеть можно рассматривать как один из сервисов облачной экосистемы», – считает технический директор компании Oxygen Михаил Нестеров. Эксперт выделил два подхода к обеспечению связности в гибридных инфраструктурах:

- маркетплейс, когда один поставщик обеспечивает весь комплекс сетевых услуг, включая связность;
- облачный интегратор, предоставляющий сервисы разных облачных провайдеров и выступающий в роли интегратора для ИТ-департамента заказчика.

Пример маркетплейса – сервисы AWS. Преимущество – предоставление хорошо интегрированных между собой услуг из одного окна. Минусы подхода – не все из предлагаемых сервисов заказчику нужны, а оплачивать пакет придется в полном объеме. Кроме того, может оказаться, что не все требуемые решения в па-

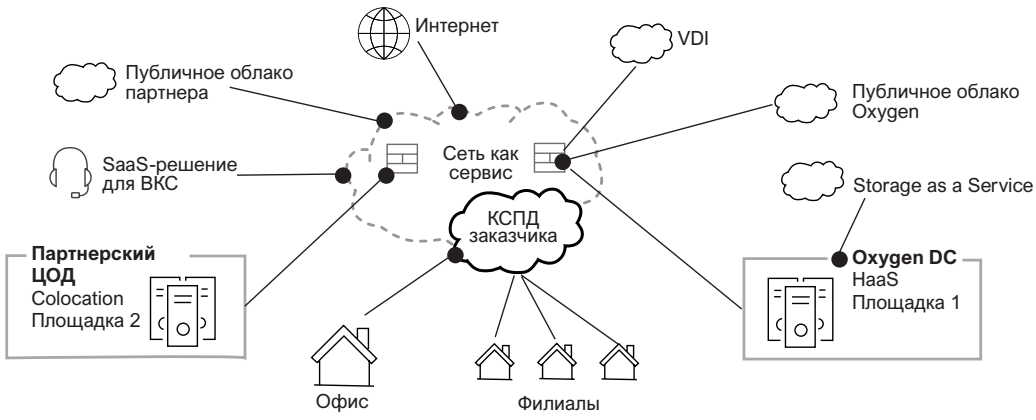


Рис. 1. ▶ Пример построения сервиса в концепции облачного интегратора

Источник: Oxygen

кете есть, а те, что есть, не всегда лучшие в своем классе. А недостаточная гибкость решений усложняет адаптацию внутренней инфраструктуры к специфике облачных сервисов.

Компания Oxygen использует второй подход и выступает в роли облачного интегратора (рис. 1). Она несет дополнительные затраты на обеспечение связности с поставщиками услуг, но зато предоставляет максимально гибкое архитектурное решение, многообразие услуг, позволяющее каждому заказчику выбрать для себя оптимальный по стоимости и функционалу сервис. Кроме того, с помощью общего домена VPLS (Virtual Private LAN Service) компания обеспечивает сетевую связность между офисами и ЦОДом клиента.

Также Oxygen, по словам ее директора по ИБ Кирилла Орлова, предлагает клиентам защиту от сетевых угроз, шифрование каналов связи, мониторинг и контроль конечных точек.

В качестве облачного интегратора, предоставляющего единое «окно» в облако, выступает и компания MasterCloud. Коммерческий директор MasterCloud Владимир Елфимов сравнил такое «окно» с МФЦ, сильно упростившими жизнь горожанам, – оно становится единой точкой обращения к ИТ- и телеком-сервисам. В предоставлении услуг не участвуют субподрядчики и третьи лица, есть единый центр обработки обращений и техподдержки. Конкурентным преимуществом компании В. Елфимов считает 12 тыс. км собственных оптоволоконных каналов по Москве и Московской области, географически распределенные ЦОДы уровня Tier III и облако с выделенным сегментом, соответствующим требованиям закона № 152-ФЗ.

Ближе к клиенту

«Облако должно быть территориально распределенным», – заявил директор по облачным технологиям МТС Михаил Соловьев. Сегодня облако МТС – это четыре страны и 14 зон доступности в России. Последняя недавно открытая зона доступности – Казань. Сеть передачи данных компании не только объединяет ее дата-центры в России, но и по собственному каналу Самара – Уральск обеспечивает выход в Казахстан. Возможность разместить свои ресурсы сразу в двух странах может быть полезной с точки зрения отказоустойчивости. МТС продолжает открывать новые зоны доступности. Для этого у нее есть хороший задел – 200 собственных дата-центров, которые в настоящее время используются для предоставления услуг связи. Их предполагается задействовать для облачных услуг, чтобы приблизить облако к существующим и потенциальным клиентам.

Кроме того, компания помогает клиентам объединить офисы, складские и другие локальные площадки с основным корпоративным дата-центром и облаками с помощью сети передачи МТС и сервиса SD-WAN, построенного на решении компании BI.ZONE. Как отметил менеджер по продукту направления Network #CloudMTS Валерий Межевов, использование SD-WAN (рис. 2) позволяет осуществлять интеллектуальную маршрутизацию в случае ухудшения качества связи, задействовать большинство типов каналов, упростить подключение каналов и обеспечить их безопасность. По сути, расположенный в облаке центр создает «умную» связанность, реагируя не только на выход из строя канала, соединяющего узлы сети, но и на снижение его пропускной способности.

Надежнее и быстрее

Облако может стать недоступным не только по вине экскаваторщика, не в том месте ковырнувшего землю ковшом, т.е. из-за разрыва на первом уровне модели OSI, но и из-за блокировок на более высоком уровне.

«Гарантированный доступ к облакам могут обеспечить только выделенные каналы связи», – считает генеральный директор MSK-IX Евгений Морозов. Он напомнил случай неработоспособности части сервисов AWS во время блокировок Роскомнадзором мессенджера Telegram. У многих облачных провайдеров услуга гарантированного подключения есть, например, Cloud Connect. А резервировать такой канал можно и через публичный интернет.

«Если компания хочет предоставлять свои данные всему миру, например, в виде приложений или сайтов, то нужна связность другого рода. Один из способов улучшить связность облачному провайдеру – заключить партнерство с CDN-провайдером, чтобы генерируемый в облаке контент раздавался не напрямую через каналы связи, а кэшировался на всех CDN-серверах и максимально быстро попадал к конечным пользователям», – подчеркнул генеральный директор компании CDNvideo Ярослав Городецкий. Такой подход поможет обеспечить непрерывность видеотрансляции с сайта клиента. Объединенная сеть CDNvideo включает в себя более 86 тыс. серверов. Узлы базовой сети компании установлены в 20 городах России и в 13 странах.

Чтобы клиенты были довольны предоставляемыми сервисами, облачным провайдерам следует увеличить количество линков (соединений) к своему облаку и подключаться в том числе к городским точкам обмена трафиком, обеспечивающим связь с городским интернетом и контент-провайдерами. Какими бы полезными ни были облачные сервисы, клиенты не станут ими пользоваться, если качество связи с облаком будет низким.

Как рост затрат на ЦОДы повлияет на уход в облака

Оуэн Роджерс, директор по исследованиям в области облаков, Uptime Institute

Исследование Uptime Institute показывает, что рост затрат на собственные ЦОДы или услуги colocation коммерческих дата-центров вряд ли вызовет массовый переход корпоративных заказчиков в публичные облака.

Не ценой единой

С тех пор как облачные вычисления вошли в мейнстрим, не прекращаются дебаты о том, что дешевле для корпоративных клиентов – облачные сервисы или собственные ЦОДы. Но без конкретики эти дебаты часто лишены смысла. Во-первых, какой вариант размещения того или иного приложения дешевле, а какой – дороже, зависит от его характеристик. Простого и однозначного ответа не существует. Во-вторых, сам вопрос подразумевает, что компания выбирает облачный сервис или собственный ЦОД только по критерию стоимости. Но выбор гораздо сложнее, а критериев гораздо больше.

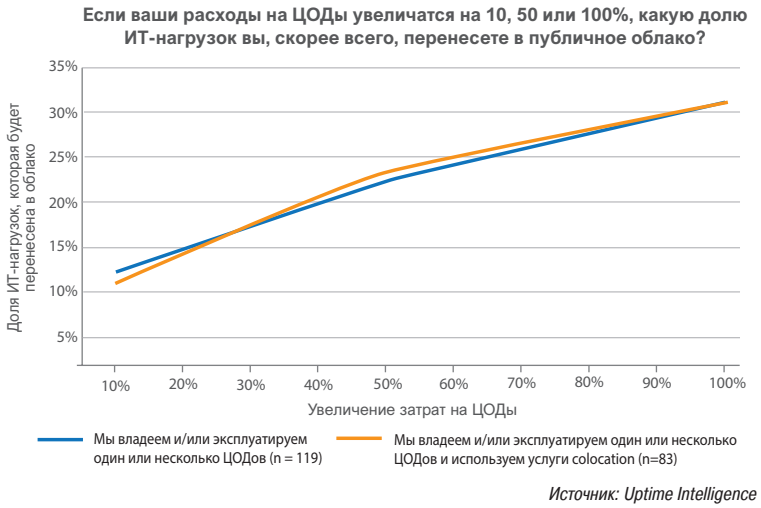
Инфраструктура не товар. Большинство компаний могут предпочесть для своих ИТ-приложений собственные ЦОДы или услуги colocation коммерческих дата-центров, поскольку хотят быть уверены, что выбранный вариант полностью соответствует нормативным требованиям или находится близко к конечным пользователям. А выбрать облачные вычисления их может подтолкнуть необходимость быстрой масштабируемости или удобство доступа к другим сервисам облачной платформы.

Один из способов определить ценность продукта – опросить пользователей, как бы они (гипотетически) отреагировали на изменение его цены. Те, кто извлекают из продукта значительную выгоду, с меньшей вероятностью изменят свое покупательское поведение после его подорожания. Более же чувствительные к цене в таком случае обычно рассматривают конкурирующие предложения для снижения затрат или поддержания их на том же уровне. Стоимость перехода от одного продукта к другому также влияет на выбор пользователя. Например, в облачных вычислениях затраты на изменение архитектуры приложения при миграции на другую платформу могут быть сочтены неоправданно высокими, если получаемая в результате экономия невелика.

В рамках проведенного Uptime Intelligence исследования Data Center Capacity Trends Survey 2022 ИТ-руководителям был задан вопрос: какую долю текущих ИТ-нагрузок они могут перенести в облако, если их затраты на ЦОДы (включая собственные объекты и услуги colocation) вырастут на 10, 50 или 100% при условии, что стоимость облачных сервисов не изменится (рис. 1). Хотя Uptime Institute не изучал подробно рост затрат, большинство операторов, вероятно, испытывают сильное (более 15%) инфляционное давление на свои операционные расходы, причем рост цен на энергоносители и дефицит персонала играют здесь основную роль.

Что же мы получили? Если затраты на собственный ЦОД или на услуги colocation увели-

Рис. 1. Вероятная доля рабочих ИТ-нагрузок, которые будут перенесены в облако при росте затрат на ЦОДы ▼



Источник: Uptime Intelligence

Печатается с разрешения Uptime Institute.

чатся на 10%, компании готовы переместить в облако лишь около 12% рабочих нагрузок (рис. 1). Если затраты увеличатся на 50%, этот показатель вырастет до 24%. Наконец, даже если затраты удвоятся, скорее всего, лишь немногим более 30% рабочих ИТ-нагрузок будут перенесены в публичное облако. Это говорит о том, что заказчики, использующие собственные ЦОДы или услуги colocation, не слишком чувствительны к расходам на них. Хотя рост этих расходов окажет определенное влияние, сам по себе он вряд ли вызовет массовый переход в публичное облако.

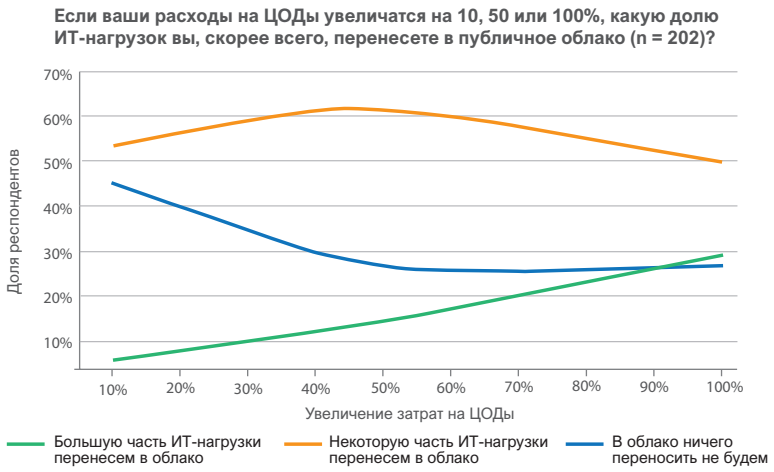
Конечно, одни заказчики более чувствительны к цене, чем другие: 42% респондентов указали, что увеличение затрат на 10% вообще не приведет к переносу каких-либо рабочих нагрузок в публичное облако (рис. 2). Четверть респондентов также вряд ли перейдут в облако, столкнувшись с повышением цен на 50%. Примечательно, что четверть респондентов не станут переносить какие-либо рабочие нагрузки, даже если затраты на ЦОДы удвоятся. Другими словам, по меньшей мере 25% опрошенных организаций в настоящее время не считают публичное облако подходящим вариантом для своих рабочих нагрузок!

Это нежелание уходить в облако может быть следствием нескольких факторов. Одни заказчики видят существенную выгоду в размещении рабочих нагрузок в необлачных ЦОДах и полагают, что она оправдывает любые дополнительные расходы. Другие могут полагать, что нормативные и технические проблемы делают публичное облако неподходящим для их задач, поэтому финансовый аспект несущественен. Некоторым организациям может показаться, что переход в публичное облако просто непомерно дорог.

Цена все же имеет значение

Но большинство пользователей восприимчивы к повышению затрат на ЦОДы. Увеличение таких затрат на 10% вынудило бы 55% организаций перенести часть или большинство своих рабочих нагрузок в облако (см. рис. 2). А столкнувшись с удвоением своих затрат, более четверти респондентов перенесли бы большую часть ИТ-нагрузок в облако. Опять же, это предполагает, что затраты на облачные сервисы остаются постоянными. Но маловероятно, что облачные провайдеры смогут сдержать рост цен на свои услуги при значительном повышении расходов, в частности, на электричество.

Другие данные нашего опроса (они не показаны на рисунках) говорят о том, что даже при удвоении расходов на инфраструктуру только 7% респондентов перенесут все свои рабочие нагрузки в облако. Учитывая, что 25% респондентов указали, что они сохранили бы все рабочие нагрузки локальными независимо от увеличения затрат, это подтверждает, что большинство пользователей придерживаются гибридного подхода к ИТ-инфраструктуре. Они предпочитают использовать и локальную, и облачную инфраструктуру, выбирая наиболее подходящий вариант для каждого приложения.



Источник: Uptime Intelligence

▲ Рис. 2. Отношение ИТ-руководителей к переносу ИТ-нагрузки в облако при увеличении затрат на ЦОДы

Хотя в исследовании Data Center Capacity Trends Survey 2022 не изучались потенциальные последствия снижения тарифов поставщиками облачных услуг, можно предположить, что снижение цен на 10% вряд ли привлечет значительно больше рабочих нагрузок в публичные облака, но снижение на 50% окажет более существенное влияние. Однако, как указывалось выше, облачные провайдеры так же страдают от подорожания электроэнергии, как и владельцы ЦОДов, поэтому снижение цен на их услуги маловероятно.

Итак, краткие выводы:

- Многие организации не имеют желания (или возможности) переходить в публичное облако даже при увеличении затрат на ЦОДы.
- Большинство организаций придерживаются гибридного подхода и сочетают облачные и локальные инфраструктуры для своих ИТ-нагрузок.
- Из-за расходов на перемещение приложений (и изменение их архитектуры для эффективной работы в облаке) небольшое увеличение затрат на ЦОДы окажет лишь минимальное влияние на миграцию.
- Более значительное увеличение затрат может привести к переносу большей доли ИТ-нагрузок в облако, поскольку экономия в долгосрочной перспективе может оправдать расходы на миграцию.
- Снижение цен на облачные сервисы могло бы ускорить миграцию в облако, однако оно крайне маловероятно. ИКС

Николай Носов

Телефонное мошенничество стало проблемой национального масштаба. Для борьбы с подменными номерами создана единая платформа, к которой должны подключиться все операторы связи.

Телефонный ад

Добро пожаловать в ад

«То, во что превратилась наша услуга за последние десять лет, можно охарактеризовать словом “ад”. Постоянно объясняю маме, что нельзя отвечать на звонки с неизвестных номеров, а если звонит незнакомец, надо сразу класть трубку. Мы постоянно находимся под атакой непонятных лиц, которые хотят сделать нам что-то плохое», – так описал ситуацию с телефонным мошенничеством генеральный директор «Вымпелкома» Александр Торбахов, открывая конференцию «Борьба с подменой номера. Реальность и перспективы».

По словам управляющего директора и начальника управления противодействия кибермошенничеству Сбербанка Сергея Велигодского, телефонное мошенничество с подменой телефонных номеров официальными телефонами банка стало заметным фактором в 2019 г. С тех пор убытки удвоились и, по официальным данным, переданным российскими банками в Центробанк, достигли в 2022 г. 14,2 млрд руб. (рис. 1). Однако есть еще статистика МВД, и по неофициальным данным с учетом заявлений граждан в полицию, общая сумма хищений с помощью телефона исчисляется 100 млрд руб. Только клиенты Сбербанка в прошлом году столкнулись с 5 млрд попыток телефонного мошенничества. Есть и другие виды мошенничества – фишинг (3%), обман с помощью опросов и лотерей (3%), обман на торговых площадках (4%), но подавляющее число попыток (90%) делается с помощью телефона. Ситуацию усугубило обострение конфликта на Украине, с которой, по информации Сбербанка, связано 90% мошеннических колл-центров.

Меняется характер телефонных преступлений. Если в 2019 г. в основном крали средства со счетов жертвы, то в 2021 г. появилось кредитное мошенничество, когда людей загоняют в кредитные долги и они не только лишаются денег, но и остаются должны банкам. В 2021 г. случалось, что у людей обманом отнимали недвижимость, в 2022 г. число таких преступлений возросло. В этом году людей с помощью социальной инженерии начали посылать совершать поджоги и другие террористические акты.

«На рынке существует мнение, что создаются отдельные операторы связи, занимающиеся пропуском телефонного трафика. Мы получали сообщения, что операторам выгодно пропускать “черный” трафик, дескать, деньги не пахнут», – рассказал С. Велигодский.

Что уже сделано?

Ситуация беспокоит не только заваленные жалобами службы безопасности банков и операторов связи, услуги которых становятся «токсичными», но и государство. Проблема приняла национальный характер, и практически не осталось абонентов, которых не обманули бы или не пытались обмануть мошенники. Не говоря уже о лавине телефонного спама.

Прежде всего государство борется с подменой номеров, штрафуя операторов. В прошлом году за неисполнение закона «О связи» прокуратура вынесла 101 постановление об административном нарушении. Но это, конечно, несоизмеримо с числом мошеннических звонков с подменой номера.

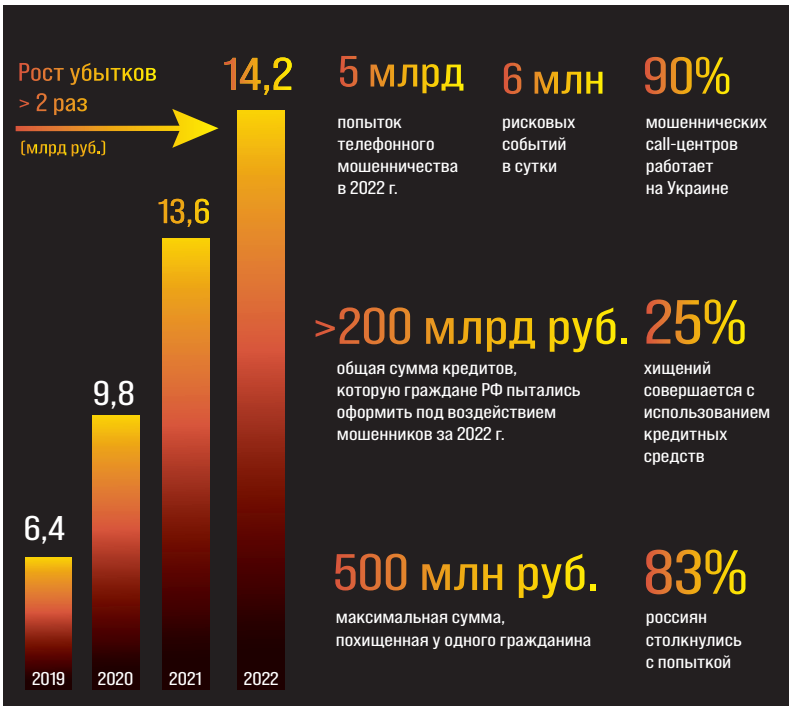
В одиночку проблему не может решить ни один оператор – нужен контроль всей телефонной сети. В 2021 г. был принят закон № 319-ФЗ от 02.07.2021, регулирующий проведение Роскомнадзором мониторинга с целью соблюдения операторами связи обязанности проверять достоверность сведений об абонентах. Для реализации закона подведомственный Роскомнадзору Главный радиочастотный центр (ГРЧЦ) стал создавать Единую платформу верификации вызовов (систему «Антифрод»), первая очередь которой введена в эксплуатацию в декабре 2022 г. Основные цели платформы определены законом:

- создание системы верификации и блокировки телефонных звонков с подменой номера;
- мониторинг Роскомнадзором выполнения операторами связи требования пропуска трафика без подмены номера.

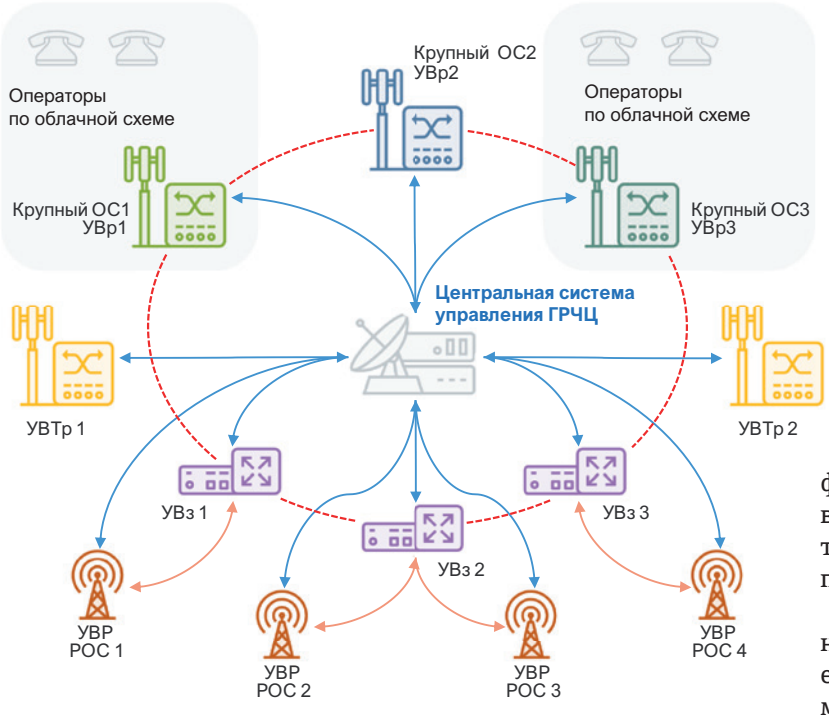
Технические подробности

Разработчиком системы «Антифрод» выступила компания «Гарда Технологии». Ее директор по направлению противодействия мошенничеству и гарантированию доходов Сергей Ва-

Рис. 1. Масштабы проблемы ▼



Источник: Сбербанк



Источник: «Гарда Технологии»

▲Рис. 2. Система «Антифрод»

ЦЕНТРАЛЬНАЯ СИСТЕМА УПРАВЛЕНИЯ (ЦСУ)

- ИНФОРМАЦИОННО-СПРАВОЧНАЯ СИСТЕМА ГРЧЦ Управление системой “Антифрод”

УЗЛЫ ВЕРИФИКАЦИИ (УВР)

- Основной компонент системы, выполняющий верификацию вызова в реальном времени

УЗЛЫ ВЗАИМОДЕЙСТВИЯ (УВЗ)

- Обеспечивают присоединение к системе в регионах
- Обеспечивают конвертацию протоколов
- Сохраняют историю транзакций

УЗЛЫ ВЕРИФИКАЦИИ ТРАНЗИТНЫХ ОПЕРАТОРОВ (УВТР)

- Обеспечивают предоставление исторической информации о вызове для проведения обратной трассировки (12 мес)

сильев рассказал о структуре системы и основных алгоритмах работы.

Единая платформа верификации вызовов – это централизованно-распределенная система (рис. 2), которая включает в себя следующие компоненты:

- центральную систему управления (ЦСУ);
- узлы верификации (УВР), осуществляющие сбор данных о вызовах и проверку запросов об их существовании. Два УВР взаимодействуют между собой, чтобы установить факт наличия вызова;
- узлы взаимодействия (УВз), обеспечивающие присоединение к системе в регионах. В стране более 2 тыс. операторов связи, и создать полносвязную систему невозможно;
- узлы верификации транзитных операторов (УВТр), предоставляющие историческую информацию о вызове с подменой номера для проведения обратной трассировки и выявления точки входа нарушителя в сеть связи общего пользования.

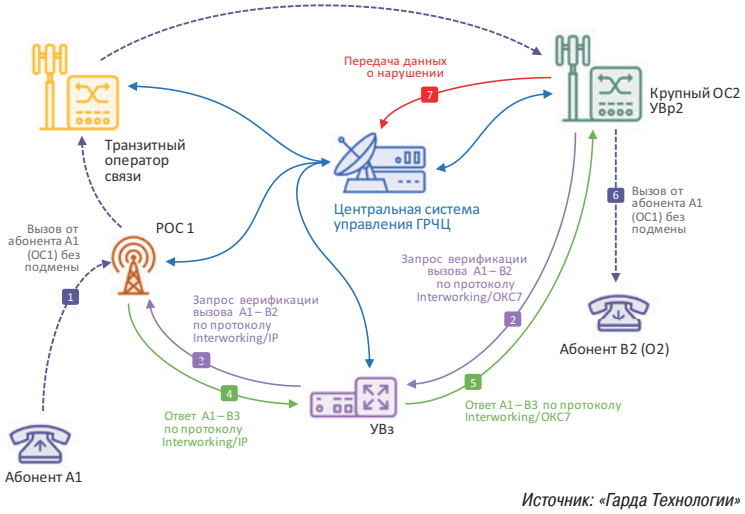
ЦСУ – огромная база, охватывающая 800 млн номеров: для каждого оператора она содержит его уникальный идентификатор, данные о номерной емкости и плане нумерации по регионам. Для каждого телефонного номера хранится информация об обслуживающем его узле верификации. Актуальность базы поддерживается централизованно. В соответствии с требованиями законодательства операторы передают в ЦСУ данные о подмененных номерах, обнаруженных при неподтвержденных вызовах. На основании этих сведений Роскомнадзор выявляет и штрафует нарушителей.

Базовая сеть верификации состоит из узлов верификации (УВр) крупных операторов связи и узлов взаимодействия (УВз). Пять крупнейших операторов (большая сотовая четверка и «Ростелеком»), владеющих более 80% номерной емкости России, связаны между собой напрямую, остальные подключаются к УВз крупных операторов. Таким образом могут проводить верификацию все операторы связи.

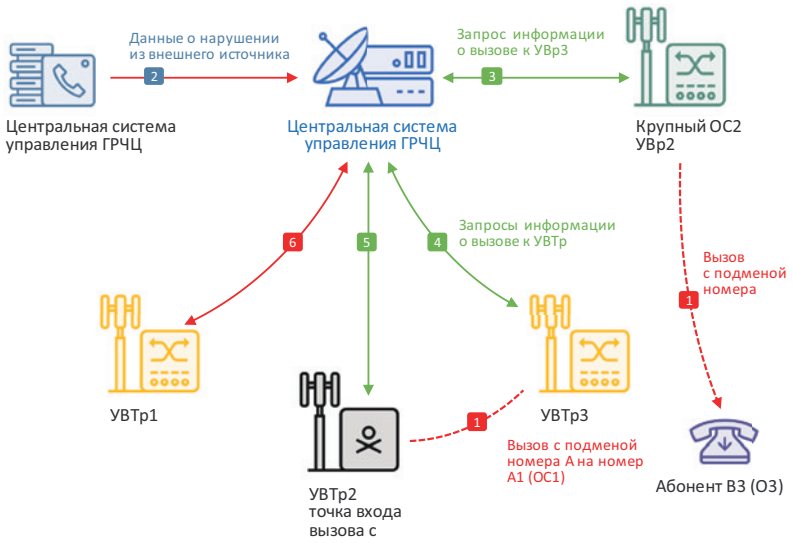
Верификация вызова происходит по двухфакторной схеме (рис. 3). Первый оператор связи (РОС1) инициирует вызов абонента А1, передавая информацию узлу взаимодействия (УВз). Звонок уходит по стандартному маршруту и поступает оператору (ОС2), владельцу вызываемого номера (абонент В2). Узел верификации второго оператора (УВр2) задерживает вызов, не передавая его абоненту, и запрашивает либо узел верификации вызывающего абонента, либо узел взаимодействия, к которому последний подключен. Получив ответ о наличии (либо отсутствии) вызова, УВр2 принимает решение о пропуске или блокировке вызова. В случае блокировки информация о подмененном номере передается в систему.

Для упрощения подключения может применяться облачная схема. Узлы крупных операто-

Рис. 3. Верификация вызова в системе «Антифрод»▼



Источник: «Гарда Технологии»



- Вызов от оператора-нарушителя к абоненту оператора ОС3 с номером В3 с подменой номера А на номер А1 оператора ОС1 через транзитного ОС2 (шаг 1);
- ЦСУ получает информацию о нарушении из внешнего источника (контрольных вызовов) (шаг 2);
- ЦСУ запрашивает у узла верификации ОС2 информацию о вызове (шаг 3);
- Получив информацию об источнике вызова, ЦСУ последовательно запрашивает информацию из узлов верификации транзитных операторов (шаги 4, 5, 6);
- В результате запроса (шаг 6) ЦСУ получает отрицательный ответ
- Данные по инциденту передаются в АРМ оператора системы для дальнейших действий

◀ Рис. 4. Обратная трассировка вызова в транзитной сети

Источник: «Гарда Технологии»

ров вполне могут осуществлять верификацию вызовов за мелких, не имеющих ресурсов и технических возможностей. «Схем подключения много, и они зависят от технических особенностей операторов связи», – пояснил С. Васильев. Есть облачные схемы верификации для работы по протоколам RADIUS и DIAMETER. Отдельно разработана схема для операторов, обеспечивающих VoIP-соединения по протоколу SIP.

Для транзитных операторов узлом верификации является узел, устанавливаемый в сети оператора связи и имеющий доступ к историческим сведениям обо всех вызовах, которые проходят через транзитную сеть. Такая информация, согласно текущему законодательству, должна храниться 12 месяцев. ЦСУ, получив информацию о нарушении из внешнего источника (из банка, ФСБ или заявления гражданина в полицию) либо в результате контрольного вызова (осуществляемого как специальным генератором вызовов, так и вручную с заведомо подменным номером), посылает запрос узлу верификации.

По запросу из ЦСУ узел должен предоставлять информацию о вызове при обратной трассировке инцидента (рис. 4).

Чтобы построить маршрут прохождения вызова, ЦСУ в автоматическом режиме по цепочке запрашивает в обратную сторону от оператора вызываемого абонента все узлы верификации. Поскольку оборудование транзитных сетей в силу технических особенностей передает информацию о вызове в базы операторов с большой (но не превышающей 6 ч) задержкой, процедура опроса начинается через 6 ч. Место обрыва цепочки – точка входа нарушителя, подменившего номер. Данные об этом опять-таки в автоматическом режиме передаются в региональное отделение Роскомнадзора для выполнения контрольно-надзорных действий.

Когда?

К единой платформе верификации телефонных вызовов Роскомнадзора все операторы связи, по словам директора центра мониторинга и управления сетью связи общего пользования ГРЧЦ Сергея Хуторцева, должны подключиться к марту 2024 г.

Каждому региональному оператору будет направлено уведомление о возможности подключения к местному узлу платформы. После получения уведомления оператор обязан подключиться к платформе в течение 224 дней. Для этого надо будет перестроить систему, обеспечить защищенный канал передачи данных и установить программное обеспечение. После настройки «Антифрода» оператор сможет верифицировать номер за 500 мс. Сегодня с системой «Антифрод» уже работают «МегаФон», МТС и «Вымпелком».

Количество мошеннических телефонных вызовов достигло пика летом 2022 г. Но с июля в основном за счет усилий пятерки крупнейших операторов оно пошло на спад. «С июля по февраль объем вызовов уменьшился на 67%. Дальнейшее улучшение будет возможно, когда в работу включатся все операторы. Когда Единая система верификации вызовов заработает в полном объеме, мы окончательно решим вопрос телефонного мошенничества с подменой номера», – с оптимизмом смотрит в будущее директор департамента обеспечения кибербезопасности Минцифры России Владимир Бенгин.

Искоренить мошенничество с использованием социальной инженерии до конца не удастся. Преступники найдут другие решения, например, использование мессенджеров. Но риски, особенно для самой незащищенной группы – старшего поколения, привыкшего доверять телефону, в условиях полноценной работы системы «Антифрод», безусловно, снизятся. ИКС

Берегите DNS!

Александр Лямин, генеральный директор, Qrator Labs

Защита DNS-сервера от посягательств злоумышленников сегодня актуальна не только для провайдеров, но и для любой компании, имеющей собственные онлайн-сервисы, будь то интернет-магазин или просто виртуальные рабочие столы для сотрудников.

В первых числах марта 2022 г. работа более 300 тыс. интернет-доменов в зоне .ru была парализована. Оказались недоступны интернет-сайты, не работала электронная почта. Отсутствовал доступ к таким популярным интернет-сервисам, как «Битрикс 24» или «Сбермаркет». Причиной стала результативная атака на DNS-серверы компании RU-Center, крупнейшего в России регистратора доменных имен и хостера интернет-сайтов.

Атаки на DNS-серверы происходят с завидной регулярностью. Впервые они были зафиксированы еще в 2002 г. и с тех пор становятся только изощреннее. Нарастает и разрушительность таких нападений.

Рост популярности нападений на DNS-серверы объясняют тем, что начиная с 2010 г. компании стали активно применять средства защиты от DDoS-атак в своей инфраструктуре. Хакеры озаботились ответными мерами, и многие из них сделали своими целями уже не отдельные ресурсы, а целые пулы из тысяч сайтов, связанных общим регистратором доменных имен или хостингом. В 2012 г., к примеру, таким атакам подверглись крупнейший в США провайдер AT&T и ведущий в мире хостинг-провайдер GoDaddy. Более того, тогда же представители хакерской группировки Anonymous угрожали обрушить весь интернет.

С тех пор масштабные DNS-атаки повторяются регулярно, а ущерб от них достигает астрономических цифр. К примеру, издание TAdviser со ссылкой на отчет компании EfficientIP за 2020 г. сообщало, что 79% организаций в мире становились жертвами подобных нападений и ущерб от каждой такой атаки в среднем превысил $900 тыс.

Между тем, по данным того же отчета, 25% компаний вовсе не анализируют свой DNS-трафик. Это говорит о том, что проблема не просто серьезна. Риски, связанные с нападениями на DNS-серверы, носят угрожающий характер.

Что такое DNS

Как известно, у любого компьютера в сети, в том числе в интернете, есть свой уникальный адрес. Этот набор из четырех трехзначных чисел и есть IP-адрес. Такая система удобна для машин, которые хорошо запоминают цифры, но, увы, неудобна для человека. Хранить в памяти много таких сочетаний мы неспособны. Поэтому создатели интернета решили давать веб-сайтам буквенные имена, связанные с тематикой ресурса, названием компании и т. п. Это и есть доменные имена, и каждое из них привязано к тем самым сложным числовым комбинациям. Для того чтобы перевести бук-

венные доменные имена в числовые IP-адреса, понимаемые машиной, и применяется система доменных имен (Domain Name System, DNS).

Структура системы доменных имен – классическое иерархическое дерево. Его корни – доменные зоны (.com, .ru и др.), путь от которых ведет к каждому листочку дерева – интернет-сайту.

Что такое DNS-серверы и как они работают

Работает DNS при помощи специальных DNS-серверов. Они хранят информацию о соответствии каждого доменного имени IP-адресу и о ресурсных записях других DNS-серверов. Это необходимо для ускорения запросов к сайтам, расположенным в других доменных зонах.

Когда пользователь при помощи браузера отправляет запрос на посещение сайта, DNS-сервер его сегмента сети ищет имя сайта в своем кэше (промежуточном буфере с быстрым доступом к нему, содержащем информацию, которая может быть запрошена с наибольшей вероятностью) и если находит его, то сразу переадресовывает запрос на конкретный IP-адрес. Если таких данных у DNS-сервера нет, то запрос пересылается серверу более высокого уровня. Иногда эта работа сервера заметна пользователям: одни сайты открываются быстро, другие ощутимо медленнее. Происходит это из-за того, что адрес сайта приходится искать на DNS-серверах в других доменных зонах.

Записи DNS-сервера

Поиск числовых IP-адресов по доменному имени – не единственная функция DNS-серверов. Для каждого сайта они хранят важную дополнительную информацию: адрес почтового сервера, аналоги доменного имени, текстовую информацию о домене, адрес DNS-сервера, на котором хранится дополнительная информация.

Эта информация называется доменными (или ресурсными) записями. Они необходимы для того, чтобы DNS-серверы могли корректно обрабатывать запросы к сайту – направлять пользователя на нужную страницу, идентифицировать почтовый домен, чтобы отправляемые с него письма доходили до получателей, подтверждать безопасность сайта при помощи SSL-сертификатов. Таких записей может быть очень много, и каждая из них непосредственно влияет на работу сайта и связанных с ним сервисов.

Чем опасны DNS-атаки

Атака на DNS-сервер – разновидность DDoS-атаки, целями которой являются отключение интернет-ресурса, его частичное или полное разрушение. Бывает, что DDoS используется как отвлекающий маневр: пока ИТ-службы заняты этой угрозой, злоумышленники пытаются взломать другие ресурсы, в том числе для кражи данных. Сегодня, когда интернет-сайты стали для множества компаний главным инструментом привлечения и обслуживания клиентов, а данные – главным бизнес-активом, такие атаки могут угрожать самому существованию бизнеса. Атакам подвергаются и государственные организации. При этом нападающие могут преследовать и политические цели, выводя из строя сервисы, обслуживающие и граждан, и системы жизнеобеспечения.

Например, простой в течение нескольких часов сайта интернет-магазина или банка может иметь для них необратимые последствия. Клиенты предпочтут другую, более устойчивую и надежную торговую площадку, банкам придется преодолевать последствия, связанные с недоступностью платежных систем, заниматься розыском «потерявшихся» транзакций. Облачные сервисы, гарантирующие заказчикам высокий уровень доступности своих систем, будут вынуждены выплачивать денежные компенсации. Наконец, имиджевые потери для бизнеса подчас даже более критичны, чем прямые финансовые убытки.

Однако вместо атаки на сам сайт можно вывести из строя сервер DNS. В таком случае браузеры пользователей не смогут определить IP-адрес, и сайт для них окажется недоступен. Злоумышленник может постоянно генерировать запросы к серверу DNS с целью исчерпания его ресурсов.

Без создания специальной защиты единственным способом нейтрализации атаки является повышение мощности серверов. Однако при постоянном наращивании мощностей такой сервер сам может использоваться злоумышленниками для организации DDoS-атак на другие жертвы.

Что еще нужно хакерам

Помимо неработоспособности сайтов цели киберпреступников могут быть куда приземленнее и рациональнее.

Одной из разновидностей DNS-атак является DNS-спуфинг (его еще называют «отравление кэша»), когда злоумышленники не «обрушивают» сайт, а подменяют его IP-адрес фальшивым. Это может быть адрес ресурса, который полностью дублирует содержание «правильного» сайта. В результате хакеры получают в свое распоряжение все данные, которые вводят пользователи во время работы с сайтом. Ими могут быть персональные данные, номера и CVV-коды банковских карт.

Злоумышленник может перенаправить не только веб-запрос пользователя. Контроль над DNS позволит ему получить доступ к электронным письмам (они просто будут приходить на

адрес хакера). Точно так же будут перехвачены и попытки аутентификации при удаленном доступе к корпоративным системам, а эти риски особенно актуальны, когда значительная часть персонала работает удаленно.

Почему риски DNS-атак актуальны для всех

Как правило, компании обращают мало внимания на безопасность DNS-серверов. Действительно, на первый взгляд она актуальна для провайдеров, которые обеспечивают работоспособность множества доменов. Но сегодня проблема DNS-безопасности касается все большего числа компаний.

Дело в том, что бизнес использует множество облачных сервисов от сторонних поставщиков – дата-центров, провайдеров, сетей доставки контента (CDN-сервисов). Число таких систем постоянно растет, они приобретают все большую популярность. Более того, организации все чаще разворачивают собственные облачные сервисы, обеспечивая доступность своих информационных ресурсов и для сотрудников, и для партнеров. Например, в период пандемии, когда практически все компании были вынуждены были отправить своих сотрудников в «домашние офисы», стали широко применяться различные средства удаленного доступа – виртуальные и удаленные рабочие столы. Таким образом, собственными онлайн-сервисами сегодня управляют тысячи самых разных компаний, от крупных корпораций до небольших бизнесов. И для их работы необходима DNS.

DNS-сервер – точно такой же сервис, который бизнес может получить непосредственно от провайдера услуги. Но любой специалист по информационной безопасности подтвердит: даже гарантия доступности от поставщика облачного сервиса не избавляет компанию-пользователя от необходимости защищать этот элемент своей инфраструктуры. То же самое касается используемых организацией DNS-серверов.

Иными словами, защита DNS-сервера сегодня стала проблемой не только провайдеров, но и любой организации, которая имеет даже небольшие собственные онлайн-сервисы, от интернет-магазина до виртуальных рабочих столов для своих сотрудников.

Как защитить DNS

Использование только одного средства защиты DNS-серверов едва ли поможет полностью предотвратить атаки на них. Необходим комплекс мер, среди которых только одна состоит в применении собственно технических решений.

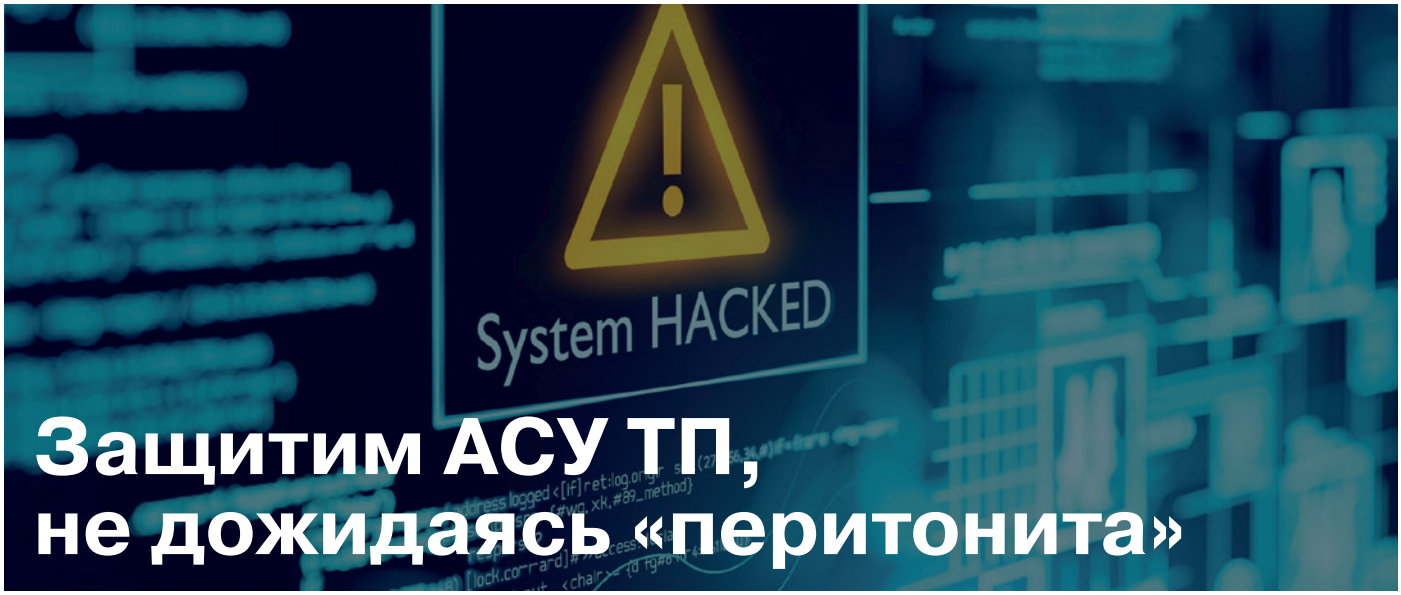
В первую очередь, повторимся, необходимо диверсифицировать DNS-серверы – не полагаться только на провайдера, но и по крайней мере развернуть резервный сервер на собственных мощностях.

Следующая мера – распределение ресурсов. Речь идет о размещении DNS-серверов на разных площадках: например, в ЦОДе провайдера и своем собственном или в двух разных дата-центрах, управляемых разными провайдерами. Такая мера существенно усложнит хакерам организацию атаки, а самой компании позволит в кратчайшие сроки восстановить работоспособность своих систем, если нападение произойдет.

DNS-серверы требуют постоянного внимания. Поэтому компания, которая управляет хотя бы одним сервером (не важно, размещен он в собственной инфраструктуре или на мощностях провайдера), должна иметь в штате грамотного администратора с соответствующими компетенциями, а кроме того, организовать управление доступом к настройкам сервера, как минимум – двухфакторную авторизацию.

Затем необходимо использовать DNSSEC – набор расширений для протокола DNS, разработанный специально для защиты DNS-серверов. Он служит своего рода сертификатом подлинности сервера и действует точно так же, как электронная цифровая подпись с криптозащитой. Для компаний, которые собирают и хранят данные пользователей (проще, наверное, найти компании, которые этого не делают), использование DNSSEC обязательно.

И, наконец, защита DNS-серверов подразумевает использование специальных средств защиты от DDoS-атак. Это могут быть и сервисы по подписке, которые предлагают провайдеры, и собственные защитные средства, как программные, так и аппаратные. При этом поставщики услуг защиты, как правило, предоставляют дополнительный сервер DNS, в котором реализованы передовые методы нейтрализации атак и разработана специальная логика обработки запросов ботов. За счет распределенных мощностей таких систем защиты будет гарантирована работоспособность DNS-серверов вне зависимости от интенсивности возможной атаки. ИКС



Защитим АСУ ТП, не дожидаясь «перитонита»

Каждая из незакрытых уязвимостей в ИТ-инфраструктуре управления производством может обернуться отключенной турбиной, нарушенным технологическим процессом, остановкой отгрузки нефти на танкер, испорченной партией продукции.

Алексей Падчин, технический специалист, Axoft

Прошлый год запомнился беспрецедентным количеством кибератак на ИТ-инфраструктуру крупных компаний и объекты КИИ. По данным исследования «Лаборатории Касперского», во втором полугодии Россия вошла в тройку лидеров в рейтинге регионов мира по доле заблокированных вредоносных объектов на компьютерах АСУ (39%). По сравнению с первой половиной года показатель вырос на 9% – это наиболее значительное изменение среди исследованных регионов.

Всего за 2022 г., как отмечается в отчете Positive Technologies, в промышленных компаниях было зафиксировано 223 инцидента, вызванных атаками злоумышленников, что на 7% больше, чем в 2021 г., а продажа доступа к промышленным предприятиям в дарквебе выросла на 40%. 87% успешных атак были направлены на компьютеры, серверы и сетевое оборудование. В 44% случаев злоумышленники проводили атаки на персонал промышленных компаний с помощью вредоносных рассылок по электронной почте (94%) и фишинговых сайтов (10%).

И в этом году хактивисты останавливаться не намерены. Многие эксперты прогнозируют усиление внимания злоумышленников к реальному сектору экономики и критической инфраструктуре. Поэтому в нынешние времена главный вопрос не в том, взломают вашу систему или нет, а в том, когда это случится.

Угроза, откуда не ждали

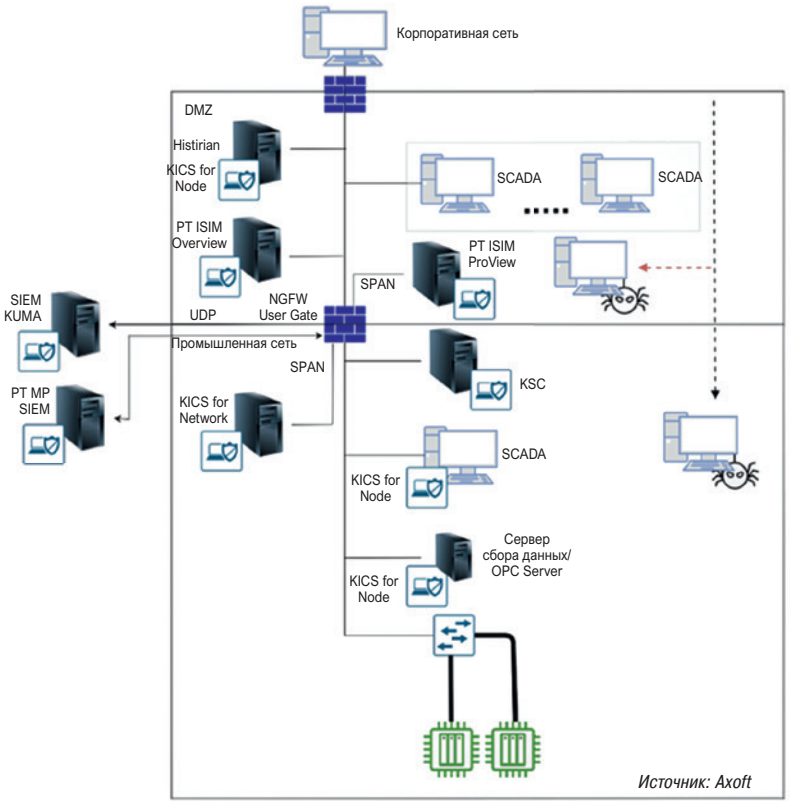
Как правило, при целенаправленных атаках с момента первой разведки до выполнения целей взлома могут пройти месяцы. Поэтому есть все шансы обнаружить и заблокировать угрозу на начальном этапе. Для этого нужно знать потенциально слабые места в инфраструктуре.

Стандартная архитектура АСУ ТП имеет три основных уровня:

- Исполнительные устройства — манометры, заслонки, арматура, датчики и пр. Атака на этот уровень чревата риском выхода из строя или некорректной работы устройств.
- Контроллеры – уровень взаимодействия «железа», он отвечает за технический процесс и его безопасность. С этим уровнем связаны риски остановки, подмены программы, изменения уставок (значений, на базе которых выполняется тот или иной алгоритм в контроллере).
- SCADA – уровень, на котором обслуживающий персонал управляет технологическим процессом. Здесь задаются уставки, происходит архивация данных, операторов уведомляют о критичных ситуациях на производстве. На этом уровне актуальны риски подмены реальных данных, выгрузки базы, изменения уставок или получения контроля над техпроцессом.

На крупных предприятиях добавляются уровни, которые позволяют наиболее эффективно работать с данными и анализировать их, а также оптимизировать как производственные, так и бизнес-процессы: MES, ERP, BPM.

Как правило, доступ к интернету появляется на уровне SCADA. Его используют для почты, подключения удаленных клиентов (сервисного обслуживания) или для личных нужд сотрудников. В редких случаях можно найти контроллеры с прямым доступом во Всемирную паути-



▲ Типовая архитектура с наложенными средствами защиты АСУ ТП (комбинированное решение)

ну. Так, по данным поисковика по интернету вещей Shodan, 502-й порт, стандартный для Modbus TCP, на момент написания статьи был доступен у 673 устройств. Кроме того, сотрудники часто подключаются к сети в обход общей. Кстати, «раздавать интернет» сейчас возможно даже с кнопочного телефона.

Что уж говорить о постоянном использовании USB-устройств, предназначенных для передачи данных? Занести через них зловред на уровень АСУ ТП, даже через закрытый периметр, без ведома владельца не составит труда.

По моему опыту, уязвимости разной критичности и сложности могут встречаться в контроллерах, OPC-серверах и SCADA-системах. Последствия их использования тоже могут быть разными: начиная от сброса системы аутентификации с помощью очистки файла .txt или перегрузки журнала подключений до изменения пароля администратора через SQL-инъекцию.

Некоторые уязвимости закрывают, но меняются технологии, инфраструктура, и через некоторое время они обнаруживаются вновь.

Например, уязвимость kb5004442((CVE-021-26414)) непосредственно связана с DCOM (Distributed Component Object Model). Данная технология была слабо защищенной в 2003 г., ее обновили, усилили и использовали вплоть до сегодняшнего дня. Недавно в ней нашли новую «дыру».

CISA, ATT&CK, «Лаборатория Касперского» и Positive Technologies ежегодно публикуют множество новостей о выявленных и закрытых вендорами уязвимостях, которые без постоянной установки обновлений могут быть использованы злоумышленниками для проникновения в систему. По данным CVE, в Windows XP SP 3 выявлено около 445 уязвимостей, а в Windows 7 – более 1000. И это только те, которые опубликованы официально и для которых разработчики в каком-либо из обновлений создали «противоядие».

Помимо устаревающих операционных систем существуют слабые места, связанные с технологиями. К примеру, на сайте CISA опубликовано более 2000 уязвимостей для промышленного оборудования, около 500 из них связано с технологиями Siemens, 40 – с технологией OPC. Безусловно, многие из них в более свежих прошивках или версиях софта и «железа» уже устранены. Но будем честны, когда вы в последний раз загружали обновление на все контроллеры или пересобирали проект?

Чем защищаться?

На промышленных предприятиях внедрение систем автоматизации занимает в среднем от трех до пяти лет, а согласование каких-либо изменений может длиться месяцами. Поэтому проекты, которые были начаты, к примеру, год назад, уже не могут быть полностью выполнены из-за отсутствия поставок. В результате складывается ситуация, когда предприятия даже при желании не имеют возможности развернуть последние обновления, что дает злоумышленникам отличный шанс для осуществления как простых, так и сложных целенаправленных атак. И если система безопасности ранее только номинально выполняла свою функцию, то сейчас стоит задуматься о реальной защите, так как количество эксплойтов для каждой уязвимости ежедневно растет.

Приведу пример: одним из слабых мест у больших компаний является доступ к базе данных («Хисториан»), который зачастую открыт для передачи информации в сторонние сети. Попав в периметр предприятия, злоумышленник начинает сканировать сеть или загружать нелегитимный софт для закрепления на этом узле и дальнейшего развития атаки. Сканируя сеть с узла «Хисториан», можно узнать, какие порты преимущественно открыты, какие драйверы или OPC-серверы используются, а следовательно, понять, какое оборудование установлено. При отсутствии эшелонированной защиты или постоянного мониторинга такие действия могут оставаться незамеченными долгое время. Обладая подобными данными и точкой входа, хакеру в дальнейшем не составит труда вмешаться в критически важный процесс.

Для устранения этих угроз компании стремятся уделять больше внимания защите промышленного периметра. На отечественном рынке присутствуют несколько разработчиков, специализирующихся в том числе на защите объектов КИИ. Комплексные решения, которые включают обеспечение безопасности сети, периметра, конечных узлов с возможностью агрегации и анализа информации в едином центре ИБ-мониторинга (SOC), не позволяют злоумышленникам проникнуть в инфраструктуру незамеченными.

Среди существующих систем для защиты АСУ ТП можно выделить следующие:

- InfoWatch ARMA. Система сегментирует промышленную сеть с возможностью настроить отправку команд и данных из одного сегмента в другой, осуществляет мониторинг трафика и разграничение прав. Позволяет надежно закрыть периметр производственного процесса и отследить все, что происходит внутри, – как сетевые взаимодействия, так и события на конечных узлах.
- Kaspersky Industrial CyberSecurity. Защищает всю сеть предприятия, включая конечные устройства, отслеживает сетевые взаимодействия, а также целостность проектов, загруженных непосредственно в контроллер. Интеграция с Kaspersky Unified Monitoring and Analysis Platform позволяет передавать ИБ-инженеру полную информацию о текущем статусе защищенности.
- PT Industrial Cybersecurity Suite – комплексная платформа для своевременного выявления киберугроз и реагирования на инциденты в промышленных системах. За счет комбинации ключевых продуктов Positive Technologies: MaxPatrol SIEM, MaxPatrol VM, PT ISIM, PT Sandbox и агентов PT XDR – платформа обнаруживает атаки на сетевом, системном и прикладном уровнях промышленных систем и автоматизирует реагирование на инциденты ИБ.

В рамках одного проекта можно создавать комбинированные решения, задействующие сильные стороны продуктов каждого разработчика. У нас есть опыт реализации проектов тестирования совместимости решений на базе продуктов KICS for Node, KICS for Network и UserGate NGFW. Тестирование продемонстрировало жизнеспособность и целостность такого подхода, который обеспечил полную защиту сети и конечных узлов и дал возможность настроить эшелонированную защиту.

Кроме того, мы регулярно тестируем совместимость различных систем в виртуальном пространстве «Демосфера». Это позволяет подобрать рабочую конфигурацию для решения конкретных задач бизнеса и в дальнейшем предоставить заказчику настроенную систему, отвечающую всем его требованиям. ИКС

Серверные шкафы

Компания «Систэм Электрик» представила монтажные шкафы серии Uniprom. Шкафы предназначены для размещения серверного, активного и пассивного телекоммуникационного оборудования, устройств внутристоечного распределения электропитания, средств организации кабельного хозяйства, кабелей передачи данных, средств организации воздушных потоков, систем мониторинга окружающей среды и контроля доступа.

Шкафы Uniprom имеют климатическое исполнение УХЛ 4.2 согласно ГОСТ 15150 и предназначены для эксплуатации в закрытых помещениях при температуре от +5 до +60°С, при верхнем рабочем значении относительной влажности 80% при температуре 25°С.

Основные характеристики:

- монтажная высота – 24, 42, 48U;
- ширина – 600, 750, 800 мм;
- глубина – 1070, 1200 мм;
- перфорация дверей – 81%;
- угол открытия дверей – 180°;
- статическая нагрузочная способность – 1800 кг;
- динамическая нагрузочная способность – 1050 кг;
- нагрузочная способность верхней панели – 60 кг;
- кабельные вводы – увеличенные с открытым контуром и защитной округленностью.

Перфорированные передние и задние двери допускают демонтаж дверного полотна без использования инструментов. Предусмотрена возможность изменения стороны навешивания. Съемные боковые панели разделены горизонтально. Демонтируемая усиленная верхняя панель имеет симметричную конструкцию. Монтажные направляющие оснащены уплотнительными материалами для предотвращения паразитной рециркуляции. В раму шкафа встроены поворотные ролики и регулируемые ножки.

В комплект поставки входит набор для фиксации шкафа на месте установки и предотвращения опрокидывания, а также фурнитура для стягивания шкафов в ряд.

Контрастная легко читаемая маркировка монтажной высоты выполнена в прямом и обратном порядке.

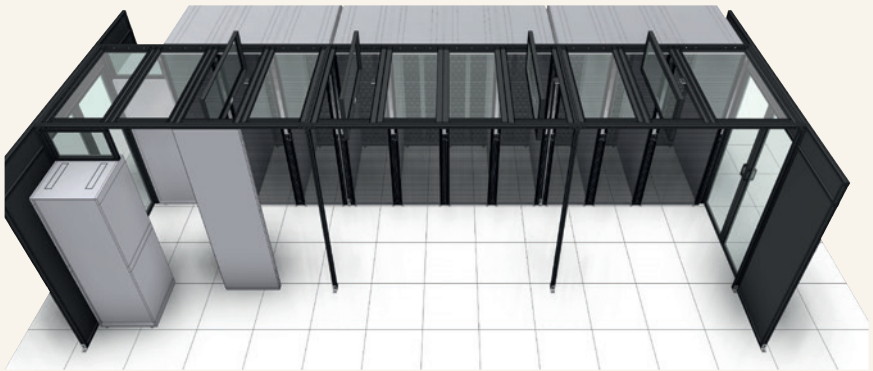
Шкафы шириной 750 и 800 мм оснащены дополнительными вертикальными установочными местами 1U (по 3 в каждой направляющей).

Гарантийный срок на монтажные шкафы Systeme Electric серии Uniprom составляет пять лет.

systeme.ru

Многофункциональные системы изоляции коридоров

Компания ART Engineering выпускает системы изоляции коридоров для установки в машинных залах центров обработки данных.



Система изоляции коридоров ART Engineering – это пассивная система охлаждения, которая физически отделяет поток холодного приточного воздуха от горячего отработанного воздуха, поступающего от ИТ-оборудования. Коридоры могут быть как горячими, так и холодными.

Решение представляет собой свободностоящий стальной конструктив, созданный по принципу «помещение в помещении». Коридор является самонесущей конструкцией без опоры на шкафы. Основная нагрузка распределяется на входные группы. Для предотвращения прогиба несущей балки коридор крепится подвесами к потолку или опирается стойками на пол.

Отличительная особенность систем изоляции коридоров ART Engineering – их полная кастомизация, в том числе в границах одного машинного зала. Специалисты компании осуществляют подбор оптимальных параметров решения для конкретного проекта и создают его BIM-модель для удобства работы и оперативного внесения изменений в конструктив.

art-engineer.ru

Интеллектуальная система мониторинга АКБ

Компания ENERGON представила интеллектуальную систему мониторинга параметров аккумуляторных батарей ENERGON DEMS.

Система решает несколько задач:

1. Информирует о рабочем состоянии АКБ.
2. Сокращает затраты на эксплуатацию массива АКБ за счет экономии на преждевременной закупке новых аккумуляторов, а также на ручном труде по контролю за состоянием АКБ.
3. Автоматизирует процесс сбора и передачи информации.

Система непрерывно измеряет ток в цепи, температуру и напряжение каждой АКБ, передавая эти данные в контроллер. Тот анализирует их и дает информацию о текущем состоянии каждой батареи, а также рекомендации о том, как продлить срок службы всего массива. В контроллер системы встроена карта памяти, на которую непрерывно записываются измеренные значения, что впоследствии поможет, например, выявить причину ускоренного старения батарей.

Для подключения к системе реализовано несколько возможностей:

- Wi-Fi-соединение «точка – точка»;
- Ethernet;
- цифровые протоколы передачи данных, например, Modbus, TCP IP/ RTU и SNMP.

Подключиться к системе DEMS можно с телефона, планшета, компьютера или существующей системы верхнего уровня. Для ее работы не требуется специальное ПО. Система DEMS просто устанавливается, переносится, настраивается и интегрируется в ИТ-ландшафт объекта. Она не передает данные во внешние ресурсы и не использует сторонние серверы для анализа получаемых данных. Имеет модульную архитектуру, которая обеспечивает возможность расширения на любое количество батарей.

Система мониторинга DEMS является утвержденным Росстандартом типом средств измерений.

www.energon.ru

Прецизионные кондиционеры

Компания «Новые технологии» представляет одну из моделей прецизионных кондиционеров «Лемминг» – L-CRA стандарта, предназначенную для поддержания точных параметров микроклимата внутри обслуживаемого помещения. Подходит для ЦОДа любой конфигурации.

L-CRA – кондиционеры с воздушным охлаждением конденсатора – поставляются в различных конфигурациях: только охлаждение, охлаждение + увлажнение, охлаждение + нагрев + увлажнение. Имеют холодопроизводительность 25,5–100,8 кВт. Явная холодопроизводительность – 23,2–90,7 кВт. Расход воздуха – от 7800 до 27000 куб. м/ч. Выдув воздуха предусмотрен вверх, вниз или фронтально. Хладагент – фреон (R410A). Уровень шума – 65,3–68,1 дБА.

Установки укомплектованы решениями известных производителей:

- спиральными компрессорами фиксированной частоты производства Copeland;
- инверторными компрессорами GMCC и Mitsubishi Electric с ПИД-алгоритмом регулирования производительности;
- осевыми AC- и центробежными EC-вентиляторами постоянного тока Ziehl-Abegg с плавной регулировкой скорости от 25 до 100%;
- электродными пароувлажнителями Beijing Tongdada или Carel производительностью от 5–13 кг/ч, поддерживающими точные параметры влажности и способствующими уменьшению содержания пыли в воздухе;
- автоматами и контакторами Siemens и Schneider Electric.

Поставляются из стран Азии и Ближнего Востока.

lemming-power.ru

РЕКЛАМА В НОМЕРЕ

Указатель фирм и организаций

Учредитель журнала «ИнформКурьер-Связь»:

ООО «ИКС-МЕДИА»:
105082, г. Москва, 2-й Ирининский пер, д. 3.;
Тел.: (495) 150-6424; E-mail: iks@iksmedia.ru.

18-я конференция и выставка

ЦОД

Москва 12 сентября 2023

Holiday Inn Moscow Sokolniki

офлайн / онлайн

16+

Реклама

За свою 18-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

ОРГАНИЗАТОРЫ

ИКС МЕДИА

iKS CONSULTING

ПРИ ПОДДЕРЖКЕ И УЧАСТИИ

Минцифры России

КООРДИНАЦИОННЫЙ СОВЕТ ПО ЦОДам И ОБЛАЧНЫМ ТЕХНОЛОГИЯМ
Автономная некоммерческая организация

ЗАРЕГИСТРИРОВАВШИМСЯ БУДЕТ ДОСТУПНА ВИДЕОЗАПИСЬ НА САЙТЕ КОНФЕРЕНЦИИ

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

KEY POINT GROUP

РЕГИОНАЛЬНАЯ СЕТЬ ЦОД

ВАЖЕН КАЖДЫЙ!

ВЛАДИВОСТОК	I очередь	440 стоек	введен в эксплуатацию - **февраль 2023**
ВЛАДИВОСТОК	II очередь	440 стоек	ввод в эксплуатацию - **1 квартал 2024**
НОВОСИБИРСК		880 стоек	ввод в эксплуатацию - **декабрь 2023**
ЕКАТЕРИНБУРГ		300 стоек	ввод в эксплуатацию - **1 квартал 2024**

keypoint-group.ru